



Cuadernos de Estrategia 185

Ciberseguridad: la cooperación público-privada

Instituto
Español
de Estudios
Estratégicos

Departamento
de Seguridad
Nacional



MINISTERIO DE DEFENSA



DSN

ieee.es
Instituto Español de Estudios Estratégicos



Cuadernos de Estrategia 185

Ciberseguridad: la cooperación público-privada

Instituto
Español
de Estudios
Estratégicos

Departamento
de Seguridad
Nacional



MINISTERIO DE DEFENSA

CATÁLOGO GENERAL DE PUBLICACIONES OFICIALES
<http://publicacionesoficiales.boe.es/>

Edita:



<http://publicaciones.defensa.gob.es/>

© Autores y editor, 2016

NIPO: 083-16-446-2 (edición papel)

ISBN: 978-84-9091-245-4 (edición papel)

Depósito Legal: M-40233-2016

Fecha de edición: marzo 2017

Imprime: Ministerio de Defensa

NIPO: 083-16-447-8 (edición libro-e)

ISBN: 978-84-9091-246-1 (edición libro-e)

Las opiniones emitidas en esta publicación son exclusiva responsabilidad de los autores de la misma.

Los derechos de explotación de esta obra están amparados por la Ley de Propiedad Intelectual. Ninguna de las partes de la misma puede ser reproducida, almacenada ni transmitida en ninguna forma ni por medio alguno, electrónico, mecánico o de grabación, incluido fotocopias, o por cualquier otra forma, sin permiso previo, expreso y por escrito de los titulares del © Copyright.

En esta edición se ha utilizado papel 100% reciclado libre de cloro.



ÍNDICE

	Página
Introducción.....	11
<i>Luis Joyanes Aguilar</i>	
Una visión global de la colaboración público-privada en ciberseguridad..	13
Capítulo primero	
Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguri- dad 4.0)	19
<i>Luis Joyanes Aguilar</i>	
La ciberseguridad en tiempo real.....	21
El índice mundial de ciberseguridad de la UIT (ITU).....	22
Clasificación mundial (índice IMC)	23
La cuarta revolución industrial	24
Industria 4.0: origen, evolución y futuro	25
<i>Industria conectada 4.0</i>	26
Las tecnologías disruptivas pilares en la Industria 4.0 y en la cibersegu- ridad	28
Tendencias en ciberseguridad: un primer avance (2015-2016).....	31
Informe de seguridad de la información de Cisco	32
Recomendaciones de Cisco	33
Los ciberriesgos	33
<i>La web profunda, la web invisible (Deep Web).....</i>	34
<i>La necesidad de un seguro de ciberriesgos en la empresa</i>	35
La ciberseguridad en la empresa y la empresa ante la ciberseguridad.....	36
<i>El negocio de la ciberseguridad</i>	37
La ciberseguridad en la industria eléctrica: necesidad de estándares.....	37
La ciberseguridad en la banca y en el sector financiero (tecnologías fi- nancieras de impacto)	39
<i>Tecnologías y empresas Fintech</i>	40
<i>Blockchain</i>	41
La ciberseguridad y la inteligencia artificial	42

	Página
<i>IBM Watson</i>	43
<i>Watson for Cyber Security</i>	44
<i>Plataforma de Ciber-Inteligencia de Accenture</i>	44
Robótica y ciberseguridad: cobots, bots y chatbots	45
<i>Robots colaborativos (cobots)</i>	45
<i>Los asistentes virtuales: bots y chatbots</i>	46
<i>Aplicaciones de los bots</i>	47
<i>Asistentes virtuales en páginas web de organizaciones y empresas</i>	48
<i>Los bots: ¿las nuevas aplicaciones móviles?</i>	48
<i>La seguridad y los riesgos de los bots</i>	49
El nuevo reglamento de protección de datos de la Unión Europea (25 de mayo de 2016)	49
<i>Novedades del nuevo reglamento</i>	50
<i>Recomendaciones de la AEPD sobre el nuevo reglamento</i>	50
Proyecto de colaboración público-privada de la Unión Europea (5 de julio de 2016)	51
Directiva de ciberseguridad (NIS) de la Unión Europea (6 de julio de 2016)	52
El escudo de privacidad Unión Europea-Estados Unidos (12 de julio de 2016)	53
La formación en ciberseguridad y en sus tecnologías disruptivas	54
<i>Los nuevos roles profesionales</i>	55
Los datos: presente y futuro de la ciberseguridad	57
La ciberseguridad en América Latina y Caribe	57
<i>Tendencias de seguridad cibernética en América Latina y el Caribe (junio 2014)</i>	58
<i>Ciberseguridad 2016 en América Latina y Caribe (marzo 2016)</i>	59
Conclusiones: tendencias en ciberseguridad	60
<i>Tendencias TIC de INCIBE (2016). Julio 2016</i>	60
<i>Nuevos escenarios y desafíos de la seguridad. Telefónica (septiembre de 2016)</i>	61
<i>Otras tecnologías de impacto en el futuro de la ciberseguridad analizadas</i>	61
Estudios de ciberseguridad	63
Bibliografía de consulta	64
 Capítulo segundo	
Crisis y ciberespacio: hacia un modelo integral de respuesta en el Sistema de Seguridad Nacional	65
<i>Joaquín Castellón Moreno</i>	
<i>María Mar López Gil</i>	
Introducción	67
La lucha por el control del ciberespacio	70
De la gestión de incidentes a la gestión de crisis en el ciberespacio	72
Los ciberataques del siglo XXI y sus consecuencias	74
<i>El soldado de bronce de Tallin</i>	74
<i>La ralentización del Programa nuclear iraní</i>	75
<i>Ataques a los servicios esenciales en la Europa del Este</i>	76
<i>Los ataques silenciosos y el robo de información</i>	77

	Página
<i>Las oportunidades del ciberespacio para la amenaza terrorista</i>	78
<i>Ataques a la reputación e influencia política</i>	79
<i>Las amenazas al sector privado</i>	80
<i>Ataques con efectos cinéticos</i>	82
La gestión de crisis en el Sistema de Seguridad Nacional	82
Colaboración público-privada y gestión de crisis de ciberseguridad en el Sistema de Seguridad Nacional	85
De la acción a la puesta en práctica. El ejercicio <i>Cyber Europe</i>	91
Conclusiones y retos	93
 Capítulo tercero	
Análisis de las ciberamenazas	97
<i>Aníbal Villalba Fernández</i>	
<i>Juan Manuel Corchado Rodríguez</i>	
Introducción	99
Las ciberamenazas en el contexto de los riesgos globales	102
Elementos esenciales en el análisis de las amenazas	105
Evolución tecnológica y ciberseguridad	106
Ciberamenazas, agentes y objetivos	110
<i>Los agentes de las ciberamenazas</i>	<i>111</i>
<i>Criterios de determinación del nivel de peligrosidad de los ciberincidentes</i>	<i>119</i>
<i>Herramientas de las amenazas</i>	<i>120</i>
<i>Tendencias de amenazas globales de ciberseguridad</i>	<i>125</i>
Ciberincidentes en España	131
Conclusiones	136
 Capítulo cuarto	
El intercambio de información de ciberamenazas	139
<i>Miguel Rego Fernández</i>	
<i>Pedro Pablo Pérez García</i>	
Situación actual	141
<i>Necesidad de intercambiar información de amenazas e incidentes</i>	<i>141</i>
<i>Inhibidores y habilitadores para la compartición de información de amenazas</i>	<i>141</i>
<i>Barreras en el intercambio de información derivados de aspectos legales</i>	<i>142</i>
<i>Barreras en el intercambio de información derivados de falta de confianza</i>	<i>143</i>
<i>Insuficiente interés por parte de las partes</i>	<i>144</i>
<i>Barreras de carácter técnico</i>	<i>144</i>
<i>Beneficios y habilitadores en el Information Sharing</i>	<i>145</i>
<i>Marco normativo y legislativo aplicable en Europa y España</i>	<i>146</i>
<i>Áreas para una cooperación efectiva en el intercambio de amenazas</i>	<i>151</i>
<i>Los problemas de la normalización: iniciativas privadas vs estándares de facto</i>	<i>154</i>
<i>Datos a intercambiar</i>	<i>154</i>
<i>Métodos de intercambio</i>	<i>155</i>
<i>Formatos de intercambio de datos de amenazas</i>	<i>156</i>
<i>OpenIOC</i>	<i>157</i>
<i>Cybox, STIX, TAXII</i>	<i>157</i>

	Página
OTX	161
MISP	161
Análisis de requisitos de los actores del ecosistema público-privado para el intercambio de amenazas	163
Empresas, Administraciones y usuarios/ciudadanos	163
ISAC vs ISAO	163
Fabricantes y proveedores de servicios de inteligencia	165
Organismos oficiales (CERT, CSIRT y agencias públicas)	165
El caso norteamericano: Cyber Threat Intelligence Integration Center (CTIIC)	166
Conclusiones y Recomendaciones	168
Bibliografía de consulta	169
 Capítulo quinto	
Cooperación público-privada en la protección de infraestructuras críticas	171
<i>Fernando Sánchez Gómez</i>	
<i>Justo López Parra</i>	
Introducción	173
Un poco de historia	174
<i>BlackEnergy</i>	176
<i>Stuxnet</i>	177
<i>Ciberataque a Estonia 2007</i>	179
<i>Titan Rain</i>	179
Pilares de la colaboración en la protección de las infraestructuras críticas	180
El sistema de planificación PIC y su encaje con la ciberseguridad	184
<i>Normativa PIC, colaboración público-privada y ciberseguridad</i>	184
<i>El Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC)</i> ..	188
<i>Los Planes Estratégicos Sectoriales (PES)</i>	192
<i>Los Planes de Seguridad del Operador (PSO)</i>	195
<i>Los Planes de Protección Específicos (PPE)</i>	196
<i>Los Planes de Apoyo Operativo (PAO)</i>	198
Herramientas para la colaboración	199
<i>Apoyo frente a incidentes</i>	199
<i>El equipo de respuesta a incidentes cibernéticos de seguridad e industria (CERTSI)</i>	201
<i>La Oficina de Coordinación Cibernética del Ministerio del Interior</i>	202
<i>Alerta temprana e intercambio de información</i>	204
<i>Ciberejercicios</i>	207
<i>Acuerdos de colaboración</i>	209
<i>Controles recomendados</i>	210
Bibliografía	213
 Capítulo sexto	
La cooperación público-privada en el fomento de la cultura de ciberseguridad	217
<i>Gregorio Miguel Pulido Alonso</i>	
<i>Rafael Rosell Tejada</i>	
Introducción	219
El eslabón más débil de la cadena	220
Ciberresiliencia y concienciación en ciberseguridad	223

	Página
Iniciativas existentes	224
<i>En España</i>	224
<i>Dentro del sector privado</i>	231
<i>Fuera del entorno laboral</i>	233
<i>A nivel multinacional</i>	234
<i>Como parte de la ciberdefensa</i>	235
Programas, planes, campañas de concienciación	237
Cooperación público-privada para la concienciación en ciberseguridad ...	240
<i>Experiencias y buenas prácticas</i>	243
<i>Un ejemplo concreto</i>	244
Conclusiones	245
 Capítulo séptimo	
I+D+i y ciberseguridad: análisis de una relación de interdependencia	247
<i>Aurelio Hinarejos Rojo</i>	
<i>José de la Peña Muñoz</i>	
Introducción	249
Investigación, desarrollo e innovación en ciberseguridad	253
<i>La investigación y el desarrollo</i>	254
<i>Innovación</i>	260
<i>Necesidad de una actuación específica de I+D+i en ciberseguridad</i>	262
<i>La inversión en I+D+i en ciberseguridad</i>	268
El papel de la colaboración público-privada en el proceso de I+D+i	275
<i>Iniciativas foráneas</i>	277
<i>Iniciativas supranacionales</i>	278
<i>España</i>	279
<i>Retos, riesgos y oportunidades</i>	280
Interdependencia entre innovación y ciberseguridad	283
Conclusión	286
 Capítulo octavo	
Capacitación profesional y formación especializada en ciberseguridad	291
<i>Óscar Pastor Acosta</i>	
<i>José Javier Martínez Herráiz</i>	
Introducción	293
Escasez de profesionales en ciberseguridad	295
Iniciativas de organismos públicos para la formación y certificación profesional en ciberseguridad	300
<i>National Cybersecurity Workforce Framework</i>	301
<i>CESG Certified Professional Scheme</i>	306
<i>DoD 8570.01-M</i>	312
<i>CCN/INAP - Esquema Nacional de Certificación de Profesionales en Ciberseguridad</i>	316
<i>SEPE - Certificado de Profesionalidad en Seguridad Informática</i>	319
Iniciativas privadas de formación y certificación en ciberseguridad	321
<i>ISACA-CSX (Cybersecurity Nexus)</i>	321
<i>(ISC)²-CISSP (Certified Information Systems Security Professional)</i>	325
<i>SANS/GIAC</i>	331
<i>EC-Council - CEH (Certified Ethical Hacker)</i>	336

	Página
Conclusiones	338
Bibliografía	342
EPÍLOGO	
Presente y futuro de la ciberseguridad: el impacto y la necesidad de la colaboración público-privada.....	351
<i>Luis Joyanes Aguilar</i>	
La ciberseguridad en la transformación digital	351
La concienciación en ciberseguridad	352
El futuro de la ciberseguridad	352
<i>El decálogo de ciberseguridad FTF & Fundación Bankinter</i>	353
<i>El decálogo de ciberseguridad de INCIBE</i>	354
Ciberseguridad 4.0	355
Composición del grupo de trabajo	357
Cuadernos de Estrategia	359

Introducción

Luis Joyanes Aguilar

Presidente de la Fundación I+D del Software Libre (Fidesol)

El objetivo principal del Cuaderno de Estrategia *Ciberseguridad: la colaboración público-privada* es identificar las tendencias actuales y futuras de la ciberseguridad y estudiar la oportunidad de la colaboración público-privada y realizar propuestas prácticas que permitan la consecución de los mayores beneficios al sector de la ciberseguridad, tanto en el aspecto tecnológico como en el económico y en el social.

La Comisión Europea puso en marcha el 5 de julio de 2016 una nueva asociación público-privada sobre ciberseguridad que, en su presentación, esperaba una inversión de 1.800 millones de euros al final del año 2020 dentro del programa «Horizonte 2020», a través de la propia Comisión Europea y de la Organización Europea de Ciberseguridad (ECSO), constituida por grandes empresas europeas con esta finalidad específica. El proyecto consta de un conjunto de iniciativas destinadas a equipar mejor a Europa contra los ciberataques y a reforzar la competitividad de su sector de ciberseguridad. La propia Comisión Europea reconoce la importancia de la colaboración público-privada y de su necesidad vital para enfrentarse a desafíos en materia de ciberseguridad.

El 6 de julio de 2016 —el día siguiente a la firma del acuerdo de la Unión Europea sobre colaboración público-privada en materia de ciberseguridad— se publicó la directiva *Network and Information Systems (NIS)* que obliga a los «prestadores de servicios esenciales a tomar las medidas necesarias para garantizar la seguridad de sus instalaciones». La reciente Directiva de

ciberseguridad (Unión Europea) 2016/1148 del Parlamento Europeo y del Consejo entró en vigor el 9 de agosto de 2016 y es relativa a las medidas destinadas a garantizar su elevado nivel común de seguridad de las redes y sistemas de información de la Unión Europea.

Entonces, ¿podríamos definir ciberseguridad? Existen numerosas definiciones de este término pero optaremos por la dada por la *ITU (International Telecommunications Union)* o UIT por su denominación en español (Unión Internacional de Telecomunicaciones), la asociación mundial de referencia en el sector de las Telecomunicaciones y de las Tecnologías de la Información y las Comunicaciones (TIC) con sede en Ginebra. La recomendación UIT-T X.1205 (04/2008) publicada en Ginebra en 2009 por el Sector de Normalización de las Telecomunicaciones de la UIT en la serie X (Redes de datos, comunicaciones de sistemas abiertos y seguridad) y en el área de «seguridad en el ciberespacio-ciberseguridad» revisada y mantenida en 2010, define la ciberseguridad como:

«El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:

- Disponibilidad.
- Integridad, que puede incluir la autenticidad y el no repudio.
- Confidencialidad».

En consecuencia, la UIT considera que la ciberseguridad ha de garantizar que se alcancen y mantengan las propiedades de seguridad de los activos y de la organización y los usuarios contra los riesgos de seguridad correspondientes al ciberentorno [ciberespacio]. La definición de la UIT también nos señala y recomienda que para conseguir el éxito en una estrategia de ciberseguridad deberemos pensar en: «el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno».

Uniendo los principios emanados de la definición de ciberseguridad de la UIT, la creación de la iniciativa de «Colaboración público-privada en ciberseguridad de la Unión Europea» junto con la Directiva (Unión Europea) 2016/1148

y las directrices emanadas de la Estrategia de Ciberseguridad Nacional de España, junto a las orientaciones y recomendaciones recibidas, a su vez, del Instituto Español de Estudios Estratégicos, los autores de este Cuaderno de Estrategia han desarrollado esta obra y la han organizado en ocho grandes sectores que de una u otra forma reflejan los principios fundamentales de la definición de ciberseguridad de la UIT en su recomendación X.1205 (04/2008).

Una visión global de la colaboración público-privada en ciberseguridad

El contenido de la obra se ha dividido en una introducción, ocho capítulos y un epílogo. La introducción a modo de resumen ejecutivo. Los temas centrales de cada capítulo tratan de contemplar la situación real en los sectores de mayor impacto en la ciberseguridad y la ineludible necesidad de una colaboración público-privada:

- El advenimiento de Industria 4.0 y la cuarta revolución industrial asociada a ella, junto con las tecnologías facilitadoras y de impacto en la ciberseguridad.
- La seguridad nacional y el sector privado en la gestión de crisis en el ámbito de la ciberseguridad.
- El análisis de las ciberamenazas, gestión de riesgos de la ciberseguridad en España y las tendencias previstas.
- El intercambio de información y su rol en la lucha contra las ciberamenazas.
- La protección de las infraestructuras críticas mediante la colaboración público-privada.
- La cultura y concienciación de la ciberseguridad en la cooperación entre los sectores público y privado.
- La I+D+i en ciberseguridad: análisis de su interdependencia.
- Análisis de la capacitación profesional y la formación especializada en ciberseguridad.
- Presente y futuro de la ciberseguridad.

Un resumen de cada capítulo, sus resultados y conclusiones más relevantes se describen a continuación, con la reseña de cada uno de los autores.

Capítulo 1. *Ciberseguridad, la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 vs Ciberseguridad 4.0).* El capítulo escrito por Luis Joyanes Aguilar, presidente de la Fundación I+D del Software Libre (Fidesol), examina la iniciativa «Industria 4.0» y en España, «Industria Conectada 4.0», como apoyo y soporte a la necesaria transformación digital de las organizaciones y empresas. Las tecnologías disruptivas de «Industria 4.0» tales como *Big Data*, *Cloud Computing*, Internet de las Cosas y Ciberseguridad, enmarcadas en Ciudades Inteligentes (*Smart Cities*) están pro-

duciendo el advenimiento de la cuarta revolución industrial. Asimismo, se mencionan otras tecnologías de impacto en la empresa, en la industria y en diversos sectores como el eléctrico, el sector financiero, etcétera: impresión en 3D (o fabricación aditiva), tecnologías financieras (*fintech* y *blockchain*), las tecnologías ponibles (*wearables*), la realidad virtual y realidad aumentada... junto con el despliegue de los drones. A destacar también las grandes tendencias tecnológicas de inteligencia artificial, los robots virtuales (*bots*) y los *bots* conversacionales (*chatbots*).

En una segunda parte el capítulo destaca la iniciativa de la Unión Europea sobre colaboración público-privada, las nuevas directivas de Ciberseguridad (NIS) de la Unión Europea junto con el impacto que supondrá la aprobación y despliegue en el pasado mes de mayo de 2016 de la Ley de Privacidad y protección de datos también de la Unión Europea.

Asimismo, se hace un breve análisis del estado del arte de la ciberseguridad en América Latina y el Caribe, para lo cual se han estudiado diferentes estudios realizados por empresas privadas y organizaciones internacionales (la OEA y el BID) sobre la situación real de la ciberseguridad, manteniendo en el estudio el tema central de nuestra obra sobre colaboración público-privada.

Capítulo 2. Crisis y ciberespacio: hacia un modelo integral de respuesta en el Sistema de Seguridad Nacional. El capítulo está escrito por Joaquín Castellón Moreno, director operativo del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno, y por María Mar López Gil, jefa de la Oficina de Tecnología y Seguridad, responsable de Ciberseguridad, también del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno. El capítulo comienza con una amplia descripción del desarrollo y evolución de la Estrategia de Seguridad Nacional de 2013, de la Estrategia de Ciberseguridad Nacional también de 2013, así como el desarrollo del Plan Nacional de Ciberseguridad. Asimismo, se describe el nacimiento y aprobación de la Ley de Seguridad Nacional.

El mundo actual es físico y virtual a la vez, por ello se analiza la convergencia entre ambos mundos y la materialización de la convergencia entre ellos. Se estudia el ciberespacio como un mundo desconocido y lleno de incertidumbres y el uso ilícito del ciberespacio y sus posibles consecuencias sobre los intereses y la Seguridad Nacional. Se describe el término moderno de *Global Commons* y se define desde la perspectiva del Derecho Internacional.

Un tema de gran interés tratado en profundidad es el de los ciberataques del siglo XXI y sus consecuencias, se recogen algunos de los casos más conocidos y de mayor impacto a nivel mundial. La casuística es muy extensa a tenor del propósito, los actores y alcance de los ataques, pero es fácil encontrar elementos comunes como pueden ser la enorme dificultad de determinar los autores, la necesidad de contar con una eficaz colaboración internacional o realizar una adecuada gestión de la comunicación para minimizar los efec-

tos. Se dedica un apartado, expresamente, a la colaboración público-privada y gestión de crisis de ciberseguridad en el Sistema de Seguridad Nacional.

Por último, se analiza un «modelo integrado de Gobernanza» en la gestión de crisis para la ciberseguridad nacional junto con el desarrollo del Plan Nacional de Ciberseguridad. También se estudia la importancia de la concienciación y la cultura de seguridad nacional y ciberseguridad, así como la importancia de entrenamiento y de ejercicios de ciberseguridad. Se destaca y describen, muy especialmente, la realización de los ejercicios de *Cyber Europe* y se cita el último realizado en octubre de 2016, *Cyber Europe 2016*.

Capítulo 3. *Análisis de las ciberamenazas.* Los autores del artículo son: Aníbal Villalba, asesor del presidente del Consejo Nacional de Ciberseguridad, y Juan Manuel Corchado Rodríguez, catedrático de Ciencias de la Computación e Inteligencia Artificial y vicerrector de Investigación y Transferencia de la Universidad de Salamanca.

El capítulo describe detalladamente el concepto de las ciberamenazas desde sus orígenes, los objetivos y los efectos a conseguir. Se realiza un estudio detallado de la evolución de los incidentes de ciberseguridad en España y de que se ha hecho frente a ellos y los métodos seguidos.

Las ciberamenazas constituyen un reto global y es necesario realizar un estudio en profundidad dado el gran reto que ellas suponen, pero también es preciso analizar las oportunidades que un buen plan de defensa, frente a las ciberamenazas, puede redundar en beneficio de organizaciones y empresas.

En los últimos años han emergido nuevos conceptos globales de impacto tales como la inteligencia y la seguridad digital. Se hace un estudio profundo de ambos conceptos por la importancia que hoy día están suponiendo para una buena estrategia de ciberseguridad.

El capítulo hace un análisis de los riesgos de la ciberseguridad y su correcta gestión desde un enfoque centrado principalmente en España. Se realiza también un estudio sobre las tendencias que muestran las ciberamenazas y un análisis de las mismas que permitan obtener la mayor eficiencia posible de los resultados del citado estudio de amenazas.

Capítulo 4. *El intercambio de información, factor clave en la lucha contra las ciberamenazas.* Este capítulo, en el que se analiza con detalle el importante factor del intercambio de información y el rol actual de los datos como elemento clave en la lucha contra las ciberamenazas, ha sido desarrollado por Miguel Rego Fernández, director general del Instituto Español de Ciberseguridad (INCIBE), y Pedro Pablo Pérez García, CEO (*Chief Executive Officer*) de la empresa especializada en seguridad de la información Telefónica Eleven Paths.

Comienza el capítulo haciendo un análisis en profundidad de la situación actual y se describe la importancia del intercambio de información de amenazas e incidentes, junto con los inhibidores y habilitadores para la compar-

tición de la información, así como el marco normativo y legislativo aplicable en Europa y España, y las áreas más eficaces para una cooperación eficiente en el intercambio de amenazas.

Se afronta y estudian detenidamente los problemas de normalización, tanto en estándares *de facto* como en iniciativas privadas y, en consecuencia, los formatos de intercambio de datos y de descripción de amenazas e incidentes cibernéticos, tales como IETF, MITRE, STIX, Taxii...

Se realiza un estudio sobre los análisis de requisitos de los actores del ecosistema público-privado para el intercambio de amenazas teniendo presente: empresas y usuarios finales, operadores críticos, compartición de inteligencia y centros de análisis (ISAC) versus organizaciones de análisis y compartición de información (ISAO), fabricantes y proveedores de productos y servicios de ciberseguridad junto a entes gubernamentales como CERT, CSIRT, agencias, empresas públicas, etcétera.

Se describe el caso emblemático norteamericano *Cyber Threat Intelligence Integration Center (CTIIC)*.

En las conclusiones y recomendaciones del capítulo se propone un modelo de incentivos, actuaciones a llevar a cabo por la Administración y el sector privado y se hace un análisis del desarrollo normativo legislativo.

Capítulo 5. *Cooperación público-privada en la protección de infraestructuras críticas.* La protección de las infraestructuras críticas de un país es uno de los sectores de la ciberseguridad donde más puede ser vital la cooperación público-privada. Por esta razón el artículo se ha escrito en coordinación por Fernando Sánchez Gómez, del CNPIC (Centro Nacional para la Protección de las Infraestructuras Críticas) del Centro Tecnológico de Seguridad del Ministerio del Interior, y Justo López Parra, de la operadora eléctrica Endesa.

El capítulo comienza con una reseña histórica de incidentes provocados o apoyados por Gobiernos contra infraestructuras críticas, comentando ejemplos significativos, tales como *Stuxnet*, *Blackenergy*... Estas amenazas sirven para la justificación de la necesidad de cooperación público-privada y los principios clave de la colaboración: confianza, transparencia... Se explica la Normativa y Ley PIC en materia de ciberseguridad y los distintos instrumentos de planificación (fundamentalmente PNPIC, PSO y los PPE).

Se describen los servicios o herramientas que sirven para cimentar la cooperación. Son servicios ofrecidos por la entidad pública a las entidades privadas. Se detallan los más importantes: CERT, alerta temprana, realización de ciberejercicios, controles recomendados (con referencias a organizaciones internacionales tales como ISO, SANDS, NIST, NIS...), compartición de información, etcétera, y el apoyo a prestar frente a incidentes.

Capítulo 6. *La cooperación público-privada en el fomento de la cultura de ciberseguridad.* El fomento de la cultura y concienciación de la ciberseguridad y el rol del sector privado es un factor clave en el desarrollo de la industria de

ciberseguridad. El capítulo ha sido escrito por el teniente coronel Gregorio M. Pulido Alonso, del Mando Conjunto de Ciberdefensa, y Rafael Rosell Tejada, director comercial de la empresa de especialidad en seguridad informática y ciberseguridad S2 Grupo.

El capítulo comienza con una amplia introducción donde se describe y analiza la necesidad de una ciberresiliencia y concienciación en ciberseguridad, cuáles son las iniciativas a nivel nacional y cuáles son las iniciativas a nivel internacional, destacando los temas más sobresalientes en cada una de estas iniciativas y su impacto en la necesaria cultura de ciberseguridad.

Dos temas se describen con detalle por su importancia en la cultura de la ciberseguridad: la necesaria concienciación en ciberseguridad en el sector privado y la ciberseguridad personal fuera del entorno laboral.

Se dedica una especial importancia a la ciberdefensa, como un caso especial y una propuesta de la necesaria cooperación entre el sector privado y el sector público en concienciación.

El capítulo termina con unas conclusiones donde se realiza por parte de los autores una propuesta de cuál ha de ser el rol o papel del sector privado en el fomento de la cultura de ciberseguridad.

Capítulo 7. I+D+i y ciberseguridad. Análisis de una relación de interdependencia. La I+D+i requiere y exige de una gran aportación del sector de ciberseguridad. El análisis de su interdependencia se estudia por dos expertos, uno perteneciente a la industria de defensa, el capitán del Cuerpo de Ingenieros Politécnicos del Ejército (CIPET) de la Dirección General de Armamento y Material, Aurelio Hinarejos Rojo, y otro dedicado al análisis holístico de la ciberseguridad, el periodista José de la Peña Muñoz, director de la revista española *SIC Seguridad en Informática y Comunicaciones*, un medio especializado pionero y referencia a nivel nacional e internacional en el sector de la seguridad de la información y las comunicaciones.

El capítulo tiene como objetivo principal analizar la relación de interdependencia que existe entre la I+D+i y la ciberseguridad y para su consecución se pretende dar respuesta a unas cuestiones básicas, tales como: deducir cuál es la contribución de la I+D+i a la ciberseguridad y, recíprocamente, cómo contribuye la ciberseguridad a la innovación y al crecimiento económico.

Se realiza un acercamiento a la situación de España en relación con otros países, organizaciones internacionales y supranacionales, y se mencionan algunas áreas y aspectos de la ciberseguridad que deberían de ser susceptibles de atención por parte de una adecuada política de I+D+i.

Los autores también ofrecen una visión de la conformación de iniciativas de colaboración público-privada (CPP) orientadas a la I+D+i, especificando algunas de gran interés e identificando su mecanismo de funcionamiento y los retos a los que se enfrentan. El capítulo termina con unas conclusiones acerca de algunos rasgos de contexto global futuro que, a su juicio, han de

tenerse en cuenta para fomentar y crear ecosistemas viables de ciberseguridad, I+D+i y CPP.

Capítulo 8. *Capacitación profesional y formación especializada en ciberseguridad.* La escasez de profesionales capacitados en ciberseguridad y la necesidad de una formación especializada de estos profesionales en organizaciones y empresas se afronta desde una perspectiva profesional de especialización y académica. Óscar Pastor Acosta, gerente de Seguridad en ISDEFE, y J. Javier Martínez Herráiz, catedrático y director de la Cátedra DARS de Ciberinteligencia de la Escuela Politécnica de la Universidad de Alcalá de Henares, han desarrollado este capítulo centrado en la capacitación y certificaciones profesionales, así como en las ofertas de especialización en ciberseguridad a nivel nacional e internacional.

El capítulo se estructura en dos partes bien definidas. Una primera parte de introducción, donde se explican los objetivos que se pretenden conseguir y el alcance del análisis enmarcado dentro del contexto de colaboración público-privada en ciberseguridad, ajustándose al objeto principal de este Cuaderno de Estrategia.

La segunda parte se centra en el tema fundamental y candente, en organizaciones y empresas, tanto a nivel nacional como internacional: la escasez de profesionales en ciberseguridad. Se ha realizado un estudio en profundidad sobre los datos aportados por informes de entidades privadas, especialmente, el reputado estudio «Global Information Security Workforce Study» de (ISC)² en los años 2011, 2013 y 2015.

De igual modo, se han estudiado las apreciaciones realizadas a este respecto en las Estrategias Nacionales de ciberseguridad de varias de las naciones más avanzadas en este campo.

Por último, se realiza un estudio en profundidad donde se reflejan los perfiles profesionales más demandados y las competencias técnicas necesarias que requieren.

Epílogo. *Presente y futuro de la ciberseguridad. El impacto y la necesidad de la colaboración público-privada.* El epílogo de la obra, a modo de síntesis práctica, ha sido escrito por el coordinador del libro, el profesor Luis Joyanes Aguilar, recogiendo ideas globales de los diferentes autores en los siguientes aspectos: la ciberseguridad en la transformación digital, la necesaria concienciación —tratada ampliamente en varios capítulos anteriores—, el futuro de la ciberseguridad y sendas propuestas de decálogo de ciberseguridad realizada por dos organizaciones: INCIBE y FTF & Fundación Bankinter, en obras citadas y referenciadas en el mencionado epílogo: 1. FTF & Fundación Bankinter. «Una hoja de ruta con diez propuestas» para avanzar hacia el objetivo de un ciberespacio más seguro. 2. INCIBE. *Decálogo de ciberseguridad. El camino a la ciberseguridad en su empresa* (manual de buenas prácticas en el tratamiento de la información de la empresa).

Capítulo primero

Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0)

Luis Joyanes Aguilar

Presidente de la Fundación I+D del Software Libre (Fidesol)

Catedrático de Lenguajes y Sistemas Informáticos

Universidad Pontificia de Salamanca

Resumen

Industria 4.0 ha sido un término acuñado por el Gobierno alemán con el soporte de industrias alemanas para describir la digitalización de sistemas y procesos industriales, y su interconexión mediante **Internet de las cosas** para conseguir llegar a una nueva visión de la fábrica del futuro o fábrica inteligente. La transformación digital de la industria y las empresas con la integración de las nuevas tecnologías disruptivas como **Big Data**, **Cloud Computing** (la nube), **Internet de las Cosas** y **Ciberseguridad**, todo ello, enmarcado en las **Ciudades Inteligentes (Smart Cities)**, está produciendo el advenimiento y despliegue de la **cuarta revolución industrial**. Las sofisticadas amenazas a la propiedad intelectual y a la privacidad, a los sistemas y los productos conectados, requieren estrategias y herramientas de ciberseguridad que garanticen en el marco de la Industria 4.0, ciberseguridad de calidad industrial y habilitados para la tendencia dominante de Internet de las Cosas.

Palabras clave

Industria 4.0, **Big Data**, computación en la nube, Internet de las Cosas, cadena de bloques, tecnologías financieras, aprendizaje automático, aprendizaje profundo, privacidad, robots conversacionales, robots virtuales, robots conversacionales, ciudades inteligentes, web profunda.

Abstract

*Industry 4.0 has been a term coined by the German Government with the support of German industries, to describe the digitization of systems and industrial processes, and their interconnection via the Internet of things to get reach a new vision of the factory of the future or intelligent factory. The digital transformation of the industry and companies with the integration of new disruptive technologies like **Big Data, Cloud Computing (Cloud), Internet of Things** and **Cybersecurity**, all framed in the Smart Cities is producing the advent and deployment of the **fourth industrial revolution**. The sophisticated threats to intellectual property and privacy, systems and connected products require strategies and tools cybersecurity to ensure within the framework of the Industry 4.0, cybersecurity industrial quality and enabled the dominant trend of Internet of Things.*

Keywords

Industry 4.0, Big Data, cloud computing, Internet of Things, blockchain, fintech, machine learning, deep learning, privacy, cobots, bots, chatbots, smart cities, deep web.

La ciberseguridad en tiempo real

Las noticias de impacto relativas a ciberseguridad se suceden casi sin solución de continuidad y, con frecuencia, la última noticia hace palidecer la anterior. En el mes de septiembre de 2015, Apple sufrió el mayor ataque informático de su historia y tuvo que retirar más de cincuenta aplicaciones que contenían un *software* malicioso (*malware*) que pretendía robar datos de los dispositivos de los usuarios. Unos meses antes, Sony Pictures Entertainment quedó paralizada por la intrusión de unos *hackers* que robaron más de 33.000 documentos con información comprometedora de la compañía y sus empleados. El propio Pentágono de Estados Unidos ha sufrido ciberataques de diferentes índoles.

El viernes 21 de octubre de 2016 se produjo una oleada de ciberataques masivos que inutilizaron las páginas web de grandes compañías¹. La prensa mundial calificó a estos ciberataques como los más graves de la última década. Los ciberataques se produjeron contra uno de los mayores proveedores de internet, la empresa Dyn, que controla los servicios de páginas web de grandes compañías y medios de comunicación como Twitter, Spotify, Reddit, Airbnb, Netflix, Paypal, eBay... y medios de comunicación como *The New York Times*, *Financial Times*, *The Guardian*... Los ataques fueron de denegación de servicios, DDoS y estimaciones publicadas hablaban de haber afectado a más de 1.000 millones de usuarios.

Durante el encuentro anual de 2015 del Foro Económico Mundial (WEF, World Economic Forum), celebrado en Davos (Suiza), John Chambers, CEO de Cisco, definió muy claramente la situación actual de la ciberseguridad como objetivo preferente de las empresas con la siguiente frase lapidaria, lanzada durante su intervención en el evento: «Las empresas se dividen en dos categorías: las que han sido *hackeadas* y las que no lo saben». Viniendo del máximo responsable de la empresa fabricante número 1 del mundo de las comunicaciones, es para hacernos pensar. En este mismo foro, la ciberseguridad estuvo en primer plano y en posición preferente como objetivo de las empresas. Entre las conclusiones de los expertos del Foro se anunció con gran resonancia que el sector tecnológico, en el que se engloba el análisis masivo de datos (*Big Data*) y el almacenamiento en la nube, podría producir unos beneficios globales de entre 9,6 y 21,6 billones de dólares, por lo que alertaron sobre la seguridad informática y advertían que si la sofisticación de los ataques superaba las capacidades defensivas de los equipos los altercados provocarían pérdidas y daños más graves.

Las empresas necesitan fondos para investigar sobre nuevos tipos de *malware* y desarrollar nuevos métodos para prevenir ciberdelitos. El citado

¹ Guillén, Beatriz; Faus Joan y Jiménez, Rosa. «Varios ciberataques masivos inutilizan las webs de grandes compañías». *El País*, 22 de octubre de 2016. http://tecnologia.elpais.com/tecnologia/2016/10/21/actualidad/1477059125_058324.html

Chambers concluyó su intervención en el Foro expresando su temor por lo que puede estar al caer: «las cuestiones relacionadas con la ciberseguridad empeoraron en 2014 y, lamentablemente, en 2015 va a ser mucho peor»².

Otra fuente solvente, IBM³, una de las grandes empresas especializadas en la actualidad en ciberseguridad, considera que una organización recibe un promedio de 1.400 ciberataques por semana y a nivel mundial estima que el cibercrimen genera anualmente 440.000 millones de dólares en ganancia, y cada día se generan nuevas amenazas a las que las empresas no tienen capacidad de enfrentarse con éxito, a menos que dispongan de una buena estrategia de ciberseguridad, así como las herramientas y programas adecuados.

¿Así pues, cómo está España en ciberseguridad con indicadores y referencias internacionales?

El índice mundial de ciberseguridad de la UIT (ITU)

El Índice Mundial de Ciberseguridad [IMC, en inglés, *GCI (Global Cybersecurity Index)*]⁴ surge de la asociación de colaboración entre el sector privado y una organización internacional, la UIT, con el fin de impulsar la cuestión de la ciberseguridad hasta el primer plano de las agendas nacionales.

El IMC es un proyecto conjunto emprendido por ABI Research y la Unión Internacional de Telecomunicaciones (ITU, International Telecommunications Union), que contribuye a una mejor comprensión del compromiso de los Estados soberanos con la ciberseguridad. Tiene sus raíces en la Agenda sobre Ciberseguridad Global de la UIT y considera el nivel de compromiso en cinco ámbitos o indicadores: medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades y cooperación internacional.

² Noticias de Panda Security: www.pandasecurity.com/spain/mediacenter/malware/la-ciberseguridad-objetivo-preferente-de-las-empresas [consultado, 30 de julio de 2016].

³ Antonio Becerra, «El reto actual de la ciberseguridad», en *El Economista*, México, 29 de agosto de 2015. www.eleconomista.com.mx/tecnociencia/2015/08/29/reto-actual-ciberseguridad [consultado, 7 de agosto de 2016].

⁴ La última edición publicada como informe «Índice Mundial de Ciberseguridad y perfiles de ciberbienestar» fue en abril de 2015 [en línea y descarga gratuita: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf]. La edición de 2016 está en construcción, aunque la última visita [5 de octubre de 2016] realizada a su página oficial en el sitio oficial, de la ITU [www.itu.int] y en la página oficial del índice GCI 2016 [en línea: <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx>] se anuncia que el índice está en elaboración y que la próxima edición del GCI tiene previsto un índice mejorado, más consultas abiertas y más *partners*. ITU manifiesta que se ha formulado el nuevo índice con un enfoque *multistakeholder* que potencia la experiencia de diferentes organizaciones, con los objetivos de mejorar la calidad del GCI, promoviendo la cooperación internacional y el intercambio de conocimiento en este tema [<http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2016.aspx>, consultado 14 de octubre de 2016].

El resultado es un índice a nivel de país y una clasificación mundial de la preparación para la ciberseguridad. El IMC no pretende determinar la eficacia ni el éxito de una medida particular, sino simplemente la existencia de estructuras nacionales para implementar y promover la ciberseguridad.

La UIT reconoce que no es posible que una sola publicación trate adecuadamente todos los aspectos de la ciberseguridad con la profundidad necesaria. Sin embargo, esperan que el perfil de ciberseguridad sea de utilidad para los debates y las investigaciones en curso ya que proporciona datos reales sobre los retos y oportunidades actuales en materia de ciberseguridad. En el anexo 3 de la publicación del IMC⁵ figura una recopilación de los perfiles de ciberseguridad de todos los Estados miembros de la UIT, actualizados en el momento de imprimir de la citada publicación.

Clasificación mundial (índice IMC)

Muchos países tienen la misma clasificación en el índice, lo que indica que se encuentran en el mismo nivel de preparación. Este índice tiene un bajo nivel de detalle, ya que su objetivo es presentar la preparación de los países para la ciberseguridad o su compromiso con esta y no el detalle de sus capacidades ni sus posibles vulnerabilidades (fuente: ITU).

Cuadro 1: Clasificación de los países por índice

País	Índice	Clasificación mundial
Estados Unidos de América*	0,824	1
Canadá*	0,794	2
Australia*	0,765	3
Malasia	0,765	3
Omán	0,765	3
Nueva Zelanda*	0,735	4
Noruega*	0,735	4
Brasil	0,706	5
Estonia*	0,706	5
Alemania*	0,706	5
India*	0,706	5
Japón*	0,706	5

Figura 1.1.

Fuente: ITU. http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf

En la clasificación mundial España ocupa el grupo 9, pero por índice numérico figuramos en el puesto 33. Destacar que en Europa los países con mayor índice (por encima de España) son: Noruega, Estonia, Alemania, Reino Unido, Austria, Hungría, Países Bajos, Letonia, Suecia, Letonia, Eslovaquia y Francia; a continuación España y nos sigue Italia. Resaltar que en el caso

⁵ Véase: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf

de Latinoamérica están delante de España: Brasil, Uruguay y Colombia, por este orden.

Índice mundial de ciberseguridad y perfiles de ciberbienestar		
País	Índice	Clasificación mundial
República de Corea	0,706	5
Reino Unido	0,706	5
Austria*	0,676	6
Hungría*	0,676	6
Israel*	0,676	6
Países Bajos*	0,676	6
Singapur	0,676	6
Letonia*	0,647	7
Suecia*	0,647	7
Turquía	0,647	7
Hong Kong	0,618	8
Finlandia	0,618	8
Qatar	0,618	8
Eslovaquia	0,618	8
Uruguay	0,618	8
Colombia	0,588	9
Dinamarca*	0,588	9
Egipto	0,588	9
Francia*	0,588	9
Mauricio	0,588	9
España*	0,588	9
Italia	0,559	10
Marruecos	0,559	10
Uganda	0,559	10

Figura 1.2.

Fuente: ITU. http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdfFig

La cuarta revolución industrial

La cuarta revolución industrial (origen del término Industria 4.0) hace referencia a las cuatro fases de la revolución industrial.

- *Primera revolución industrial.* Máquinas de vapor y ferrocarril en el siglo XIX.
- *Segunda revolución industrial.* Motores eléctricos y producción en masa a principios del siglo XX. Aparece el motor de combustión, se desarrolla el aeroplano y el automóvil, y como grandes inventos aparece el teléfono y la radio.
- *Tercera revolución industrial.* Automatización y la informática en los años 70 del siglo XX.
- *Cuarta revolución industrial.* Los actuales «sistemas ciberfísicos» que recopilan y procesan información, toman decisiones inteligentes y ejecutan tareas en entornos cambiantes.

La Industria 4.0 es el producto más tangible de la cuarta revolución industrial y está favoreciendo la fabricación inteligente en un marco revolucionario.

rio para diseñar, implantar y gestionar ecosistemas complejos que proporcionan información en tiempo real y posibilitan las interacciones autónomas entre máquinas, sistemas, objetos y cosas. Este modelo permite sacar el máximo partido y rendimiento del **Internet de las Cosas (IoT)**, la nube, los *Big Data* y la analítica de datos, las aplicaciones de última generación y la ciberseguridad.

Industria 4.0: origen, evolución y futuro

Industria 4.0 ha sido un término acuñado por el Gobierno alemán para describir la digitalización de sistemas y procesos industriales y su interconexión mediante el Internet de las Cosas; en otras palabras, conseguir la transformación digital de la industria. Pese a todo el esfuerzo de propagación del término, en el caso alemán, como origen del mismo, todavía muchas empresas de ese país —en el año 2015— no sabían bien qué hacer con ese nuevo paradigma industrial y cómo posicionarse⁶. «Uno de cada dos directivos de la industria alemana, austriaca y suiza desconocen el término Industria 4.0, solo una cuarta parte sí dice conocer el término, sin saber bien qué entender del mismo y solo la cuarta parte restante conoce bien los cambios que traerá consigo la Industria 4.0».

En España, el País Vasco ha sido pionero y el Gobierno vasco lanzó una iniciativa para impulsar la Industria 4.0 haciendo propio el concepto y poniéndose un objetivo: «que la industria vasca vuelva a alcanzar el 25 % del PIB⁷». Más tarde comentaremos la iniciativa a nivel nacional conocida como «Industria Conectada 4.0».

El término Industria 4.0 ha hecho fortuna y, tanto en Europa como en Asia y América, ya existen iniciativas sobre el mismo. En realidad, el significado inherente al término es la creación del concepto de **fábrica inteligente** que ha sido impulsada, principalmente por las empresas industriales alemanas Siemens y Bosch.

Industria 4.0 viene asociado con el nacimiento de la cuarta revolución industrial y se corresponde con una nueva manera de organizar los medios de producción utilizando las tecnologías digitales y la información inteligente de datos a partir del *Big Data* (los grandes volúmenes de datos que se podrán transmitir entre objetos inteligentes a través del Internet de las Cosas).

⁶ Resultados de la encuesta realizada por el proveedor de servicios informáticos CSC entre novecientos altos directivos de empresas en Alemania, Austria y Suiza. Ver «Industria 4.0: hacia el futuro de la producción industrial» en *Economía Hispano-Alemana*, n.º 2, 2015, pp. 7-8.

⁷ Eneko Ruiz Jiménez, «La cuarta revolución industrial llega desde Alemania», *El País*, 2 de julio de 2015. <http://www.elpais.com/ccaa/2014/10/15/paisvasco/1413383975:967198.html> [consultado 2 de octubre de 2015].

El concepto fue utilizado por primera vez en 2011 en la Feria de Hannover (Salón de Tecnología Industrial). Posteriormente, en 2013, el Gobierno alemán encargó a una comisión de trabajo e investigación de la National Academy of Science and Engineering (ACATECH) un informe que detallara el significado y el posible poder del término.

Las tecnologías disruptivas tales como *Cloud Computing* (la nube), Computación Ubicua, Internet de las Cosas (*IoT*, *Internet of Things*), *Big Data* y *Analytics*... o las tendencias de consumo como **BYOD** (Bring Your Own Device) están revolucionando la forma de entender la tecnología y el modo en que interactuamos las personas con ella. A la industria están llegando las tecnologías anteriores unidas a otras que ya se apoyan en el campo de los sensores, las redes inalámbricas, los objetos inteligentes... Así, tecnologías ya clásicas como **M2M** (*Machine to Machine*), soporte de la comunicación entre máquinas y dispositivos; redes inalámbricas de sensores **WSN** (*Wireless Sensor Networks*) y la evolución del Internet de las Cosas en el Internet Industrial de las Cosas, **IIoT** (*Industrial Internet of Things*) o internet de todo, **IoE** (*Internet of Everything*), como prefiere denominarlo Cisco —el gigante mundial de las telecomunicaciones—.

Industria conectada 4.0

La iniciativa «Industria Conectada 4.0» es la extensión del concepto Industria 4.0 a la realidad nacional española y se lanzó a finales de julio de 2015, habiéndose presentado ya el programa oficial y todo el proyecto el 8 de octubre del mismo año. El proyecto busca impulsar la transformación digital de la industria española mediante la actuación conjunta y coordinada del sector público y privado. Por parte oficial, el antiguo Ministerio de Industria, Energía y Turismo y, por parte privada, las empresas multinacionales españolas, Banco de Santander, Telefónica e Indra, en una primera presentación.

El proyecto Industria Conectada 4.0 contempla los denominados «habilitadores digitales» que son el conjunto de tecnologías que hacen posible esta nueva industria que explota el potencial del Internet de las Cosas. Estos habilitadores se agrupan en tres grandes categorías⁸ (figura 3 del Proyecto Oficial).

- **Hibridación del mundo físico y digital** que permiten poner en relación el mundo físico con el digital mediante sistemas de captación de información o de materialización de la información digital en el mundo físico. Los habilitadores de mayor relieve en la actualidad según el informe:
 - Impresión 3D (impresión o fabricación aditiva).
 - Robótica avanzada.
 - Sensores y sistemas embebidos.

⁸ Informe «Industria Conectada 4.0. La transformación digital de la industria española».



Figura 1.3. Marco conceptual de habilitadores digitales. Fuente: Informe original «Industria Conectada 4.0». Ministerio de Industria, Energía y Turismo (8 de octubre de 2015). <http://www.industriaconectada40.gob.es/Paginas/Index.aspx#inicio>

- **Comunicaciones y tratamiento de datos.** La información anterior se canaliza y procesa. Son las tecnologías que permiten trasladar la información de forma segura desde los habilitadores de hibridación del mundo físico y digital hasta el siguiente grupo. Esos habilitadores —indispensables para que todos los restantes puedan funcionar adecuadamente— son, fundamentalmente:
 - Computación y *cloud* (computación en la nube).
 - Conectividad (hiperconectividad) y movilidad.
 - Ciberseguridad.
- **Aplicaciones de gestión intraempresa/interempresa.** La información alimenta a la tercera capa de habilitadores aplicando la inteligencia y los datos recibidos en aplicaciones de gestión. Conforman la capa de inteligencia o procesamiento de la información obtenida de los dos primeros bloques. Se consideran:
 - Soluciones de negocio.
 - Soluciones de inteligencia (*Big Data* y *Analytics*) y control.
 - Plataformas colaborativas.

En el citado informe oficial, presentado el 8 de octubre de 2015, se insistía en la necesidad de la digitalización para mantener posiciones competitivas y hacía hincapié en la hiperconectividad y las nuevas tecnologías ya implantadas: la computación en la nube, el Internet de las Cosas, el *Big Data* y la sensorización (sensores, contadores inteligentes...) que permitirían que la industria pueda alcanzar la cuarta revolución industrial.

La Industria 4.0 está soportada en cuatro grandes pilares, los tres citados del Internet de las Cosas, la nube y *Big Data* y un cuarto, la ciberseguridad.

Son numerosos los estudios publicados durante 2015 y 2016 —probablemente continuarán— sobre las tecnologías disruptivas de la Industria 4.0. Deseamos resaltar uno, en especial, que ha tenido gran impacto en el mundo de la empresa e industria. Ha sido realizado por la consultora multinacional The Boston Consulting Group. Este estudio define nueve pilares o parámetros de la Industria 4.0. A los cuatro citados anteriormente añade:

- Robots autónomos (colaborativos, inteligentes...).
- Los drones con énfasis en los drones programables y autónomos que, por una parte, están llamados a revolucionar a la industria y, por otra, a traer grandes riesgos a la ciberseguridad pública y privada.
- Simulación 3D.
- Sistemas integrados.
- Realidad aumentada (geolocalización).
- Fabricación aditiva (impresión en 3D).

Las tecnologías disruptivas pilares en la Industria 4.0 y en la ciberseguridad

The Boston Consulting Group, en el estudio⁹ citado anteriormente —publicado en abril de 2015—, identifica nueve áreas básicas (pilares del avance tecnológico) de la Industria 4.0.

Traducción de la figura original en sentido de las agujas del reloj

Robots autónomos.

Simulación.

Sistemas de integración horizontal y vertical.

Internet industrial de las cosas.

Ciberseguridad.

La nube (*Cloud*).

Fabricación aditiva (impresión 3D).

Realidad aumentada.

Big Data & Analytics.

El pie del recuadro.

Industria 4.0 es la visión de la producción industrial del futuro.

Fuente: BCG.

⁹ Michael Rüßmann, Markus Lorenz, Philipp Gerbert, Manuela Waldner, Jan Justus, Pascal Engel, y Michael Harnisch. The Boston Consulting Group. *Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries*. Capítulo 1. *The Nine Pillars of Technological Advancement*, 9 de abril de 2015.

https://www.bcgperspectives.com/content/articles/engineered_products_project_business_industry_40_future_productivity_growth_manufacturing_industries/#chapter1

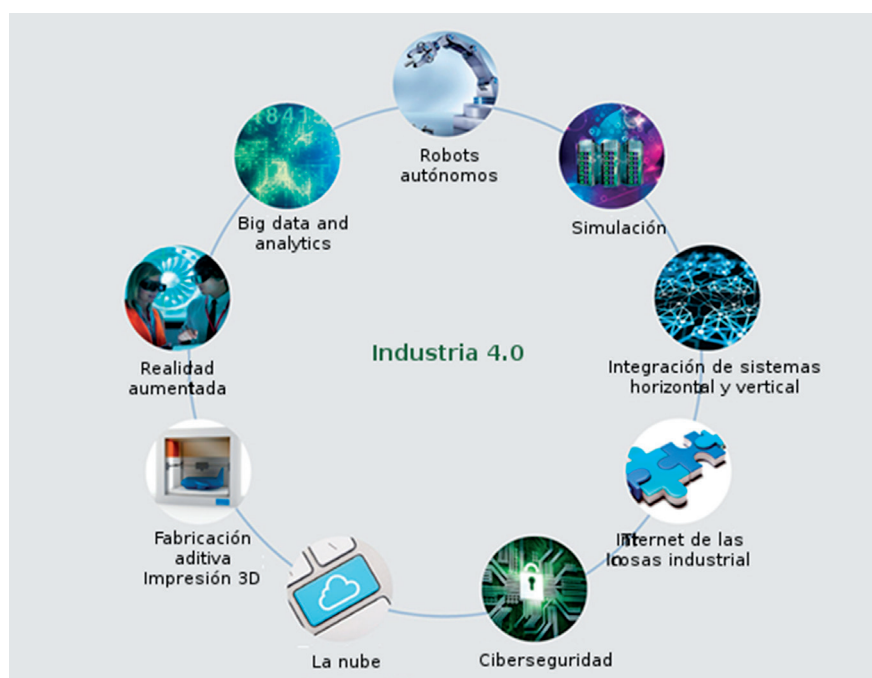


Figura 1.4. Nueve pilares del avance tecnológico en la Industria 4.0: la visión de la producción industrial del futuro. Fuente: The Boston Consulting Group.

La mayoría de estas nueve tecnologías ya se usan actualmente en las fábricas, sin embargo, es en la Industria 4.0 donde estas tecnologías transformarán la producción: células aisladas y optimizadas se unirán conjuntamente para formar flujos de producción totalmente integrados, automatizados y optimizados, lo que conllevará mayor eficiencia y un cambio en las relaciones tradicionales de producción entre distribuidores, productores y clientes, así como entre máquinas y humanos. Un extracto en traducción libre del estudio se describe a continuación.

«Muchas industrias han usado robots desde hace mucho tiempo para abordar tareas complejas, pero es ahora cuando los robots industriales están evolucionando para alcanzar una mayor utilidad. Cada vez son más autónomos, flexibles (colaborativos) y cooperativos, hasta tal punto que interactuarán con otros robots y trabajarán lado a lado con humanos de forma segura, aprendiendo de ellos. Estos robots costarán menos y tendrán más capacidades que los usados actualmente en la fabricación».

«En la fase de ingeniería ya se usan hoy día simulaciones 3D de productos, materiales y procesos de producción. Pero en el futuro las simulaciones se usarán también más extensivamente en operaciones de planta. Estas simulaciones explotarán datos en tiempo real que reflejarán el mundo físico en

un modelo virtual, el cual incluirá máquinas, productos y humanos. Esto permitirá a los operadores realizar pruebas y optimizar las configuraciones de las máquinas para el producto siguiente en la línea de producción virtual antes de cualquier cambio en el mundo físico, reduciendo así los tiempos de configuración de las máquinas y aumentando la calidad».

«La mayoría de los sistemas TI (tecnologías de la información) no están plenamente integrados actualmente. Las compañías, los distribuidores y los clientes no suelen estar estrechamente vinculados; tampoco los departamentos como los de ingeniería, producción o servicio. Las funciones desde la empresa hasta el nivel de planta no están totalmente integradas. Incluso el departamento de ingeniería en sí (producto-planta-automatización) carece de completa integración. Sin embargo, con la Industria 4.0 las compañías, los departamentos, las funciones y las capacidades estarán mucho más cohesionadas. Redes universales de integración de datos evolucionarán y permitirán cadenas de valor verdaderamente automatizadas».

«A día de hoy, solo algunos sensores y máquinas trabajan en red y hacen uso de computación empotrada (embebida). Típicamente están organizados en una pirámide de automatización vertical en la cual los sensores, los dispositivos de campo con inteligencia limitada y los controladores de automatización están gobernados por un sistema de control global. Con el Internet Industrial de las Cosas un mayor número de dispositivos (a veces, incluso productos no terminados) se enriquecerán de la computación empotrada y se conectarán a través de estándares tecnológicos. Esto permitirá a los dispositivos de campo comunicarse e interactuar, tanto con otros iguales a ellos como con controladores más centralizados, según sea necesario. También descentraliza el análisis y la toma de decisiones, lo que permitirá respuestas en tiempo real».

«Muchas compañías todavía dependen de sistemas de gestión y producción desconectados o cerrados, pero con la creciente conectividad y uso de protocolos de comunicación estándar que conlleva la Industria 4.0, la necesidad de proteger los sistemas industriales críticos y líneas de fabricación de las amenazas de ciberseguridad aumentan dramáticamente. Como resultado, son esenciales tanto comunicaciones seguras y fiables, como sofisticados sistemas de gestión de identidad y acceso de máquinas y usuarios».

«Las compañías ya usan *software* basado en la nube para algunas aplicaciones de empresa y de análisis, pero con la Industria 4.0 un mayor número de tareas relacionadas con la producción requerirán mayor intercambio de datos entre lugares y compañías. Al mismo tiempo, el rendimiento de las tecnologías en la nube mejorará, alcanzando tiempos de reacción de solo unos milisegundos. Como resultado, los datos y la funcionalidad de las máquinas irán poco a poco haciendo uso cada vez más de la computación en la nube, permitiendo más servicios basados en datos para los sistemas de producción. Incluso los sistemas de monitorización y control de procesos podrán estar basados en la nube».

«Las compañías acaban de empezar a adoptar la fabricación aditiva como, por ejemplo, la impresión 3D, la cual es usada, principalmente, para crear prototipos y producir componentes individuales. Con la Industria 4.0 estos métodos de fabricación aditiva serán ampliamente usados para producir pequeños lotes de productos personalizados que ofrecen ventajas de construcción, como son los diseños ligeros y complejos. Los sistemas de fabricación aditiva descentralizados, de alto rendimiento, reducirán las distancias de transporte y el *stock* de productos».

«Los sistemas basados en realidad aumentada soportan una gran variedad de servicios, como por ejemplo la selección de piezas en un almacén y el envío de instrucciones de reparación a través de dispositivos móviles. Estos sistemas se encuentran aún en sus primeros pasos, pero en el futuro las compañías harán un uso mucho más amplio de la realidad aumentada para proporcionar a los trabajadores información en tiempo real con el objetivo de mejorar la toma de decisiones y los procedimientos de trabajo. Por ejemplo, los trabajadores podrían recibir instrucciones de cómo sustituir una pieza en particular mientras están mirando el propio sistema bajo reparación a través de unas gafas de realidad aumentada, por ejemplo. Otra aplicación podría ser la formación de trabajadores de forma virtual».

«El análisis de grandes cantidades de datos ha surgido recientemente en el mundo industrial, permitiendo optimizar la calidad de la producción, ahorrar energía y mejorar el equipamiento. En la Industria 4.0, la obtención y exhaustiva evaluación de datos procedente de numerosas fuentes distintas (equipos y sistemas de producción, sistemas de gestión de clientes...) se convertirá en norma para el apoyo de toma de decisiones en tiempo real».

Tendencias en ciberseguridad: un primer avance (2015-2016)

El *Informe Anual de Seguridad Nacional 2015*¹⁰ del Gobierno de España, publicado por el Departamento de Seguridad Nacional en mayo de 2016, dedica la parte 3 de la sección «Ámbitos de la Seguridad Nacional» a la ciberseguridad (pp. 53-64). En este último informe se destaca «la importancia de la colaboración público-privada que resulta clave en un ámbito como la ciberseguridad». Asimismo, resalta la realización de varios eventos, entre ellos la realización en 2015 del Foro Nacional para la Confianza Digital dentro del enfoque de colaboración público-privada, con veintiuna instituciones participantes y otros eventos de gran impacto.

Otras iniciativas notables y muy destacadas en el citado *Informe Anual 2015* son:

¹⁰ <http://www.lamoncloa.gob.es/presidente/actividades/Paginas/2016/270516rajoycsn.aspx>
http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/Documents/INFORME_%20ANUAL_%20DE_%20SEGURIDAD_%20NACIONAL_%202015.pdf [consultados 30 de septiembre, 2016].

- Promoción de la capacitación de profesionales en ciberseguridad e impulso a la industria española a través de un Plan de I+D+i.
- Implantación de una cultura de ciberseguridad sólida.
- Intensificación de la colaboración internacional.

En el anterior *Informe Anual de Seguridad Nacional de 2014*¹¹, publicado el mes de abril de 2015 por el Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno, con la participación de otros organismos públicos, se incluyó por primera vez un apartado único sobre ciberseguridad (pp. 64-75). El Informe destaca cuatro tipos de ataques a los sistemas de información:

- El **ciberspionaje**: una de las mayores preocupaciones durante el año 2014 para los gobiernos occidentales.
- La **ciberdelincuencia**: durante 2013 los criminales han aumentado la frecuencia, variedad y amplitud de ataques a cambio de una recompensa.
- El **ciberterrorismo**: en sus dos vertientes, bien como instrumento facilitador de sus actividades, o bien como objeto de su acción para la comisión de actividades terroristas.
- El **hacktivismo**: aunque con menor representación, engloba aquellos ataques dirigidos por grupos movidos por una determinada ideología y que tienden a atacar la seguridad de los sistemas y la información.
- La **ciberguerra**, que engloba operaciones militares y aquellas otras orientadas a negar, modificar, llevar a engaño o destruir las capacidades propias residentes en los sistemas de información y telecomunicaciones que afecten a la defensa nacional.

Informe de seguridad de la información de Cisco

Entre los numerosos estudios de tendencias de ciberseguridad, citar los de Intel, Karspesky, Panda, McKinsey... aunque hemos decidido quedarnos con el de Cisco¹², publicado en agosto de 2015, en el que destaca las tendencias hacia fuentes de ciberinteligencia.

Analiza las principales tendencias de ciberseguridad durante la primera mitad del citado año y desvela cómo la evolución hacia el Internet de Todo (*Internet of Everything, IoE*) y la transformación digital están generando nuevos vectores de ataque y nuevas oportunidades de lucro para los cibercriminales.

Cisco señalaba en el estudio que: «restaurar la confianza en el año 2015 requerirá una mayor colaboración por parte de la industria y la creación de nuevos estándares para hacer frente a este panorama de amenazas y con mejores estrategias de seguridad que reduzcan el tiempo de detección, haciendo un mayor y mejor uso de todas las fuentes de ciberinteligencia. Sería necesario

¹¹ http://www.dsn.gob.es/sites/dsn/files/Informe_Seguridad_Nacional%202014.pdf

¹² Cisco, *Informe Semestral de Seguridad de Cisco 2015*, 6 de agosto de 2015.

llegar a un modelo donde la seguridad sea un elemento crítico desde el proceso mismo de diseño y desarrollo de cada dispositivo y de cada aplicación».

«Amenazas asociadas con Flash y explotadas por kits como Angler, la evolución de *ransomware* o campañas de *malware* mutante como Dridex requieren imperiosamente reducir los tiempos de detección. Estos se sitúan hoy entre los cien y doscientos días, según las estimaciones de la industria, frente a las cuarenta y seis horas —según Cisco— de media que ofrecen las soluciones de nueva generación, tales como Cisco Advanced Malware Protection (**AMP**) que incluye seguridad retrospectiva».

Recomendaciones de Cisco

La batalla entre cibercriminales y proveedores de seguridad —marcada principalmente por la rápida innovación en técnicas de ataque y defensa— se está acelerando, generando un mayor riesgo para empresas y usuarios. Los proveedores deben así centrarse en el diseño de soluciones de seguridad integradas que ayuden a las organizaciones a ser más proactivas y a establecer políticas alineadas con los usuarios, los procesos y la tecnología. Cisco ofrece algunas recomendaciones al respecto:

Defensa integrada. Las organizaciones demandan soluciones de seguridad integradas en lugar de puntuales, que permitan incluir la seguridad en todas partes y reforzarla en cualquier punto, desde el centro de datos (*data center*) hasta los terminales, las oficinas remotas y la nube (*Cloud*).

Servicios profesionales. La proliferación de amenazas avanzadas, dinámicas y persistentes, la creciente carencia de expertos en ciberseguridad y la fragmentación de la industria requiere que las organizaciones se apoyen en servicios profesionales efectivos.

Marco regulatorio global de ciberseguridad. Es necesario establecer un marco regulatorio global y cohesionado en el que participen múltiples Gobiernos y empresas para evitar problemas jurisdiccionales a la hora de hacer frente a las ciberamenazas, resolver los problemas geopolíticos y sostener el crecimiento económico.

Proveedores contrastados. Para que un proveedor tecnológico pueda considerarse contrastado y fiable debe integrar la seguridad desde el principio, en todas sus soluciones y a través de todo su ciclo de vida, desde el proceso de desarrollo y test hasta la cadena de suministro y soporte.

Los ciberriesgos

Las amenazas (ciberamenazas o ciberriesgos) son cada vez más frecuentes y avanzadas, por lo que gestionar una crisis cibernética es algo más que probable: los ataques de denegación de servicio distribuidos (**DDoS**), el robo

de credenciales mediante técnicas de *phishing* o *malware*, la fuga masiva de información digital, el *ransomware*¹³ (programas que impiden el acceso a la información mediante técnicas de cifrado, pidiendo un rescate para el descifrado) o las amenazas avanzadas persistentes (*APT, Advanced Persistent Threats*).

Los *hackers*, sin ninguna duda, nunca descansan. Uno muy sonado realizado en agosto de 2015 fue el robo de datos de clientes de la página web de contactos Ashley Madison, que durante las siguientes semanas trajo de cabeza no solo a la compañía, sino también a sus 37 millones de usuarios.

La web profunda, la web invisible (Deep Web)

Existe una creciente dificultad para detectar y erradicar las redes de robots (*botnets*) que se siguen utilizando para la diseminación de *spam*, para la ejecución de ataques *DDoS*, *spear-phishing*, *click-fraud*, *keylogging*, así como la difusión de *ransomware* o la sustracción de dinero digital. Los datos de 2014 señalaban, por aquel entonces, un descenso en el número de *botnets* detectadas, aunque no su eficacia y su peligrosidad. De hecho, los atacantes ahora utilizan la red **TOR** para ocultar *botnets* y/o servidores de mando y control (C & C), lo que dificulta enormemente su detección y erradicación [CCN-CERT 2015, 14-15]. Recordemos que el CCN-CERT define *TOR*¹⁴ como:

«**TOR** (abreviatura de *The Onion Router*) es un software diseñado para permitir el acceso anónimo a internet. Aunque durante muchos años ha sido utilizado principalmente por expertos y aficionados, el uso de la red **TOR** se ha disparado en los últimos tiempos, debido principalmente a los problemas de privacidad de internet. Correlativamente, **TOR** se ha convertido en una herramienta muy útil para aquellos que, por cualquier razón, legal o ilegal, no desean estar sometidos a vigilancia o no desean revelar información confidencial».

La razón de todo ello podemos encontrarla en la cada vez mayor sencillez para desarrollar ataques *DDoS* y la facilidad para acceder a determinadas herramientas (adquiridas en el mercado negro de la *hidden-wiki*¹⁵, por ejemplo).

¹³ Véase Informe «Ciberamenazas 2014. Tendencias 2015» del CCN-CERT IA-09/15.

¹⁴ CCN-CERT IA-09/15. *Ciberamenazas 2014. Tendencias 2015*. Resumen ejecutivo, p. 15. <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/795-ccn-cert-resumen-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html>

¹⁵ Es una enciclopedia que se encuentra alojada en la web oculta (*Hidden web* llamada también *invisible web* o *deep web*) y funciona como índice para acceder a páginas de dominio (.onion) que indica una dirección IP anónima accesible por medio de la red **TOR** (*The Onion Route*) (CCN-CERT 2015, p. 15).

La necesidad de un seguro de ciberriesgos en la empresa

Los ciberriesgos han dejado de ser una amenaza esporádica para las empresas y se constituyen ya como un problema importante en todos los sectores. La Administración, la banca, organizaciones y empresas de todo tipo, la industria, deben estar alertas ante su peligrosidad. El Instituto Nacional de Ciberseguridad (INCIBE) publicó un informe a finales de septiembre de 2015¹⁶ donde alertaba de un importante aumento de ciberataques durante ese año y, en concreto, cincuenta y dos ciberataques a infraestructuras críticas y servicios básicos del país, la mitad dirigidos a operadores de suministro eléctrico; en cuanto a ataques contra empresas, el INCIBE advierte que se han doblado en 2016, hasta llegar a los 36.000 en el mes de agosto de ese año.

Por estas razones, los ciberriesgos han pasado a ser uno de los principales focos de atención de los gerentes de riesgos de las empresas, de cualquier tamaño y sector. Ello ha obligado al «estudio y posible implantación de un seguro de ciberriesgos» al igual que cualesquiera otros riesgos relevantes en las empresas y en cualquier industria.

Un informe de Allianz Global¹⁷ sobre ciberseguridad, dado a conocer el 8 de septiembre de 2015, señalaba que las primas mundiales de seguros cibernéticos superarán los 20.000 millones de dólares en la próxima década frente a los 2.000 millones que captan en la actualidad. El aumento de este negocio se producirá por una mayor concienciación sobre estos riesgos y por los cambios normativos que propician la contratación de esta cobertura asegurada por parte de las empresas, señala el citado estudio. «En la actualidad menos del 10 % de las empresas suscriben una póliza para cubrirse de los riesgos cibernéticos». La «ciberdelincuencia» cuesta 445.000 millones de dólares anuales a la economía mundial y la mitad de este importe recae en las diez principales economías mundiales (Estados Unidos con 108.000 millones lidera la clasificación, seguida de China con 60.000 millones y Alemania con 59.000 millones).

Los expertos recomiendan a las compañías que, además de ser innovadoras en tecnología y atención al cliente, deberían hacer una inversión especial en ciberseguridad, tanto en protección como en la respuesta a los ataques de los *hackers*, ya que los datos que manejan a diario son un material sensible por contener información personal de sus clientes.

¹⁶ Anuncio realizado en León el 24 de septiembre de 2015, por el Instituto Nacional de Ciberseguridad (INCIBE), a través del CERT de Seguridad e Industria. Véase *La Vanguardia*: <http://www.lavanguardia.com/tecnologia/20150924/54436823384/espana-ha-sufrido-52-ciberataques-a-infraestructuras-criticas-en-2015.html>

¹⁷ Citado por Marimar Jiménez en «El negocio de la ciberseguridad se dispara ante las nuevas amenazas», *Cinco Días*, 30 de noviembre de 2015 [en línea]. http://cincodias.com/cincodias/2015/11/29/tecnologia/1448814144_530160.html

«Los usuarios deben estar seguros y tranquilos con los datos personales que ceden a las empresas. Con la revolución tecnológica existe el “ciberriesgo”, pero para responder a estos ataques nos reinventamos constantemente para crear barreras de contención», afirmaba un directivo de Axa en un foro empresarial, organizado por el periódico *Expansión*¹⁸ y la consultora Cap Gemini.

La ciberseguridad en la empresa y la empresa ante la ciberseguridad

La naturaleza de los ciberriesgos existentes requiere la definición de una estrategia en materia de seguridad, alineada con los objetivos de la empresa. ¿Cómo definir esta estrategia? Para ello será necesario determinar cuál es el punto de partida de la empresa, en qué situación se encuentra en ese momento en materia de seguridad y cuál debería ser el nivel de seguridad de la organización, en función de una serie de factores, como el sector de negocio al que pertenecemos, los objetivos estratégicos o los requisitos que define el mercado, entre otros. El camino entre nuestro punto de partida y nuestro objetivo de seguridad determinarán cuál es nuestra hoja de ruta hacia la ciberseguridad.

Para ayudar a definir la hoja de ruta de su empresa, INCIBE ha creado el decálogo hacia la ciberseguridad: un conjunto de diez pasos orientados a mejorar el nivel de seguridad de su empresa y, por tanto, proteger su negocio. El *Decálogo de Ciberseguridad*¹⁹ es el siguiente:

1. Analizar los riesgos.
2. Los responsables de seguridad.
3. Seguridad en el proyecto de trabajo.
4. La protección de la información.
5. Movilidad con seguridad.
6. Protección *antimalware*.
7. Actualización y parcheo.
8. La seguridad de la red.
9. Monitorización.
10. Seguridad gestionada.

Como casos de estudio a considerar queremos destacar el caso de Bankia²⁰, que en septiembre de 2015 creó un «Comité de respuesta a incidentes de ciberseguridad» y otro «Comité de gestión del fraude tecnológico».

¹⁸ Carmen Alaba, 14 de septiembre de 2015. www.expansion.com/empresas/banca/2015/06/22

¹⁹ INCIBE. «*Decálogo de Ciberseguridad: «El camino hacia la ciberseguridad en su empresa. Diez pasos para garantizar la ciberseguridad en su empresa»*». 2015. <https://www.incibe.es/protege-tu-empresa/blog/decalogo-ciberseguridad-empresas>, 30 de octubre de 2014 [consultado, 1 de septiembre de 2016].

²⁰ Junta general de accionistas 2015 de Bankia. *Expansión*, 22 de septiembre de 2015.

También, y por seguir con el sector bancario y en este caso a nivel europeo, mencionar al Banco Central Europeo (BCE) que en el *Informe de Estabilidad Financiera*, publicado en 2015, advirtió de que el riesgo de ciberataques es creciente dado que las amenazas cada vez son más complejas e intensas y recomendaba a las ciento veintitrés principales entidades de la Eurozona bajo su vigilancia, activar medidas de seguridad contra el cibercrimen e instaba a dichas entidades a revisar los sistemas y protocolos de protección frente a los ciberataques para impedirlos y garantizar así la continuidad del negocio y el buen servicio a los clientes.

El negocio de la ciberseguridad

Como muestra del negocio que ofrece la ciberseguridad, en España, Telefónica ha alcanzado ya un volumen de negocio global en el ámbito de la ciberseguridad de 400 millones de euros²¹. Solo en España las ventas de productos y servicios de Telefónica a empresas superan los 100 millones con un crecimiento anual del 30 %.

A nivel global, un informe publicado a mediados de septiembre de 2015 por la consultora Gartner evaluaba en 75.000 millones de dólares la cifra que gastarán las organizaciones de todo el mundo en materia de ciberseguridad durante ese año 2015.

La ciberseguridad en la industria eléctrica: necesidad de estándares

La industria eléctrica, según INCIBE, requerirá como infraestructura crítica:

- Identificar y conocer los conceptos de ciberseguridad en Sistemas de Control Industrial y Protección de Infraestructuras Críticas, sus definiciones y relaciones.
- Descubrir y analizar el estado del arte de la Protección de Infraestructuras Críticas a nivel internacional.
- Detectar y analizar la situación actual de la seguridad en el sector industrial y las amenazas y vulnerabilidades de los Sistemas de Control Industrial reconociendo su riesgo asociado.

Y además será necesario identificar, describir y adoptar marcos y estándares aplicables en estos entornos: **ISA/IEC 62443, ISO 27001, BS 25999, NIST SP 800-82**, etcétera; establecer, implementar y adoptar un *Programa de Seguridad de los Sistemas de Control Industrial* y *Diseñar un Plan de Seguridad y Protección de la Infraestructura Crítica*.

²¹ Santiago Millán. «Telefónica supera los 400 millones de dólares en su negocio global de ciberseguridad», *Cinco Días*, 9 de octubre de 2015, p. 6.

De un modo sectorial las redes inteligentes (*Smart Grid*), fiel reflejo de la fábrica inteligente y estandarte de la Industria 4.0, unido a las nuevas normativas legales y a la creciente implantación de los contadores inteligentes junto con la infinidad de objetos inteligentes que utilizan, inundarán las infraestructuras críticas del suministro eléctrico y conducirán, sin ninguna duda, a la necesidad de actualización de las estrategias de ciberseguridad existentes para hacerlas más fiables y eficientes y que deberán desplegar las operadoras eléctricas.

Para afrontar con las debidas garantías de éxito las estrategias de ciberseguridad en las redes inteligentes se requiere del uso de estándares de obligado cumplimiento por las operadoras eléctricas (INCIBE 2015) y deberán implementar estos estándares tanto en los dispositivos como en el proceso. Los estándares que nuestras operadoras, nos consta, ya utilizan, y aprobados por el organismo de estandarización CENELEC/ETSI, son los siguientes²²:

- *Estándares específicos del sector eléctrico.* Se desarrollan para asegurar los mecanismos eléctricos en términos de seguridad lógica y ciberseguridad: estándares **ISO/IEC TR 27019:2013** y el estándar clásico de seguridad de la información **ISO 27002**.
A estos estándares que recomienda INCIBE consideramos sería preciso añadir el cumplimiento del estándar **ISO/IEC 27032** «para la ciberseguridad» con el que la organización ISO pretende garantizar la seguridad en los intercambios de información en la Red que puede ayudar a combatir el cibercrimen con cooperación y coordinación, así como luchar contra ataques de ingeniería social, *hackers*, *malware*, *spyware* y otros tipos de *software* no deseado.
- *Estándares de seguridad lógica provenientes del campo de las TIC.* Pueden servir (total o parcialmente) para guiar la seguridad de las redes inteligentes. Estándar **ISO/IEC 15408**.
- *Estándares provenientes del campo de automatización industrial.* En general y sin excepciones es el campo de la ciberseguridad. Son más cercanos a la operativa real de las redes inteligentes al proyecto del sector industrial. Estándar **ISA/IEC 62443**.

Otros temas importantes a considerar por las empresas: la monitorización de los Centros de Datos (*Data Centers*), la reciente Ley de Protección de Infraestructuras Críticas, la ciberseguridad en el sector eléctrico, el papel de la ética y de la situación de la industria de la seguridad informática en diferentes regiones geográficas del planeta.

²² INCIBE (2015). *Estándares de ciberseguridad en las redes inteligentes*, 3 de septiembre de 2015. https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Estandares_ciberseguridad_redes_inteligentes

Las operadoras eléctricas disponen de Sistemas de Gestión de la Ciberseguridad Industrial (**SGCI**) que contemplan los riesgos relacionados con la ciberseguridad que se han de centrar en la indisponibilidad de los sistemas y en el acceso indebido a determinadas aplicaciones así como la gestión de:

- *Firewalls* y sistemas antintrusión.
- Sistemas antivirus.
- Mejora del sistema de seguridad de los requisitos de acceso.
- Mecanismos de detección de incidencias.
- Actualización de *software*.
- Simulacros de ataques.
- ...

La ciberseguridad en la banca y en el sector financiero (tecnologías financieras de impacto)

El informe «Financial Services Technnnology 2020 and Beyond: Embracing disruption», elaborado por la consultora PwC²³ y publicado en julio de 2016, analiza las grandes tendencias relacionadas con la tecnología que van a transformar el sector financiero en los próximos cuatro años y que, por consiguiente, tendrán gran impacto en la ciberseguridad de la información en este campo:

«FinTech, la economía colaborativa; Blockchain, la inteligencia artificial y la robótica; la nube; la ciberseguridad; el empuje de Asia como centro tecnológico y de innovación; la inteligencia de cliente; la tecnología aplicada en el ámbito de la regulación y la digitalización de todos los procesos y actividades»²⁴.

En lo relativo a la ciberseguridad, el informe destaca que: «la ciberseguridad ya es una de las principales preocupaciones de los máximos ejecutivos de las entidades financieras y esa situación no hará sino continuar en los próximos años como consecuencia, entre otros factores, del rápido crecimiento del Internet de las Cosas, especialmente las áreas de pagos, seguros y banca comercial» (Nacenta, 2016)²⁵. Sin embargo, son las otras dos tecnologías, **fintech** y **blockchain**, esencialmente «financieras», a las que dedicaremos nuestra atención, reiterando, claro está, el impacto que prevé el informe de la nube, la robótica y la inteligencia artificial, que trataremos en otro momento en este capítulo.

²³ <http://www.pwc.es/es/publicaciones/tecnologia/assets/informe-financial-services-technology%202020.pdf>

²⁴ Nota de prensa, de la filial española, elaborada por Salvador Nacenta, socio del Sector Financiero de PwC: <http://www.pwc.es/es/sala-prensa/notas-prensa/2016/informe-financial-services-technology-2020.html>.

²⁵ *Ibíd.*

Tecnologías y empresas Fintech

Fintech, contracción de las palabras *Finance* y *Technology*, aglutina y define a todas aquellas empresas que se sirven de las últimas novedades tecnológicas para brindar productos y servicios financieros innovadores, incluyendo aquellos que facilitan la vida cotidiana gracias a la disrupción tecnológica, englobando prestaciones como: la banca digital, los créditos y pagos *online* o el cambio de divisas a través de la Red. De información extraída —esencialmente de la prensa económica y los portales de los grandes bancos españoles, BBVA y Santander, entre otros— las empresas Fintech aglutinan a todas aquellas que desarrollan y ofrecen servicios financieros que utilizan la última tecnología existente para poder ofrecer productos innovadores. Así aparecen los nuevos productos financieros basados en innovación tecnológica tales como: negociación de mercados, financiación colectiva, desarrollo de sistemas de seguridad financiera, asesoramiento en línea, dinero digital, criptomonedas, monederos digitales (*wallets*), etcétera. Estas empresas y tecnologías asociadas implicarán políticas de seguridad de la información (ciberseguridad) en el ámbito de las instituciones financieras, retos normativos y técnicos de la seguridad, de cooperación internacional, de protección de datos, etcétera.

Una definición más académica, del IEBS, considera que: *Fintech* es un concepto que aglutina a aquellas empresas financieras tecnológicas que tratan de aportar nuevas ideas y que reformulan, gracias a las nuevas tecnologías de la información, las aplicaciones móviles o el *Big Data*, la forma de entender y prestar los servicios financieros. Las *Fintech* producen y producirán una transformación radical del sector financiero (IEBS, 2016)²⁶. La escuela de negocios IEBS enumera un gran número de áreas y sectores sobre los que actuará IEBS (de ahí, los retos y oportunidades que supondrán las *fintech* y los riesgos y necesidad de políticas claras y eficaces en ciberseguridad en las empresas y en la banca que adopten dichas tecnologías):

- Banca móvil.
- *Big Data* y modelos predictivos.
- *Crowdfunding* y *crowdlending*.
- Criptomonedas y monedas alternativas.
- Mercado de divisas.
- Gestión automatizada de procesos y digitalización.
- Gestión de riesgos.
- Pagos y transferencias.
- Préstamos P2P.
- Seguros.

²⁶ Raúl Jaime Maestre. *¿Qué es el Fintech, definición, sectores y ejemplos de startups?* <http://comunidad.iebschool.com/iebs/finanzas-2-0-y-control/que-es-fintech/>. Diciembre de 2015.

- Seguridad y privacidad.
- Servicios de asesoramiento financiero.
- *Trading*.
- ...

Blockchain

El *World Economic Forum*, en el informe publicado en junio de 2016 relativo a las «10 tecnologías emergentes de 2016»²⁷, en colaboración con la prestigiosa revista *Scientific American*, destaca de modo muy especial las tecnologías *blockchain*. ¿Qué es *blockchain*? Es una tecnología de transferencia de información, soporte de las monedas digitales, en particular del *bitcoin*. Técnicamente *blockchain* (cadena de bloques) es una base de datos descentralizada donde las transacciones electrónicas se registran de forma segura y verificada. La cadena de bloques conforma una gigantesca base de datos abierta al público y a través de la cual se envía información de un emisor a un receptor. Por el camino los datos de ese intercambio se verifican por distintos actores independientes conectados a la misma red, que otorgan veracidad a esta transmisión. Al decir de grandes expertos, la futura economía mundial se basará en transacciones en cadenas de bloques y las organizaciones de terceros pueden no ser necesarias.

El *blockchain*, asociado a *bitcoin*, es público aunque las personas que intervienen en la base de datos son anónimas a ojos del usuario. De hecho, la historia del término considera que esta tecnología de transferencia de información nació para posibilitar la aparición del *bitcoin*.

¿Por qué su impacto en la economía mundial y en la economía de la ciberseguridad? Visa, Microsoft, Accenture, la banca (en España, una iniciativa liderada por el Banco de Santander)... se están subiendo al carro de este protocolo de transferencia segura de datos. Algunos bancos comienzan a utilizarlo como alternativa a su sistema propio *SWIFT*. Grandes empresas tecnológicas como IBM²⁸ cuentan también con su propio sistema de *blockchain*; Microsoft, a mediados de septiembre de 2016, ha lanzado su proyecto de *blockchain*: *Microsoft's Bletchley Blockchain Project*²⁹.

El Banco de Santander, según noticias de *El Confidencial*³⁰, estima que la adopción de esta tecnología le permitirá ahorrar alrededor de 20.000 millo-

²⁷ weforum.org/es/agenda/2016/06/las-10-tecnologias-emergentes-de-2016

²⁸ Sitio de *blockchain* de IBM: www.ibm.com/blockchain

²⁹ Christine Avanesians Senior Program Manager, Microsoft Azure. 20 de septiembre de 2016. <https://azure.microsoft.com/en-us/blog/project-bletchley-blockchain-infrastructure-made-easy/>.

³⁰ Jaume Esteve. «Avalancha Blockchain: la tecnología que está reinventando el negocio de la banca». *El Confidencial*, 22 de septiembre de 2016. http://www.elconfidencial.com/tecnologia/2016-09-22/blockchain-fintech-banca-online_1263534/

nes de dólares al año. El propio Banco de Santander está promoviendo el uso de dinero digital entre bancos utilizando la tecnología.

El diario *Expansión*³¹, en un detallado artículo, explica cómo el Grupo del Santander se ha aliado con UBS, BNY Mellon, Deutsche Bank, el operador de mercado ICAP y la *start-up* Clearmatics para desarrollar la moneda digital *Utility Settlement Com (USC)*. Se trata de un sistema que utiliza la tecnología *blockchain* para facilitar los pagos y liquidaciones de forma eficiente, rápida y segura. La tecnología *blockchain*, sobre la que se basan criptomonedas como el *bitcoin*, permite la «transaccionalidad» de activos reales como euros o dólares. Así, un USC sería una «moneda» que existe en un registro contable distribuido, es decir, en un *blockchain*.

La nueva divisa digital podría ponerse en funcionamiento a comienzos de 2018. Según las fuentes de *Expansión* se considera que «además de mejorar los servicios para los clientes, Santander estima que el uso de esta nueva divisa digital genera al sector un ahorro de costes de 20.000 millones de dólares (cerca de 17.750 millones de euros), según se incluye en *The Fintech 2.0 Paper*, un estudio realizado por el propio Santander con Oliver Wyman»³².

La ciberseguridad y la inteligencia artificial

La inteligencia artificial desde el advenimiento de *Big Data* está llegando a numerosos sectores que hasta hace unos años prácticamente era impredecible y que en la actualidad están impactando en la ciberseguridad de las organizaciones y empresas.

El conocimiento en la inteligencia artificial integrada con *Big Data* está ayudando y ayudará a los delitos informáticos. Una nueva generación de plataformas de negocio está surgiendo en la convergencia del **aprendizaje automático** (*machine learning*) —recientemente el **aprendizaje profundo** (*deep learning*)— y *Big Data* que generarán un gran cambio en materia de ciberseguridad. Los algoritmos de aprendizaje automático y la ciberinteligencia asociada están potenciando las predicciones de ataques cibernéticos que mejorarán las tasas de detección y pueden ser la clave para revertir la tendencia actual en cuanto a crecimiento de delitos cibernéticos y potenciar la ciberseguridad.

³¹ *Expansión*, «Santander promueve el uso de dinero digital entre bancos», 26 de julio de 2016. <http://www.expansion.com/empresas/banca/2016/08/26/57bf44d8e5fdea8b4c-8b464a.html>. El artículo, además de comentar todo el proyecto, incluye una ilustración muy significativa del funcionamiento del *blockchain* como sistema de pago.

³² *The Fintech 2.0 Paper: rebooting financial services*. <http://santanderinnovations.com/fintech2/>

IBM Watson

IBM decidió hace varios años cambiar su modelo de negocio principal y centrarse en las tecnologías cognitivas a través de su supercomputador *Watson*, la referencia central del fabricante.

Watson se hizo famoso al competir en 2011 en un famoso concurso de televisión estadounidense de preguntas, «Jeopardy!», al derrotar a sus dos oponentes humanos, como ya lo hiciera en el año 1977 el supercomputador *DeepBlue* que ganó a Gary Kasparov —campeón mundial— jugando al ajedrez.

IBM Watson es el primer sistema cognitivo diseñado de forma que los computadores no se programan sino que son capaces de entender el lenguaje natural de las personas y aprender. Se ha convertido, desde aquel año 2011, en una tecnología comercial accesible a través de la nube y que cuenta con clientes en numerosos sectores y países del mundo, entre ellos España, donde, gracias a la colaboración con CaixaBank ha aprendido, además de técnicas financieras, el lenguaje español.

IBM Watson es un sistema informático de inteligencia artificial diseñado para realizar labores de computación cognitiva (entre ellas el procesamiento de lenguajes naturales y el razonamiento y el aprendizaje automático), desarrollado sobre la tecnología DeepQA de IBM. Una plataforma tecnológica que utiliza el procesamiento del lenguaje natural y el aprendizaje automático para analizar y revelar información clave de las grandes cantidades de datos no estructurados.

En la práctica *Watson* analiza datos no estructurados (artículos, reportes de investigación, datos empresariales, datos de redes sociales, datos de sensores...) utilizando procesos de lenguaje natural para entender la gramática y el contexto, entiende preguntas complejas —evaluando los posibles significados y determinando qué es lo que se está preguntando—, contesta a la preguntas más exigentes de sus clientes, extrae —casi en tiempo real— información clave de documentos y descubre y presenta información, patrones y relaciones entre datos. *Watson* aprende sobre un nuevo tema antes de contestar preguntas relacionadas. Utiliza algoritmos de aprendizaje automático investigando en grandes volúmenes de datos (*Big Data*) para encontrar las muchas respuestas posibles.

Watson se utiliza hoy día en un gran número de aplicaciones en todo tipo de sectores, desde empresariales e industriales hasta la Administración, la universidad y la investigación. Las más recientes inauguraciones relacionadas con *IBM Watson* ha sido el Centro de *IBM Watson* para Internet de las Cosas³³

³³ El centro inaugurado por IBM, según el propio IBM, es su mayor inversión en Europa en las dos últimas décadas. Contará con mil expertos en Internet de las Cosas y en Industria 4.0. Integrará las tecnologías cognitivas de IBM con *IoT*, Industria 4.0 en la nube de IBM a través de la plataforma *IBM Watson IoT Cloud* [en línea: <https://www-03.ibm.com/press/es/es/pressrelease/48491.wss>].

—un centro de referencia mundial con sede en Múnich (Alemania), inaugurado el 15 de diciembre de 2015— y la plataforma expresa para ciberseguridad inaugurada a finales de mayo de 2016 y disponible comercialmente que comentamos a continuación.

Watson for Cyber Security

IBM Security³⁴ anunció en mayo de 2016 que va a dedicar a la ciberseguridad una nueva versión basada en la nube (*Cloud*) de la tecnología cognitiva de la empresa, entrenada en el lenguaje de seguridad como parte de un proyecto de investigación a largo plazo. *Watson* va a ser entrenado con la ayuda de varias universidades estadounidenses en el lenguaje de la ciberseguridad. IBM pretende optimizar las capacidades de los analistas en seguridad utilizando sistemas cognitivos que automaticen la búsqueda de conexiones entre los datos, las amenazas emergentes y las distintas estrategias de protección. IBM ha denominado a este nuevo modelo de seguridad como «seguridad cognitiva» que generará hipótesis, razonamientos basados en evidencias y recomendaciones para mejorar la toma de decisiones en tiempo real.

Plataforma de Ciber-Inteligencia de Accenture

La consultora Accenture, una de las «cuatro grandes» (*big four*) compañías a nivel mundial (junto con PwC, KPMG y EY) lanzó a primeros de marzo de 2016 una «plataforma de Ciber-Inteligencia»³⁵ que hace uso de los avances en tecnología y permite identificar ciberamenazas en tiempo real, monitorizando en tiempo real comportamientos sospechosos.

Según Accenture es la primera solución del mercado que combina servicios de seguridad gestionada, inteligencia artificial, *cloud* y *analytics*; es una plataforma que permite a la compañía identificar amenazas en tiempo real. «Hace uso de los avances en tecnología de procesadores (chips) con una combinación patentada de inteligencia artificial, aprendizaje automático y análisis de datos constante que permite a las organizaciones identificar ciberamenazas en tiempo real. La plataforma examina la actividad en las redes para aprender, determinar y reportar comportamientos sospechosos atribuibles a ciberataques»³⁶. Es de resaltar, según Accenture, que la plataforma se puede implementar en una semana y una vez instalada la plataforma empieza a aprender «automáticamente» —lo que es normal— y ella misma mejorará continuamente.

³⁴ www-03.ibm.com/press/us/en/pressrelease/49683.wss#feeds

³⁵ www.accenture.com/es-es/company-news-release-new-cybersecurity-platform

³⁶ *Ibíd.*

Robótica y ciberseguridad: *cobots, bots y chatbots*

El informe del *World Economic Forum* (WEF), «The future of Jobs and Skills» presentando en Davos en enero de 2016, y que ha tenido una gran repercusión mundial, predecía para los próximos años la desaparición de 7,1 millones de empleos debido a la implantación de las tecnologías disruptivas que traería la cuarta revolución industrial y, especialmente, la robótica unida a la inteligencia artificial, *Big Data* y el Internet de las Cosas. Por suerte, también consideraba la creación en el mismo periodo de 2 millones de empleos que traerían las nuevas profesiones y oficios para cubrir los nuevos puestos de trabajo derivados de las mismas tecnologías.

En este apartado queremos destacar, por su innegable presencia en la ciberseguridad —y su impacto fundamental en la privacidad y protección de datos—, a los nuevos modelos de robots colaborativos (*cobots*), así como los robots virtuales o asistentes virtuales (*bots* y *chatbots*).

Robots colaborativos (cobots)

Una nueva generación de robots está llegando a las fábricas y cadenas de producción, así como a muchos otros sectores como el turismo, la medicina, los centros comerciales o los aeropuertos, son los robots colaborativos que, a su vez, están originando una nueva tendencia en ingeniería: la **cobótica**.

Los robots colaborativos (*cobots*) son una nueva generación de robots, que aprovechando la integración de la inteligencia artificial y el inmenso caudal de datos que proporcionan los *Big Data* y el Internet de las Cosas, se están integrando con los humanos³⁷, permitiendo trabajar de una manera estrecha a robots y personas humanas, sin restricciones de seguridad como las requeridas en aplicaciones típicas de robótica industrial. Los *cobots* son unas nuevas generaciones de robots que están llegando a las fábricas y otros sectores de la industria y la empresa para colaborar de forma segura con los trabajadores gracias a los avances ya citados y además las tecnologías visuales —realidad virtual y realidad aumentada— y la innumerable presencia de los sensores.

Los robots colaborativos están diseñados para trabajar con seguridad e interactuar con los humanos en una fábrica, un taller, un hotel... haciendo que los trabajadores sean más productivos ya que ayudan a reducir algunas o muchas de las tareas repetitivas que hacen esos trabajadores a lo largo de su jornada laboral.

Los *cobots* están permitiendo el nacimiento de una nueva era en la automatización industrial y en las cadenas de producción. Los robots colaborativos,

³⁷ También se les suele conocer en algunos ámbitos académicos e industriales como «robots humanoides».

al decir de los grandes expertos en robotización y cobotización, compiten con los robots industriales por la sencillez, flexibilidad y facilidad de programación. Se verán cada vez más en los procesos de producción y en sectores diferentes a los procesos industriales.

Un caso de estudio muy implantado es el sector de la hostelería y el turismo. Hosteltur —la organización profesional de turismo— en su revista oficial³⁸ (el número de julio-agosto de 2016) describe varias aplicaciones prácticas ya en funcionamiento que están trabajando en el diseño de robots sociales para ferias, museos y hoteles. Algunas de ellas son las siguientes:

«Incorporación de robots a la plantilla de nuevos hoteles. 1. El hotel “Ghent Marriot”, en Bélgica, cuenta desde finales de 2015 con *Mario*, un robot que ayuda a los recepcionistas a efectuar el *check-in*, habla diecinueve idiomas e incluso entretiene a los clientes con sus bailes». Cita la revista un caso excepcional: el hotel “Henn-na”, situado en Nagasaki, «es el primero del mundo en atender a sus clientes exclusivamente con robots. Cuenta con dos robots en recepción, dos en conserjería, uno en cada habitación que realiza las tareas usuales del servicio añadiendo pronósticos del tiempo, turismo y varios robots para transportar equipaje».

Los asistentes virtuales: bots y chatbots

Un **bot** (también llamado asistente virtual personal) es un programa informático basado en inteligencia artificial que imita el comportamiento humano para realizar diferentes tareas o funciones por su cuenta y sin la ayuda de un ser humano. El *bot* es capaz de comunicarse con los seres humanos (a través de texto, voz, emociones...) manteniendo una conversación con una persona utilizando el lenguaje natural en dicha conversación. Un **chatbot** (*chatter bot*) o *bot conversacional* es el modelo de *bot* más popular, capaz de simular una conversación con una persona y se ha integrado en las aplicaciones de mensajería, tipo *chat*.

Los asistentes virtuales más populares son: *Siri* de Apple (para sistemas operativos iOS y Mac) es el más conocido, dado que también es uno de los más populares desde su incorporación a los teléfonos móviles iPhone; *Cortana* de Microsoft incorporado al sistema operativo Windows 10 y *Google Now* para el sistema operativo móvil Android. Sin embargo, muchos de los grandes fabricantes de computación, tanto de *hardware* como de *software*, así como empresas pequeñas innovadoras, están creando plataformas comerciales de *bots* a las que empresas clientes o particulares pueden conectarse y también desarrollar sus propios asistentes virtuales. Estos son los casos

³⁸ Xavier Canalis *et al.* «La próxima revolución del turismo. Los robots toman el mando». Madrid: Hosteltur, julio-agosto de 2016, pp. 7-19 [en línea: www.hosteltur.com/edicion-impresa/robots-y-turismo-la-proxima-revolucion] [consultada 24 de septiembre de 2016].

del ya mencionado *Watson* de IBM, Amazon con su plataforma *Echo* y asistente virtual *Alexa*, Google que ha convertido su *Google Now* en una nueva plataforma denominada *Google Assistant*, *Facebook Messenger* con su plataforma *M* para *bots* presentada en abril de 2016 que facilitará las *API* (*Application Programming Interface*, interfaz de programación de aplicaciones) para el desarrollo de sus propios *chatbots* por empresas y particulares que los podrán integrar en su propia red social. Samsung ha comprado en 2016 el asistente virtual *Viv* y tiene el proyecto de incluirlo en todos sus productos (aparatos de televisión, teléfonos...). Además de estas plataformas de las grandes empresas de computación, han nacido empresas que han creado sus propias plataformas de *bots* y que tienen también cientos de millones de usuarios, como es el caso de *Kik* y *Slack*, diseñadas especialmente para clientes empresariales y profesionales.

Aplicaciones de los bots

Algunas aplicaciones de asistentes citados anteriormente son:

El asistente virtual *Cortana* de Microsoft, *Siri* de Apple o *Alexa* de Amazon con su altavoz *Echo* —por citar algunos ejemplos— pueden actuar como agentes inteligentes y son capaces de interactuar con *bots* para la ejecución de aplicaciones de comercio electrónico o soluciones de atención al cliente, bien con programas de gestión de relaciones con los clientes (CRM) o con *call centers*.

WeChat —una aplicación de mensajería instantánea muy popular— ha desarrollado sus propios *bots* que permiten, por ejemplo, realizar reservas de hotel, confirmar citas médicas o comprar entradas para el cine a través de mensajes de texto que son interpretados por *bots*.

Google Assistant apoyado por el servicio de mensajería **Allo**, lanzado en septiembre de 2016 y basado en aprendizaje profundo (*deep learning*), pretende dar respuestas predictivas de modo instantáneo y tiene la capacidad de aprender sobre el usuario y las personas con las que se relaciona habitualmente para hacer sugerencias u ofrecer información. La revista *Hosteltur*³⁹, en el número ya citado (julio-agosto de 2016), describe numerosas aplicaciones de *bots* en la industria del turismo y, en particular, comenta diferentes aplicaciones presentadas en la feria «Fiturtech 2016». Así, en el caso de *Google Assistant* cita algunas aplicaciones de interés: «por ejemplo, si una persona habla con un contacto sobre una cita para cenar, el asistente virtual de Google le ofrecerá restaurantes y la posibilidad de realizar la reserva sin salir de la aplicación *Allo* (lanzada oficialmente en septiembre de 2016) y teniendo en cuenta sus preferencias culinarias permitirá acceder a recorridos virtuales de hoteles, restaurantes u otros recursos turísticos basa-

³⁹ *Ibíd.*, pp. 11-12.

dos en tecnología “StreetView” (la aplicación de Google Maps) que estarán integrados».

Elies Campo (2016)⁴⁰, en un artículo de referencia sobre el tema de *chatbots* publicado en *El País*, considera que «empresas y Gobiernos serán los primeros en beneficiarse de esta tendencia de aplicaciones conversacionales, ya que por fin se podrán comunicar de manera privada de la misma forma en que lo hacen sus clientes y ciudadanos». También en el mismo artículo destaca, en su opinión, los «tres principales tipos de aplicaciones y oportunidades de los *chatbots*»:

- «Las aplicaciones conversacionales para el usuario final, que ofrecen un servicio y experiencia única y resuelven un problema concreto. Asistentes virtuales, asesores financieros, entrenadores personales, etcétera.
- *Software de backend* y herramientas para poder gestionar conversaciones de atención al cliente. Compañías, organizaciones y gobiernos se comunicarán e interactuarán con sus clientes y ciudadanos a través de mensajería.
- Los medios de comunicación y periodistas tendrán una nueva manera de comunicarse con su audiencia, distribuir su contenido y facilitar la participación de la audiencia. Para una creciente mayoría de medios de comunicación la mensajería ya es su principal distribución de contenidos».

Asistentes virtuales en páginas web de organizaciones y empresas

Algunos asistentes virtuales ya en uso en numerosas páginas web de organizaciones y empresas que hemos seleccionado:

- **Elvira**, asistente de la Universidad de Granada, con una interfaz elaborada con apariencia de ser humano y que trata de dar respuestas acerca de información del sitio web (<https://www.ugr.es>; <http://tueris.ugr.es/elvira>).
- **Irene**. Ayuda en la compra de billetes de tren en Renfe (<http://consulta.renfe.com/renfe0/index.jsp>).
- **Anna**. Asistente al usuario en la compra de muebles en IKEA —cadena de almacenes— (www.ikea.com/es/es).

Los bots: ¿las nuevas aplicaciones móviles?

Existe una tendencia creciente de sustitución de aplicaciones móviles por *bots*. Esta es la opinión de Satya Nadella, presidente de Microsoft, que en la

⁴⁰ Elies Campo Cid ha sido responsable del crecimiento y negocio de WhatsApp para España, Portugal y América Latina, *El País*, 11 de abril de 2016 [en línea: http://tecnologia.elpais.com/tecnologia/2016/04/11/actualidad/1460348403_483191.html] [consultado 2 de agosto de 2016].

presentación de su plataforma de *bots* planteaba que en lugar de tener que utilizar multitud de aplicaciones móviles los usuarios podrán interactuar con los *bots* de una manera mucho más natural utilizando su propio lenguaje. Con este motivo, Microsoft —y muchos de los gigantes tecnológicos o empresas especializadas— facilitará el desarrollo de *bots* compatibles con su plataforma por parte de empresas y usuarios finales.

En Facebook, en tan solo algo más de seis meses, desde su presentación en abril de 2016 de su plataforma M (Messenger) de *bots*, se han abierto más de 30.000 *chatbots* para ofrecer servicios personalizados. El cometido principal de estos *chatbots* es facilitar la relación entre el cliente y la marca y desde la propia red social de la empresa. Facebook permite de esta manera que la red social de la empresa pueda ser el canal de comunicación con clientes, proveedores, socios... utilizando un *chatbot* propio de la empresa como complemento a las funcionalidades propias de su red social.

La seguridad y los riesgos de los bots

Hemos visto las grandes ventajas que aportan los *bots*. Pero los *bots* también representan grandes riesgos para la seguridad de la información, ya que pueden ser utilizados para realizar tareas maliciosas, como, por ejemplo, promover ciberataques, fraudes, robos, envío de *spam* y propagación de virus, entre muchas otras tareas delictivas. Por eso, el uso de *bots* impone la necesidad de establecer ciertos límites éticos en lo referente a su programación y sus funciones, asumiendo los riesgos que para las estrategias de ciberseguridad de las empresas deben contemplarse.

El nuevo reglamento de protección de datos de la Unión Europea (25 de mayo de 2016)

El 27 de abril de 2016 fue aprobado en Bruselas el Reglamento General de Protección de Datos (UE 2016/679) por el Parlamento y el Consejo Europeo. El Reglamento aprobado se centra en el tratamiento de datos personales y la libre circulación de estos datos. Este Reglamento deroga la Directiva 95/46/EC que ejercía como anterior reglamento.

El Reglamento ha entrado en vigor el 25 de mayo del citado año pero no comenzará a aplicarse hasta dos años después, el 25 de mayo de 2018. Hasta entonces tanto la Directiva 85/46 como las normas nacionales que la trasponen, entre ellas la española, siguen siendo plenamente válidas y aplicables.

La Agencia Española de Protección de Datos (www.agpd.es) ha publicado un amplio documento en el que con un formato «pregunta-respuesta» trata de facilitar la comprensión del nuevo marco normativo a los ciudadanos y ayudar a las organizaciones a adaptarse a los cambios que incorpora y cumplir así con sus obligaciones.

Novedades del nuevo reglamento

Estrella Barrionuevo, abogada de la Asesoría Jurídica de Telefónica España, se adelantó a la entrada en vigor del Reglamento y publicó un artículo en el blog *aunclidelastic* del también blog de Telefónica, *blogthinkbig.com*, con las novedades más sobresalientes —en su opinión— del nuevo Reglamento de Protección de Datos de la Unión Europea. Un resumen de estas novedades es el siguiente⁴¹:

- «Introducción del concepto “pseudoanonimización” como categoría intermedia entre los datos personales y los datos anónimos.
- En cuanto al consentimiento, se concreta de forma específica que será necesario que el usuario realice una acción afirmativa para consentir, de manera que las casillas “premarcadas” o la inactividad del usuario no constituirá un consentimiento válido, lo que elimina la posibilidad del conocimiento tácito.
- Se modifica la edad por defecto para que los menores puedan consentir por sí mismos y no a través de quien ostente su patria potestad que pasa de los 14 años que establece actualmente la Ley Orgánica de Protección de Datos (LOPD) a 16, aunque este límite podrá reducirse por parte de los Estados miembros sin bajar de los 13 años.
- Nuevos derechos para el usuario.
 - Derecho al olvido.
 - Derecho a la portabilidad de los datos personales.
- Se crea el nuevo rol profesional de **DPO** (*Data Protection Office*), delegado o director de Protección de Datos para Administraciones públicas y entidades que traten datos personales a gran escala.
- Se establece la obligación de realizar análisis de riesgos y evaluaciones de impacto para determinar el cumplimiento normativo.
- Se amplía la obligación de comunicar las brechas o incidentes de seguridad, tanto a los afectados como a la AEPD, a todos los operadores del mercado que traten datos de carácter personal, en un plazo de setenta y dos horas».

Recomendaciones de la AEPD sobre el nuevo reglamento

La AEPD ha elaborado y publicado un documento simplificado —como ya se comentó anteriormente— con el objeto de intentar resolver las posibles dudas de los ciudadanos, organizaciones y empresas, relativas a la puesta en marcha del mencionado Reglamento de la Unión Europea. El modo elegido para redactar el documento ha sido el de «pregunta-respuesta» y para ello ha seleccionado un conjunto de doce preguntas clave con doce respuestas a

⁴¹ aunclidelastic.blogthinkbig.com/nuevo-reglamento-europeo-de-proteccion-de-datos- [consultado el 27 de julio de 2016].

las mismas y cuya lectura y consulta recomendamos, precisamente, basadas en la procedencia de la fuente, AEPD⁴². Estas preguntas son:

1. La entrada en vigor del Reglamento ¿supone que ya no se aplica la Ley Orgánica de Protección de Datos española?
2. ¿Cuál es, entonces, el significado de que el Reglamento haya entrado en vigor?
3. ¿A qué empresas u organizaciones se aplica?
4. ¿Qué implica para los ciudadanos que el Reglamento amplíe el ámbito de aplicación territorial?
5. ¿Qué nuevas herramientas de control de sus datos poseen los ciudadanos?
6. ¿A qué edad pueden los menores prestar su consentimiento para el tratamiento de sus datos personales?
7. ¿Qué implica la responsabilidad activa recogida en el Reglamento?
8. Entonces, ¿supone una mayor carga de obligaciones para las empresas?
9. ¿Cambia la forma en la que hay que obtener el consentimiento?
10. ¿Deben las empresas revisar sus avisos de privacidad?
11. ¿En qué consiste el sistema de «ventanilla única»?
12. ¿Tienen las empresas que empezar a aplicar ya las medidas contempladas en el Reglamento? No, el Reglamento está en vigor, pero no será aplicable hasta 2018.

Proyecto de colaboración público-privada de la Unión Europea (5 de julio de 2016)

La expansión del Internet de las Cosas y el aumento exponencial de las comunicaciones de datos entre personas y objetos de todo tipo aumenta también la preocupación de los ciudadanos, organizaciones y empresas, por la posibilidad de que se produzca un ataque contra sus datos personales y corporativos.

El inmenso valor de los datos relevantes de la vida de la gente que se vuelcan en la Red crece de igual modo que el auge del citado Internet de las Cosas y restantes tecnologías disruptivas presentes en la actual sociedad. Como señala el suplemento «Negocios» del diario *El País*, todas estas circunstancias harán: «redoblar la importancia de la ciberseguridad para la economía del continente europeo, no solo para la defensa del consumidor y empresas sino como un mercado de 75.000 millones de dólares del que Europa necesita participar»⁴³.

El 5 de julio de 2016, la Comisión Europea, anunció un **acuerdo de colaboración público-privada** por valor de 1.800 millones de euros hasta 2020, de los que Bruselas pone 450 millones a través del programa «Horizonte 2020» y el

⁴² www.agpd.es

⁴³ NEGOCIOS. «Hacia un mercado común en la Red». Periódico *El País*, suplemento NEGOCIOS, 28 de agosto de 2016, p. 12.

resto tiene previsto venir de la industria concertada a través del convenio de colaboración con la European Cyber Security Organization (*ECSO*, en sus siglas en inglés)⁴⁴. La Comisión Europea, a la hora de definir la estrategia de I+D de los próximos años en el ámbito de la ciberseguridad, «tendrá en cuenta la opinión del sector empresarial de la ciberseguridad», teniendo como interlocutor a la citada asociación *ECSO*. La Comisión ha firmado a este efecto un contrato **cPPP** (contractual Public-Private Partnership) de colaboración público-privada con *ECSO*, «el plan de acción tiene su origen en la *Estrategia de Mercado Único Digital*⁴⁵ de 2015, en la *Estrategia de Ciberseguridad de la Unión Europea*⁴⁶ y en la directiva sobre Seguridad de Redes y Sistemas de Información “*The Directive on security of network and information systems*”» (*NIS Directive*)⁴⁷.

Directiva de ciberseguridad (*NIS*) de la Unión Europea (6 de julio de 2016)

El 6 de julio de 2016 —el siguiente día a la firma del acuerdo de la Unión Europea sobre colaboración público-privada en materia de ciberseguridad— se publicó la Directiva *Network and Information Systems (NIS)* que obliga a los «prestadores de servicios esenciales» a tomar las medidas necesarias para garantizar la seguridad de sus instalaciones. El objetivo final es el mercado común digital: «Europa tiene que estar preparada para parar amenazas digitales cada vez más sofisticadas y que no reconocen frontera alguna»⁴⁸.

La directiva (UE) 2016/1148⁴⁹ del Parlamento Europeo y del Consejo de la Unión Europea de 6 de julio de 2016 es la primera directiva europea en ciberseguridad y la primera norma relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea. La directiva sobre Seguridad de Redes y Sistemas de Información «*The Directive on security of Network and Information Systems*» (*NIS Directive*) constituye un paso decisivo para hacer frente al reto que suponen las amenazas de ciberseguridad. La norma establece un enfoque común para evitar ataques a empresas y servicios clave.

⁴⁴ Ibíd. La empresa española S2 Grupo ha sido una de las participantes en la firma del contrato que se celebró el 5 de julio de 2016 en la sede del Parlamento Europeo de Estrasburgo, en el que han colaborado cincuenta organizaciones europeas. S2 será una de las empresas que liderará la estrategia de I+D de ciberseguridad europea en los próximos años. Representando a la empresa española, como socio de *ECSO*, asistió Miguel A. Juan, CEO de S2 Grupo.

⁴⁵ Digital Single Market. ec.europa.eu/priorities/digital-single-market_en

⁴⁶ <https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-open-safe-and-secure-cyberspace>

⁴⁷ <https://ec.europa.eu/digital-single-market/eu/news/directive-security-network-and-information-systems-nis.directive>

⁴⁸ Andrus Ansip, Comisario Encargado de Seguridad de la Unión Europea, ibíd. «Negocios», *El País*, p. 12.

⁴⁹ <https://www.boe.es/doue/2016/194/L00001-00030.pdf>

El objetivo es acabar con la fragmentación de los sistemas de seguridad cibernética entre los países para actuar de forma cohesionada en el seno de la Unión Europea y exige a las empresas de servicios críticos cumplir con nuevos requisitos. En la práctica busca producir un aumento del nivel general de ciberseguridad en la Unión Europea y es esencial para asegurar la ciberseguridad en Europa.

La citada directiva en ciberseguridad entró en vigor en agosto de 2016 y los Estados miembro tendrán veintidós meses para transponerla y seis meses más para identificar a los operadores de servicios esenciales. Para conseguir sus objetivos establece la obligación, para todos los Estados miembros, de adoptar una estrategia nacional de seguridad de las redes y sistemas de información:

- Crea un grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos.
- Crea una red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo «red de *CSIRT*», por sus siglas en inglés de *computer security incident response teams*) con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz.
- Establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales.
- Establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y *CSIRT* con funciones relacionadas con la seguridad de las redes y sistemas de información.

El escudo de privacidad Unión Europea-Estados Unidos (12 de julio de 2016)

La Comisión Europea adopta y pone en marcha el Escudo de la Privacidad (*Privacy Shield*) Unión Europea-Estados Unidos⁵⁰: «más protección para los flujos de datos transatlánticos», el día 23 de julio de 2016.

Este nuevo marco protege los derechos fundamentales de cualquier persona de la Unión Europea cuyos datos personales se transfieran a Estados Unidos y aporta claridad jurídica para las empresas que dependen de transferencias transatlánticas de datos.

El Escudo de la Privacidad Unión Europea-Estados Unidos se basa en los siguientes principios:

⁵⁰ europea.eu/rapid/press-release_IP_16_2461_es.htm

- Obligaciones rigurosas para las empresas que trabajan con datos.
- Obligaciones en materia de transparencia y salvaguardias claras para el acceso de la Administración estadounidense: Estados Unidos han dado a la Unión Europea garantías de que el acceso de las autoridades públicas a efectos de aplicación de la ley y de seguridad nacional está sujeto a limitaciones, salvaguardias y mecanismos de supervisión claros.
- Protección eficaz de los derechos individuales.
- Mecanismo de revisión conjunta anual.

La formación en ciberseguridad y en sus tecnologías disruptivas

Empresas de todo tipo, desde multinacionales a pequeñas y medianas empresas, requieren y buscan expertos en seguridad informática y, en especial, en ciberseguridad. Diferentes son los campos de la ciberseguridad más demandados. Entre ellos podríamos destacar:

- Ciberinteligencia.
- Análisis forense.
- *Hacking* ético.
- Desarrollo de *hardware* y *software* seguro.
- Ciberespionaje.
- Encriptación.
- Seguridad en la nube.

En España, América Latina y Caribe existe una amplia oferta de másteres (maestrías), especializaciones, diplomaturas y expertos, cursos profesionales y de posgrado especializados en ciberseguridad e impartidos por universidades y escuelas de negocio con el apoyo de las grandes empresas informáticas, de seguridad informática y de las grandes consultoras. Estas ofertas hoy día son tanto presenciales como *online* (virtuales) o híbridos.

Los perfiles demandados son muy variados. Desde analistas y consultores de ciberseguridad a expertos en ciberinteligencia, análisis forense, seguridad en la nube... Y cada día más se comienzan a solicitar analistas de *Big Data* para aplicaciones de ciberseguridad, así como desarrolladores de Internet de las Cosas y de Ciudades Inteligentes para gestión de objetos inteligentes de todo tipo (ingenieros de objetos inteligentes).

Asimismo, y dado que la nube (*cloud computing*) es la espina dorsal de la transformación digital de las organizaciones y empresas, soporte de la Industria 4.0 y base de la cuarta revolución industrial, las empresas requieren especialistas y profesionales de la nube, apareciendo nuevos perfiles profesionales tales como «Diseñador de “nubes”» y «Gestores de seguridad en la nube».

Como nota de interés, comentar que los **científicos de datos** (*Data Scientist*), una de las profesiones emergentes más demandada en la actualidad —re-

lacionada directamente con los analistas y desarrolladores de *Big Data*—, comienza a ser ya solicitada para roles en ciberseguridad, especialmente para análisis de datos y ayuda en la toma de decisiones en las estrategias de ciberseguridad fundamentalmente de las grandes empresas para asesoramiento en los grandes volúmenes de datos que hoy día maneja. Por eso se han puesto en boga cursos especializados de Análisis de Datos y de Estadística Computacional, así como de **Aprendizaje Máquina** (*Machine Learning*) y **Aprendizaje Profundo** (*Deep Learning*), programación y desarrollo de lenguajes de programación especializados en análisis de datos, como **R** y **Python**, además, claro, de posgrados (máster y especializaciones) en **Ciencia de Datos** (*Data Science*).

Los nuevos roles profesionales

El sector de las tecnologías de la información tiene en la actualidad un carácter transversal y cada día reclama además de las formaciones clásicas de ingeniería informática, de telecomunicaciones, industriales, electrónica, matemáticas, estadística... otras disciplinas. Asimismo, recomienda formación en empresa, *marketing*, recursos humanos... y, con la creciente preocupación por la privacidad y la protección de datos, también perfiles jurídicos para afrontar las nuevas competencias profesionales hoy demandadas en las empresas y que, a continuación, comentamos.

Las empresas y la Administración requieren ya no solo los departamentos de seguridad de la información y ciberseguridad, sino también de departamentos —independientes o relacionados con los anteriores— de privacidad y protección de datos junto a la concienciación de los riesgos y oportunidades de la ciberseguridad en todos los niveles profesionales de la empresas a nivel personal de directivo o simple empleado.

Así a los perfiles o roles profesionales ya implantados de director de Tecnología (*CTO, Chief Technology Officer*) con unas competencias muy abiertas y transversales en toda la organización y empresa, el director de Informática o de Sistemas de Información (*CIO, Chief Information Officer*), director de Seguridad de la Información (*CISO, Chief Information Security Officer*), hay que sumar dos perfiles profesionales que cada día serán muy demandados en la Administración, organizaciones y en empresas de todo tipo:

- *Chief Data Officer (CDO)* (director de Datos). Es un cargo dependiente del máximo ejecutivo de la empresa, a quien reporta directamente. Une las dos disciplinas hoy imperantes en la transformación digital: *Big Data* y *Ciberseguridad*. Su misión es impulsar el crecimiento de la organización y la empresa mediante la transformación digital de la misma. Ha de tener una amplia visión de la gestión de la empresa y del mundo digital, de análisis de datos y de seguridad de la información con el objeto de diseñar estrategias y políticas de ciberseguridad. Requiere una formación

multidisciplinar de ingeniería, estadística, analista digital, especialista en ciberseguridad, además de una amplia visión y conocimiento de la empresa.

- *Data Protection Officer (DPO)*. Es un perfil jurídico pero con formación informática y de seguridad de la información y ciberseguridad, aunque también podría ser un tecnólogo con formación jurídica en protección de datos y privacidad. Este perfil va a ser exigible en la Administración y en determinadas empresas a partir de 2018, en el que entre en vigor con todas sus consecuencias la nueva Ley de Protección de Datos y Privacidad de la Unión Europea, aprobada en mayo de 2016.

Además de las acreditaciones anteriores, las organizaciones y empresas valorarán cada día con mayor intensidad a los demandantes de empleo y a los propios empleados, las certificaciones internacionales en seguridad como CISA, CISSP, CISM... o certificaciones propias de los grandes fabricantes y proveedores de soluciones de seguridad de la información, *hardware* y *software* propietario o de código abierto, con estándares como OpenStack y otros.

Además y conforme se despliegan las nuevas tecnologías y tendencias tecnológicas como: inteligencia artificial (*machine learning* y *deep learning*), robótica, tecnologías cognitivas (robots, *bots*, *cobots* y *chatbots*, Watson de IBM), drones, fabricación aditiva (impresión 3D), tecnologías ponibles (*wearables*), aplicaciones de la banca digital, especialmente *fintech* (aplicaciones financieras), tecnologías *blockchain* (cadenas de bloques encriptadoras), aplicaciones de cartografía, GIS, geodesia y ciencias de la tierra... es preciso constatar que aunque las oportunidades que traerán estas tecnologías son innumerables, los incidentes cibernéticos irán en aumento si les unimos los riesgos del «Internet Industrial de las Cosas o Internet de Todo» y el crecimiento exponencial de los datos (*Big Data*) alojados en grandes centros de datos, desplegados a lo largo y ancho del mundo en la nube (*cloud computing*), junto con los enormes riesgos a la privacidad y protección, por parte de los innumerables *hackers* y de *empresas* del «cibercrimen como servicio». Los retos en formación e investigación serán innumerables y una gran oportunidad para el sector.

Por estas razones continuarán emergiendo nuevos perfiles o profesiones que como los grandes sociólogos, especialistas en recursos humanos, nos recuerdan todavía no han nacido y son difíciles de imaginar. Un listado de nuevas profesiones —algunas ya citadas— es la siguiente:

- *Growth Hacker* (responsable de la imagen digital que combina conocimientos de *marketing*, *SEO*, *Community Manager*, *Social Media Manager*, programación web... Twitter, Facebook, Uber, Airbnb... han potenciado esta nueva profesión).
- Analista de *Big Data*.
- Ingeniero de *Big Data*.

- Científico de datos.
- Ingeniero de Internet de las Cosas.
- Consultor de *hacking ético* (analista de los peligros informáticos y de su prevención y corrección).
- Gestor de robots colaborativos.
- Desarrollador de APIs para *bots*, *chatbots*...
- Diseñador de «nubes».
- Gestor de seguridad en la nube.
- Expertos en impresoras 3D y fabricación aditiva.
- Ingenieros de robótica y de inteligencia artificial.
- Ingenieros de objetos inteligentes.
- ...

Todos los roles y profesiones citados guardarán una estrecha relación con la nube, la ciberseguridad, Internet de las Cosas y *Big Data*, los cuatro pilares de la transformación digital de las organizaciones y empresas del final de esta década y de la próxima.

Los datos: presente y futuro de la ciberseguridad

En 2020, según estima Cisco, habrá 50.000 millones de objetos conectados (computadores, teléfonos inteligentes, tabletas, sensores, electrodomésticos, etcétera). Por esas fechas, las tecnologías móviles 5G es previsible se comercialicen con velocidades de transmisión de datos doscientas cincuenta veces mayor que la actual 4G (LTE y LTE-Advanced). Estos datos significan que el Internet de las Cosas, Internet de Todo o el Internet Industrial de las Cosas se habrá implantado a lo largo y ancho del mundo, por lo que «el futuro del Internet de la cosas estará en manos de la ciberseguridad». Esta situación significa que se requiere, desde ya, una alta inversión en ciberseguridad, dado que la falta de inversión producirá grandes problemas en organizaciones y empresas.

Los datos se alojarán preferentemente en la nube, por lo que el análisis de los grandes volúmenes de datos será una práctica diaria, de tal forma que *Big Data*, Internet de las Cosas y ciberseguridad serán la piedra angular de la sociedad de la tercera década de nuestro siglo.

Las grandes carreras tecnológicas del futuro —además de las relacionadas con inteligencia artificial y robótica— serán los citados anteriormente: **científicos de datos, desarrolladores del Internet de las Cosas** junto a los **arquitectos y especialistas de ciberseguridad**.

La ciberseguridad en América Latina y Caribe

Existen varios informes sobre el estado del arte y el impacto de la ciberseguridad en la región y tras analizar y estudiar una extensa documentación dispo-

nible en internet de grandes empresas consultoras, empresas especializadas en seguridad informática y organizaciones internacionales de la región hemos decidido seleccionar dos informes, ambos respaldados por organizaciones internacionales como el Banco Internacional de Desarrollo (BID) y la Organización de Estados Americanos (OEA), que han contado con la colaboración, en un primer caso, de una empresa multinacional de seguridad, Symantec, presentado en junio de 2014 y, en un segundo caso, por una institución docente de gran prestigio como la Universidad de Oxford, presentado en marzo de 2016.

- *Tendencias de Seguridad Cibernética en América Latina y el Caribe*⁵¹, realizado por Symantec, la Organización de Estados Americanos (OEA), la Secretaría de Seguridad Multidimensional (SMS) y el Comité Interamericano contra el Terrorismo. Presentado en junio de 2014.
- *Informe Ciberseguridad 2016. ¿Estamos preparados en América Latina y el Caribe?*⁵², realizado por el BID (Banco Iberoamericano de Desarrollo), la OEA y el Centro Global de Capacitación de Seguridad Cibernética (GCSCC) de la Universidad de Oxford. Presentado el 14 de marzo de 2016.

Tendencias de seguridad cibernética en América Latina y el Caribe (junio 2014)

Symantec, la Organización de Estados Americanos (OEA), la Secretaría de Seguridad Multidimensional (SMS) y el Comité Interamericano contra el Terrorismo (CICTE) presentaron un informe⁵³ que analiza el panorama de amenazas, las tendencias de ciberseguridad e incluye información sobre las acciones de los Gobiernos en América Latina y el Caribe frente a estos temas.

El informe (reporte) desarrollado en conjunto explora diferentes aspectos relacionados con la seguridad cibernética, incluyendo el incremento exponencial de las fugas de datos y tendencias como:

- «Crecimiento del *Ransomware* y *Cryptolocker*.
- *Malware* en cajeros automáticos.
- Estafas en redes sociales.
- Vulnerabilidades y riesgos en cómputo móvil.
- Código malicioso (*malware*).
- *Spam*.
- *Spear phishing*».

A diferencia de otros reportes de amenazas sobre vulnerabilidades cibernéticas que existen en el mercado este informe es único, ya que está enfocado en la región e incluye las perspectivas de los Gobiernos de los Estados miembros de la OEA, así como información detallada sobre el panorama de

⁵¹ <https://www.symantec.com/es/mx/page.jsp?id=cybersecurity-trends>

⁵² <https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/>

⁵³ <https://www.symantec.com/es/mx/page.jsp?id=cybersecurity-trends>

amenazas cibernéticas actual obtenida de la Red Global de Inteligencia de Symantec.

Ciberseguridad 2016 en América Latina y Caribe (marzo 2016)

El Informe *Ciberseguridad 2016. ¿Estamos preparados en América Latina y el Caribe?*⁵⁴ fue presentado el 14 de marzo de 2016 en la sede del Centro de Estudios Estratégicos e Internacionales (CSIS) en Washington DC. En el evento participaron, entre otros, el presidente del BID, Luis Alberto Moreno; el secretario general de la OEA, Luis Almagro, y el presidente del CSIS, John Hamre, entre otras autoridades. El informe fue presentado posteriormente en varios países de la región y su recomendación principal ha sido el mensaje de «considerar “urgente” que América Latina y Caribe actúen para proteger su ciberespacio».

El informe analiza el estado de preparación de treinta y dos países basado en cuarenta y nueve indicadores y en la nota de prensa de la presentación oficial se consideró que era la primera radiografía profunda del nivel de preparación de América Latina y el Caribe ante la creciente amenaza del cibercrimen. El informe presenta una imagen completa y actualizada sobre el estado de la seguridad cibernética (riesgos, retos y oportunidades) de los países de América Latina y el Caribe, y consta de dos secciones principales.

La primera sección incluye una serie de ensayos sobre las tendencias de la seguridad cibernética en la región, aportados por reconocidos expertos internacionales en el tema.

La segunda sección examina la «madurez cibernética» de cada país mediante la aplicación del Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM, por sus siglas en inglés) que toma en cuenta las consideraciones de seguridad cibernética a través de cinco dimensiones y las evalúa en cinco niveles de madurez para cada uno de sus cuarenta y nueve indicadores. El CMM es el primero de su tipo en términos de extensión y profundidad en cada aspecto de capacidad de la seguridad cibernética. Está construido sobre una base de consulta de múltiples partes interesadas y el respeto de los derechos humanos, equilibrando cuidadosamente la necesidad que se tiene de seguridad para permitir el crecimiento económico y la sostenibilidad, al tiempo que se respetan el derecho a la libertad de expresión y el derecho a la privacidad.

Las conclusiones más destacadas en la presentación⁵⁵ fueron:

⁵⁴ Vídeo presentación informe OEA-BID: *Cybersecurity Report 2016: Are We Ready in Latin America and the Caribbean?*

<https://www.csis.org/events/cybersecurity-report-2016-are-we-ready-latin-america-and-caribbean>

⁵⁵ www.iadb.org/es/noticias/comunicados-de-prensa/2016-03-14/informe-sobre-ciberseguridad-en-america-latina,11420html

- El informe demuestra que la región presenta vulnerabilidades «potencialmente devastadoras».
- Cuatro de cada cinco países de la región carecen de estrategias de ciberseguridad o planes de protección de infraestructuras críticas.
- Dos de cada tres países no cuentan con un centro de comando y control de seguridad cibernética.
- La gran mayoría de las fiscalías carecen de capacidad para perseguir los delitos cibernéticos, entre otras carencias.

El informe destaca que —en el primer trimestre de 2016— solo seis países de América Latina y el Caribe, Brasil, Colombia, Jamaica, Trinidad y Tobago, Panamá y Uruguay tienen estrategias de seguridad cibernética, mientras que Argentina, Antigua y Barbuda, Bahamas, Costa Rica, Dominica, El Salvador, Haití, México, Paraguay, Perú y Surinam están en proceso de articular una estrategia.

El secretario general de la OEA, Luis Almagro, enfatizó en su presentación que: «los riesgos de abusos aumentan a medida que América Latina y el Caribe se incorporan a la revolución digital. La región es el cuarto mayor mercado móvil del mundo. La mitad de la población usa internet. Hay países en América Latina que procesan el 100 % de sus compras gubernamentales por vía electrónica. Los riesgos se multiplicarán con el advenimiento de la “Internet de las Cosas”, donde ya no solo estarán interconectadas las computadoras sino un universo de máquinas y sensores inteligentes, controlando virtualmente todo lo que usamos a diario»⁵⁶. En lo relativo a formación en ciberseguridad, Almagro considera que «apenas seis países de la región cuentan con un programa estructurado de educación en seguridad cibernética, que incluye estabilidad presupuestaria así como mecanismos de investigación y transferencia de conocimiento».

Conclusiones: tendencias en ciberseguridad

En la sección de bibliografía se incluyen los informes considerados de mayor impacto, publicados a lo largo del bienio 2015-2016 en España, y algunos a nivel internacional y queremos destacar las recomendaciones de dos de ellos, INCIBE y Telefónica, como conclusión del capítulo, dado que la mayoría de las tendencias TIC publicadas en ambos informe han sido recogidas en el mismo.

Tendencias TIC de INCIBE (2016). Julio 2016

INCIBE resalta la conexión y ubicuidad de los datos basados en Internet de las Cosas, *Cloud Computing*, dando lugar a la creación de redes y ciudades

⁵⁶ Ibíd.

inteligentes donde el *Big Data* es un elemento esencial y las tendencias TIC que recomienda son:

- *Big Data*, *Cloud Computing* e Internet de las Cosas (*IoT*).
- *Smart Cities* y *Smart Grids*.
- Industria 4.0.
- Redes sociales.
- Tecnologías cognitivas (incluyendo aprendizaje automático, procesamiento en lenguaje natural «NLP» y reconocimiento de voz).
- Sistemas ciberfísicos (incluyendo el uso de *drones*, redes de sensores y realidad aumentada).
- Tecnologías móviles, WiFi óptico y Redes 5G.
- Nuevos modelos de pago.

INCIBE recomienda también tendencias específicas en ciberseguridad, agrupándolas en veinte tendencias globales catalogadas en torno a seis sectores de actividad.

Nuevos escenarios y desafíos de la seguridad. Telefónica (septiembre de 2016)

Telefónica publicó en septiembre de 2016, en coedición con Ariel, el informe «Ciberseguridad, la protección de la información en un mundo digital». En un extenso capítulo 4, los autores del informe consideran los nuevos escenarios y desafíos de la seguridad y hacen una clasificación de las principales tendencias actuales e identifican sus principales vulnerabilidades, así como sus necesidades de seguridad:

- *Cloud Computing*, *Big Data* e Internet de las Cosas.
- BYOD (trae tu propio dispositivo al trabajo y empresa).
- Internet industrial (Industria 4.0).
- *Apps* móviles.
- Múltiples identidades digitales.
- Desafíos legales a la ciberseguridad.

Otras tecnologías de impacto en el futuro de la ciberseguridad analizadas

En este capítulo 1 también hemos considerado otras tecnologías de gran impacto en el ámbito de la ciberseguridad:

- Tecnologías financieras: *Fintech* y *Blockchain*,
- Robots colaborativos (*cotbots*), *bots* y *chatbots* (*bots* conversacionales),
- Aprendizaje profundo (*Deep Learning*). Una tecnología cognitiva de inteligencia artificial y un tipo específico de gran impacto del aprendizaje automático (*machine learning*).

En un mundo actual donde la transformación digital de las organizaciones y empresas es una necesidad ineludible, estas han de contemplar una estrategia de ciberseguridad actualizada y como Miguel Rego (director de INCIBE) manifestó en Santander en el Encuentro de Telecomunicaciones y Economía de la Universidad Menéndez Pelayo: «Sin ciberseguridad no se puede construir una España digital... y la razón es sencilla, los usuarios no recurrirán a servicios *online* si no se sienten seguros»⁵⁷.

⁵⁷ Encuentro de Telecomunicaciones y Economía Digital, Universidad Menéndez Pelayo, Santander, 9 de septiembre de 2016 [en línea. <http://www.ciospain.es/seguridad/sin-ciberseguridad-no-se-puede-construir-una-espana-digital-asegura-el-incibe>]

Estudios de ciberseguridad

- BANKINTER (2016). *Ciberseguridad. Un desafío mundial*, mayo de 2016. www.fundacionbankinter.org
- INCIBE (2016a). *Tendencias en el mercado de la Ciberseguridad*. León, julio de 2016. www.incibe.es
- INCIBE/OSI/AEPD (2016b). *Guía de privacidad y seguridad en Internet*. León, octubre de 2016. www.incibe.es
- INCIBE (2016c). *Punto de partida al modelo de gestión y seguimiento del TALENTO en ciberseguridad en España. Visión conjunta de la industria, sector académico e investigador y profesionales del sector* https://www.incibe.es/sites/default/files/contenidos/notasprensa/doc/modelo_gestion_talento_incibe.pdf
- INCIBE (2015). *Decálogo de ciberseguridad. El camino hacia la ciberseguridad en su empresa*. https://www.incibe.es/extfrontinteco/img/File/empresas/blog/2014Octubre/decalogo_ciberseguridad_empresas.pdf
- McAfee Labs (2016a). *Predicciones sobre amenazas para 2016*. Intel Security/McAfee. Agosto de 2016. <http://www.mcafee.com/es/resources/reports/rp-threats-predictions-2016.pdf>
- McAfee Labs (2016b). *Informe de McAfee Labs sobre amenazas. Septiembre 2016*. Intel Security/McAfee. Septiembre de 2016. <http://www.mcafee.com/es/resources/reports/rp-quarterly-threats-sep-2016.pdf>
- MINISTERIO DE LA PRESIDENCIA (2015). *Informe anual de Seguridad Nacional 2014*. Madrid: Gobierno de España. http://www.dsn.gob.es/sites/dsn/files/Informe_Seguridad_Nacional%202014.pdf
- MINISTERIO DE LA PRESIDENCIA (2016). *Informe anual de Seguridad Nacional 2015*. Madrid: Gobierno de España. <http://www.lamoncloa.gob.es/presidente/actividades/Paginas/2016/270516rajoycsn.aspx>
- <http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/Documents/INFORME%20ANUAL%20DE%20SEGURIDAD%20NACIONAL%202015.pdf>
- OEA-BID (2016). *Ciberseguridad 2016. ¿Estamos preparados en América Latina y el Caribe?* Marzo de 2016. <https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/>
- ONTSI (2016). *Estudio sobre la ciberseguridad y confianza en los hogares españoles*. Junio de 2016. <http://www.ontsi.red.es/ontsi/es/estudios-informes/ciberseguridad-y-confianza-en-los-hogares-espa%C3%B1oles-junio-2016>
- TELEFÓNICA (2016). *Ciberseguridad. La protección de la información en un mundo digital*. Madrid: Ariel/Fundación Telefónica. Septiembre de 2016. http://www.fundaciontelefonica.com/artes_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/531/

Bibliografía de consulta

- AYALA, Luis (2016). *Cyber-Physical Attack REcovery Procedures. A Step-by-Step Preparation and Response Guide*. New York: Apress.
- DONALDSON, Scott E., et al. (2015). *Enterprise Cibersecurity. How to Build a Successful Cyberdefense Program Against Advanced Threats*. New York: Apress.
- INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS (2011). *Ciberseguridad. Retos y amenazas a la seguridad nacional en el Ciberespacio*. Cuadernos de Estrategia, no. 149. JOYANES, Luis (Coord). Madrid: Ministerio de Defensa.
- JOYANES AGUILAR, Luis (2015). *Sistemas de información en la empresa. El impacto de la nube, la movilidad y los medios sociales*. Barcelona: Marcombo; México DF: Alfaomega.
- JOYANES AGUILAR, Luis (2014). *Big Data. Análisis de grandes volúmenes de datos en organizaciones*. Barcelona: Marcombo; México DF: Alfaomega.
- JOYANES AGUILAR, Luis (2013). *Computación en la nube. El imacto del cloud computing en las empresas*. Barcelona: Marcombo; México DF: Alfaomega.
- MEDINA, Manel y MOLIST, Mercè (2015). *Cibercrimen*. Barcelona: Tibidabo Ediciones
- SEGURA, Antonio y GORDO, Fernando (Coords). *Ciberseguridad global. Oportunidades y compromisos en el uso del ciberesepecio*. Granada. Universidad de Granada/Mando de Adiestramiento y Doctrina.
- SIKORSKI, Michael y HONIG, Andrew (2012). *Practical Malware Analysis. The Hands-On Guide to Dissecting Malicious Software*. San Francisco: No Starch Press.
- TOUHIL, Gregory J. y TOUHILL, C. Joseph (2014). *Cibersecurity for Executives. A Practical Guide*. New Jersey: Wiley.
- ULSCH, MacDonnell. *Cyber Threat! How to Manage the Growing Risk of Cyber Attacks*. New Jersey: Wiley

Capítulo segundo

Crisis y ciberespacio: hacia un modelo integral de respuesta en el Sistema de Seguridad Nacional

Joaquín Castellón Moreno

Director Operativo

Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno

María Mar López Gil

Jefa de la Oficina de Tecnología y Seguridad. Responsable de Ciberseguridad

Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno

Resumen

La hiperconectividad y los constantes avances tecnológicos nos llevan a enfrentarnos a un mundo completamente desconocido y lleno de incertidumbre. El ciberespacio es un espacio de grandes oportunidades, pero también es imposible ocultar que en él se tensionan los intereses de los Estados con fines distintos, organizaciones terroristas y redes de crimen organizado se sirven de las facilidades que ofrece el medio.

Desde la creación del Departamento de Seguridad Nacional de la Presidencia del Gobierno hemos impulsado un modelo integrado de gobernanza para la ciberseguridad. Un modelo basado en la implicación de todos los actores y recursos del Estado y en la participación del sector privado y de la sociedad en general.

La participación del sector privado en la Seguridad Nacional es hoy en día ineludible y quizás sea la ciberseguridad un ámbito paradigmático en este sentido. Así ha quedado recogido en la Estrategia de Seguridad Nacional, la Estrategia de Ciberseguridad Nacional y, sobre todo, en la Ley de Seguridad Nacional.

El aspecto más innovador de la nueva Ley se encuentra en el articulado dedicado a la gestión de situaciones crisis y muy especialmente en la figura de la «situación de interés para la Seguridad Nacional».

Palabras clave

Seguridad Nacional, tecnología, hiperconectividad, ciberespacio, riesgos, amenazas, ciberseguridad, ciberamenazas, ciberataques, gestión de crisis, colaboración público privada, cultura, estrategia.

Abstract

The constant technological development and hyper connectivity are leading us through an uncharted and uncertain world. In this sense, the cyberspace represents great opportunities, but also a space where the diverging interests of states conflict and terrorist organizations and organized crime networks take advantage of its possibilities.

Since the establishment of the National Security Department, within the Presidency of the Government, we have promoted an integrated cybersecurity governance model. This model is based on the involvement of all state actors and their resources together with the participation of the private sector and civil society at large.

Nowadays, the participation of the private sector in National security issues is imperative and the field of cybersecurity is a paradigmatic example to this effect. This main idea has been included in the National Security Strategy, in the National Cybersecurity Strategy and, most importantly, in the recently passed National Security Act.

The most innovative aspect of this Act is found on the sections regulating crisis management and particularly the concept of «situation of interest for the National Security».

Keywords

National security, technology, hyperconnectivity, cyberspace, risks, threats, cybersecurity, cyberthreats, cyberattacks, crisis management, public and private collaboration, culture, strategy.

Introducción

Desde el Departamento de Seguridad Nacional de la Presidencia del Gobierno (DSN) hemos impulsado a través de la Estrategia de Seguridad Nacional, la Estrategia de Ciberseguridad Nacional y, sobre todo, la Ley de Seguridad Nacional¹, la construcción de un sistema nuevo de gobernanza para la ciberseguridad en España. Un modelo integrado de gobernanza basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado, en la colaboración público-privada y en la participación de la ciudadanía. Además, y dado el marcado carácter global de la ciberseguridad, la cooperación internacional forma parte esencial de este modelo.

En este capítulo recogemos algunos de los avances más importantes que se han dado en este ámbito prioritario de la Seguridad Nacional centrándonos fundamentalmente en la gestión de situaciones de crisis y cómo el sector privado está llamado a jugar un papel cada vez más relevante.

Hace poco más de tres años finalizamos los trabajos de elaboración de la Estrategia de Seguridad Nacional 2013². Lógicamente, un trabajo de esta naturaleza requiere un ineludible esfuerzo previo para tratar de entender el mundo en que vivimos e intentar, al menos a grandes trazos, dibujar nuestro mundo futuro. En el DSN, entendimos el momento actual como una transición a lo que podríamos denominar una nueva era. Una nueva era que se va conformando por infinidad de factores, algunos de singular importancia, como el cambio climático, pero donde, por encima de cualquier otro factor, destacan las nuevas tecnologías y una conectividad sin precedentes.

La hiperconectividad y los constantes avances tecnológicos nos llevan a enfrentarnos a un mundo completamente desconocido y lleno de incertidumbre donde todos, en mayor o menor medida, somos vulnerables, donde se nos plantean nuevos retos, riesgos y amenazas que no pueden ser ignorados. Un mundo que se hace, día a día, cada vez más dependiente del ciberespacio dado que cualquier actividad dentro del ámbito público o privado tiene en este medio el marco idóneo para desarrollarse.

En la mencionada Estrategia de Seguridad Nacional del año 2013 destaca, como un objetivo prioritario de la Seguridad Nacional, garantizar el uso seguro del ciberespacio. Concretamente, la estrategia reconoce que España

¹ Ley 36/2015, de 28 de septiembre, de Seguridad Nacional].

² La Estrategia de Seguridad Nacional constituye el marco político estratégico de referencia de la Política de Seguridad Nacional. Contiene el análisis del entorno estratégico, concreta los riesgos y amenazas que afectan a la seguridad de España, define las líneas de acción estratégicas en cada ámbito de actuación y promueve la optimización de los recursos existentes. Se elabora a iniciativa del presidente del Gobierno, quién la somete a la aprobación del Consejo de Ministros. La actual Estrategia de Seguridad Nacional fue aprobada por el Consejo de Ministros en su reunión del 31 de mayo de 2013, disponible en www.dsn.gob.es

está expuesta a los ciberataques, que no solo generan elevados costes económicos, sino también, y lo que es más importante, la pérdida de confianza de los ciudadanos en unos sistemas que, en la actualidad, resultan críticos para el normal funcionamiento de la sociedad.

Plenamente conscientes de la importancia de la cuestión, el Consejo de Seguridad Nacional³ aprobaba en diciembre de ese mismo año la Estrategia de Ciberseguridad Nacional⁴, primer documento del más alto nivel político-estratégico dedicado a la ciberseguridad adoptado en nuestro país y que nos equiparaba a los países más avanzados de nuestro entorno en esta cuestión. La Estrategia implanta un modelo de gobernanza adaptado a la fisonomía de los retos que debemos afrontar.

Como señala el propio presidente del Gobierno en su carta de presentación: «la aprobación del presente documento de carácter estratégico pone de manifiesto las capacidades colectivas y el compromiso de una nación que apuesta firme por garantizar la seguridad en el ciberespacio. Para España, los avances en el ámbito de la ciberseguridad contribuyen además a incrementar nuestro potencial económico, ya que promueven un entorno más seguro para la inversión, la generación de empleo y la competitividad⁵».

Una de las principales novedades de la Estrategia es la puesta en pie de un sistema orgánico para facilitar la toma de decisiones. El centro de esta estructura orgánica es el Consejo Nacional de Ciberseguridad, órgano dependiente del Consejo de Seguridad Nacional.

Cabe destacar, como uno de los principales logros del Consejo Nacional de Ciberseguridad, el desarrollo del Plan Nacional de Ciberseguridad⁶ y los Planes Derivados de Ciberseguridad (ver tabla 1).

El Plan Nacional de Ciberseguridad constituye el primer nivel en la planificación de la Estrategia y es donde se definen las amenazas a las que se enfrenta España, se establece la misión y los cometidos concretos para el

³ El Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, es el órgano al que corresponde asistir al presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional, así como ejercer las funciones que se le atribuyan en la Ley de Seguridad Nacional y se le asignen por su reglamento, disponible en www.dsn.gob.es

⁴ Asimismo, la Estrategia de Ciberseguridad Nacional desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2013 en el ámbito de la ciberseguridad, fijando como objetivo global lograr que España haga un uso seguro de los sistemas de información y las telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques. La Estrategia de Ciberseguridad Nacional fue aprobada por el Consejo de Seguridad Nacional el 14 de diciembre de 2013, disponible en www.dsn.gob.es

⁵ Rajoy Brey, Mariano, carta de presentación de la «Estrategia de Ciberseguridad Nacional», Departamento de Seguridad Nacional de la Presidencia del Gobierno, disponible en www.dsn.gob.es

⁶ Consejo de Seguridad Nacional, *Plan Nacional de Ciberseguridad*, octubre de 2014.

cumplimiento de los objetivos señalados por la Estrategia y se articula la asignación de responsabilidades de los implicados en la materia⁷.

Por otra parte y como parte del Plan, el Consejo de Seguridad Nacional aprobó el Marco General de desarrollo del Plan Nacional de Ciberseguridad, en el cual se apunta el modelo de gobernanza nacional futuro para reforzar la coordinación y la cooperación nacional, internacional y con la Unión Europea a fin de mantener los avances en línea con las estrategias y modelos de los países de nuestro entorno.

Al mismo tiempo, en el Plan Nacional de Ciberseguridad se contemplaba la elaboración de nueve Planes Derivados⁸ (ver tabla 2) que desarrollasen, a través de actuaciones concretas, las medidas incluidas en cada una de las Líneas de Acción de la Estrategia (ver tabla 3).

Los Planes Derivados vienen a responder a la necesidad de desarrollar proyectos concretos dirigidos a alcanzar de manera ordenada, coordinada y a través de la creación de sinergias, los objetivos planteados en la Estrategia.

Pero, sin duda, el hito más importante a tener en cuenta en la ciberseguridad nacional fue la aprobación de la Ley de Seguridad Nacional. La Ley declara la ciberseguridad como un ámbito de especial interés para la Seguridad Nacional e introduce una serie de novedades encaminadas a dar respuesta a los nuevos riesgos y amenazas a los que nos enfrentamos, todos ellos caracterizados por un marcado carácter transversal y transnacional, como las ciberamenazas.

Quizás el aspecto más innovador de la nueva Ley se encuentre en el articulado dedicado a la gestión de situaciones crisis y muy especialmente en la figura de la «situación de interés para la Seguridad Nacional». Esta nueva situación se concibe como aquella en la que, por la gravedad de sus efectos y la dimensión, urgencia y transversalidad de las medidas para su resolución, requiere de la coordinación reforzada de las autoridades competentes bajo la dirección del Gobierno. Se busca, en definitiva, el funcionamiento óptimo, integrado y flexible de todos los recursos disponibles.

Un ataque cibernético a los principales operadores de un servicio esencial que suponga una suspensión de los servicios durante un tiempo prolongado

⁷ Presidencia del Gobierno a través del Departamento de Seguridad Nacional; Ministerio de Asuntos Exteriores y de Cooperación; Ministerio de Justicia; Ministerio de Defensa; Ministerio de Hacienda y Administraciones públicas; Ministerio del Interior; Ministerio de Fomento; Ministerio de Educación, Cultura y Deporte; Ministerio de Empleo y de Seguridad Social; Ministerio de Industria, Energía y Turismo; Ministerio de la Presidencia a través del Centro Nacional de Inteligencia; Ministerio de Economía y Competitividad.

⁸ Desarrollados por los grupos de trabajo interministeriales del Consejo Nacional de ciberseguridad, validados por este último y aprobados por el Consejo de Seguridad Nacional.

y con afección directa a la población, sería un caso susceptible de ser declarado «situación de interés para la Seguridad Nacional».

La lucha por el control del ciberespacio

En 1609 publicaba Hugo Grocio su conocido libro *Mare Liberum*, en el cual defendía la libertad de los mares como piedra angular del desarrollo del comercio y argumentaba cómo los océanos eran ilimitados, como lo es el aire, y no pertenecían a ninguna persona o nación en particular. El derecho de su uso y disfrute era común ya que en su origen no eran propiedad de nadie. *Mare Liberum* constituyó un auténtico hito que sentó las bases modernas del Derecho Internacional Marítimo y también inspiró el término moderno de *Global Commons*.

Desde el punto de vista del Derecho Internacional, los *Global Commons* son aquellos espacios y recursos que se encuentran fuera de la soberanía de cualquier país, es decir, todo el mundo puede acceder a ellos y consecuentemente beneficiarse. Son reconocidos como *Global Commons* los océanos, el espacio aéreo, el espacio ultraterrestre, el Ártico y el ciberespacio.

Todos estos espacios, en los que conviven actores estatales y no estatales, ofrecen sin duda grandes oportunidades y riesgos, desde el punto de vista tanto civil como militar. Uno de los principales problemas que presentan es su escasa regulación, normalmente fijada mediante tratados o convenciones internacionales, en forma parcial y no siempre aceptadas por todos los actores.

El gran desarrollo del comercio internacional por vía aérea y marítima originó la adopción de instrumentos normativos internacionales, la Convención sobre Aviación Civil Internacional⁹ y la Convención de las Naciones Unidas sobre el Derecho del Mar¹⁰. En el caso del espacio exterior, su uso queda reducido actualmente a un pequeño número de países que hace que este sea un ámbito poco regulado. Por su parte, el ciberespacio, por su corto recorrido histórico y sus características peculiares se presenta como un ámbito carente de una regulación clara¹¹.

Los avances tecnológicos y nuestra forma de vida conceden a los *Global Commons* un innegable valor estratégico, como queda reflejado en la Estrategia de Seguridad Nacional del 2015 de los Estados Unidos, promulgada

⁹ Convención sobre Aviación Civil Internacional, «Convención de Chicago», diciembre de 1944, disponible en <http://www.aviacioncivil.gob.ec/wp-content/uploads/downloads/2015/04/Convenio-de-Aviacion-Civil-Internacional-de-Chicago.pdf>

¹⁰ Naciones Unidas, «Convención de las Naciones Unidas sobre el Derecho del Mar», abril de 1982, disponible en «http://www.un.org/depts/los/convention_agreements/texts/unclos/convemar_es.pdf»

¹¹ Kutt Nebrera, Alexander, «La importancia de dominar los global commons en el siglo XXI», Documento Marco 29/12, Instituto Español de Estudios Estratégicos, 2012.

por el presidente Barack Obama¹²: «El mundo está conectado por espacios compartidos –ciberespacio, espacio exterior, aire y océanos– que permiten el libre flujo de gente, bienes, servicios e ideas. Ellos son las arterias de la economía global y la sociedad civil y el acceso a ellos está en riesgo dado el incremento de la competencia y comportamientos ilícitos. Por ello, continuaremos promoviendo reglas para el comportamiento responsable asegurando al mismo tiempo las capacidades que permitan el acceso a esos espacios compartidos».

El control de los *Global Commons* se ha convertido en un objetivo estratégico de primer orden y entre todos ellos a nadie se le escapa que el ciberespacio ocupa el primer lugar. El ciberespacio es un codiciado objeto de deseo, no solo para los propios estados sino también para organizaciones terroristas y grupos de crimen organizado, donde sus fines pueden ser conseguidos a un menor coste y con una asunción de riesgos mucho menor.

El papel nuclear del ciberespacio en la Seguridad Nacional ha quedado recogido en las Estrategias de Seguridad Nacional de los Estados Unidos y Rusia y en la Estrategia Militar China, todas ellas publicadas en el año 2015.

La más reciente de las estrategias presentadas ha sido la Estrategia Global de Política de Seguridad de la Unión Europea, presentada al Consejo Europeo en el pasado mes de junio. En ella se contempla la ciberseguridad como una de las áreas prioritarias junto a la defensa, la lucha contra el terrorismo o la seguridad energética. Ello implica reforzar las capacidades tecnológicas destinadas a mitigar las amenazas y reforzar la resiliencia de las infraestructuras críticas, las redes y servicios, así como la reducción de la delincuencia informática.

La Estrategia apoya la gobernanza digital multilateral y un marco de cooperación mundial en materia de ciberseguridad, respetando la libre circulación de la información, y marca como ejes de actuación la cooperación a nivel político, operativo y técnico entre los Estados miembros, así como con los Estados Unidos y la OTAN.

En el artículo publicado en abril de 2016 por Ignacio Torreblanca en el diario *El País*¹³, se compara la pugna entre la Rusia zarista y el Imperio británico por el territorio que se extendía entre Persia y la India, entre 1813-1907, con la lucha actual de los Estados por el control del ciberespacio. Esa competición geopolítica por el corazón de Asia, popularizada por Rudyard Kipling en su genial obra *Kim*, es conocida como «El gran juego»¹⁴. Para el autor el gran juego actual es la pugna por el control de internet de las grandes potencias,

¹² The White House, Washington, US National Security Strategy, febrero de 2015.

¹³ Torreblanca, José Ignacio, «El nuevo gran juego digital», *El País*, 27 de abril de 2016, disponible en http://tecnologia.elpais.com/tecnologia/2016/04/27/actualidad/1461767882_557672.html.

¹⁴ Kipling, Joseph Rudyard, «The Great Game», 1913.

es decir, nos encontramos sumidos en la versión digital de «El gran juego» de Kipling.

El artículo señala que estamos jugando un juego geopolítico y geoeconómico con inmensas consecuencias sobre el poder, la prosperidad y la seguridad de los Estados y las sociedades. Un juego que carece todavía de reglas claras que lo ordenen y hasta que las tengamos habrá margen para malentendidos fatales.

De la gestión de incidentes a la gestión de crisis en el ciberespacio

Uno de los aspectos donde quizás más toca incidir actualmente es el relativo a la gestión de crisis en ámbito del ciberespacio. Una vez sentadas las bases normativas, debemos ahora desarrollar un sistema que nos permita pasar de la gestión de incidentes cibernéticos a la gestión integral de crisis que tengan en el ciberespacio su campo de batalla.

Según recoge el *Informe Anual de Seguridad Nacional* del año 2015¹⁵, el Equipo de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) resolvió durante 2015 un total de 18.232 incidentes de seguridad, de ellos 430 clasificados como muy altos o críticos. En cuanto a la gestión del Centro de Respuesta a Incidentes de Ciberseguridad para empresas, ciudadanos e infraestructuras críticas (CERTSI), durante 2015 se gestionaron alrededor de 50.000 incidentes, lo que supone un 180 % más que el año anterior. Es preciso tener en cuenta que nuestras capacidades de detección son cada vez mayores aunque, indiscutiblemente, también ayuda a que año a año las cifras de incidentes registrados aumenten significativamente.

Uno de los datos más interesantes además del número de incidentes registrados son, sin lugar a dudas, las pérdidas económicas que ocasionan, dato que generalmente no es fácil de estimar. Calcular el perjuicio económico debido a un incidente de ciberseguridad es una tarea sumamente compleja, dado que existe multiplicidad de tipos de ataques, actores y factores. Además, colateralmente, pueden ser muchos los servicios afectados lo que complica enormemente el cálculo de las pérdidas totales. A los costes que podríamos considerar directos hay que sumarle otros muchos como pudieran ser el deterioro de la confianza de los usuarios en un servicio, pérdida de reputación de una empresa, pérdida de la propiedad intelectual, la disminución de la ventaja tecnológica frente a competidores o, incluso, la pérdida de puestos de trabajo.

¹⁵ Departamento de Seguridad Nacional de la Presidencia del Gobierno, *Informe Anual de Seguridad Nacional 2015*, mayo 2016 disponible en www.dsn.gob.es.

En un reciente estudio¹⁶ realizado por la Agencia de Seguridad de las Redes y de la Información (ENISA), delimitado al ámbito de los incidentes producidos en Infraestructuras Críticas, se expone la dificultad para determinar el impacto real del coste de los incidentes de ciberseguridad en términos de recuperación del servicio afectado. Aun así, el estudio muestra una serie de conclusiones interesantes entre las que cabe destacar:

- En algunos países de la Unión Europea se estima que el coste de los incidentes de ciberseguridad podría suponer alrededor del 1,6 % del Producto Interior Bruto del país y que esta cifra, a nivel mundial, podría suponer entre 330 y 506 billones de euros.
- Los sectores financiero, energético y TIC (Sistemas de Información y Comunicaciones) son en los que los ciberincidentes tienen un mayor coste.
- El activo más afectado suelen ser los datos.

Cuando nos enfrentamos a un incidente cibernético, y en relación con el objeto principal de este capítulo, es muy importante poder discernir si nos enfrentamos a un incidente aislado, orientado a un fin concreto y de efecto limitado, o, por el contrario, nos encontramos ante un incidente que puede contribuir a originar una verdadera situación de crisis para una organización concreta o, incluso, para un Estado.

Tradicionalmente se ha tendido a aislar los incidentes de ciberseguridad al plano técnico, al entenderse que se trataba de un problema exclusivamente técnico y consecuentemente la respuesta debía ser también exclusivamente técnica. Este enfoque en ocasiones nos impide calcular las consecuencias reales de un incidente y responder de forma completa y eficiente.

Cuando pensamos en los autores de los ciberataques frecuentemente nos encontramos con potentes redes de crimen organizado, organizaciones terroristas e incluso los propios Estados. Cuando miramos a las consecuencias de los ciberataques nos encontramos en numerosas ocasiones con situaciones inesperadas y de gran impacto sobre los principales sectores económicos, las infraestructuras críticas o las administraciones.

Es fácil deducir que atendiendo a las causas y efectos de un ciberataque una respuesta técnica no será suficiente, en numerosas ocasiones, para afrontar el problema con garantía de éxito, es necesario articular respuestas que abarquen desde el plano técnico-táctico al político-estratégico, igual que en cualquier ámbito de la seguridad.

Se hace necesario intentar definir lo que entendemos por incidente de ciberseguridad y por cibercrisis, cuestión esta no ausente de dificultad. Entre las

¹⁶ European Union Agency for Network and Information Security (ENISA), «The cost of incidents affecting CILs», agosto de 2016.

muchas referencias encontradas creemos que la que más se puede ajustar es la que propone *ENISA*¹⁷.

Bajo su criterio, un incidente de ciberseguridad es una interrupción de los servicios de tecnología de la información (TI) donde la disponibilidad prevista del servicio desaparece por completo o en parte. También puede ser la publicación ilegal, obtención y/o modificación de la información almacenada en los servicios de TI.

ENISA también estima que una ciber crisis es una situación anormal e inestable que amenaza a los objetivos estratégicos de una organización, la reputación o la viabilidad.

Pero este tipo de ataques, además de afectar a las relaciones económicas y políticas entre Estados, tiene un importante impacto en la percepción pública, particularmente con su difusión a través de los medios de comunicación.

Los ciberataques del siglo XXI y sus consecuencias

Prácticamente en todas las crisis que se han producido en el siglo XXI la ciberseguridad ha tenido un papel estelar. Hemos recogido algunos de los casos más conocidos y de mayor impacto, que nos pueden servir para tener una noción aproximada de los riesgos futuros a los que quizás debamos de hacer frente.

La casuística es muy extensa a tenor del propósito, los actores y alcance de los ataques, pero es fácil encontrar elementos comunes como puede ser la enorme dificultad de determinar los autores, la necesidad de contar con una eficaz colaboración internacional o realizar una adecuada gestión de la comunicación para minimizar los efectos.

El soldado de bronce de Tallin

Sin lugar a dudas, una de las crisis paradigmáticas en el ámbito de la ciberseguridad fue la sufrida por Estonia en el año 2007. La «maravilla cibernética» creada por Estonia fue gravemente amenazada tras uno de los peores acontecimientos que se recuerdan en el país¹⁸.

Todo surge con el desmantelamiento y traslado del monumento erigido en Tallin a los soldados soviéticos caídos en la II Guerra Mundial. El monumento, conocido como «el soldado de bronce», se encontraba en el centro de Tallin

¹⁷ European Union Agency for Network and Information Security (*ENISA*), «Report on Cyber Crisis Cooperation and Management», noviembre de 2014.

¹⁸ El orden mundial en el siglo XXI: Agosto de 2015, <http://elordenmundial.com/2015/08/12/estonia-ciberseguridad-europea/>.

desde 1947 y bajo este fueron enterrados los cuerpos de trece miembros del ejército rojo que combatió a los alemanes en este país.

El Gobierno estonio anunció su decisión de desmontar el monumento con el argumento de que su presencia provocaba división entre los ciudadanos. Esta situación incitó una serie de protestas violentas de grupos prorosos contra su retirada y la intervención, a favor y en contra, de varios políticos rusos y estonios en un marco de tensiones diplomáticas.

En este clima de tiranteces y protestas comenzaron a surgir los problemas. La disponibilidad de varios servicios esenciales y los principales sitios web del país fueron interrumpidos, incluyendo el Parlamento, bancos, comercios, ministerios, periódicos y emisoras de radio. Nunca antes se había atacado a todo un país y en casi todos los frentes digitales a la vez.

Los efectos de los ataques sufridos llevaron al país a una verdadera situación de crisis que golpeó a numerosos sectores, principalmente al financiero, causando daños económicos significativos. Dados los servicios afectados, se necesitó de una estrecha coordinación entre el sector público y privado para solucionar la crisis.

La ralentización del Programa nuclear iraní

Otro incidente de alto impacto fue el surgido en el marco de la crisis diplomática sobre el Programa nuclear iraní en 2005, conocido como el virus Stuxnet.

En el año 2002 se reveló la construcción, no declarada, de una planta de enriquecimiento de uranio subterránea en Natanz. En 2005 y en contra de las recomendaciones de la Comunidad Internacional, Irán reactivó su programa nuclear. Ante estos hechos, la Comunidad Internacional se planteó la posible imposición de sanciones económicas e incluso se consideró la opción de un ataque militar. Finalmente, la tensión descendió notablemente cuando en un informe de la Agencia Central de Inteligencia de los Estados Unidos (CIA) se descartaba que el Programa nuclear iraní pudiera permitir el desarrollo de armas nucleares.

En julio de 2010, según un informe publicado por una empresa de *software* de seguridad¹⁹ se descubrió un virus informático que al parecer llevaba activo desde 2005 y cuya concentración de infecciones se encontraba en Irán, lo que probablemente indicaba que este era el objetivo inicial. Concretamente, su descubrimiento dio pie a especulaciones sobre el objetivo del ataque, que habían sido infraestructuras críticas de este país, entre ellas la central nu-

¹⁹ Symantec, «W32.Stuxnet Dossier», febrero de 2011, disponible en http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

clear de Bushehr o el complejo nuclear de Natanz, puesto que aprovechaba varias vulnerabilidades de los sistemas que controlaban estas centrales.

Según las intervenciones recogidas en el Comité del Senado para Asuntos Gubernamentales de Seguridad Nacional de Estados Unidos²⁰, Stuxnet es un *malware* altamente sofisticado, con una complejidad sin precedentes y una gran amenaza para las infraestructuras críticas.

En las diversas participaciones recogidas en el Comité, se exponen una serie de interrogantes, entre ellas: la dificultad de determinar los motivos y las personas que estaban detrás de los ataques; que se trataba de un ataque complejo producido, posiblemente, a través de una infección interna y, lo último y más importante, que este tipo de ataques podría potencialmente resultar en daño físico, la pérdida de la vida, y crear una serie de incidentes con efectos en cascada que podrían interrumpir los servicios esenciales.

De acuerdo con algunas estimaciones especulativas publicadas en los medios de comunicación, el Programa iraní fue retrasado unos dieciocho meses. El retraso en el programa suponía ganar más tiempo a los esfuerzos por hallar una solución diplomática a la disputa internacional.

En 2015 se firmó el Plan de Acción Conjunto y Completo, donde Irán acordó con Estados Unidos, Rusia, China, Reino Unido, Francia y Alemania una serie de medidas para el desarrollo de un programa atómico civil, garantizando el no hacerse con un arsenal atómico²¹.

Ataques a los servicios esenciales en la Europa del Este

Otros ciberataques que han supuesto un efecto colateral importante fueron los sufridos por Georgia en 2008²² durante la guerra de Osetia del Sur. Según el informe realizado por la *United States Cyber Consequences Unit*, organismo independiente, la colaboración con las autoridades de Estonia fue esencial en la resolución de los ciberataques desde el punto de vista técnico. La razón de la petición de ayuda a Estonia fue, por un lado, por los ataques sufridos por estos en 2007, y, por otro, la falta de una organización internacional con la que ponerse en contacto para pedir ayuda.

²⁰ United States Senate Committee on Homeland Security and Governmental Affairs, «Securing Critical Infrastructure in the Age of Stuxnet», noviembre de 2010, disponible en <http://www.hsgac.senate.gov/hearings/securing-critical-infrastructure-in-the-age-of-stuxnet>

²¹ The White House Washington, «The Iran nuclear deal: what you need to know about the JCPOA», julio de 2015, disponible en https://www.whitehouse.gov/sites/default/files/docs/jcpoa_what_you_need_to_know.pdf

²² United States Cyber Consequences Unit, «Overview of the Cyber Campaign against Georgia in August of 2008», agosto de 2009, disponible en <http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>

Este mismo informe presenta las consecuencias estratégicas de la campaña cibernética como parte de un esfuerzo a largo plazo de algunos países, con el fin de poner a prueba la capacidad de respuesta internacional a los ciberataques.

Esta lección fue reforzada por los ciberataques contra Lituania a finales de junio de 2008, tras la decisión del Parlamento local sobre la prohibición de la utilización de símbolos soviéticos en reuniones públicas, y los de Kazajistán en enero de 2009, donde se produjo una cobertura internacional casi inexistente.

En este sentido merece también citarse el ciberataque a Ucrania en 2014, sufrido durante las protestas prorusas y en paralelo a la crisis de Crimea, donde los sistemas de comunicaciones quedaron fuera de servicio aislándola de las comunicaciones internas y con el mundo exterior. Otro ciberataque importante fue el sufrido en 2015²³, donde diversas centrales eléctricas del país dejaron de proporcionar sus servicios durante más de seis horas, afectando a un total de veintitrés subestaciones que dejaron de dar servicio durante horas a más de 225.000 usuarios.

Desde los ataques contra Estonia en 2007 se puso de manifiesto que este tipo de ciberataques podían causar graves problemas económicos y psicológicos en un país, sin provocar importantes respuestas internacionales.

Los ataques silenciosos y el robo de información

Otro tipo de ataques silenciosos que se han ido perpetrando a lo largo de estos años son las acciones de ciberespionaje. Desde 1999 se llevan detectando virus cuyo objetivo principalmente ha sido el robo de información: Moonlight Maze²⁴, Titan Rain²⁵, Duqu, Flame, Red October²⁶ o Gauss²⁷, son algunos de ellos.

²³ United States Homeland Security, Industrial Control Systems Cyber Emergency Response Team, «Cyber-Attack Against Ukrainian Critical Infrastructure», febrero de 2016, disponible en <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>

²⁴ Descubierto a finales de 1999, habían pasado dos años robando información clasificada del Departamento de Defensa, del Departamento de Energía, de la NASA y contratistas militares.

²⁵ Comenzó en 2003 y se refiere a la ola de ataques a las redes de defensa de Estados Unidos para el robo de información clasificada. No hay datos sobre la cantidad de datos robados, pero el ataque es considerado uno de los más grandes en la historia de espionaje cibernético.

²⁶ Descubierto en 2012 aunque llevaba cinco años actuando. El *software* malicioso se infiltró en los sistemas informáticos de distintos países con el objetivo de robar información. La mayor parte de los objetivos eran antiguos países soviéticos en Europa del Este, pero fue descubierto en países de todo el mundo.

²⁷ Descubierto en 2012 era capaz de espiar las transacciones bancarias y robar información de acceso a redes sociales, correo electrónico y mensajería instantánea. Según sus descubridores también podía servir para atacar a infraestructuras críticas.

En concreto, estos fueron lanzados principalmente contra objetivos diplomáticos, gubernamentales, científicos y empresariales robando datos de todo tipo, desde información sensible o clasificada hasta propiedad intelectual.

Pero este tipo de ataques, además de afectar a las relaciones económicas y políticas entre Estados, tiene un importante impacto en la percepción pública, particularmente con su difusión a través de los medios de comunicación.

El ciberespionaje ha impactado profundamente en las relaciones internacionales y probablemente continuará haciéndolo en el futuro. En este sentido cabe destacar el Informe Anual de la Amenaza 2016²⁸, presentado por el director de Inteligencia Nacional de los Estados Unidos en el Comité de las Fuerzas Armadas del Senado, en el cual plantea las principales amenazas para Estados Unidos y, entre ellas, las actividades maliciosas en el ciberespacio.

Apunta particularmente a la importancia de las acciones de ciberespionaje perpetradas y centradas en el robo de propiedad intelectual y secretos comerciales u otra información confidencial empresarial que permita obtener ventajas comerciales.

Asimismo, muestra especial preocupación por los ataques a los sistemas de las infraestructuras críticas, las acciones propagandísticas ciberterroristas para estimular los ataques de «lobos solitarios» o las acciones cibercriminales dirigidas al robo, la extorsión o el tráfico de drogas.

Las oportunidades del ciberespacio para la amenaza terrorista

La aparición de grupos terroristas en el ciberespacio no pasa desapercibida. La principal amenaza a la seguridad internacional ha supuesto un enorme salto cualitativo y cuantitativo para el ciberterrorismo. Así, la organización terrorista Dáesh²⁹ ha sabido utilizar las oportunidades que les brinda el ciberespacio para, por un lado, realizar actividades de propaganda, comunicaciones internas, formación y adoctrinamiento, financiación reclutamiento y obtención de información y, por otro, y aún menos desarrolladas, realizar ciberataques que causen terror³⁰.

Según unas recientes declaraciones del secretario de Estado de Seguridad³¹, la mayoría de las operaciones desarrolladas por las Fuerzas y Cuerpos de Seguridad del Estado responden a actuaciones ligadas a la propaganda, ra-

²⁸ James R. Clapper, «Statement for the Record Worldwide Threat Assessment of the US Intelligence Community», 2016, disponible en http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf

²⁹ Al-Dawla al-Islamiya al-Iraq al-Sham.

³⁰ Consejo de Seguridad Nacional, «Plan Nacional de Ciberseguridad», octubre de 2014.

³¹ Sesión inaugural del Encuentro Internacional de Seguridad de la Información, organizadas por el Instituto de Ciberseguridad Nacional, León, 2016.

dicalización y reclutamiento de esta organización terrorista a través de la Red. Asimismo, afirmó que Dáesh ha conseguido atraer a más de 30.000 combatientes extranjeros para luchar en Siria e Irak a través de las redes sociales.

Las comunicaciones de propaganda mediante el uso de internet son ampliamente conocidas. El portavoz de Dáesh, Abu Mohammad Al-Adnani, realizó en 2014 un llamamiento difundido a través de las redes sociales que incitaba a sus seguidores a cometer ataques individuales, indiscriminados y empleando cualquier vía. Este mensaje, que se convirtió en viral, ha servido de inspiración para muchos de los ataques que se han producido en el territorio europeo³². Desde entonces, Dáesh ha difundido y distribuido, a través de las redes sociales, vídeos de ejecuciones de prisioneros con el objetivo de crear terror.

Hasta finales de 2015, el Ministerio del Interior del Gobierno de España estimaba que Dáesh había difundido aproximadamente mil vídeos a través de sus cuentas de Twitter (en esa fecha se contabilizaban entre 35.000 y 75.000 cuentas gestionadas directamente por Dáesh). El 16 % de estos vídeos muestran la ejecución de rehenes y en total se habría mostrado al público el asesinato de más de mil quinientas personas.

Por otro lado el uso de la web profunda³³, en la cual la navegación es totalmente anónima, supone una oportunidad para el desarrollo de este tipo de actividades, y más concretamente el denominado internet oscuro, donde imperan actividades englobadas en el marco del mercado negro. Desde hace años se sabe de la existencia de foros extremistas pertenecientes a grupos terroristas, extremistas y radicales utilizados principalmente como medio de captación o para que usuarios se ofrezcan como candidatos para unirse a las causas. Así, también se reconoce su utilización, como parte de sus acciones de financiación, mediante la utilización de la moderna moneda virtual Bitcoin.

Ataques a la reputación e influencia política

Según recoge un comunicado oficial de la Comunidad de Inteligencia de Estados Unidos³⁴ sobre la exfiltración de *emails* de personas, instituciones y organizaciones políticas de Estados Unidos, indican, además, que los robos y

³² «si no eres capaz de encontrar una bala o un dispositivo explosivo improvisado, entonces selecciona al impío americano, francés o cualquiera de sus aliados. Golpéale la cabeza con una roca, asesínale con un cuchillo, atropéllale con tu vehículo, tírale desde un lugar elevado, estrangúlele o envenénale.»

³³ Esglobal, Daesh en la 'Deep Web': las profundidades de la Red al servicio de la 'yihad', enero de 2016, disponible en <https://www.esglobal.org/daesh-en-la-deep-web-las-profundidades-de-la-red-al-servicio-de-la-yihad/>

³⁴ Department of Homeland Security and Office of the Director of National Intelligence, «Election Security Statement», octubre de 2016, disponible en <https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement>

revelaciones están destinados a interferir en el proceso electoral en Estados Unidos con el fin de influir en la opinión pública. El comunicado expone que algunos Estados también han sufrido incidentes en sus sistemas relacionados con las elecciones sin poder indicar fehacientemente el origen.

No obstante, la Comunidad de Inteligencia y el Departamento de Seguridad Nacional estiman que sería extremadamente difícil alterar el conteo de votos o los resultados de las elecciones a través de un ciberataque, asegurando que las máquinas de votación no están conectados a internet, y que existen numerosos controles y supervisión en el proceso electoral.

Otro incidente no considerado en sí mismo como un ciberataque pero que tuvo un impacto enorme sobre la sociedad americana fue el falso anuncio, en la cuenta de Twitter de la agencia de noticias de Associated Press, de un atentado en la Casa Blanca en el que el presidente Barack Obama había sido herido en el mismo.

La cuenta de la agencia de noticias había sido *hackeada*³⁵, pero en solo tres minutos, el tiempo que tardó la agencia en anunciar el pirateo de su cuenta, el Dow Jones cayó 150 puntos, lo que causó un efecto cascada en otros índices y la caída del dólar frente al yen.

Las amenazas al sector privado

Un ejemplo del daño que este tipo de acciones pueden suponer para el sector privado son los ciberataques sufridos por Sony Pictures tras el anuncio del estreno de la película *La entrevista*, donde se parodía al líder norcoreano Kim Jong-Un. En este caso, Sony sufrió una serie de ataques que le han supuesto pérdidas de más de 200 millones de dólares³⁶ por la filtración de información estratégica para la empresa. O el del grupo financiero JP Morgan Chase³⁷, donde se comprometieron los datos de 76 millones de clientes y siete millones de negocios en Estados Unidos.

El último gran ciberataque relacionado con el robo de información ha sido el relacionado con la empresa americana de medios de comunicación y servicios de internet Yahoo, que ha sufrido el robo de más de quinientas cuentas

³⁵ *USA Today*, «AP Twitter feed hacked; no attack at White House», abril de 2013, disponible en <http://www.usatoday.com/story/money/markets/2013/04/23/stocks-gyrate-wildly-after-fake-terror-tweet/2107089/>

³⁶ *EFE*, «Pérdidas de Sony Pictures por el ciberataque superarán los 200 millones de dólares», diciembre de 2014, disponible en <http://www.emol.com/noticias/magazine/2014/12/22/695769/perdidas-de-sony-pictures-por-el-ciberataque-superaran-los-200-millones-de-dolares.html>

³⁷ *The New York Time*, «JPMorgan Chase Hacking Affects 76 Million Households», octubre de 2014, disponible en <http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues>.

con información de clientes³⁸ desde 2014. Esta información además, se ha hecho pública durante el anuncio de compra de Yahoo por parte de Verizon, el mayor operador de telecomunicaciones de Estados Unidos. Aunque la compra aún está pendiente de la autorización de los reguladores, el incidente podría afectar a un ajuste del precio de la compra.

Por último, resaltar los ataques sufridos el pasado mes de octubre por uno de los proveedores más importantes de soluciones de *DNS* (*Domain Name System*)³⁹, la compañía americana DynDNS (Dynamic Network Services, Inc.). La empresa sufrió un tipo de ataque denominado de denegación de servicios distribuida (*DDos*)⁴⁰.

Los ataques, cuyo origen aún se desconoce, podrían estar relacionados con la *botnet*⁴¹ Mirai, conexa con el Internet de las Cosas. El ataque afectó a la disponibilidad de los servicios de importantes empresas americanas, bien ralentizando el acceso a sus páginas web o incluso llegando a afectar a la disponibilidad total de algunas de ellas.

Sus efectos están por llegar. La falta de disponibilidad de los servicios de las empresas afectadas ha acarreado, con total certeza, la pérdida de ingresos, ya sea por servicios o publicidad, además de la disminución de la confianza de los usuarios y daños a su reputación. Además, Dyn DNS tendrá que hacer frente también a la pérdida de confianza de sus clientes, a demandas legales y, por supuesto, al efecto reputacional que esto conlleva. Aún no se puede traducir en cifras el coste del ataque, pero seguro que alcanzará varios millones de dólares.

Pero, además, este tipo de ataques ya se preveía. En 2002 la seguridad del sistema de nombres de dominios (*DNS*) ya se encontraba en entredicho. En este sentido, la Internet Corporation for Assigned Names and Numbers (ICANN)⁴², creó el Comité de Seguridad y Estabilidad ante la inquietud de empresas y Gobiernos por la fiabilidad del Sistema de Nombres de Dominio. Además, varios expertos ya habían avisado sobre la posibilidad de que un ataque contra los principales servidores de nombres de dominio a nivel internacional, podrían echar abajo internet por el efecto cascada que podría suponer. Una de las principales empresas de nombres de dominio negó por entonces esta posibilidad.

³⁸ *Business Wire*, «An Important Message to Yahoo Users on Security», septiembre de 2016 disponible en <http://www.businesswire.com/news/home/20160922006198/en/>

³⁹ Sistema que traduce de números (direcciones IP) a nombres a las páginas web.

⁴⁰ Ataque que busca saturar las conexiones de una web o de un servidor con peticiones aparentemente lícitas pero que en realidad provienen de equipos infectados con *software* malicioso (conocidos como *bots*), a fin de hacerlos inaccesibles.

⁴¹ Las *botnets* se forman por un conjunto de dispositivos conectados a internet (Internet de las Cosas) e infectados por algún tipo de *software* malicioso. Su control remoto permite que dichos dispositivos infectados puedan ser usados como medio para lanzar ataques.

⁴² Organismo privado que gestiona los dominios de internet.

Ataques con efectos cinéticos

A pesar de que todos estos ciberataques se encuentran dirigidos a la consecución de diferentes fines, una de las amenazas más significativas que podrían darse en un futuro no muy lejano son aquellos incidentes que podrían causar directa o indirectamente daño físico, lesión o muerte, los denominados ciberataques con efectos cinéticos⁴³. Esto es, aquellos ciberataques en los que el mundo físico y el virtual se aproximan.

Casos como el del virus Stuxnet o el reportado⁴⁴ por la Oficina Federal para la Seguridad de la Información en Alemania (BSI) sobre el daño causado en una fábrica de acero alemana, en la cual fue imposible apagar el alto horno originando un daño masivo al sistema y provocando cortes que interrumpieron la producción.

La dependencia tecnológica y la hiperconectividad, incluida la de los servicios esenciales e infraestructuras críticas, implican una ciberamenaza cinética significativa y el reto por excelencia de todo el desarrollo en ciberseguridad. Si bien los ejemplos anteriores no afectaron a vidas humanas, sí afectaron a infraestructuras que podrían ocasionar un daño físico mayor.

La gestión de crisis en el Sistema de Seguridad Nacional

Entre las principales responsabilidades del Gobierno se encuentran las de proporcionar seguridad y protección a los ciudadanos y a sus propiedades, garantizar la integridad territorial, contribuir al buen funcionamiento de los mercados y al sostenimiento de la infraestructura estratégica del país. Tanto los ciudadanos como el sector privado esperan que el Gobierno esté preparado para hacer frente a una amplia gama de posibles situaciones de crisis que pudiesen afectar a estos elementos esenciales.

La Ley de Seguridad Nacional se aprobó precisamente con el propósito de mejorar la coordinación de las diferentes Administraciones públicas en la prevención y la respuesta integral frente a situaciones de crisis de elevada complejidad, bajo la dirección del presidente del Gobierno y en el marco del Sistema de Seguridad Nacional. A estos efectos, tal y como se apunta en la introducción de este capítulo sobre la gestión de situaciones crisis, la Ley diseña un modelo de gestión que contempla la prevención, detección, respuesta, retorno a la normalidad y evaluación, basado en la gradualidad y amplia

⁴³ Applegate, Scott, «The Dawn of Kinetic Cyber». 5th International Conference on Cyber Conflict. NATO CCD COE Publications, junio de 2013.

⁴⁴ Bundesamt für Sicherheit in der Informationstechnik, «Die Lage der IT-Sicherheit in Deutschland 2014», noviembre de 2014, disponible en https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

participación de todos los actores afectados, espacio donde cobra especial sentido la colaboración público-privada.

Antes de detallar el sentido y la instrumentalización de la participación del sector privado en la gestión de las actuaciones relativas a crisis de ciberseguridad, es preciso referirse a la situación de interés de Seguridad Nacional y a la estructura orgánica que se ha establecido bajo la dirección del Gobierno para hacer frente a estas crisis.

Esta nueva situación constituye la frontera con el estado más leve de las denominadas situaciones de anomalía constitucional agrupadas en la Ley Orgánica⁴⁵ de los estados de alarma, excepción y sitio, concretamente, el estado de alarma.

Se trata de situaciones en las que, sin concurrir las circunstancias extraordinarias que dan lugar a los estados de alarma y excepción, ni requerir de la adopción de las medidas en ella contempladas, sin embargo, por la gravedad de sus efectos y la dimensión, urgencia y transversalidad de las medidas para su resolución, precisan de la coordinación reforzada de las autoridades competentes en el desempeño de sus atribuciones ordinarias, bajo la dirección del Gobierno, en el marco del Sistema de Seguridad Nacional, garantizando el funcionamiento óptimo, integrado y flexible de todos los recursos disponibles.

La situación de interés para la Seguridad Nacional se afrontará con los poderes y medios ordinarios de las distintas Administraciones públicas. En ningún caso supondrá la suspensión de los derechos fundamentales y libertades públicas en los términos previstos constitucionalmente para la declaración de los estados de excepción y sitio.

Esta categoría responde a la morfología de las crisis actuales o potenciales que se deben encarar en la sociedad del riesgo del siglo XXI, que vienen marcadas por su transversalidad, su naturaleza abierta o su incierta evolución, y a ella subyace la necesaria activación en tiempo útil de los medios necesarios del Estado, siempre primando la prevención y mitigación, en aras de proveer una actuación más ágil, modular, eficaz y eficiente.

Las actuaciones a desarrollar deben ir encaminadas a poner en marcha la estructura del Sistema de Seguridad Nacional prevista en la Ley⁴⁶ de Seguridad Nacional, en el marco de la regulación de la gestión de crisis del Título III, entendida como el conjunto ordinario de actuaciones dirigidas a detectar y valorar los riesgos y amenazas concretos para la Seguridad Nacional, facilitar el proceso de toma de decisiones y asegurar una respuesta óptima y coordinada de los recursos del Estado que sean necesarios⁴⁷.

⁴⁵ Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio.

⁴⁶ Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

⁴⁷ Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, art. 22.1.

La participación de las distintas Administraciones públicas es un principio ineludible del Sistema de Seguridad Nacional⁴⁸, y para ello el sistema contará, cuando se constituya, con la actuación cooperadora de la Conferencia Sectorial para asuntos de la Seguridad Nacional⁴⁹, así como con los mecanismos de enlace y coordinación necesarios que se determinen oportunamente, que aseguran la participación de los órganos de las autoridades competentes, para garantizar la coordinación de las actuaciones⁵⁰.

En cuanto a la estructura orgánica que la Ley de Seguridad Nacional establece en el marco del Sistema de Seguridad Nacional y su desempeño en la gestión de las actuaciones de crisis, es preciso referirse al Consejo de Seguridad Nacional, el Comité Especializado de Situación y el Departamento de Seguridad Nacional.

En su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, al Consejo de Seguridad Nacional le corresponde asistir al presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional. En este sentido, el Consejo de Seguridad Nacional se reúne a iniciativa del presidente del Gobierno como mínimo con carácter bimestral.

El Consejo es un órgano permanente de dirección de las actuaciones de gestión de crisis. Además de ser el responsable de determinar los mecanismos de enlace y coordinación necesarios para que el Sistema de Seguridad Nacional se active preventivamente y realice el seguimiento de los supuestos susceptibles de derivar en una situación de interés para la Seguridad Nacional; asesorará al presidente del Gobierno cuando la situación requiera la aplicación de medidas excepcionales previstas en los instrumentos de gestión de crisis de las organizaciones internacionales de las que España sea miembro.

En cuanto al Comité Especializado de Situación, como órgano colegiado y experto de muy alto nivel y de carácter único para el conjunto del Sistema de Seguridad Nacional, la fuerza de actuación que puede desarrollar en la gestión de ciber crisis es de singular importancia. En el desarrollo de sus funciones se le asignan cometidos que engloban: desde la valoración de las primeras acciones de alerta temprana, tan indispensable en las ciber crisis; hasta la valoración del impacto y los efectos ocurridos. Además, propondrá las directrices de una política informativa coordinada cuyo fin sea informar a la sociedad sobre la situación acontecida.

Así, y en el caso de que la situación fuese declarada situación de interés para la Seguridad Nacional, sus cometidos se amplían sobre todo en lo que se refiere a la coordinación de mecanismos y medios nacionales e internacionales.

⁴⁸ Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, art. 22.2.

⁴⁹ Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, art. 6.

⁵⁰ Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, arts. 11.1 y 18.2.

Por último, bajo la dependencia orgánica y funcional de su Director, y como órgano de asesoramiento al presidente del Gobierno en materia de Seguridad Nacional, el DSN, entre otras funciones, es el organismo permanentemente responsable de realizar el análisis de la evolución de los riesgos y amenazas a la Seguridad Nacional y de sus potenciadores.

Este análisis se realiza de una manera inclusiva y en coordinación con los órganos y autoridades competentes, así como con el sector privado, lo que le permite realizar un seguimiento continuo y constante 24 x 7 permitiéndole, con ello, realizar la alerta temprana y asesorar sobre acciones preventivas, de anticipación o de preparación en la respuesta. También es el responsable de mantener y asegurar el adecuado funcionamiento del Centro de Situación de la Presidencia del Gobierno, y las comunicaciones especiales de la Presidencia del Gobierno, así como proteger su documentación.

El DSN cumple además un importante papel de fomento de una amplia cultura de Seguridad Nacional inclusiva de la sociedad en todas sus manifestaciones y de potenciación y desarrollo de la colaboración público-privada en materia de Seguridad Nacional.

Por tanto, el DSN es un organismo llamado a establecer una acción coordinada a nivel internacional, europeo y nacional en aquellas cuestiones de nivel estratégico relacionadas con la alerta temprana y seguimiento de los riesgos, amenazas a la ciberseguridad, así como en el apoyo en la dirección y coordinación de las actuaciones de gestión de las situaciones de ciber crisis. Ejemplo de ello es su actuación como punto de contacto nacional en el ámbito del Dispositivo Integrado de Respuesta Política de la Unión Europea a las Crisis (IPCR)⁵¹.

De manera especialmente relevante, es importante partir de la premisa de que sin esta colaboración no es posible una respuesta ajustada a las crisis de ciberseguridad. Para hacer frente de forma efectiva a las eventuales situaciones de crisis que puedan provocarse, la inclusión del sector privado en actuaciones de prevención, defensa, detección, respuesta y recuperación es esencial.

Colaboración público-privada y gestión de crisis de ciberseguridad en el Sistema de Seguridad Nacional

El sector privado es uno de los principales agentes de la Seguridad Nacional. Así se encuentra recogido en la Ley de Seguridad Nacional, y así se refleja en su posible participación en el Sistema de Seguridad Nacional, tanto en la

⁵¹ Consejo de la Unión Europea, «Dispositivo Integrado de Respuesta Política de la Unión Europea a las Crisis» disponible en <http://www.consilium.europa.eu/en/documents-publications/publications/2014/eu-ipcr/>

formulación y ejecución de la política de la Seguridad Nacional, como en la gestión de crisis y la contribución de recursos.

Se debe seguir avanzando de manera coordinada en distintos aspectos de la gestión de crisis que deben materializarse a través de proyectos y actuaciones concretas, tal y como establece la Ley.

En este sentido, varias son las actividades que el Departamento de Seguridad Nacional viene desarrollando con el sector privado. En las líneas que siguen, se destacarán algunas de estas, tales como: la organización del primer seminario⁵² público-privado nacional sobre gestión de crisis en el ámbito de la ciberseguridad; la coordinación del proyecto para aumentar la ciberseguridad en el ámbito marítimo; la instrumentalización de la participación del sector privado a través de planes de actuación que contempla su colaboración e inclusión tanto en el plano estratégico, como en el operativo y táctico; la llamada de la Directiva de Seguridad de las Redes y de la Información (Directiva NIS)⁵³ a contemplar su papel en la implementación de una orgánica que abunde en el fomento de sinergias cooperativas entre los Estados miembros de la Unión Europea; el establecimiento de protocolos o la implantación de un modelo nacional de ejercicios de ciberseguridad de amplio espectro.

Respecto del seminario público-privado de ciberseguridad, al margen de la novedad de su celebración que amplifica y da voz al mensaje de que «no hay ciberseguridad real sin un sector privado bien plantado y comprometido», son varias las ideas fuerza que de un foro de este nivel se pueden extraer: la necesaria determinación de modelos de gobernanza de la ciberseguridad a nivel internacional, europeo y nacional; la ampliación del compromiso basado en la cooperación para la prevención, defensa, detección, respuesta y recuperación a los ciberataques; el aumento de la confianza entre los actores implicados para fomentar el intercambio de información; trabajar conjuntamente en las implicaciones estratégicas de la gestión de crisis; la singular importancia de los ejercicios de ciberseguridad y el necesario compromiso

⁵² Una de las actuaciones desarrolladas por el Departamento de Seguridad Nacional, en colaboración con la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), fue la organización del primer seminario público-privado nacional sobre gestión de crisis en el ámbito de la ciberseguridad.

El seminario, impartido por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) así como por el Departamento de Seguridad Nacional, tuvo como objetivo plantear las distintas implicaciones de la Ley de Seguridad Nacional para el ámbito de la ciberseguridad, además de exponer los diversos proyectos nacionales realizados tras la aprobación de la Estrategia de Ciberseguridad Nacional y la puesta en marcha del Consejo Nacional de Ciberseguridad.

⁵³ La Directiva de Seguridad de las Redes y de la Información adoptada por el Parlamento Europeo el 6 de julio de 2016 con entrada en vigor en agosto, comunicado de prensa de la Comisión Europea del 5 de julio de 2016.

para progresar en la sensibilización y concienciación mediante el desarrollo de una fuerte cultura de ciberseguridad nacional.

Asimismo, las actuaciones del Consejo Nacional de Ciberseguridad, abierto a la participación del sector privado y los órganos y organismos responsables de la ciberseguridad en España, han venido respondiendo a estas necesidades a través del ya mencionado Plan Nacional de Ciberseguridad, su marco general de desarrollo y los planes derivados de ciberseguridad.

En cuanto se refiere a la coordinación del proyecto para aumentar la ciberseguridad en el ámbito marítimo, la iniciativa parte del Consejo Nacional de Seguridad Marítima en coordinación con el Consejo Nacional de Ciberseguridad. El DSN, en colaboración con el Clúster Marítimo Español y el Instituto Nacional de Ciberseguridad, ha desarrollado un plan integral para aumentar la ciberseguridad en el sector marítimo que engloba actuaciones concretas dirigidas al sector privado que van desde la elaboración de guías de buenas prácticas sobre medidas de ciberseguridad a la organización de ejercicios de ciberseguridad en este ámbito.

Uno de los aspectos que contemplan los Planes Derivados, y punto nuclear de este artículo es el englobe de actuaciones concretas relativas a la gestión de crisis, llevadas a cabo en el marco de la colaboración público-privada, y que implican a las tres esferas que debe cubrirse en la gestión de crisis.

Para el nivel estratégico, es necesario desarrollar un Sistema Nacional Integral de Comunicación e Intercambio de Información⁵⁴ con la finalidad de crear mecanismos e instrumentos de enlace y coordinación para la prevención, detección, respuesta, retorno a la normalidad y evaluación ante situaciones de crisis en el ámbito de la ciberseguridad, esto es, un punto único de coordinación público-privado, ya contemplado en la Estrategia y en la Ley de Seguridad Nacional.

Las aportaciones de ambos sectores en el sistema, además de beneficiar el conocimiento sobre las ciberamenazas y contribuir a plantear aquellas situaciones que le alertan o le son de interés, servirá para identificar fuerzas y debilidades, analizar áreas potenciales de ciber crisis y mantener el enlace del sector privado con los organismos del Sistema de Seguridad Nacional, centrados en el Consejo de Seguridad Nacional, el Comité Especializado de Situación y el Departamento de Seguridad Nacional.

Así, también es de vital importancia el intercambio de información sobre ciberamenazas⁵⁵ en el plano operativo, dados los posibles efectos de la ejecución de ciberataques que pudieran plantearse de manera simultánea sobre los sectores públicos y privados nacionales y, especialmente, sobre las infraestructuras críticas tal y como se planteó al principio de este artículo.

⁵⁴ Actividad recogida en el «Plan de fortalecimiento y potenciación de capacidades y aseguramiento de la cooperación para la ciberseguridad y la ciberdefensa».

⁵⁵ «Plan de intercambio de información sobre ciberamenazas».

En este sentido es necesario contar con herramientas tecnológicas y mecanismos que permitan llevar a cabo este intercambio de información de manera proactiva con el sector privado y a través de puntos de contacto concretos para ello. Además, la información podrá ser sectorial, dado que las ciberamenazas no afectan de igual manera a todos los sectores y las respuestas tampoco tienen por qué serlo.

Por tanto, este mecanismo supone integrar, definir, desarrollar e implantar los procedimientos de actuación en un marco singular de colaboración directa con el sector privado. Un ejemplo de implantación de estas iniciativas ha sido la creación de la Oficina de Coordinación Cibernética del Ministerio del Interior que sirve como mecanismo de enlace entre las Fuerzas y Cuerpos de Seguridad del Estado, el Centro Nacional de Protección de Infraestructuras Críticas y el sector privado.

En el plano técnico, el fomento del intercambio de información sobre incidentes de ciberseguridad entre los sectores público y privado⁵⁶ supone la creación de sinergias significativas y el aumento de eficacia de las actividades de los Equipos de Respuesta ante incidentes de ciberseguridad públicos y privados.

La puesta en marcha de iniciativas que faciliten la cooperación en el intercambio de información de nivel técnico entre el sector público y privado, permite aumentar los niveles de prevención, defensa, detección, respuesta y recuperación a incidentes de ciberseguridad. Ejemplo de ello es el desarrollo de la herramienta ICARO⁵⁷ por el Equipo de Respuesta ante Incidentes de Ciberseguridad de Seguridad e Industria (CERTSI_)⁵⁸. Un servicio de compartición de información sobre incidentes de ciberseguridad, particularmente diseñado para el intercambio de información con el sector privado y basado en el proyecto *MISP (Malware Information Sharing Platform)*⁵⁹.

Por lo que se refiere a la cooperación en la gestión de incidentes entre los sectores público y privado⁶⁰ en el marco de la Directiva NIS, cabe recordar que la Comisión Europea presentó en febrero de 2013 la propuesta de Direc-

⁵⁶ Actividad recogida en el «Plan derivado de ciberseguridad del sector privado y la industria».

⁵⁷ Equipos de respuesta ante incidentes de Ciberseguridad de Seguridad e Industria, «Icaro» disponible en: <https://www.certs.es/servicios-operadores/icaro>

⁵⁸ El CERT de Seguridad e Industria, es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Ministerio de Industria, Energía y Turismo y del Ministerio del Interior. Operado técnicamente por INCIBE, y bajo la coordinación del CNPIC e INCIBE, el CERTSI se constituyó en el año 2012 a través de un Acuerdo Marco de Colaboración en materia de ciberseguridad entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Actualmente es regulado mediante Acuerdo de 21 de octubre de 2015, suscrito por ambas Secretarías de Estado.

⁵⁹ *Malware Information Sharing Platform*, disponible en <http://www.misp-project.org/>

⁶⁰ Actividad recogida en el «Plan derivado de ciberseguridad del sector privado y la industria».

tiva⁶¹ para su consideración por el Consejo de la Unión Europea y el Parlamento Europeo. La entonces propuesta de Directiva era una de las medidas recogidas en la *Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro*. Finalmente, y tras varios años de negociaciones, la Directiva fue adoptada por el Parlamento Europeo el 6 de julio de 2016 y entró en vigor en agosto del mismo año.

La Directiva NIS establece los requisitos mínimos comunes que deben cumplir los Estados miembros en materia de seguridad en las redes y de la información, y obliga, entre otras cuestiones, a: identificar y comunicar a la Comisión los operadores de servicios esenciales y los proveedores de servicios digitales de los Estados miembros⁶²; comunicar y notificar a la Comisión incidentes con efecto perturbador significativo; desarrollar y comunicar a la Comisión la Estrategia nacional de seguridad de las redes y sistemas de información o definir un marco de gobernanza⁶³ que se coordine con las estructuras europeas de manera que pueda aplicarse la Directiva.

Algunos de los aspectos relevantes que incluye la Directiva es la cooperación y el intercambio de información, por lo que también obliga a: cooperar a escala nacional y a escala internacional. Esta última se realizará a nivel técnico a través de la creación de una red de Equipos de Respuesta ante Incidentes de Ciberseguridad a fin de intercambiar información; a nivel estratégico con la creación del Grupo de Cooperación formado por representantes de los Estados miembros, la Comisión y ENISA. Además de definir y establecer las disposiciones legales, reglamentarias y administrativas, en coordinación con aquellos que posean competencias en la materia.

Impulsar un esquema de cooperación público-privada como el previsto por la Directiva NIS es de singular importancia a fin de identificar, prevenir y mitigar los ciberataques que puedan afectar a Europa y a España, además,

⁶¹ La Directiva de Seguridad de las Redes y de la Información adoptada por el Parlamento Europeo el 6 de julio de 2016 con entrada en vigor en agosto, «Comunicado de prensa de la Comisión Europea del 5 de julio de 2016».

⁶² Energía, transporte, banca, infraestructuras de los mercados financieros, sector sanitario, suministro y distribución de agua potable, infraestructura digital y proveedores de servicios digitales (mercado en línea, motores de búsqueda y servicios de computación en nube) y Administraciones públicas que hayan sido identificadas como operadores de servicios esenciales. Quedan excluidas: las microempresas y pequeñas empresas que sean proveedores de servicios digitales y las empresas que están sujetas a los requisitos de las Redes Públicas de Comunicaciones, así como los proveedores de servicios de confianza (firma digital, sellos de tiempo, etcétera).

⁶³ Designar una o más Autoridades Competentes que supervisarán la aplicación de la Directiva a escala nacional y estén facultadas para adoptar directrices nacionales sobre la notificación de incidentes. Designar un único punto de contacto nacional que se encargue de coordinar las cuestiones relacionadas con la seguridad de las redes y sistemas de información y de la cooperación transfronteriza a escala de la Unión. Designar uno o varios Equipos de Respuesta ante Incidentes de Ciberseguridad (CSIRT), responsables de la gestión de incidentes.

y puesto que esta obliga a la cooperación a escala nacional, la trasposición de la Directiva ayudará a implementar el modelo de gobernanza nacional.

Por otra parte, la colaboración del sector privado en las decisiones relativas a la trasposición de la Directiva son de especial relevancia y el proceso incluye la consulta pública al sector, a fin de realizarla con total eficacia y transparencia.

En cuanto a la creación del Modelo Nacional de Ejercicios de Ciberseguridad⁶⁴ y participación y ejecución de ejercicios de ciberseguridad⁶⁵, sin duda y en todo el contexto presentado, es de vital importancia que las organizaciones españolas se encuentren preparadas para hacer frente a los ciberrataques, disponiendo de los recursos más adecuados en cada momento y adaptados a cada situación.

Para verificar la idoneidad de los medios empleados en los distintos procesos de la gestión de crisis de ciberseguridad, es necesario realizar periódicamente ejercicios de ciberseguridad. En estos ejercicios deben simularse desde las distintas fases de gestión de crisis, como los distintos niveles de actuación y de toma de decisiones (niveles técnico, operacional y político-estratégico) con el fin de verificar el grado de coordinación entre instituciones responsables ante cada una de las fases y de estas con el sector privado. Asimismo, sirven para entrenar los protocolos existentes y valorar su funcionamiento, poner a prueba el conocimiento de capacidades, la comunicación y el intercambio de información entre ambos sectores, lo que favorece la creación de un marco de confianza y colaboración directa.

Para mejorar la gestión de los recursos disponibles a nivel nacional, se debe elaborar un Catálogo Nacional de Ciberejercicios que persiga el identificar áreas deficitarias a potenciar tanto por el sector público como por el sector privado, promuevan la participación de ambos sectores, al presentar una planificación coordinada y ordenada a nivel nacional y de estos con aquellos ejercicios que se desarrollen a nivel internacional y europeo.

Por último, además de las actividades señaladas anteriormente, se deben añadir aquellas recogidas en los planes que indirectamente influyen en la prevención de cibercrisis. En este sentido caben resaltar las acciones e iniciativas en marcha que persiguen aumentar la conciencia en ciberseguridad mediante el desarrollo de la Cultura Nacional de Ciberseguridad y otras complementarias que incluyen el aumento de las capacidades de inteligencia; el aumento de confianza entre sector público privado o la apuesta por el desarrollo del mercado nacional de la ciberseguridad; la I+D+i o la capacitación y formación en materia de ciberseguridad.

⁶⁴ Actividad recogida en el «Plan de fortalecimiento y potenciación de capacidades y aseguramiento de la cooperación para la ciberseguridad y la ciberdefensa».

⁶⁵ Actividad recogida en el «Plan de intercambio de información sobre ciberramenazas».

De la acción a la puesta en práctica. El ejercicio *Cyber Europe*

Finalmente, el modelo planteado y las actuaciones propuestas no funcionan si no se practican y ejercitan mediante decisiones y procedimientos simulados. Los ejercicios no solo ofrecen oportunidades para analizar los incidentes de ciberseguridad a nivel técnico, sino que, además, se puede elevar su complejidad operativa y estratégica a fin de examinar situaciones de continuidad de negocio y de gestión de crisis complejas.⁶⁶ España ha avanzado significativamente en este sentido con su participación en el ejercicio *Cyber Europe*⁶⁷.

El Ejercicio *Cyber Europe*, organizado cada dos años por la Agencia de Seguridad de las Redes y de la Información (ENISA), es el mayor ciberejercicio que se realiza a nivel mundial. En estos ejercicios se simulan incidentes de ciberseguridad a gran escala, que se intensifican hasta convertirse en una crisis de ciberseguridad a nivel europeo.

El principal objetivo de las diferentes ediciones ha sido trabajar en la cooperación y el intercambio de información a nivel europeo entre los Estados miembros y de estos con la Agencia, involucrando, asimismo, al sector privado en su ejecución.

En este sentido, el DSN, como coordinador de la participación nacional y punto único de contacto con ENISA, ha participado en las ediciones de 2010, 2012, 2014 y 2016.

Sin duda, a lo largo de estos años la coordinación y planificación nacional ha ido avanzando con una mayor implicación del sector privado. Si bien en 2010 España tan solo participó como observador, en las ediciones de 2012, 2014 y 2016 se ha evolucionado significativamente en la planificación y en una mayor colaboración y participación del sector público y del sector privado.

Dado que la edición del ejercicio *Cyber Europe* 2016 se encuentra en proceso de ejecución, sus conclusiones aún no se encuentran disponibles, pero sin duda es importante resaltar que este año España ha participado con la aportación de once empresas y los órganos y organismos con competencias en materia de ciberseguridad del sector público.

En la edición de 2014, el ejercicio fue el mayor y más completo ciberejercicio de la Unión Europea realizado hasta el momento. Su ejecución se dividió en tres fases, probando por primera vez tres niveles de respuesta a una situación de ciber crisis: el técnico; el operativo y el estratégico-político.

⁶⁶ Agencia Europea de Seguridad de las Redes y de la Información, «Cyber Exercises» disponible en <https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme>

⁶⁷ Agencia Europea de Seguridad de las Redes y de la Información, «Cyber Exercises» disponible en <https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme>



Fig. 2.1. Ejercicio Cyber Europe 2016. Fuente: ENISA.

Como lecciones aprendidas se concluyó que había que seguir avanzando en la mejora de los procedimientos de escalada a nivel estratégico, sobre todo en la cooperación internacional; la diferenciación entre las causas, el medio y las consecuencias, en cuanto a que las consecuencias deben ser gestionadas por otros organismos no relacionados con la ciberseguridad; en que el intercambio de información en el nivel técnico y operacional está fundamentalmente basado en la confianza, pero que a nivel estratégico debe plantearse bajo otro enfoque y basarse en acuerdos formales; en la utilización del *IPCR* (*Integrated Political Crisis Response*)⁶⁸, sistema para responder a crisis de nivel estratégico/político y donde existe una conexión entre todos los Estados miembros y el Consejo, y, por último, en la inexistencia de un Organismo europeo con competencias coordinadoras para la ciberseguridad.

Los retos y oportunidades que plantea la participación en este tipo de ejercicios permiten probar el nivel de cooperación, colaboración y comunicación público-privada y público-pública a distintos niveles y en tiempo real (táctico-técnico, operacional y estratégico).

Asimismo, incrementa el conocimiento sobre los recursos y capacidades para la prevención, detección y respuesta a los ciberataques y la gestión de crisis, ejercitando la gestión en la toma de decisiones para cada uno de los niveles involucrados, además de permitir practicar y coordinar la comunicación pública de forma coordinada y bajo un liderazgo único.

⁶⁸ Consejo de la Unión Europea, «Dispositivo Integrado de Respuesta Política de la Unión Europea a las Crisis» disponible en <http://www.consilium.europa.eu/en/documents-publications/publications/2014/eu-ipcr/>

Conclusiones y retos

Crisis y ciberespacio son palabras que no será raro verlas juntas en un mundo donde la tecnología y la hiperconectividad condicionan cada vez más el desarrollo de nuestra sociedad. El ciberespacio es un espacio de grandes oportunidades, si bien es imposible ocultar que en él se tensionan los intereses de los Estados con fines distintos y organizaciones terroristas y redes de crimen organizado se sirven de las facilidades que ofrece el medio.

Desde la creación del Departamento de Seguridad Nacional de la Presidencia del Gobierno, en el verano de 2012, hemos impulsado un modelo integrado de gobernanza para la ciberseguridad. Un modelo basado en la implicación de todos los actores y recursos del Estado y en la participación del sector privado y de la sociedad en general. La participación del sector privado en la Seguridad Nacional es hoy en día ineludible y, quizás, sea la ciberseguridad un ámbito paradigmático en este sentido. Así ha quedado recogido en la Estrategia de Seguridad Nacional, la Estrategia de Ciberseguridad Nacional y, sobre todo, en la Ley de Seguridad Nacional.

Quizás el aspecto más innovador de la nueva Ley se encuentre en el articulado dedicado a la gestión de situaciones de crisis y muy especialmente en la figura de la «situación de interés para la Seguridad Nacional». La nueva Ley contempla la participación de las distintas Administraciones públicas y del sector privado, para lo cual se activarán los mecanismos de enlace y coordinación del Sistema de Seguridad Nacional necesarios, centrados en el Consejo de Seguridad Nacional, el Comité Especializado de Situación y el Departamento de Seguridad Nacional.

Es verdad que hemos trabajado mucho y bien en estos últimos años pero el horizonte se vislumbra repleto de nuevos retos que seguirán requiriendo la participación decidida de todos. Entre los principales a corto plazo merecen destacarse, a nuestro juicio:

- Trasladar al plano nacional la Directiva de Seguridad de las Redes y de la Información de la Unión Europea.
- Mejorar nuestros sistemas y protocolos de intercambio de información, tanto a nivel nacional como internacional y entre el sector público y privado y a distintos niveles.
- Planear y ejecutar ciberejercicios con la participación de la Administración y del sector privado en todos los niveles de gestión de crisis.
- Desarrollar una fuerte cultura de ciberseguridad que incremente los niveles de prevención y, por tanto, una minimización del riesgo.

Las iniciativas presentadas en este capítulo nos han llevado a mejorar sustancialmente nuestras capacidades para «garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques»⁶⁹.

⁶⁹ Estrategia de Seguridad Nacional, objetivo para la ciberseguridad nacional, p. 42.

Desde el Departamento de Seguridad Nacional de la Presidencia del Gobierno seguiremos trabajando con ilusión por mejorar nuestra ciberseguridad nacional, en la idea y el propósito de que se trata de un proyecto compartido, de todos y para todos.

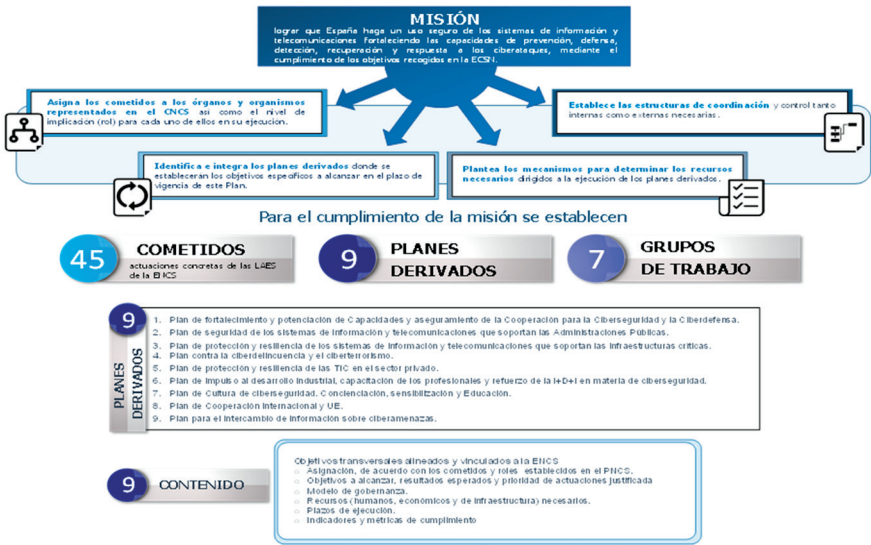


Fig. 2.2. Estructura del plan nacional de ciberseguridad

TABLA 2.1. Planes derivados de ciberseguridad

N.º	NOMBRE DEL PLAN DERIVADO
1	Plan de fortalecimiento y potenciación de capacidades y aseguramiento de la cooperación para la ciberseguridad y la ciberdefensa.
2	Plan de seguridad de los sistemas de información y telecomunicaciones que soportan las Administraciones públicas.
3	Plan de protección y resiliencia de los sistemas de información y telecomunicaciones que soportan las infraestructuras críticas.
4	Plan contra la ciberdelincuencia y el ciberterrorismo.
5	Plan de protección y resiliencia de las TIC en el sector privado.
6	Plan de impulso al desarrollo industrial, capacitación de los profesionales y refuerzo de la I+D+i en materia de ciberseguridad.
7	Plan de cultura de ciberseguridad. Concienciación, sensibilización y educación.
8	Plan de cooperación internacional y Unión Europea.
9	Plan para el intercambio de información sobre ciberamenazas.

TABLA 2.2. Líneas de acción de la estrategia nacional de ciberseguridad

LÍNEA DE ACCIÓN		OBJETIVOS
1	Capacidad de prevención, detección y respuesta ante las ciberamenazas	Incrementar las capacidades de prevención, defensa, detección, explotación, análisis, recuperación, respuesta y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional.
2	Seguridad de los Sistemas de Información de las Administraciones públicas	Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados.
3	Seguridad de las Redes y los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas	Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales.
4	Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia	Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.
5	Seguridad y resiliencia de las TIC del sector privado	Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.
6	Conocimientos, competencias e I+D+i	Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i para la ciberseguridad.
7	Cultura de ciberseguridad	Concienciar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.
8	Compromiso internacional	Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales.

Capítulo tercero

Análisis de las ciberamenazas

Aníbal Villalba Fernández

Doctor en Ciencias Políticas y Sociología, UNED

Asesor del Presidente del Consejo Nacional de Ciberseguridad

Juan Manuel Corchado Rodríguez

Doctor en Informática, Universidad de Salamanca

Doctor en Inteligencia Artificial, University of the West of Scotland

Catedrático Ciencias de la Computación e Inteligencia Artificial, Universidad de Salamanca

Vicerrector de Investigación y Transferencia, Universidad de Salamanca

Director del Parque Científico de la Universidad de Salamanca

Member of the Advisory Group on Online Terrorist Propaganda of the European

Counter Terrorism Centre (ECTC)

Resumen

El ciberespacio ha introducido una nueva dimensión en las sociedades, favoreciendo el progreso gracias a las nuevas tecnologías y al uso extensivo de internet. No obstante, esta situación presenta nuevos retos a los que no se sustraen los diferentes actores políticos, principalmente los Estados. Entre estos desafíos se encuentran el ciberespionaje; las acciones de grupos terroristas y de corte yihadista; la ciberdelincuencia; y la protección y recuperación de los sistemas de infraestructuras críticas, entre otros.

España se ha dotado de un Consejo Nacional de Ciberseguridad, que preside el secretario de Estado director del Centro Nacional de Inteligencia; en cuya persona recae además la Autoridad Nacional para la protección de la información clasificada —que dispone de la Oficina Nacional de Seguridad—; la Autoridad Nacional de Inteligencia y Contrainteligencia; y la dirección del Centro Criptológico Nacional, que cuenta con el CERT Nacional Gubernamental CCN-CERT, con responsabilidad en la protección ante ciberataques sobre sistemas clasificados de las Administraciones públicas; y de empresas y organizaciones de interés estratégico.

Palabras clave

inteligencia, ciberespacio, ciberamenazas, riesgos, amenazas, ciberseguridad, ciberataques, CERT.

Abstract

Cyberspace has introduced a new dimension in societies, favoring progress thanks to new technologies and the extensive use of the Internet. However, this situation presents new challenges to which different political actors, especially States, do not escape. Among these challenges are cyber espionage, the actions of terrorist and jihadist groups, cybercrime, and the protection and recovery of critical infrastructure, among others.

Spain has been endowed with a National Cybersecurity Council, chaired by the Secretary of State Director of the National Intelligence Center; in whose person also falls the National Authority for the protection of classified information—which has the National Security Office—; the National Intelligence and Counterintelligence Authority; and the direction of the National Cryptological Center, which has the National Government CERT CCN-CERT, with responsibility in the protection against cyber attacks on classified systems, Public Administrations; and of companies and organizations of strategic interest.

Keywords

intelligence, cyberspace, cyber threats, risks, threats, cybersecurity, cyber attacks, CERT.

Introducción

El ciberespacio ha introducido una nueva dimensión en las sociedades, y su uso se ha incorporado a las mismas de modo cotidiano y generalizado. Gracias a las nuevas tecnologías y al uso extensivo de internet, se están desarrollando proyectos que abarcan las áreas más diversas de las actividades humanas. Los adelantos en las comunicaciones y el abaratamiento de los costes están generando una red en la que pocos elementos escapan a estar conectados, incluso los objetos de uso cotidiano, en lo que se ha venido a llamar el Internet de las Cosas.

Los aspectos positivos de la utilización del ciberespacio son numerosos. La generación de nuevas capacidades en campos como las comunicaciones, la investigación científica, los procesos industriales o la gestión del conocimiento son evidentes. Además, el acceso de modo casi generalizado a las redes ha constituido un escenario rico en oportunidades para una gran parte de la población. Esta revolución tecnológica y su impacto social están conformando un escenario que impregna la vida de las sociedades. No obstante, esta situación presenta nuevos retos a los que no se sustraen los diferentes actores políticos, principalmente los Estados. Entre estos desafíos se encuentran la protección y recuperación de los sistemas de infraestructuras críticas ante agresiones que utilizan el ciberespacio como entorno y vehículo para interferir en las actividades de los ciudadanos y de las instituciones.

De esta forma, hoy en día los Estados deben hacer frente a ataques contra la seguridad de los sistemas de las Tecnologías de la Información y las Comunicaciones (TIC) de gobiernos, administraciones públicas y empresas con alto valor estratégico. Esta situación ha conformado un nuevo escenario, que precisa atención de los diferentes actores políticos para adaptarse adecuadamente.

Los riesgos y amenazas derivados de la utilización del ciberespacio han generado además discusiones relacionadas con la soberanía. La nueva dimensión que aporta el ciberespacio ha desdibujado las fronteras tradicionales, abriendo un debate acerca de las responsabilidades de los Estados. Aspectos como la deslocalización de los ciberataques y la dificultad de atribución de responsabilidades, dibujan un nuevo escenario relacionado con su interacción y con los intereses nacionales.

España no ha permanecido inmune a las agresiones que utilizan el ciberespacio para atentar contra los más variados aspectos de la seguridad, llegando a verse comprometidos servicios críticos y otros aspectos que afectan a la seguridad nacional.

En este escenario, se han desarrollado diferentes medidas de carácter político, de planeamiento estratégico de la ciberseguridad y de creación de estructuras organizativas y de carácter técnico, con el objetivo de hacer frente a los desafíos que el uso del ciberespacio presenta para la seguridad nacional.

En el ámbito del planeamiento de la seguridad nacional en España, cabe destacar la aprobación por el Consejo de Ministros, el 24 de junio de 2011, de la primera estrategia de seguridad nacional en España: «Estrategia Española de Seguridad. Una responsabilidad de todos», donde por vez primera se incorpora la ciberseguridad a los niveles superiores de planeamiento estratégico nacional.

Esta estrategia se actualizó con la aprobación por el Consejo de Ministros, el 31 de mayo de 2013, de la «Estrategia de Seguridad Nacional. Un proyecto compartido». Como señala la referencia del Consejo de Ministros: «la Estrategia de 2013 concibe la Seguridad Nacional de una forma amplia y global, por lo que incluye muy distintos ámbitos de actuación. Tradicionalmente, el concepto de Seguridad Nacional se ceñía a la defensa y la seguridad pública, pero hoy se extiende a nuevos actores y amenazas y, por ello, la Seguridad Nacional hace frente a nuevos riesgos como las ciberamenazas».

En este sentido, la Estrategia de Seguridad Nacional de 2013 contempla hasta doce riesgos para nuestra seguridad: conflictos armados, terrorismo, ciberamenazas, crimen organizado, inestabilidad económica y financiera, vulnerabilidad energética, flujos migratorios irregulares, armas de destrucción masiva, espionaje, emergencias y catástrofes naturales, vulnerabilidad del espacio marítimo y vulnerabilidad de las infraestructuras críticas y servicios esenciales.

Es interesante señalar que, aunque las ciberamenazas se contemplan como un riesgo en sí mismas, se encuentran presentes en prácticamente todo el resto de riesgos identificados, en mayor o menor medida, a excepción de los flujos migratorios irregulares y las emergencias y catástrofes naturales. Este carácter transversal de las ciberamenazas ha llevado al desarrollo de estrategias específicas en ámbitos que se consideran prioritarios. Además de la Estrategia de Ciberseguridad Nacional, es de destacar el componente de ciberseguridad de que se dotan las Estrategias Nacionales de Seguridad Marítima y de Seguridad Energética.

El Consejo de Seguridad Nacional ha creado también diferentes Comités especializados, ligados al desarrollo de las estrategias, entre ellos, el Consejo Nacional de Ciberseguridad. El Consejo Nacional de Ciberseguridad (CNCS) se constituyó formalmente el 24 de febrero de 2014, según decisión del Consejo de Seguridad Nacional de 5 de diciembre de 2013, que creó este comité especializado en ciberseguridad en la estela de la aprobación de la Estrategia Nacional de Ciberseguridad en esa misma fecha. El CNCS se encuentra compuesto por representantes de diferentes ministerios que tienen competencia en ciberseguridad en España, y su función principal consiste en desarrollar las líneas de acción y los cometidos especificados en la Estrategia Nacional de Ciberseguridad.

En este tiempo, el CNCS ha elaborado un Plan Nacional de Ciberseguridad, que desarrolla la Estrategia Nacional de Ciberseguridad, el cual fue aproba-

do por el Consejo de Seguridad Nacional el 14 de octubre de 2014. El Plan Nacional de Ciberseguridad, a su vez, establecía la necesidad de incorporar de modo integral los elementos relacionados con la ciberseguridad que son competencia, en diferentes ámbitos, de distintos organismos. De esta forma, el 14 de julio de 2015, el Consejo Nacional de Ciberseguridad aprobó los nueve Planes Derivados del Plan Nacional de Ciberseguridad,

El secretario de Estado director del Centro Nacional de Inteligencia (SED CNI) es, desde su creación, el presidente del Consejo Nacional de Ciberseguridad. Además, la Autoridad Nacional para la protección de la información clasificada recae en la persona del SED CNI, que es, asimismo, el director del Centro Criptológico Nacional (CCN). El SED CNI también es la Autoridad Nacional de Inteligencia y Contrainteligencia.

El CNI, como Servicio de Inteligencia de España, proporciona al Gobierno elementos de juicio para facilitar su toma de decisiones estratégicas, lo que incluye el ámbito de la ciberseguridad. Para llevar a cabo su misión utiliza los procesos, procedimientos y herramientas que distinguen a un Servicio de Inteligencia, de carácter técnico y humano, dentro y fuera del territorio nacional; así como el intercambio de información y análisis de inteligencia con otros Servicios de Inteligencia extranjeros. En el caso de las ciberamenazas, además de la obtención y análisis propios, cobra un especial valor la relación con otros Servicios, al tener las ciberamenazas un carácter global.

La Autoridad Nacional para la protección de la información clasificada, dispone de un órgano de trabajo, la Oficina Nacional de Seguridad (ONS). La ONS tiene por misión fundamental la de velar por el cumplimiento de la normativa relativa a la protección de la información clasificada tanto nacional como aquella que es entregada a la Administración o a las empresas en virtud de Tratados o Acuerdos internacionales suscritos por España. En el ámbito de la ciberseguridad, la ONS colabora para la protección de los sistemas y de la propia información clasificada ante las ciberamenazas.

El Centro Criptológico Nacional (CCN) es el organismo responsable de coordinar la acción de los diferentes organismos de la Administración para que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

En este escenario, en relación con las ciberamenazas, cobra un valor especial la labor del CCN-CERT, que constituye la capacidad de respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el Real Decreto 421/2004 de regulación del CCN y en el Real Decreto 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad, modificado por el Real Decreto 951/2015 de 23 de octubre.

De acuerdo a esta legislación, el CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones públicas y de empresas y organizaciones de interés estratégico para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional para que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

EL CCN-CERT viene desarrollando, desde el año 2008, un Sistema de Alerta Temprana (SAT) que busca actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance. Este sistema para la detección rápida de incidentes y anomalías dentro de la Administración y de las empresas de interés estratégico, se enmarca dentro de las acciones preventivas, correctivas y de contención realizadas por el CERT Gubernamental Nacional. El SAT cuenta con dos vertientes con un denominador común: la detección temprana de intrusiones. En ambos casos existe un portal de informes al que los responsables de seguridad autorizados pueden acceder para la consulta en tiempo real de eventos de seguridad y para la generación de informes a medida¹.

El CCN-CERT da servicio también a la red SARA (Sistema de Aplicaciones y Redes para las Administraciones) que es un conjunto de infraestructuras de comunicaciones y servicios básicos que conecta las redes de las Administraciones públicas españolas e instituciones europeas facilitando el intercambio de información y el acceso a los servicios.

La información que se facilita en este capítulo, cuando no exista una referencia específica, proviene de la obtención y análisis propios del CNI, ONS, y –especialmente– del CCN-CERT.

Las ciberamenazas en el contexto de los riesgos globales

Es interesante situar los ciberataques en perspectiva con otros riesgos globales. El Foro Económico Mundial ha publicado el estudio «Riesgos Globales 2016»² en el que ofrece un análisis de la percepción del impacto y de la probabilidad de los riesgos globales.

En su 11.^a edición, el Informe Riesgos Globales 2016 destaca las formas en las que los riesgos globales podrían evolucionar e interactuar en la próxima década. El año 2016 marca un claro punto de quiebre con respecto a resultados anteriores, ya que los riesgos sobre los que el informe ha estado alertando durante la última década están empezando a manifestarse de

¹ Véase la información facilitada por el CCN-CERT en <https://www.ccn-cert.cni.es/gestion-de-incidentes/sistema-de-alerta-temprana-sat.html> consulta: 31 de octubre de 2015.

² World Economic Forum: *The Global Risks Report 2016; 11th Edition*. <http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf>

formas nuevas y en ocasiones inesperadas y a afectar a las personas, las instituciones y las economías.

Señala el informe que los delitos cibernéticos cuestan a la economía mundial aproximadamente 445.000 millones de dólares, lo que supera los ingresos de Chile. En este contexto, el informe hace un llamamiento a la creación de resiliencia (el «imperativo de resiliencia») e identifica ejemplos prácticos sobre cómo podría lograrse.

Entre los riesgos globales que siguen siendo importantes debido a su impacto combinado y probabilidad se encuentran algunos riesgos económicos, como por ejemplo las crisis fiscales en economías clave y un alto desempleo estructural o subempleo. Estos se encuentran complementados por los ciberataques y una profunda inestabilidad social. El informe también analiza los riesgos y tendencias globales emergentes, señalando como el cambio climático, las desigualdades económicas y el aumento de la ciberdependencia.

En este estudio del Foro Económico Mundial se refleja la probabilidad y el impacto de los riesgos individuales. Los ciberataques se encuentran en cuarto lugar en la combinación entre su probabilidad e índice de impacto. Los riesgos asociados a los ciberataques son superados solo, en relación a la combinación de ambos parámetros, por la negativa adaptación al cambio climático, las crisis relacionadas con el agua y las migraciones involuntarias

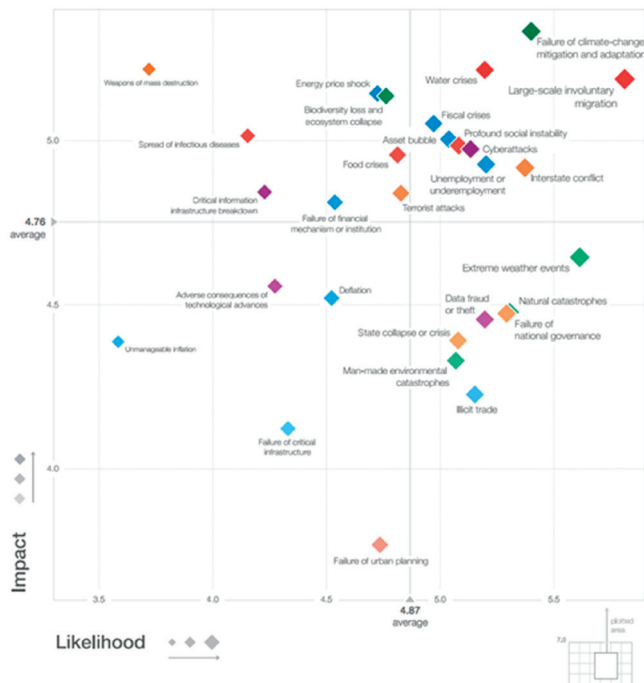


Figura 3.1. Mapa de riesgos globales 2016.
Fuente: World Economic Forum: The Global Risks Report 2016, p 3.

a gran escala. En relación con el anterior informe de 2015, los ciberataques han superado a dos riesgos que se encontraban por delante: el desempleo y los conflictos entre Estados. De este paisaje de riesgos globales se desprende la percepción de la alta probabilidad y el elevado impacto de los ciberataques en comparación con el resto de riesgos globales.

El mencionado *Informe de Riesgos Globales 2016* ofrece también un mapa de interconexión de los riesgos, donde se puede observar que continúa, como en la edición anterior, la conexión directa de los ciberataques con otros riesgos tecnológicos como la ruptura de la infraestructura de información crítica, el mal uso de las tecnologías, el fraude y el robo de datos. También existe un enlace directo con un riesgo que en el informe se asocia a la economía, el fallo en las infraestructuras críticas. El resto de conexiones directas con otros riesgos caen en el ámbito de los riesgos denominados geopolíticos, ataques terroristas, fallo de la gobernanza nacional y conflictos entre Estados.

En el caso de los riesgos asociados al uso del ciberespacio, se observa en el gráfico que las conexiones de segundo nivel alcanzan a otros riesgos que tienen unos niveles elevados tanto de probabilidad como de peligrosidad, y que se incorporan a áreas económicas, sociales, ambientales y de riesgos geopolíticos.

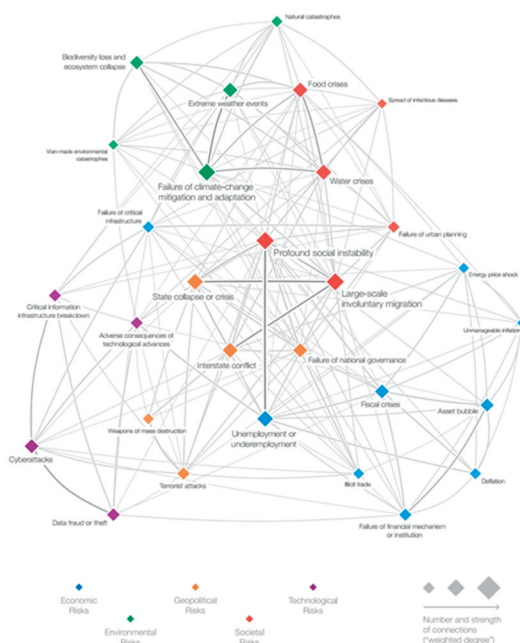


Figura 3.2. Mapa de interconexiones de riesgos globales 2016. Fuente: World Economic Forum: The Global Risks Report 2016, p 4.

Elementos esenciales en el análisis de las amenazas

La metodología empleada por el CCN-CERT, en el informe anual *Ciberamenazas 2015. Tendencias 2016*, señala como elementos esenciales a tener en cuenta para desarrollar un análisis coherente de las ciberamenazas los siguientes:

- 1. Intereses.** Aquello que puede verse afectado por ciberataques contra las dimensiones de la seguridad: confidencialidad, disponibilidad, integridad, trazabilidad y autenticidad de la información tratada o los servicios prestados. ¿Qué intereses españoles, de sus socios o aliados, están viéndose afectados negativamente y en qué medida, por las restricciones de la disponibilidad de las tecnologías de la información y la comunicación (TIC), la pérdida de la confidencialidad de la información tratada o la agresión a la integridad de la información?
- 2. Amenazas.** Agentes de la amenaza y objetivos: determinación de los eventos, circunstancias o actividades que, llevadas a cabo por los diferentes atacantes, pueden afectar a los intereses nacionales (o internacionales) considerados. ¿Qué tipo de actividades podrían llevar a cabo los atacantes o qué situaciones podrían darse, que pudieran afectar al normal desenvolvimiento de las TIC, en cualquier entorno? Esta cuestión incluye el examen de las herramientas usadas para todo ello, así como las tendencias observadas.
- 3. Resiliencia.** Determinación de en qué medida los sistemas de información han sabido afrontar los ciberataques, así como las medidas que se han adoptado o están siendo adoptadas para mitigarlos. Obviamente,



Figura 3.3. Diagrama de elementos para análisis de ciberamenazas.
Fuente: CCN-CERT. Ciberamenazas 2015. Tendencias 2016, p. 14.

la resiliencia consiste tanto en la ausencia de vulnerabilidades, como en la adopción de medidas que incrementen la fortaleza de los sistemas frente a agresiones.

En el análisis de las ciberamenazas se aplican a estos elementos un esquema en el que se incluyen dos nuevas metacaracterísticas: la sociopolítica, que vincula al adversario con su víctima y la tecnológica, que vincula la infraestructura con la capacidad.



Figura 3.4. Metacaracterísticas aplicadas a los elementos en las ciberamenazas. Fuente: CCN-CERT. Guía CCN-STIC 425 Ciclo de Inteligencia y Análisis de Intrusiones.

Evolución tecnológica y ciberseguridad

Probablemente nos encontremos lejos del denominado punto de saturación de las TIC. Es de esperar todavía mayores tasas de crecimiento gracias a la miniaturización de los elementos tecnológicos y el desarrollo de redes y sistemas inteligentes.

La presencia de la tecnología en todo tipo de dispositivos (automóviles, equipos médicos, etcétera) los hacen igualmente vulnerables, provocando que la superficie de ataque esté en permanente crecimiento, y esta es una situación que, además, no tiene vuelta atrás: cada vez hay menos medios analógicos sustitutivos de los medios digitales.

La industria sabe muy bien que aquellos proveedores que descuidan innovación y competitividad corren el riesgo de ser expulsados del mercado. Esta realidad se traduce en un incremento de la presión para situarse por encima de la competencia, lo que no siempre permite conciliar adecuadamente las necesidades de seguridad de los usuarios finales con los intereses económicos.

La tendencia actual hacia la masiva utilización de los sistemas dirigidos por *software* (*software-driven systems*) escenifica el conflicto entre funcionalidad y seguridad. El término viene describiendo la tendencia hacia arquitecturas en las que los sistemas, redes, almacenamiento, etcétera no están estáticamente definidos y constreñidos por el *hardware* utilizado sino que se pueden configurar de forma dinámica mediante el *software* adecuado. Los beneficios de esta evolución son claros: los recursos se pueden mover rápidamente y a menor coste allí donde se necesitan. Sin embargo, esta tendencia puede entrar en clara confrontación con un concepto de seguridad sustentado en la separación de los procesos y sistemas clave. En un entorno dinámico *software-driven*, esta separación no puede efectuarse con la misma profundidad técnica que usando arquitecturas tradicionales, lo que hace imprescindible el uso de plataformas específicas que faciliten la separación virtual de entornos de manera segura.

De otra parte, la tendencia en el uso de los dispositivos móviles sigue en aumento. En el sector privado han venido comercializándose nuevos tipos de dispositivos que se van incorporando a la vida cotidiana y se suman al masivo despliegue de teléfonos inteligentes y *tablets*. Estos últimos, que ya forman parte del equipamiento estándar de los profesionales, se han incorporado a procesos corporativos tratando en ocasiones información sensible, lo que genera especiales medidas de seguridad para proteger aquella información corporativa especialmente valiosa.

En numerosas ocasiones la conciliación entre la utilización de productos modernos y seguros y la compatibilidad que deben poseer se torna una tarea difícil. Frecuentemente, la incorporación de medidas de seguridad a tecnologías tradicionales es un proceso lento que no permite siempre el desmantelamiento oportuno de aquella tecnología. Un ejemplo de esto es el protocolo TLS/SSL¹⁴, muy utilizado en internet para el cifrado del tráfico de datos. Muchos servidores *online* están configurados para permitir el uso de métodos criptográficos inseguros, al objeto de garantizar el acceso a una porción significativa de usuarios que pueden seguir usando navegadores con versiones sin actualizar. Otro ejemplo significativo es el uso de sistemas operativos para los que el fabricante ya no proporciona actualizaciones de seguridad.

De otra parte, se ha generado una cierta pérdida de confianza en los servicios electrónicos entre los usuarios, debido en buena parte a constantes y alarmantes informaciones sobre brechas de seguridad. Las razones más importantes esgrimidas por los usuarios han sido esencialmente las inadecuadas garantías de privacidad, lo que ha llevado a que determinados proveedores de servicios de mensajería hayan empezado a ofrecer a sus usuarios un cifrado extremo-a-extremo de forma que ni siquiera tales proveedores puedan tener acceso a los mensajes intercambiados.

La utilización de las TIC en nuevas áreas de aplicación y las vulnerabilidades de los sistemas utilizados, el denominado Internet de las Cosas, podría

tener un impacto importante en el normal desenvolvimiento de la vida cotidiana. Un buen ejemplo lo constituye el ataque del 21 de octubre de 2016, que dificultó el acceso a una serie de servicios en la red por causa de un importante ataque de denegación de servicio distribuido (*DDoS*) vertido contra la empresa de servicios de DNS Dyn, y que afectó a actores como Twitter, Spotify, Reddit, SoundCloud, Airbnb o Github, entre muchos otros. Este *DDoS* concentró un gran conjunto de peticiones de acceso a Dyn con el fin de colapsar el servicio. Para ello se utilizaron múltiples dispositivos —cámaras IP y otros— infectados con *malware* que permitía al atacante tener control del sistema, creando una red zombi o *botnet* (red de robots). Estos dispositivos suelen tener unas claves de seguridad generales y el *software* o el *firmware* no suele estar actualizado, lo que facilita el acceso a intrusos y su control de forma remota.

En lo relativo a los medios de transporte —automóviles, aeronaves y otros— se está incorporando a los mismos un amplio catálogo de componentes TIC, potencialmente sujetos a fallos, no es de extrañar, por tanto, que las tendencias en la instalación de tales tipos de dispositivos pase actualmente por separar adecuadamente las redes que conectan los sistemas de estos vehículos, que afectan a la seguridad, respecto a aquellos otros no directamente relacionados con la seguridad. No obstante, a pesar del establecimiento de redes separadas, no es descartable la explotación de vulnerabilidades. Obviamente, el desarrollo de los coches autónomos incrementará los problemas de seguridad en el futuro.

En el sector sanitario, la presencia de sistemas TIC vulnerables puede tener graves consecuencias, ya que cada vez son más los dispositivos médicos que pueden administrarse de forma remota, a través de conexiones *WiFi* o *Bluetooth*.

Como consecuencia de la penetración de las TIC en todos los sectores de la vida social, política, administrativa o económica de un país, la existencia de alternativas analógicas está desapareciendo de una manera rápida. Esta realidad hace a los sistemas TIC especialmente importantes, sistemas que, en muchos casos, son enormemente más complejos que sus antecesores analógicos y que suelen estar conectados a internet, lo que aumenta su riesgo.

Otro aspecto muy significativo es la dependencia tecnológica de las Infraestructuras Críticas respecto a la utilización de los medios electrónicos y la interconexión de sistemas. La prestación de sus servicios depende cada vez más de un correcto funcionamiento de las TIC. Un fallo o disfunción de cualquiera de sus componentes podría dar lugar, bajo determinadas circunstancias, a limitar o impedir tal prestación. Por otro lado, las interdependencias entre sectores o industrias individuales aumentan aún más los riesgos. Los fallos en un sector pueden propiciar fallos en otros sectores provocando un efecto dominó.

Los puntos siguientes tratan de esquematizar el nivel de amenazas específico contra las Infraestructuras Críticas.

1. En general puede afirmarse que no existe diferencia entre el nivel de amenaza que soportan las Infraestructuras Críticas u otro tipo de organizaciones, salvo en lo relativo al ciber sabotaje o el terrorismo, que ofrecen características distintas toda vez que el objetivo de los atacantes sea provocar el mayor daño social posible.
2. La amenaza de la ciberdelincuencia es particularmente relevante para el sector financiero y el de seguros. Los delitos perpetrados van desde el robo de identidades a los ciberataques a las infraestructuras técnicas de las instituciones financieras pasando por la mera extorsión.
3. Es muy frecuente que los ataques realizados por grupos *hacktivistas* –grupos de *hackers* que utilizan el activismo político o social– se desarrollen contra empresas de medios de comunicación (desfiguraciones o emplazamiento de informaciones incorrectas en los sitios web de los medios secuestrados), energía y sector financiero.
4. El ciber sabotaje es una amenaza permanente. Desde Stuxnet, se ha sabido que el sabotaje de las infraestructuras por medio de ciberataques no es solo posible sino real. El ataque contra el grupo audiovisual francés *TV5Monde* o las interrupciones de fluido eléctrico en Ucrania son ejemplos de este tipo de ataques.
5. La posibilidad de ciberataques con origen en otros Estados representa una amenaza real para la economía de cualquier país desarrollado.
6. No solo los ataques dirigidos representan una amenaza para las Infraestructuras Críticas. También los ataques no dirigidos con código dañino pueden interrumpir la operación de tales infraestructuras. Por ejemplo, los problemas detectados de *ransomware* en instituciones sanitarias.
7. El crecimiento de las redes que gestionan Infraestructuras Críticas supone el crecimiento correlativo de posibles vulnerabilidades.
8. Es muy difícil señalar qué sector en concreto está afectado por tal o cual amenaza. Un ataque dirigido contra un sector determinado también puede afectar inadvertidamente a otro sector, por ejemplo si ambos utilizaran los mismos protocolos o el mismo *software*.

Como ejemplo del impacto de un ciberataque contra una infraestructura crítica, el director general del Organismo Internacional de Energía Atómica (OIEA), Yukiya Amano, ha desvelado en octubre de 2016 que una central nuclear fue el objetivo de un ciberataque hace dos o tres años y que existe una seria amenaza de más ciberataques contra estas instalaciones nucleares. Señalaba Amano que «este tema de ataques cibernéticos a instalaciones o actividades relacionadas con el uso de la energía nuclear debe tomarse muy en serio. Nunca sabemos si lo sabemos todo o si es la punta del iceberg». Amano se negó a dar detalles de cualquiera de los incidentes, pero dijo que el ataque cibernético había causado «alguna interrupción» en la planta,

aunque no resultó ser muy grave ya que la planta no tuvo que cerrar sus operaciones³.

Ciberamenazas, agentes y objetivos

El cuadro que muestra la siguiente figura muestra la relación entre los orígenes de las ciberamenazas, sus objetivos y el nivel de peligrosidad.

Objetivos				
Origen de la amenaza	Sector Público	Sector Privado	Ciudadanos	
Estados	Ciberspionaje político	Ciberspionaje económico	Ciberspionaje instrumental	
	Cibercapacidades ofensivas	Cibercapacidades ofensivas		
Ciberdelincuentes	Sustracción, publicación o venta de información	Sustracción, publicación o venta de información	Sustracción, publicación o venta de información	
	Manipulación de información	Manipulación de información	Manipulación de información	
	Interrupción de sistemas	Interrupción de sistemas	Interrupción de sistemas	
	Toma de control de sistemas	Toma de control de sistemas	Toma de control de sistemas	
Grupos terroristas	Interrupción de Sistemas / Toma de control	Interrupción de Sistemas / Toma de control		
Grupos yihadistas	Interrupción de Sistemas / Toma de control	Interrupción de Sistemas / Toma de control		
	Desfiguraciones	Desfiguraciones		
			Propaganda y reclutamiento	
Cibervándalos y script kiddies	Sustracción de información	Sustracción de información	Sustracción de información	
	Interrupción de sistemas	Interrupción de sistemas		
Hacktivistas	Sustracción y publicación de la información sustraída	Sustracción y publicación de la información sustraída		
	Desfiguraciones	Desfiguraciones		
	Interrupción de sistemas	Interrupción de sistemas		
	Toma de control de sistemas	Toma de control de sistemas		

³ Reuters, IAEA chief: Nuclear power plant was disrupted by cyber attack, 10 de octubre de 2016. <http://www.reuters.com/article/us-nuclear-cyber-idUSKCN12A10C>

Actores internos	Sustracción, publicación o venta de información	Sustracción, publicación o venta de información	
	Interrupción de sistemas	Interrupción de sistemas	
Ciberinvestigadores	Recepción y publicación de información	Recepción y publicación de información	
Organizaciones privadas		Sustracción de información (espionaje industrial)	Uso/abuso o reventa de información de clientes

Nivel de peligrosidad:

Bajo: - No se han observado nuevas amenazas o tendencias, o - Se dispone de medidas suficientes para neutralizar la amenaza, o - No ha habido incidentes especialmente significativos en el periodo analizado.	Medio: - Se han observado nuevas amenazas o tendencias, o - Se dispone de medidas (parciales) para neutralizar la amenaza, o - Los incidentes detectados no han sido especialmente significativos.	Alto: - Las amenazas o su tendencia se ha incrementado significativamente. - Las medidas adoptadas tienen un efecto muy limitado, por lo que la amenaza permanece. - Los incidentes detectados han sido especialmente significativos.

Figuras 3.5.1. y 3.5.2. Matriz de ciberamenazas. Fuente: Centro Nacional de Ciberseguridad de los Países Bajos: *Cyber Security Assessment Netherlands 2016*, 24 de octubre de 2016, p. 12. Con elaboración propia.

Los agentes de las ciberamenazas

Actores estatales

La posición de los Estados, como elementos activos o pasivos de los ciberataques, no es irrelevante para valorar el impacto de la ciberseguridad mundial. Sus actitudes, sus compromisos y sus respuestas pueden adoptar formas diferentes.

Todos los Estados occidentales, en mayor o menor medida, son objeto de ciberataques con origen en otros Estados, interesados en obtener información de relevancia económica, geoestratégica o militar.

Los ciberataques constituyen uno de los marcos de acción preferidos por su bajo coste si se compara con los importantísimos beneficios que pueden obtenerse, lo limitado de los riesgos asumidos y la dificultad de determinar sus autores. No se puede pasar por alto que este tipo de acciones permite que la infraestructura tecnológica de un tercer país pueda servir de base para la perpetración de un ataque, lo que dificulta aún más su atribución.

Los casos de ciberespionaje conocidos demuestran, sin lugar a dudas, que la mayor amenaza se encuentra en los Servicios de Inteligencia extranjeros, por sí mismos, o a requerimiento de empresas u organizaciones, vinculadas de alguna forma a tales Servicios.

Esta evidencia es especialmente peligrosa toda vez que los Servicios de Inteligencia suelen disponer de importantes recursos económicos, materiales y humanos, de la posibilidad de utilizar cualquier tipo de herramienta de ataque y de cualquier procedencia: grupos *hacktivistas*, organizaciones privadas, empresas tecnológicas o las propias universidades.

En muchas ocasiones se ha podido evidenciar que las infraestructuras técnicas de estas organizaciones han contribuido decisivamente en la perpetración de este tipo de ataques.

Además de lo anterior, los actores-estado con gobiernos totalitarios o formas de estado no democráticas gozan de ventajas añadidas a la hora de utilizar este tipo de mecanismos de ataque. A pesar del consenso internacional sobre la aplicación del Derecho Internacional también al ciberespacio, este tipo de Estados suelen prestar poca atención al cumplimiento de las normas jurídicas, permitiéndose usar sus capacidades de ataque sin control alguno, perpetrando, en consecuencia, acciones verdaderamente eficaces, toda vez que sus ataques no están limitados por ninguna supervisión estatal o por la exigencia de transparencia.

En este tipo de países, además y con frecuencia, determinados intereses privados están en condiciones de desarrollar actividades de ataque sin interferencia gubernamental, pudiendo gozar, incluso, de protección oficial cuando no de cooperación soterrada. Obviamente, el número de actores implicados dificulta enormemente la atribución de tales ataques.

En general, del análisis realizado por el CNI y el CCN-CERT se desprenden los siguientes principios o elementos comunes de los ciberataques realizados por actores estatales:

- **Primer vector de ataque.** Obtención de información estratégica: pueden aprovecharse y analizarse todos los datos obtenidos de internet y de las comunicaciones entre sus nodos. En particular, el tráfico de datos de cualquier usuario. Siempre podrá monitorizarse aquella información que no esté cifrada. Todas estas acciones se desarrollan, generalmente, de forma automática siendo capaces de procesar enormes cantidades de datos.
- **Segundo vector de ataque.** Ataques individuales: ataques dirigidos a los sistemas pertenecientes a personas o instituciones que pueden revestir determinado interés. Los sistemas TIC identificados durante la recopilación de información son atacados mediante herramientas específicamente adaptadas, utilizando la información técnica y social que se dispone de la víctima.
- **Tercer vector de ataque.** Debilitar las implementaciones técnicas: durante este proceso se manipula la implementación de los estándares criptográficos para que sean vulnerables a ataques.

- **Cuarto vector de ataque.** Manipulación selectiva de equipos informáticos: durante este proceso se manipulan los sistemas o los servicios. Lo cual incluye, por ejemplo, la inserción de puertas traseras o el debilitamiento de la seguridad perimetral que podrán explotarse posteriormente durante la fase de recopilación de información o en ataques individualizados.

Conocedores de la potencialidad de tales acciones, mientras algunos estados han declarado públicamente que los ciberataques constituyen un elemento central de su estrategia militar, otros han sido acusados de perpetrar ciberataques dirigidos a magnificar los efectos de operaciones militares tradicionales. Estos programas de ciberataques, de naturaleza indirecta, suelen estar diseñados para inutilizar o dañar la infraestructura y las comunicaciones de los adversarios o dirigirse contra sistemas públicos de salud o de respuesta a emergencias, en cuyo caso los efectos sobre el adversario son directos.

En este sentido es ya significativo el número de países que están desarrollando capacidades para llevar a cabo operaciones militares ofensivas en el ciberespacio. Estas operaciones se denominan *CNE (Computer Network Exploitation)* y/o *CNA (Computer Network Attack)*. En ambos casos se trata de términos de origen militar. *CNE* es, en esencia, ciberespionaje. *CNA*, sin embargo, suele implicar acciones dirigidas a destruir o inutilizar las redes y sistemas del adversario o hacer inaccesible su información.

En el lado opuesto, se usa el término *CND (Computer Network Defense)*, entendido como el conjunto de medidas dirigidas a proteger, monitorizar, analizar, detectar y responder a los ataques anteriores incluyendo intrusiones, interrupciones u otras acciones no autorizadas que puedan llegar a dañar o comprometer las redes o los sistemas de información.

La agrupación de estos tres términos (*CNE*, *CNA* y *CND*) es lo que se denomina *CNO (Computer Network Operation)*.

Finalmente, no puede olvidarse tampoco que los Estados también pueden desarrollar sus ataques contratando servicios de otros actores (y operando, en consecuencia, bajo otra bandera) o haciéndose pasar por movimientos *hacktivistas*.

Terrorismo y ciberyihadismo

Como es sabido el objetivo de los grupos terroristas es provocar cambios políticos y/o ideológicos a través de acciones que provoquen pánico, generando terror en las sociedades.

Aunque la actividad terrorista en el ciberespacio está incrementándose en los últimos años todavía no debe considerarse una gran amenaza, especialmente debido a sus limitadas capacidades tecnológicas.

No obstante, la más importante amenaza proviene sin duda de los grupos yihadistas (pertenecientes o afines a Dáesh), que en repetidas ocasiones han

hecho llamamientos a la «ciber yihad» contra Occidente, lo que ha puesto en evidencia la necesidad de analizar hasta qué punto disponen de los elementos necesarios (capacidades y conocimientos) para desarrollar tales ataques.

Hasta el momento, los ataques atribuibles al yihadismo se han limitado a actividades que no exigen grandes conocimientos o infraestructura como la desfiguración de páginas web, ataques *DDoS* a pequeña escala o, más comúnmente, al uso de internet y de las redes sociales para la diseminación de propaganda o el reclutamiento y radicalización.

Quizás, una de las evidencias más significativas en 2015 de la actividad ciberyihadista fue el incipiente uso de código dañino. En Siria, por ejemplo, se detectaron ciberataques (atribuidos a Dáesh) con el propósito de obtener datos sobre posiciones de los objetivos locales.

Además de ello, grupos yihadistas han colgado en internet información y vídeos al objeto de difundir las capacidades tecnológicas digitales de sus partidarios. Estas instrucciones persiguen concienciar en materia de ciberseguridad a yihadistas potenciales. Además de esto, se localizaron en internet instrucciones para el uso de una herramienta de acceso remoto (*RAT*) utilizada para el control de equipos en remoto y que, al parecer, han sido usadas por diversos grupos enfrentados en Oriente Medio.

Para financiarse los ciberyihadistas recurren a las mismas tácticas que los ciberdelincuentes, mediante ataques de *phishing* para obtener los datos de tarjetas de crédito robadas. El dinero se utiliza, fundamentalmente, para sufragar los gastos derivados de operaciones de propaganda y reclutamiento o el pago de los proveedores de internet. Además de ello, lo utilizan para recaudar fondos directamente. Por ejemplo, la red mundial de recaudación de fondos de Al-Qaeda se sustenta en donaciones y en la utilización de ONG que se comunican con sus donantes a través de redes sociales y foros *online*.

Dáesh ha elevado su despliegue mediante el diseño de la aplicación móvil *Dawn of Glad Tidings*, que actualiza regularmente, y que enlaza con *tuits* a través de sus propias cuentas personales, ayudando al grupo a lograr más seguidores, incluidos potenciales donantes.

Los ciberyihadistas también han ampliado su uso de internet para perpetrar ataques a los gobiernos e instituciones occidentales. Al-Qaeda, por ejemplo, alienta abiertamente a sus seguidores a atacar sitios web occidentales y páginas «moralmente corruptas». La «ciber yihad» también se menciona explícitamente como un deber sagrado para todos los musulmanes en una de sus documentos titulado *The 39 Principles of Jihad*.

Casos recientes demuestran que el ciberejército yihadista está creciendo en número y sofisticación. El grupo CyberCaliphate afiliado a Dáesh (supuestamente liderado por un ciudadano británico conocido como Abu Hussain Al Britani, quien dejó Birmingham para desplazarse a Siria) atacó y tomó el control de las cuentas de Twitter y Youtube del US Central Command.

Sea como fuere, todo lo anterior hace vaticinar que las capacidades del ciberihadismo no han hecho sino empezar a mostrarse. Es de esperar ciberataques más numerosos, más sofisticados y más destructivos en los próximos años en tanto persista la actual situación en torno a Dáesh.

Profesionales del ciberdelito

Las capacidades de los profesionales de la ciberdelincuencia, cuyo objetivo es obtener beneficios económicos, han seguido creciendo. Las características más significativas de los ataques evidenciaron una magnífica organización, una ejecución inmejorable y una importante sofisticación técnica, con independencia de la ubicación geográfica mundial del atacante y sus víctimas.

Se está comprobando que las organizaciones cibercriminales están dispuestas a invertir grandes cantidades de dinero en la preparación de sus acciones, cada vez más creativas, como pudo demostrarse por ejemplo en la campaña «Carbanak», dirigida contra entidades financieras de Europa del Este.

Como decimos la creatividad de los ciberdelincuentes para convertir en dinero información sustraída, se ha incrementado notablemente. Algunos ejemplos:

En Estados Unidos, un grupo de ciberdelincuentes desarrolló una campaña utilizando una muestra de código dañino específico para obtener información relativa al comportamiento económico del sector farmacéutico, lo que les permitió predecir los precios de los medicamentos y obtener importantes beneficios.

Otro tipo de ataque especialmente significativo de los últimos años ha venido siendo el uso de código dañino dirigido a TPV (Terminales Punto de Venta). Ataques que cobran especial peligrosidad cuando se usan tarjetas bancarias de banda magnética, más inseguras que las basadas en chip.

Las acciones delictivas a fin de lograr datos o información médica de los pacientes de instituciones sanitarias o clientes de compañías de seguros de salud han cobrado especial importancia en los Estados Unidos. Además de todo lo anterior, el denominado Cibercrimen como Servicio (CAAS *Cybercrime-As-A-Service*) ha incrementado su penetración y profesionalización, habiéndose percibido una cierta «competencia» entre los propios ciberdelincuentes. Lo que obliga a sus autores a prestar a sus «clientes» un «servicio» cada vez más fiable.

El acceso a las herramientas de perpetración de este tipo de ataques es cada vez más fácil, lo que propiciará el incremento del número de ciberdelincuentes y, en consecuencia, de sus acciones. Hay que tomar en consideración, no obstante, que el nivel de conocimientos técnicos de los agentes de las amenazas puede ser muy variable.

Los métodos utilizados por los ciberdelincuentes se basan tanto en el progreso tecnológico como en las medidas de protección existentes. Cuando se trata de usuarios privados, las herramientas preferidas son el correo basura o *spam* y los correos electrónicos de *phishing*, el código dañino para robo de identidad y la utilización de *ransomware*. Las organizaciones, por su parte, se enfrentan, además, a otras formas de ataque, tales como la extorsión o la infección por código dañino para terminales de punto de venta, por ejemplo.

Asimismo, algunas organizaciones delictivas ofrecen sus capacidades y servicios a otras organizaciones (o Estados) que no tienen estas capacidades. Se trata del mercado de la ciberdelincuencia en el que se ofrecen las vulnerabilidades, los métodos de ataque y se garantiza el rendimiento de los mismos.

Cibervándalos y script kiddies

Se vienen denominando cibervándalos a aquellos individuos que, poseyendo significativos conocimientos técnicos, llevan a cabo sus acciones con el único motivo de demostrar públicamente que son capaces de hacerlo.

Por su parte, los denominados *script kiddies* son aquellos que, con conocimientos limitados y haciendo uso de herramientas construidas por terceros, perpetran sus acciones a modo de desafío, sin ser, en muchas ocasiones, plenamente conscientes de sus consecuencias.

Pese a la difusión mediática que han recibido en ocasiones las acciones de los cibervándalos, no constituyen una amenaza seria a los intereses de las organizaciones.

En algunas ocasiones, los cibervándalos o los *script kiddies* han utilizado la referencia al autodenominado Estado Islámico como un engaño para crear un efecto mediático mayor, tal y como pudo apreciarse en los ataques *DDoS* a plataformas de juegos *online* o la desfiguración de la página web de Malaysian Airlines.

Hacktivistas

Los *hacktivistas*, personas o grupos, más o menos organizados, que desarrollan sus acciones en el ciberespacio movidos generalmente por motivos ideológicos, se han mostrado activos en diferentes campañas políticas y sociales.

En los últimos años, sus ciberataques (desfiguración de páginas web, ataques *DDoS* o sustracción de datos confidenciales de sus objetivos) pretendieron ser la respuesta a determinadas medidas adoptadas por gobiernos y que consideraban perjudiciales para la libertad de internet.

Con frecuencia, las acciones de estos agentes pueden situarse dentro de un contexto geopolítico, es decir, allí dónde se han producido hechos que, a su entender, han sido injustos o desproporcionados, por lo que el riesgo

de ciberataques por grupos *hacktivistas* aumenta significativamente durante conflictos nacionales o internacionales.

La disparidad de intereses hace que, en ocasiones, se generen confrontaciones como la ocurrida entre grupos en la órbita de «Anonymous», por un lado, contra identidades *hacktivistas* con configuración islamista no afiliadas directamente pero sí apoyando o mostrando simpatía por el grupo yihadista Dáesh.

En Iberoamérica, por su parte, se ha mantenido prácticamente constante una ofensiva *hacktivista* reactiva contra el Gobierno de Nicolás Maduro en Venezuela, se han programado varias operaciones antigubernamentales en México y se han desarrollado algunas acciones en Colombia, Chile, Brasil y, en menor medida, Argentina, Guatemala o Nicaragua.

El ecosistema *hacktivista* en España está caracterizado por una baja densidad de identidades de propaganda adoptando la iconografía del colectivo «Anonymous», instaladas con vocación de permanencia a través de perfiles y canales de comunicación en redes sociales pero sin apenas capacidades operativas, con la excepción de «La 9.^a Compañía de Anonymous».

Actores internos

Los llamados actores internos (*insiders*) son personas que están o han estado trabajando para una organización tales como empleados o exempleados, trabajadores temporales, colaboradores y proveedores.

Son muchos los casos que han demostrado que el compromiso de un sistema de información (de naturaleza pública o privada) no se origina siempre por motivos económicos o políticos, sino que, en muchas ocasiones, la negligencia de los usuarios o el despecho de determinadas personas son causa directa de importantes brechas de seguridad.

En varios de los ciberincidentes se ha podido observar como algunos empleados colocaron información sensible en servidores privados sin adoptar las adecuadas medidas de seguridad, lo que provocó que fuera accesible por terceros a través de internet.

Análogamente, la disponibilidad de los sistemas de información también puede verse alterada debido a errores humanos. En todo caso, pese a su peligrosidad, los actores internos solo han venido representando un pequeño porcentaje de los agentes de las amenazas.

Ciberinvestigadores

Los llamados ciberinvestigadores buscan vulnerabilidades en entornos TIC al objeto de verificar la protección de los sistemas objeto de sus investigaciones. Con frecuencia, además de informar a las empresas, se publica en los medios de comunicación el resultado de sus investigaciones, con un doble efecto: positivo y negativo.

En el plano negativo es evidente que la publicidad de cualquier vulnerabilidad conlleva que los sistemas identificados sean más vulnerables a ataques exteriores, facilitando la acción de los atacantes, que pueden llegar a beneficiarse de los resultados de las investigaciones. Esto sucede con frecuencia cuando ciberinvestigadores (por sí mismos o a través de periodistas) deciden publicar determinadas vulnerabilidades de sistemas críticos o sensibles, pudiendo llegar a incurrir en responsabilidades administrativas, civiles o penales, según los casos.

Además, es preciso tener en cuenta que estos actores internos pueden ser empleados por otros actores agentes de la amenaza, especialmente por Estados y empresas dedicados al ciberespionaje, para la infección preliminar de la red objetivo o para la exfiltración de información de la misma. Este comportamiento no exige necesariamente amplios conocimientos técnicos, la conexión a un ordenador de la organización de una simple memoria USB conteniendo código dañino puede ser suficiente

Algunos países han publicado una guía para la revelación responsable de vulnerabilidades y fallos de seguridad. Tal es el caso de la *Policy for arriving at a practice for Responsible Disclosure*, publicación del Centro Nacional de Ciberseguridad de los Países Bajos. Desde la publicación de esta guía, en 2013, los ciberinvestigadores, junto con la comunidad de seguridad IT, han venido reportando vulnerabilidades de forma confidencial y responsable siguiendo un procedimiento que permite resolver rápidamente las vulnerabilidades detectadas. Siendo una práctica deseable, todavía no se ha extendido el uso internacional de este tipo de iniciativas.

Organizaciones privadas

Las motivaciones para perpetrar ciberataques también se encuentran en las organizaciones privadas cuando, movidas por el interés económico que supone poseer los conocimientos que tiene la competencia, desarrollan acciones de ciberespionaje industrial.

Por otro lado, también se han dado casos de empresas que, como consecuencia de las aplicaciones que venden o los servicios que prestan, recaban datos –en muchos casos de carácter personal– de sus clientes que pueden utilizar para propósitos comerciales no legítimos o que, incluso, pueden llegar a vender a terceros sin solicitar el consentimiento del cliente o bien le hayan sido requeridos de manera engañosa. Este problema adquiere especial relevancia cuando se trata de servicios en la nube, en los que el usuario depende totalmente del comportamiento del proveedor y de las medidas de seguridad que hayan sido adoptadas por las organizaciones para garantizar el adecuado tratamiento de sus datos.

Los analistas que tratan de determinar el origen de un ciberataque encuentran a menudo obstaculizada esta labor por el uso de *botnets* o redes de ordenadores infectados que son utilizados como robots. En primer lugar, los

ordenadores infectados a través de una *botnet* pueden estar ubicados en diferentes países de todo el mundo, limitando la capacidad de definir el país de origen del ciberataque.

En segundo lugar, la identidad del control de la *botnet* también puede ser ensombrecida por la utilización de *software peer-to-peer* o red entre pares (*P2P*, por sus siglas en inglés). Además, la dirección facilitada por un proveedor de internet (IP) que podría facilitar la ubicación de un equipo que lanzó un ataque puede ser falsificada (lo que se conoce como *spoofing*) e incluso con una dirección IP válida puede ser prácticamente imposible verificar el actor que se encontraba tras un sistema en el momento en que se produjo el ataque.

De otra parte, en las *botnet* se encuentran equipos que han sido infectados sin el conocimiento del usuario. En este escenario, a nivel de estado-nación, es plausible un cierto nivel de ausencia de responsabilidad, dada la proliferación de organizaciones de *hackers* y las herramientas cibernéticas a su disposición lo que facilita que los Estados puedan reclamar fácilmente la falta de responsabilidad ante ataques que parecen provenir del interior de sus fronteras estatales.

Crterios de determinación del nivel de peligrosidad de los ciberincidentes

Los incidentes de seguridad provocados por los diferentes actores se tipifican, atendiendo a su peligrosidad, en cinco niveles: bajo, medio, alto, muy alto y crítico. La tabla siguiente muestra el nivel de peligrosidad de los ciberincidentes, atendiendo a la repercusión que la materialización de la amenaza de que se trate podría tener en los sistemas de información de las entidades.

CRITERIOS DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES			
NIVEL	AMENAZAS SUBYACENTES MÁS HABITUALES	VECTOR DE ATAQUE	CARACTERÍSTICAS POTENCIALES DEL CIBERINCIDENTE
CRÍTICO	Ciberspionaje	APTs, campañas de <i>malware</i> , interrupción de servicios, compromiso de sistemas de control industrial, incidentes especiales, etcétera.	- Capacidad para exfiltrar información muy valiosa, en cantidad y en poco tiempo. - Capacidad para tomar el control de los sistemas sensibles, en cantidad y en poco tiempo.

MUY ALTO	- Interrupción de los Servicios IT. - Exfiltración de datos. - Compromiso de los Servicios.	- Códigos dañinos confirmados de Alto Impacto (RAT, troyanos enviando datos, <i>rootkit</i>, etcétera). - Ataques externos con éxito.	- Capacidad para exfiltrar información valiosa, en cantidad apreciable. - Capacidad para tomar el control de los sistemas sensibles considerable.
ALTO	- Toma de control de los sistemas. - Robo y publicación o venta de información sustraída. - Ciberdelito. - Suplantación.	- Códigos dañinos medio impacto (virus, gusanos, troyanos). - Ataques externos compromiso de servicios no esenciales (<i>DoS/DDoS</i>). - Tráfico DNS con dominios APTs o campañas <i>malware</i>. - Accesos no autorizados. - Suplantación. - Sabotaje. - <i>Cross-Site Scripting</i>. - Inyección <i>SQL</i>. - <i>Spear phishing/pharming</i>.	- Capacidad para exfiltrar información valiosa. - Capacidad para tomar el control de ciertos sistemas.
MEDIO	- Logro o incremento de capacidades ofensivas. - Desfiguración de páginas web. - Manipulación de información.	- Descargas de archivos sospechosos - Contactos con dominios o direcciones IP sospechosas - Escáneres de vulnerabilidades. - Códigos dañinos de bajo impacto (<i>adware, spyware</i>, etcétera). - <i>Sniffing</i>. - Ingeniería social.	- Capacidad para exfiltrar un volumen apreciable de información. - Capacidad para tomar el control de algún sistema.
BAJO	- Ataques a la imagen. - Errores y fallos.	- Políticas. - <i>Spam</i> sin adjuntos. - <i>Software</i> desactualizado. - Acoso, coacción, comentarios ofensivos. - Error humano. - Fallo HW-SW.	- Escasa capacidad para exfiltrar volumen de información. - Nula o escasa capacidad para tomar el control de sistemas.

Tabla 3.1. CRITERIOS DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES. CR

Fuente: CCN-CERT: *Guía de seguridad de las TIC, CCN-STIC-817, Esquema Nacional de Seguridad, Gestión de Ciberincidentes, p. 18.*

Herramientas de las amenazas

Herramientas construidas para otros fines.

Los atacantes están haciendo un uso masivo de herramientas desarrolladas para otros fines, tales como la monitorización de sistemas o la realización de pruebas de penetración. Algunos ejemplos de ello son los servicios *SaaS* (*Software as a Service* o *booter services*) que permiten a los atacantes perpetrar ataques de denegación de servicios distribuidos (*DDoS*) a través de un sitio web.

Como ejemplo, los responsables de las campañas de ataque denominadas Cleaver, Hurricane Panda y Anunak/Carbanak utilizaron la herramienta MimiKatz (diseñada originariamente para recuperar contraseñas, tickets Kerberos y funciones resumen —hashes¹⁵— de memoria de un sistema Windows) para obtener datos de registro (*log*) a una red Windows y lograr acceder a los sistemas de la red.

En otras ocasiones, los atacantes prefirieron seguir utilizando *exploits* ya contruidos provenientes de Metasploit (una herramienta concebida para desarrollar pruebas de penetración) posibilitando a los atacantes explotar vulnerabilidades ya conocidas sin necesidad de poseer amplios conocimientos técnicos.

Exploits, Exploit-Kits y Exploit Drive-By.

Las herramientas más utilizadas para realizar los ataques, al igual que en los últimos años, son *exploits*, *exploit-kits* y *exploit DriveBy* (permiten infectar el sistema de la víctima con código dañino cuando accede a una determinada página web, distribuyéndose habitualmente mediante *banners* de publicidad).

Windows y las aplicaciones *PHP* (*plug-ins* para Wordpress y Joomla, sobre todo) siguen constituyendo el foco de los *exploits*, aunque es cierto que se ha reducido sustancialmente su publicación. Sin embargo, los *exploit-kits* más habituales se centran en Adobe Flash.

Estas herramientas no solo se utilizan en páginas web dudosas, sino también en aquellas otras absolutamente legítimas y fuera de sospecha. También son muy comunes los ataques por Watering Hole que constituyen un mecanismo habitual para iniciar ataques dirigidos, especialmente cuando las páginas web infectadas son de visita frecuente por parte de personas de la organización-víctima.

Los *exploits Drive-By* son mecanismos de ataque que permiten infectar el sistema de la víctima con código dañino cuando accede a una determinada página web previamente infectada, código que explota las vulnerabilidades de los navegadores web, sus complementos o el propio sistema operativo. Los llamados *exploits Drive-By* pueden usarse aisladamente o en conjunción con *exploits-kits* tradicionales, distribuyéndose habitualmente mediante *banners* de publicidad infectados o servidores web comprometidos. Obviamente, si una página web es muy popular, el número de infecciones será muy significativo y se logrará en muy corto período de tiempo.

Mientras que los *exploits-kits* suelen utilizarse principalmente para ataques masivos (no-dirigidos), los mecanismos *Drive-By* suelen utilizarse cuando se trata de ataques inmersos en campañas específicas de ataques dirigidos específicamente a un objetivo concreto (*APT* por ejemplo).

Código Dañino/*Ransomware*/*Cryptoware*.

El código dañino (en la bibliografía anglosajona suele denominarse también *malware*) tiene en la actualidad una tipificación muy compleja porque se compone de una multiplicidad de módulos con funciones diferentes (módulos adicionales que pueden descargarse de internet) en función de las características del ataque o de la víctima, etcétera.

Los mecanismos de infección suelen ser los archivos adjuntos a correos electrónicos o la visita a páginas web infectadas.

El código dañino representa una de las herramientas más utilizadas para realizar las infecciones que preceden a los ataques. El número total de versiones de código dañino para *personal computer* se estima actualmente en más de 439 millones (siendo Windows el sistema más afectado), al tiempo que el número de *malware* en plataformas móviles sigue aumentando de manera incesante (un 96 % de este código dañino afecta al sistema operativo Android).

La variedad de muestras de *ransomware* o *cryptoware* (Critroni, CryptoFortress, CTB-Locker, Cryptolocker y Cryptowall) no ha dejado de crecer y sus métodos de distribución van variando: *exploits Drive-By*, correos electrónicos con enlaces a programas dañinos, alojamiento en macros de los productos de Microsoft Office, etcétera.

Durante 2016 se han podido constatar infecciones por *cryptoware* en multitud de organizaciones, públicas y privadas, de todos los tamaños, incluyendo instituciones sanitarias y pymes.

A modo de ejemplo, podemos citar el caso Coinvault, una infección investigada conjuntamente por la Policía holandesa y Kaspersky Lab, en la que pudo determinarse que, aproximadamente, el 1,5 % de las víctimas hicieron efectivo el pago del rescate. Es lógico que aparezcan nuevas variantes, dado que se calcula que un tanto por ciento de las víctimas satisfizo el rescate, lo que estimula a los delincuentes para mejorar continuamente sus herramientas y sus objetivos: grandes empresas, pymes y consumidores finales; nuevos sistemas operativos y nuevos dispositivos, incluyendo los dispositivos móviles.

Spam (correo basura) y *phishing*/*spearphishing*.

El término *spam* se puede subdividir en varios tipos: *spam* tradicional, *spam* de código dañino y mensajes de *phishing*. Tras un aumento en 2014 el *spam* tradicional disminuyó en 2015, aproximadamente el 30 % del volumen del año anterior, manteniéndose en la actualidad en esos niveles. Sin embargo, el *spam* que lleva incorporado *malware* y que utiliza direcciones de correo electrónico obtenidas en otros sistemas infectados, aumentó significativamente y constituye la principal la principal fuente de infecciones.

Se han encontrado numerosas muestras de código dañino de la familia Geodo. Se ha observado, además, que se distribuyen cada vez más profesionalmente. La utilización de técnicas de engaño y suplantación, el uso de versiones individuales del código dañino y el control horario de la descarga, son herramientas dirigidas a provocar la infección del sistema del usuario sin que el *software* antivirus sea capaz de detectarlo. En cuanto al *phishing* y *spearphishing* (correo dirigido de alguien conocido) son las herramientas más utilizadas para iniciar ataques personalizados y realizar ciberespionaje.

Botnets.

Las redes de robots, *botnets*, son utilizadas por los ciberdelincuentes de forma masiva al objeto de sustraer información, cometer fraude de banca *online*, atacar a la disponibilidad de los sistemas informáticos o enviar *spam*.

Debido a la profesionalización de los ciberdelitos operar una *botnet* es relativamente fácil y poco costoso para los no especialistas. Por ello, el nivel de peligrosidad actual continúa siendo crítico y la tendencia va en aumento.

Debido a su cuota de mercado, los sistemas comprometidos principalmente por *botnets* utilizan Windows, aunque los atacantes están aumentando sus esfuerzos para dirigirse contra sistemas Mac OS X y Android. Persiste la tendencia del uso dañino de servidores web comprometidos para operar servidores C&C (mando y control).

Ataques DDoS.

Aunque siguen produciéndose ataques *DDoS*, los perjuicios que han podido causar en los sistemas de información, especialmente del sector privado, han sido cuantitativamente menores que los ocurridos en 2014. Ello ha sido debido a la adopción de las medidas anti-*DDoS* que han podido tomar las organizaciones más vulnerables a este tipo de ataques, singularmente las entidades financieras. Estas medidas, que suelen ser significativamente onerosas, sin embargo, no eliminan los riesgos: los ataques siguen estando ahí y, para tener éxito, solo necesitan ser más sofisticados que las medidas adoptadas.

Otra consideración significativa que puede hacerse es que la duración media de un ataque *DDoS* disminuye. La mayoría de los ataques tienen una duración de entre treinta minutos y una hora. El 59 % de los ataques se detiene en quince minutos y más del 87 % lo hacen en la primera hora. En algunas ocasiones, los ataques solo duran cinco minutos, lo que podría estar indicando el uso de una prueba gratuita de los llamados servicios *booter*, que pueden utilizarse con facilidad para desarrollar ataques de denegación de servicio distribuida *DDoS*. Sea como fuere, la experiencia señala que, a menudo, cuanto más corto es un ataque más intenso es.

Por otro lado, y al objeto de asegurar que un ataque *DDoS* es efectivo, se emplean técnicas de amplificación: enviar una consulta pequeña que requiera

una respuesta de gran volumen. Se ha comprobado que, en ciertos casos, la respuesta puede llegar a ser casi 360 veces más grande que la consulta, lo que supone un alto grado de amplificación.

El motivo principal que inspira los ataques *DDoS* es la extorsión, aunque el *hacktivismo* también suele utilizar este mismo vector de ataque.

La modalidad denominada Ataque por Reflexión constituye también una amenaza significativa de este tipo de ataques. En esta modalidad, servidores de acceso público (por ejemplo, servidores *NTP*) se utilizan para reforzar el ataque. Esto hace que los operadores de este tipo de servidores se conviertan en coautores (involuntarios) de las acciones dañinas. Este tipo de ataque logra un efecto comparable al de un ataque mediante una *botnet* tradicional.

Ofuscación.

Se denomina ofuscación a cualquier actividad llevada a cabo por los atacantes para dejar el menor número posible de trazas de sus acciones con el objeto de dificultar su identificación, la metodología seguida, etcétera.

Rastrear el tráfico sospechoso dentro de una red es más difícil si se utilizan nombres de dominio, sitios web o servicios de comunicaciones que gocen de buena reputación. En muchos casos, la detección se centra en direcciones IP y nombres de dominio dañinos conocidos por su participación en ciberataques.

En general, los creadores de código dañino ofuscan el *software* tanto como es posible, al objeto de dificultar su análisis aunque, en ocasiones, no lo hacen como sucedió con los códigos dañinos Foxy148 y Babar. Esta situación hace que sea más fácil para los investigadores diseccionar el *malware*. La detección de este dentro de una red es, sin embargo, más difícil.

La utilización de técnicas de ofuscación y cifrado puede ser una señal para el *software* antivirus y otras herramientas de detección que conduzcan a desconfiar del programa.

Ingeniería social.

Constituye uno de los vectores de ataque preferidos por los agentes de las amenazas, que engañan a sus víctimas, para que permitan la instalación de programas dañinos y todo ello al objeto de acceder a la información del sistema atacado. En este caso, los atacantes tienen la posibilidad de obtener de forma rápida y anónima datos personales de sus víctimas a través de las redes sociales y suele constituir la primera fase de los ataques dirigidos (tratando de adivinar la contraseña de la víctima, generando confianza, correos electrónicos personalizados o *spearphishing*).

El ataque del «falso presidente» ha sido muy lucrativo en el entorno comercial (el atacante se hace pasar por un directivo de la organización, encargando a un empleado la transferencia urgente destinada a un proyecto secreto).

Watering Hole.

Suele ser la segunda opción para los atacantes cuando no tiene éxito un ataque mediante *spearphishing*. Los atacantes aprovechando una vulnerabilidad conocida infectan previamente con código dañino una página web que las víctimas visitan frecuentemente. También se ha incrementado el uso de mensajes publicitarios dañinos (lo que se ha denominado *malvertising*).

Librerías Javascript.

La inclusión de Javascript y otras librerías en una página web han propiciado en 2015 una importante serie de incidentes. Con frecuencia, los desarrolladores de sitios web invocan directamente una librería en lugar de copiarla a su propio sitio web. Si un atacante logra manipular una librería, está en condiciones de atacar a todos los sitios web que contengan una llamada dinámica a la misma.

Las macros como vector de ataque.

Varias familias recientes de *software* dañino, tales como Dridex, Vawtrak y Cryptodefense son claros ejemplos de código dañino que se instala en los sistemas de los usuarios finales a través de macros.

Routers inalámbricos.

Los *routers* de particulares y pymes comprometidos permiten, por ejemplo, ajustar la configuración del *DNS* (*Domain Name System*) para redirigir el tráfico a páginas web infectadas, formar parte de una *botnet*, propagar código dañino y penetrar en la red o manipular el tráfico sin ser detectado.

Robo de identidad.

Habitualmente el robo de identidad (usuario, contraseña u otros datos) se lleva a cabo mediante mecanismos de ingeniería social, instalación de código dañino en los sistemas de la víctima (incluso existen programas cuya función es precisamente este robo) o a través de ataques previos a sitios web. Así pues los atacantes pueden obtener un beneficio económico directo con la venta de identidades robadas y con un margen muy amplio, por lo que esta actividad se mantendrá como una amenaza permanente en los próximos años.

Tendencias de amenazas globales de ciberseguridad

En este escenario, se apuntan a continuación las tendencias de amenazas globales de ciberseguridad detectadas en los diferentes ámbitos.

Ciberespionaje. Muy probable.

El empleo del ciberespacio para la obtención de inteligencia se ha incrementado por todos los países de nuestro entorno por su eficacia y dificultad de

atribución. Debido a la publicación de campañas de ciberespionaje realizadas por compañías de seguridad, los países emplearán más recursos en la seguridad de sus operaciones aislando infraestructuras y diversificando las Técnicas, Tácticas y Procedimientos (TTP) de ataque.

Seguimos siendo testigos de acciones de ciberespionaje, consistentes en ciberataques originados o patrocinados por Estados y perpetrados por ellos mismos o por agentes a sueldo y siempre con la intención de apropiarse de información sensible o valiosa desde los puntos de vista político, estratégico, de seguridad o económico.

A modo de resumen, podemos decir que el ciberespionaje presenta las siguientes características generales: con origen en Estados, industrias o empresas. Utilizando, generalmente ataques dirigidos (APT, Amenazas Persistentes Avanzadas) contra los sectores público (información política o estratégica) y privado (información económicamente valiosa), con una enorme dificultad de atribución y persiguiendo obtener ventajas políticas, económicas, estratégicas o sociales.

Ante la peligrosidad de las campañas de ciberespionaje, especialmente las originadas por los propios Estados y la sofisticación de las técnicas y tácticas usadas, se realizan las siguientes recomendaciones:

- Es necesario aumentar la capacidad de vigilancia de las redes y los sistemas. Para ello, es indispensable contar con el adecuado equipo de seguridad interno o disponer de una consultoría externa, de eficacia debidamente contrastada.
- Es necesario disponer de herramientas de gestión centralizada de registros, incluyendo monitorización y correlación de eventos. Las herramientas utilizadas deberán ser capaces de monitorizar el tráfico de red, usuarios remotos, contraseñas de administración, etcétera.
- Es necesario disponer de la adecuada política de seguridad corporativa que contemple una restricción progresiva de los permisos de los usuarios, así como una aproximación práctica a los servicios en la nube o la utilización de dispositivos y equipos propiedad del usuario *Bring your own device (BYOD)*.
- Es necesario aplicar configuraciones de seguridad a los distintos componentes de la red corporativa, incluyendo a los equipos móviles y portátiles.
- Es necesario emplear productos, sistemas y servicios confiables, certificados y redes y equipos acreditados para el manejo del nivel de clasificación que se determine.
- Es necesario automatizar e incrementar el intercambio de información con los Equipos de Respuesta ante Ciberincidentes (*CERT*) adecuados.
- Es necesario que la Dirección acepte la existencia de los riesgos y promueva las políticas de seguridad dentro de la organización.

- Es necesario formar y sensibilizar a todos los usuarios de la organización, incluyendo todos los niveles (dirección, gestión e implantación) para que tomen conciencia de los riesgos y actúen en consecuencia.
- Es necesario atenerse a la legislación y buenas prácticas vigentes, adecuándose a los diferentes estándares de seguridad (en el caso de las Administraciones públicas al Esquema Nacional de Seguridad).
- La organización debe trabajar como si los sistemas estuvieran comprometidos o lo vayan a estar pronto.

Los ataques como servicio. Muy probable.

A través de grupos con conocimiento y capacidad técnica sería posible contratar sus servicios y planificar un ataque «a medida» con garantías de éxito. Requerirá ampliar el conocimiento de las redes *Deep Web*, incrementar la cooperación público privada y armonizar la legislación internacional.

Fusión de tácticas, técnicas y procedimientos (TTP) utilizadas por el ciberespionaje y la ciberdelincuencia. Muy probable.

Evolución de la actividad cibercriminal a TTP empleados en el ciberespionaje usando herramientas del tipo Amenazas Persistentes Avanzadas (APT) y dirigidas especialmente contra el sector financiero persiguiendo la sustracción de dinero. Durante el último año se ha apreciado un aumento de los ataques, sustentados en la acción de código dañino y métodos propios de las APT, cuyo objetivo han sido entidades financieras, persiguiendo la sustracción de dinero, de varias formas:

- Control remoto de cajeros automáticos.
- Realización de transferencias *SWIFT* de las cuentas de ciertos clientes.
- Manipulación de los sistemas informáticos *online* para ordenar transferencias ilícitas.

Estabilización de los ataques *hacktivistas*. Muy probable.

Es de esperar una continuación de la actividad de grupos como «Anonymous» y una proliferación de células *hacktivistas* que operen con distintas narrativas en diversos países con una marcada orientación hacia la producción de ciberataques por desfiguración de páginas web, con incorporación de elaboradas composiciones gráficas en los sitios web de los objetivos atacados.

Herramientas de ataque para dispositivos móviles. Probable.

Además del crecimiento del número de las actuales amenazas de Android, se prevé que el crecimiento de vulnerabilidades en los dispositivos móviles, plataformas y aplicaciones presentará ciertos riesgos de seguridad especialmente graves: los datos almacenados en los dispositivos móviles podrán ser usados por los ciberdelincuentes para perpetrar otros ataques o para su venta en el mercado negro. Por otro lado, las vulnerabilidades no solo residen en los dispositivos sino también en las plataformas y aplicaciones.

El «secuestro» de organizaciones por *ransomware*. Muy Probable.

Durante 2016 se ha estado asistiendo a la expansión de los ataques por *ransomware*, especialmente de su variante más agresiva: el *cryptoware*. De esta forma, los atacantes solicitan un rescate por descifrar la información que ellos han encriptado al tomar el control del dispositivo.

Una nueva tendencia que está resultando exitosa en 2016 es el cambio de paradigma respecto a la liberación de la información y la disminución de la cuantía del pago del rescate. A diferencia de los comienzos del *ransomware*, en el que tras solicitar a los atacados una elevada cantidad de dinero por descifrar la información, en el caso de que estos hicieran efectivo el pago del rescate no se liberaban los sistemas, en la actualidad se han disminuido las cantidades solicitadas a la vez que si se pagaba se liberaba la información, lo que ha generado un mayor volumen de ingresos a los atacantes.

El uso de este tipo de código dañino y el consiguiente lucro obtenido con él han podido dar argumentos a los atacantes para diseñar ataques a mayor escala, todavía más lucrativos: los ataques a grandes empresas o instituciones. Perpetrando un ataque de este tipo, en caso de tener éxito, los agentes de las amenazas lograrían un nivel de compromiso tan grande de los sistemas atacados que podrían detener la normal actividad de la organización. Esta situación obligaría a las víctimas, presumiblemente, a satisfacer el rescate exigido. Obviamente, la publicidad del éxito de un ataque de este tipo alentaría a nuevos atacantes.

Incremento de los ataques contra cajeros automáticos y procedimientos de pago. Probable.

Los ataques contra cajeros automáticos han evidenciado la vulnerabilidad de tales dispositivos. Es presumible, por tanto, que se produzca un incremento y evolución tecnológica de los ataques contra estos dispositivos. No es desdeñable, tampoco, la utilización de técnicas *APT* para, a través de tales equipos, penetrar en la red de la entidad financiera y explotar acciones que persigan mayores objetivos. Este problema puede hacerse extensivo a los ataques dirigidos contra máquinas expendedoras de *tickets* y que, en muchas ocasiones, también aceptan tarjetas de crédito. Presumiblemente, asistiremos a nuevas y más sofisticadas acciones tendentes, por ejemplo, a obtener los datos de las tarjetas de crédito utilizadas por los clientes de las máquinas de *ticketing*. Además, es de esperar que en los próximos años los agentes de las amenazas desarrollen acciones contra sistemas virtuales de pago, atacando los puntos finales (teléfonos móviles, en la mayoría de casos). Este temor puede extenderse a Apple Pay, que utiliza la tecnología *NFC* (*Near Field Communications*) para manejar transacciones de forma inalámbrica.

Nuevas amenazas a los dispositivos móviles. Muy Probable.

Debido a la consolidación y a la comercialización de nuevos accesorios para los dispositivos móviles se incrementarán especialmente los incidentes de seguridad

sobre estos complementos o *wearables* (relojes, pulseras, etcétera) y sobre los nuevos (y ya existentes) métodos de pago basados en tecnologías inalámbricas, como *NFC* (*Near Field Communications*) o monedas virtuales. Pese a que la seguridad de los dispositivos móviles se fortalece con el paso del tiempo, las nuevas funcionalidades que son incorporadas cada año no están exentas de debilidades.

La tendencia parece evolucionar hacia escenarios más complejos, avanzados y profesionalizados de ataque, tanto en la investigación y descubrimiento de nuevas vulnerabilidades, como en la explotación de las debilidades existentes en las principales plataformas móviles. Por otro lado, no debe ignorarse la existencia de vulnerabilidades más sencillas de explotar, incluso ya conocidas en otras tecnologías y que a lo largo del tiempo vuelven a afectar a tecnologías más modernas o de última generación.

Asimismo, será importante permanecer alerta ante nuevas revelaciones asociadas a la privacidad y seguridad del usuario y a esquemas de espionaje globales por parte de agencias gubernamentales. Desde el punto de vista corporativo la integración de forma segura de los dispositivos móviles tanto corporativos como personales en las infraestructuras de información de las organizaciones a través de soluciones *MDM* (*Mobile Device Management*) sigue siendo un reto complejo que hay que afrontar.

Nuevas vulnerabilidades en *software* y protocolos habituales. Probable.

Las especialmente peligrosas vulnerabilidades reveladas el pasado año en *software* habitual, (tales como Shellshock, Heartbleed y OpenSSL), han sumido a la comunidad tecnológica en importantes dudas acerca de la fiabilidad de un *software* muy común que, a la fecha, permanece sin auditar debidamente. Pese a los esfuerzos de muchas organizaciones dedicando recursos para analizar tal tipo de *software* —incluso contratando a grupos de expertos para descubrir nuevas vulnerabilidades—, es muy posible que todavía sean muchas las que permanecen ocultas.

Ataques contra Infraestructuras Críticas. Posible.

La especialmente peligrosa combinación de tecnologías antiguas —sin mantenimiento, en muchos casos— y una superficie de ataque cada vez mayor, hacen a ciertas Infraestructuras Críticas especialmente vulnerables a los ataques. Es sabido que son muchos los Estados que están desarrollando capacidades para atacar de forma remota los sistemas SCADA (Supervisión, Control y Adquisición de Datos) —que permiten controlar y supervisar procesos industriales a distancia— y otros sistemas críticos. Los analistas coinciden en señalar que las grandes cadenas de fabricación y las redes de energía eléctrica constituyen los objetivos más probables para este tipo de ataques.

Ataques contra Linux y OS-X. Posible.

Hasta el momento, tanto Linux como OS-X no han sido objeto de grandes ataques, aunque esto puede cambiar en los próximos años. La adopción

masiva de Linux en muchas organizaciones ha provocado un repunte del número de muestras de código dañino para este sistema operativo, tales como Cdorker.

La ampliación de la superficie de ataque supondrá previsiblemente para los agentes de las amenazas un estímulo para perpetrar acciones contra esta plataforma. Por su parte, a pesar de los esfuerzos de Apple para fortalecer el sistema operativo de los Mac, se sigue constatando la presencia de código dañino, introducido a través de paquetes de *software* pirateado. La creciente popularidad de los dispositivos Mac OS-X en todos los ámbitos —junto con la aparición de *exploits* día cero específicos— está despertando la atención de los ciberdelincuentes por desarrollar *malware* específicamente dirigido a este tipo de dispositivos. Dada la dificultad que supone penetrar en esta plataforma, y a la vista de que son muchos los usuarios de Mac que están desactivando determinadas medidas de seguridad por defecto —al objeto, generalmente, de permitir la instalación de software pirata—, los agentes de las amenazas están incorporando código dañino camuflado dentro de programas al objeto de infectar las máquinas.

Quizás, como así se ha considerado por muchos analistas, el mayor motivo de preocupación para los usuarios radica en que, gracias a la imagen de seguridad de la que hasta ahora han gozado estos equipos, no se han desarrollado significativamente herramientas de seguridad para ellos, lo que puede convertirlos en dispositivos vulnerables.

Los ataques contra el Internet de las Cosas (*IoT*). Probable.

Aunque, hasta el momento, los ataques contra el Internet de las Cosas no han ido más allá de unos pocos intentos o algunas amenazas sobre la posibilidad de utilizar *botnets* para desplegar ataques masivos contra televisores o frigoríficos inteligentes. Sin embargo, a medida que un mayor número de estos dispositivos se conecten, asistiremos a un mayor debate sobre los problemas de seguridad y, especialmente, de privacidad derivados de su conexión. En todo caso, es presumible que se produzcan ataques contra dispositivos de red, que pueden facilitar a un atacante mantener la persistencia en la organización y desarrollar movimientos laterales dentro de una red corporativa, como parte de una acción *APT* a mayor escala.

En el nivel de los usuarios domésticos, es presumible que las primeras acciones de compromiso de la *IoT* se traduzcan en la manifestación de ciertas vulnerabilidades de los dispositivos y la posibilidad de incrustar publicidad (*adware/spyware*) en, por ejemplo, la programación del receptor de televisión inteligente.

En cambio, si se han mostrado especialmente vulnerables algunos de estos dispositivos a ser infectados por *malware* que permitía incorporarlos a una *botnet* que los ha utilizado para realizar ataques de denegación de servicio distribuido. El ataque *DDoS* a la empresa de servicios de DNS Dyn del 21 de

octubre de 2016, con impacto en importantes plataformas y redes sociales, ha marcado un punto de inflexión en este ámbito. La modificación de las claves de seguridad por parte de los usuarios y la actualización del *software* o *firmware* de estos dispositivos limitarían este impacto.

Ciberincidentes en España

Un documento que se estima relevante, para situar a España en el contexto de la comunidad internacional en el ámbito de las Tecnologías de la Información y Comunicaciones (TIC), es el *Informe Global de Tecnología 2016*. Desde 2001, este informe publicado por el Foro Económico Mundial, en colaboración con la Universidad de Cornell y el INSEAD, ha medido diferentes parámetros de ciento cuarenta y tres países⁴. En este informe se realiza un estudio comparativo de diferentes factores, elaborando una clasificación que en 2015 coloca a España en el puesto número treinta y cinco de este estudio, el cual valora la penetración en la sociedad de las tecnologías de la información y comunicaciones, como se refleja en el gráfico:

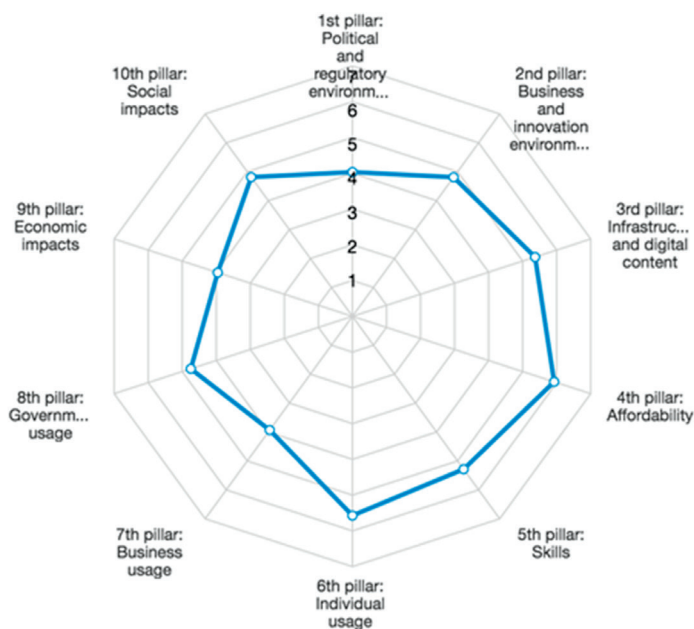


Figura 3.6. Informe sobre España TIC 2016.
Fuente: Foro Económico Mundial. Global Information Technology Report 2016.

⁴ DUTTA Soumitra, GEIGER Thierry y LANVIN Bruno, Eds.: *The Global Information Technology Report 2016*, World Economic Forum & INSEAD, Ginebra, 2016. <http://reports.weforum.org/global-information-technology-report-2016/>

El grado del cumplimiento de España de los diez pilares que analiza el informe en relación con las TIC se refleja en la siguiente figura.

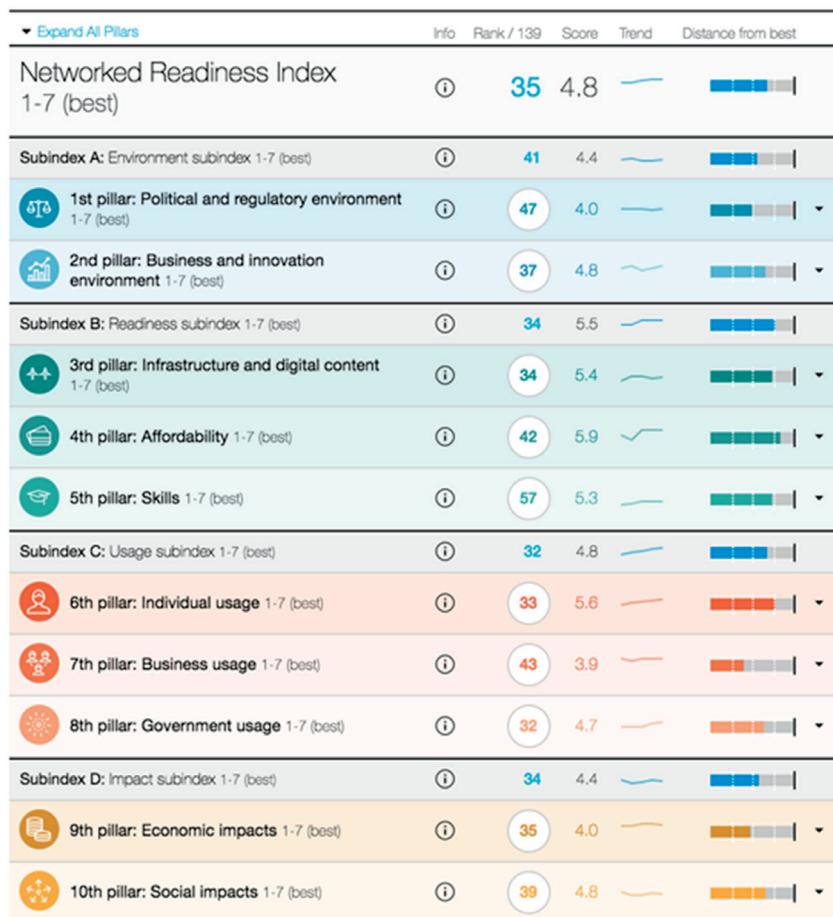


Figura 3.7. Grado de cumplimiento de España en el sector TIC.
Fuente: Foro Económico Mundial. Global Information Technology Report 2016.

Microsoft en su informe de inteligencia de seguridad global más reciente⁵ ofrece datos sobre la situación en España⁶. En relación a las tendencias de las tasas de encuentro⁷ y de infección, Microsoft señala que en el cuarto

⁵ Microsoft Corporation: *Microsoft Security Intelligence Report, Volume 20, julio a diciembre de 2015, España*, Redmond, WA, 2016.

⁶ *Ibidem*, p. 3. Microsoft Corporation señala que las estadísticas son generadas por los programas de seguridad de Microsoft y servicios que se ejecutan en los ordenadores en España. Se utiliza la geolocalización utilizando la dirección IP para determinar el país o la región.

⁷ Tasa de encuentro es el porcentaje de equipos que ejecutan productos de seguridad de Microsoft en tiempo real que reportan un encuentro con *malware*, independientemente de si produce o no la infección en el equipo.

trimestre de 2015 el 23,3 % por ciento de los ordenadores en España tuvo un encuentro con *malware*, en comparación a la tasa de encuentro de todo el mundo en este periodo, que fue del 20,8 %. Además, la herramienta de eliminación de *software* malicioso de Microsoft detectó y eliminó el *malware* de treinta y cuatro de cada mil ordenadores escaneados en España en el cuarto trimestre de 2015 (una puntuación CCM⁸ de 34, comparada con la medición CCM mundial de 16,9).

La siguiente figura muestra las tendencias de las tasas de encuentro y de infección para España en 2015, en comparación con el mundo en su conjunto.

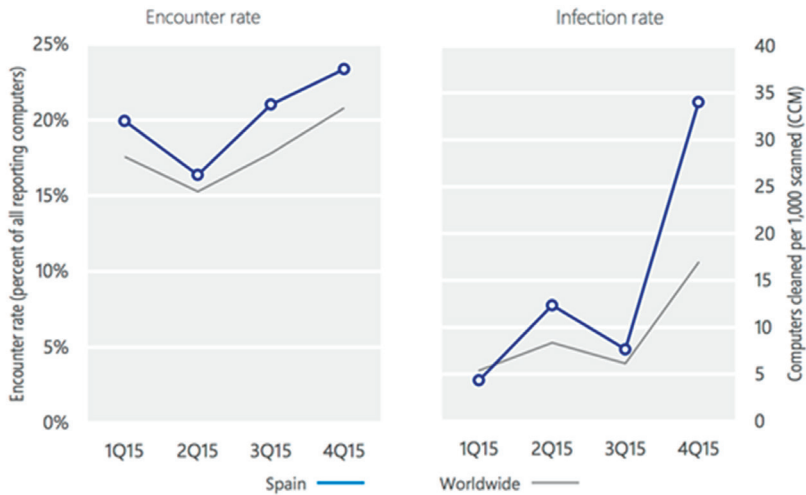


Figura 3.8. Tasas de encuentro y de infección para España en comparación global.
Fuente: Microsoft Corporation: Microsoft Security Intelligence Report, Volume 20, julio a diciembre de 2015, p. 840

La categoría de *malware* más común en España, detectada por Microsoft en el cuarto trimestre de 2015, corresponde a los troyanos, que fueron encontrados en un 5,8 % de todos los ordenadores, por debajo del 7,4 % contabilizado en el tercer trimestre de 2015. La segunda categoría de *malware* más común en España durante el cuarto trimestre de 2015 fue la de los gusanos, que se encontraron en un 2,3 % de los ordenadores, frente al 2,6 % del anterior trimestre. La tercera categoría de *malware* más común en España en el cuarto trimestre de 2015 fue la correspondiente a los «descargadores» y «cuentagotas» (*downloaders & droppers*) con un 2,2 % de los ordenadores, frente al 1,6 % en el anterior trimestre.

⁸ CCM (*Computers cleaned per mille*) o número de equipos limpiados por cada mil, es una medición de la tasa de infección de ordenadores únicos que ejecutan la herramienta de eliminación de *software* malintencionado (MSRT).

Malware categories

Malware encountered in Spain in 4Q15, by category

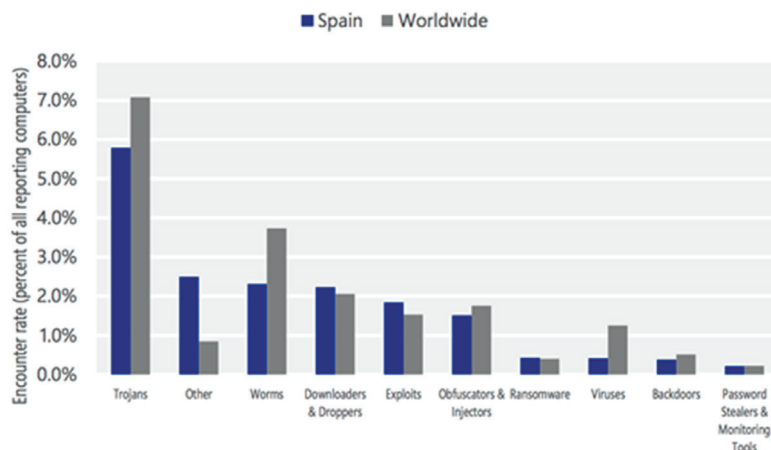


Figura 3.9. Categorías de malware en España detectadas el cuarto trimestre de 2015.
Fuente: Microsoft Corporation: Microsoft Security Intelligence Report, Volume 20, julio a diciembre de 2015, p. 841.

En cuanto al *malware* que infectó los equipos en España durante el cuarto trimestre de 2015, Microsoft ofrece los datos reflejados en los gráficos que se muestran a continuación.

Top malware families by encounter rate

The most common malware families encountered in Spain in 4Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.1%
2	Win32/Dynamer	Trojans	0.9%
3	Win32/Obfuscator	Obfuscators & Injectors	0.9%
4	Win32/Peals	Trojans	0.9%
5	Win32/Sventore	Downloaders & Droppers	0.8%
6	Win32/Skeeyah	Trojans	0.8%
7	INF/Autorun	Obfuscators & Injectors	0.7%
8	Win32/Dorv	Trojans	0.6%
9	Win32/Conficker	Worms	0.5%
10	HTML/Meadgive	Exploits	0.5%

Figura 3.10. Familias de malware encontradas en España en el cuarto trimestre de 2015.
Fuente: Microsoft Corporation: Microsoft Security Intelligence Report, Volume 20, julio a diciembre de 2015, p. 843.

El CCN-CERT ha proporcionado la siguiente información actualizada a 4 de noviembre de 2016.

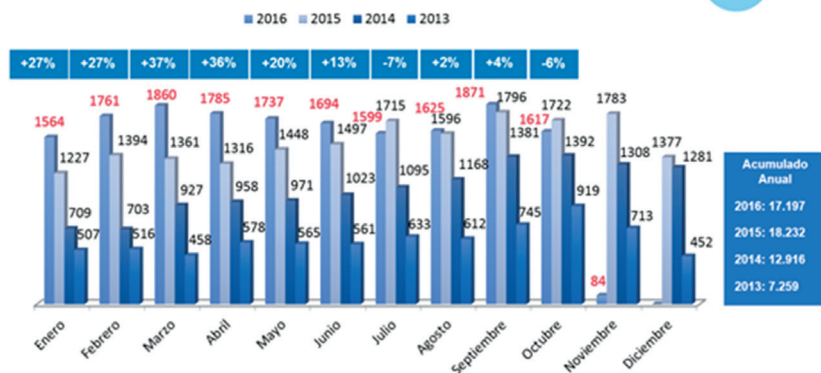


Figura 3.11. Número de incidentes de ciberseguridad gestionados por el CCN-CERT 2013-2016. Fuente: CCN-CERT. 4 de noviembre de 2016.

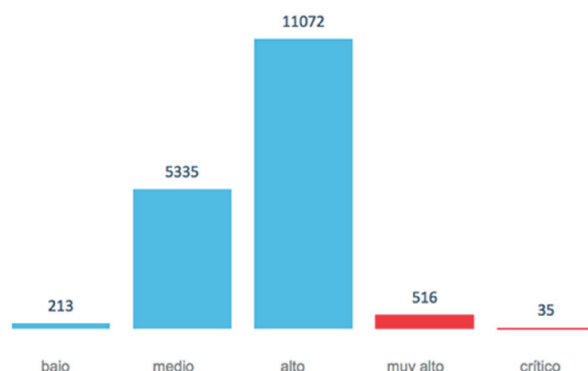


Figura 3.12. Peligrosidad de los ciberincidentes gestionados por el CCN-CERT en 2016. Fuente: CCN-CERT. 4 de noviembre de 2016.

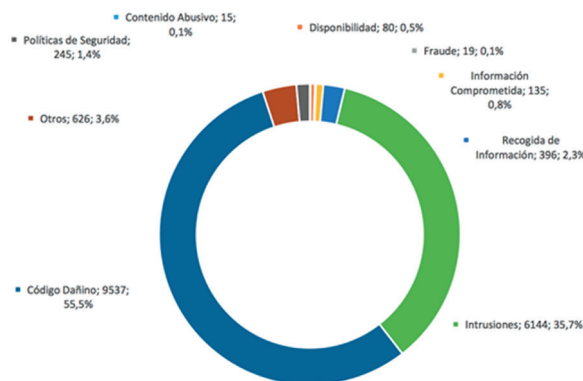


Figura 3.13. Tipología de los incidentes gestionados por el CCN-CERT en 2016. Fuente: CCN-CERT. 4 de noviembre de 2016.

Es significativo resaltar que aunque el CCN-CERT, como CERT Gubernamental Nacional, sirve a las Administraciones públicas (en sus tres niveles, nacional, autonómico y local), a los sistemas clasificados y a las empresas de interés estratégico para el país, buena parte de sus servicios (formación, informes, guías, herramientas, etcétera) están publicados en su portal web y son de libre disposición para cualquier persona.

Conclusiones

El ciberespacio ha introducido una nueva dimensión en las sociedades y su uso se ha incorporado a las mismas de modo cotidiano y generalizado. Los aspectos positivos de la utilización del ciberespacio son numerosos, especialmente en campos como las comunicaciones, la investigación científica, los procesos industriales o la gestión del conocimiento.

Esta revolución tecnológica tiene un elevado impacto social. Los adelantos en las comunicaciones y el abaratamiento de los costes están generando una red en la que pocos elementos escapan a estar conectados, incluso los objetos de uso cotidiano, en lo que se ha venido a llamar el Internet de las Cosas.

Gracias a las nuevas tecnologías y al uso extensivo de internet se están desarrollando proyectos que abarcan las áreas más diversas de las actividades humanas.

Este escenario presenta también nuevos retos a los que no se sustraen los diferentes actores políticos, principalmente los Estados. Entre estos desafíos se encuentran la protección y recuperación de los sistemas de infraestructuras críticas ante agresiones que utilizan el ciberespacio como entorno y vehículo para interferir en las actividades de los ciudadanos y de las instituciones.

De esta forma, hoy en día los Estados deben hacer frente a ataques contra la seguridad de los sistemas de las Tecnologías de la Información y las Comunicaciones de gobiernos, administraciones públicas y empresas con alto valor estratégico.

En este capítulo se han analizado las ciberamenazas en el contexto de los riesgos globales, así como su interconexión con el resto de riesgos. De igual forma se han estudiado los criterios de clasificación de las ciberamenazas, los actores, ámbitos, objetivos, los niveles de peligrosidad de las ciberamenazas y las principales herramientas utilizadas.

Posteriormente se ha presentado la situación en España y los ciberincidentes gestionados por el CERT Gubernamental Nacional, CCN-CERT. España no ha permanecido inmune a las agresiones que utilizan el ciberespacio para atentar contra los más variados aspectos de la seguridad, llegando a verse comprometidos servicios críticos y otros aspectos que afectan a la seguridad nacional.

Desde el Centro Nacional de Inteligencia, la Oficina Nacional de Seguridad y el Centro Criptológico Nacional —destacando su capacidad CERT—, se generan los elementos de prevención y recuperación de los sistemas de las Tecnologías de la Información y las Comunicaciones para que España y los españoles puedan desarrollarse en el entorno digital de forma segura.

Capítulo cuarto

El intercambio de información de ciberamenazas

Miguel Rego Fernández

Director General del Instituto Nacional de Ciberseguridad (INCIBE)

Pedro Pablo Pérez García

Global Security VP en Telefónica & CEO 11paths

Resumen

Las amenazas cibernéticas son cada vez más complejas y por lo tanto más difíciles de gestionar. La compartición de información y el trabajo conjunto entre equipos de respuesta de distintos CERT/CSIRT facilitan la generación de una Inteligencia Global que mejora la capacidad de actuar de forma preventiva. Para ello, es necesario que los agentes públicos y privados se sientan implicados con la ciberseguridad, se establezcan mecanismos que faciliten la coordinación entre los distintos actores públicos y privados y la cooperación, facilitando el intercambio de información

El objetivo principal del *Information Sharing* es la recopilación, el almacenamiento y la distribución de la información necesaria para actuar de forma homogénea, rápida y eficaz contra las ciberamenazas, generando un conocimiento común y compartido. Aunque la regulación presente y futura impone la necesidad de compartir información y de notificar las brechas de seguridad es necesario armonizar a nivel internacional la legislación, superar la desconfianza de facilitar información, frecuentemente considerada de alta sensibilidad y establecer y adoptar estándares para la homogeneización de los formatos.

Abstrac

Cyber threats are becoming more complex and therefore more difficult to manage. Information sharing between different CERT/CSIRT facilitates the creation of a Global Intelligence and improves the ability to act preventively. Therefore, it is necessary to facilitate coordination between public and private actors involved in cybersecurity in order to foster cooperation and the exchange of information.

The main objective of the Information Sharing is the collection, storage and distribution of information necessary to act quickly and effectively against cyber threats, creating a common and shared knowledge. Although the present and future regulation imposes the need to share information and to notify security breaches, it is necessary to harmonize international law, overcome mistrust to provide information, often considered highly sensitive, and establish and adopt standards for homogenization formats.

Palabras clave

CERT, CSIRT, incidente, amenaza, vulnerabilidades, plataforma, formato, regulación, barreras, beneficios, inteligencia, respuesta, mitigación, estándares, cooperación, conocimiento.

Keywords

CERT, CSIRT, incident, threats, vulnerabilities, platform, format, regulation, barriers, benefits, intelligence, response, mitigation, standards, cooperation, knowledge.

Situación actual

Necesidad de intercambiar información de amenazas e incidentes

Ante la creciente complejidad en los ciberataques se requiere un mayor nivel de colaboración entre los actores públicos y privados relacionados con la gestión de las ciberamenazas. La identificación y caracterización de las amenazas del ciberespacio y la detección de incidentes, que realiza localmente un Equipo de Respuesta ante Incidentes (*Computer Emergency Response Team, CERT*), cuando se intercambia de forma controlada mediante servicios de compartición de información, facilita la prevención global de los ciberataques. De esta forma la identificación, análisis y compartición de información por parte de un *CERT* puede facilitar que estos eventos se repitan de forma global y contribuirá a mejorar la eficiencia y al ahorro de tiempo y esfuerzo en la respuesta ante los incidentes, en los análisis forenses posincidente, incrementando las sinergias entre *CERT/CSIRT* y la adopción de prácticas y procedimientos comunes.

Con objeto de mejorar la respuesta ante incidentes y prevenir, por ejemplo, que campañas de *malware* puedan hacerse extensivas globalmente, aparecen en escena las actividades de colaboración potenciadas por organismos internacionales, compañías y multinacionales de seguridad así como *CERT* de todo el mundo. Bajo esta óptica toma forma el concepto de *Information Sharing*.

Equipos de Respuesta ante Incidentes con diferentes niveles de madurez pueden trabajar de forma activa en una respuesta ante incidentes coordinada de forma global, aportando y compartiendo información de valor y mejorando la seguridad de todo el ecosistema. Dado que la naturaleza de los ciberataques frecuentemente es global, es fundamental que la respuesta y neutralización no se limite al ámbito local o nacional sino que se actúe desde una perspectiva transfronteriza. Para que esta acción global sea posible se necesita colaborar intercambiando, de forma segura y confiable, información sobre dichos incidentes.

Sin embargo, poner en marcha y mantener un procedimiento de compartición de información no es tarea tan sencilla como en principio podría suponerse. En general, habrá que superar múltiples escollos que dificultan este proceso. Entre estas dificultades podemos citar: el establecimiento de una relación de confianza, superar el recelo a dar visibilidad a la información obtenida y llegar a un consenso para dar formato a la información y a las cuestiones relacionadas con su tratamiento, mantenimiento, clasificación y difusión. Estamos hablando del uso de estándares.

Inhibidores y habilitadores para la compartición de información de amenazas

Los aspectos técnicos son la barrera más común para el intercambio de información eficaz entre *CERT*. Estos problemas técnicos están relacionados

con la solución utilizada para facilitar el intercambio automatizado y la capacidad de interoperar con otros sistemas desplegados por los CERT/CSIRT locales. Otro problema muy importante está relacionado con la calidad de los datos, es decir, que la información compartida por uno de los actores sea identificada como relevante y de valor para el resto de la comunidad.

Sin embargo, los obstáculos técnicos son más fáciles de superar que los problemas legales, sobre todo con la creciente estandarización para el intercambio, almacenamiento y procesado de la información. En el intercambio de información con los CERT las barreras legales y los problemas de confianza son a menudo los principales obstáculos para que el intercambio se materialice.

Finalmente, a menudo los operadores miembros de la comunidad de intercambio, inmersos en la operativa del día a día, manifiestan un bajo nivel de interés tanto en compartir como en utilizar la información compartida, lo que provoca que el sistema global, poco a poco, vaya perdiendo utilidad y valor.

Barreras en el intercambio de información derivados de aspectos legales

En torno a los aspectos jurídicos y de procedimiento de intercambio de información entre los CERT y otras partes interesadas, los aspectos legales y procedimentales son las barreras más frecuentes. En esencia, los CERT y otras organizaciones similares frecuentemente tienen dudas acerca de si un conjunto particular de información puede ser compartida, con quién y en qué condiciones. Se generan dudas respecto a si la información que se intercambia presenta problemas legales en materia de protección de datos y protección de la privacidad dado que, incluso en el ámbito de la Unión Europea, se pueden encontrar diferentes interpretaciones relativas a los criterios de protección de la privacidad. Debido a estas cuestiones, a menudo el intercambio de información entre los CERT y otros actores se inhibe.

Entrando en detalle sobre los puntos más complicados:

- Retención de datos: la vigencia y periodo de conservación de los datos, así como el ciclo de vida de la información desde su generación, procesado, almacenado, uso y borrado/destrucción es clave para una compartición que legalmente sea viable. Normativas que homologan tratamientos en privacidad a nivel Europeo, mecanismos como Safe Harbour o Privacy Shield ayudan a establecer garantías entre las partes.
- Alojamiento de datos: La complejidad legal que supone el alojamiento *cloud* es relevante, dado que es importante conocer donde están ubicados los sistemas que almacenan los datos así como la legislación del país y los tratados con países afines.
- Compartición de datos de carácter personal: Evidentemente, la transmisión de datos requiere los consentimientos oportunos acorde con la ley

de protección de datos del país y, además, el tener datos tan comunes como las *IP* (considerados datos de carácter personal en varias geografías) añade complejidad legal. Asimismo, siempre que aparecen datos de carácter personal tenemos la complejidad adicional de gestionar adecuadamente los derechos de los titulares, tema que debe ser tenido en cuenta en el proceso de transferencia.

Según algunas opiniones, los problemas legales en el intercambio de información no son únicamente el resultado de la falta de armonización internacional en la legislación de protección de datos sino, y especialmente dentro de la Unión Europea, de las diferentes interpretaciones de las leyes nacionales por parte de diferentes organismos.

Barreras en el intercambio de información derivados de falta de confianza

Los problemas de confianza son algunos de los obstáculos más importantes para la comunicación mejorada y eficaz entre los *CERT* y otras partes interesadas. En ciberseguridad la confianza es la característica más importante de una relación de cooperación exitosa. Además, la confianza se debilita cuando solamente una de las partes está activa en el intercambio de información, sin obtener mucho a cambio de la otra parte.

Comúnmente aparecen diferentes actores donde las fronteras del uso de la información no están claras y requieren clarificar en alto detalle el uso de la misma, así como el alcance del tratamiento. Por ejemplo, es frecuente la aparición de actores en la empresa privada que pueden usar la información para su uso o para la venta, igualmente organismos públicos pueden usar la información para su protección o ayudar a otras administraciones.

	PÚBLICO	PRIVADO
CONSUMIDOR INFO	AAPP X + AAPP Y	ACME
PRESTADOR INFO	AAPP Y	ACME

En relación a la falta de confianza, y especialmente en los *CERT/CSIRT* de ámbito privado, se añade un nuevo problema en base a la desventaja competitiva que supone para un *CERT/CSIRT* que comparte información frente a otro que solo recibe, invirtiendo el primero en recursos humanos y técnicos de los cuales saca provecho el contrario. Esto hace a menudo que la colaboración entre *CERT/CSIRT* privados sea muy escasa.

También es habitual que la información de incidentes críticos, especialmente relacionados con los ataques de tipo APT, en los que de forma frecuente hay robo de información a la víctima no sea compartida en la comunidad con el fin de evitar los problemas reputacionales que puede suponer.

Insuficiente interés por parte de las partes

La comunicación operativa entre los CERT/CSIRT, es una práctica habitual y, por tanto, no es frecuente ver desinterés en el intercambio de información por parte de los mismos. Por lo general, los CERT no solo están dispuestos a compartir información de incidentes de seguridad, sino también a redactar informes y estudios descriptivos que se comparten con la comunidad, informes que son generalmente muy bien recibidos y apreciados entre todos los actores. Sin embargo, debido a las cargas de trabajo, a menudo esta información de alto valor se demora excesivamente en el tiempo. Cuando los CERT están gestionando un incidente los expertos se centran en aspectos muy operativos como la mitigación y la coordinación y a veces no tienen tiempo para compartir informes detallados con el resto de los CERT. La descripción de incidentes de alto impacto, a gran escala, son un ejemplo típico de una situación que generaría un informe a intercambiar. La cultura de compartir y la demanda de información no es sin duda un problema, pero las cargas de trabajo son, a menudo, un inhibidor importante.

Barreras de carácter técnico

Muchos CERT agradecerían recibir entradas de información automáticas de otros Equipos de Respuesta ante Incidentes para utilizar esa información dentro de su comunidad y prevenir incidentes. Sin embargo, esta automatización basada en plataformas de intercambio cuenta, a menudo, con distintos problemas de índole técnico debido a:

Cambios de formato en la información.

Problemas de sincronización horaria o con el sello de tiempo del evento que se está compartiendo.

Los datos recibidos en relación con los incidentes no contienen suficiente información para iniciar una investigación.

Se necesita seguir trabajando de forma global para mejorar los formatos de información a compartir y, aunque existen muchos estándares en el campo de la seguridad, los CERT/CSIRT frecuentemente actúan de forma *ad hoc*.

Es muy importante, antes de convertir los *Data Lakes* donde se aloja la gran cantidad de información generada en auténticos vertederos, tener claros los procesos de conversión de los datos en información, los procesos de generación de metadatos (datos sobre datos), contextualización, etcétera, así como la agregación, correlación y demás procesados con el fin de preparar la conversión final de dicha información en inteligencia (actionable intelligence).

DATOS → INFORMACION → INTELIGENCIA

Beneficios y habilitadores en el Information Sharing

El objetivo principal de *Information Sharing* es el de establecer un procedimiento que permita la recopilación, el almacenamiento y distribución de la información necesaria para actuar de forma homogénea, rápida y eficaz contra las ciberamenazas. Esto, además, revertirá en un mejor conocimiento del *malware*, sus mecanismos de ataque y en facilitar las tareas de prevención y respuesta ante incidentes relacionados con actividad.



Figura 4.1. Beneficios del Intercambio de Información (Fuente: Blog de ERTS/CSIRT SI).

Los beneficios derivados del intercambio de información son:

Generar una conciencia del estado global de seguridad

La compartición de información de incidentes y amenazas entre *CERT/CSIRT* nacionales e internacionales permite construir un mapa de situación de la ciberseguridad a nivel global que aporta la visión de lo que está ocurriendo en el ciberespacio y facilita la generación de un conciencia global, en todos los estamentos de la sociedad, sobre la importancia y necesidad de proteger la información y los servicios digitales.

Un estudio realizado en 2013 por ENISE recalca que seguridad y funcionalidad son las dos causas raíz que nos obligan a una mayor compartición, destacando con menor presión rendimiento, interoperabilidad y ahorro de costes.

Las amenazas cibernéticas son cada vez más complejas y por lo tanto más difíciles de gestionar. La compartición de información y el trabajo conjunto entre equipos de respuesta de distintos *CERT/CSIRT* facilitan la generación de una Inteligencia Global que mejora la capacidad de actuar de forma preventiva y facilita la persecución y neutralización de las amenazas.

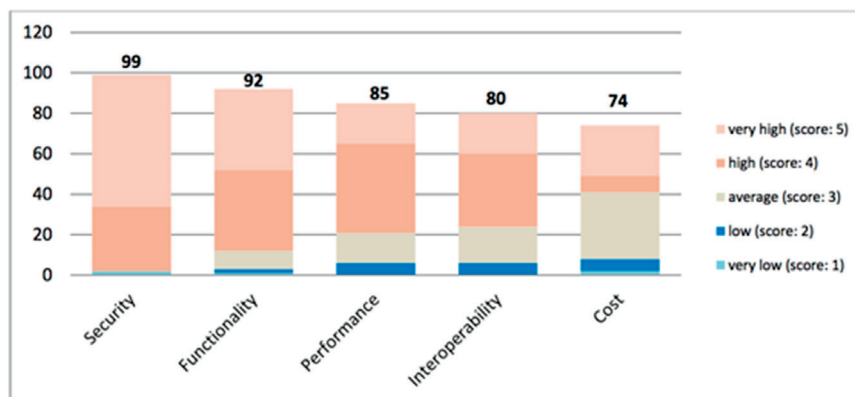


Figura 4.2. Comprensión avanzada de amenazas.

Maduración del conocimiento

Uno de los elementos de información que aportan más valor cuando se intercambian son las «lecciones aprendidas» en relación con la actuación ante una amenaza o un incidente. Esta información mejora el conocimiento colectivo y facilita a los técnicos una mejora en sus niveles de capacitación.

Prevención

Los informes generados por los *CERT* facilitan la caracterización de las amenazas y la descripción de los vectores de ataques y de las ventanas de exposición. Esta información es muy valiosa para que el resto de la comunidad pueda actuar de forma preventiva dentro de su comunidad, identificando de forma temprana situaciones de riesgo y actuando sobre las mismas.

Respuesta ágil

Al compartir información detallada sobre el procedimiento que ha aplicado un *CERT* para la mitigación de un incidente, se facilita que el resto de la comunidad pueda aplicar esas técnicas de forma inmediata, por lo que se ganará en eficacia, reducción del tiempo de mitigación y en eficiencia, aplicando solo recursos estrictamente necesarios en la actuación.

Marco normativo y legislativo aplicable en Europa y España

Europa

Un primer ejemplo en este sentido es la Directiva 2002/58/CE¹ que tiene por objeto proteger la privacidad de los datos personales en el sector de las comunicaciones electrónicas. Sobre la base de un requisito de esta directiva

¹ Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sec-

los proveedores de servicios de comunicaciones electrónicas están obligados por ley en todos los Estados miembros de la Unión Europea, bajo ciertas circunstancias también sus ciudadanos, a notificar fallos de seguridad que afecten a datos de carácter personal.

En segundo lugar, la normativa europea del sector de las telecomunicaciones ha definido el deber de notificación de incidentes de seguridad. Sobre la base de la Directiva marco² (artículo 13 bis) (Parlamento Europeo y del Consejo, 2009), «los Estados miembros se asegurarán de que las empresas que suministran redes de comunicaciones públicas o presten servicios de comunicaciones electrónicas notifiquen a la autoridad reguladora nacional competente de una violación de seguridad o pérdida de la integridad que haya tenido un impacto significativo sobre el funcionamiento de las redes o servicios. En su caso, la Autoridad Nacional informará a las autoridades nacionales de reglamentación de otros Estados miembros y a la Agencia Europea de Seguridad de las Redes y de la Información (ENISA). Por otra parte, la Agencia y la Comisión Europea deben recibir un informe que resuma las medidas adoptadas para resolver los problemas detectados».

Como tercer ejemplo relacionado con la notificación de incidentes, se encuentra la Directiva NIS 2016/1148³, aprobada por el Parlamento Europeo el pasado 6 de julio, que recoge la obligación para los operadores de los siete sectores estratégicos afectados por la directiva de notificar incidentes que tengan un impacto significativo en la seguridad, o continuidad, de los servicios principales que suministran. La Directiva NIS será traspuesta a las leyes nacionales, en el plazo máximo de veintiún meses desde su aprobación, a través de un acto legislativo (ley, decreto o de un instrumento reglamentario de otro tipo).

Un cuarto ejemplo en relación con las obligaciones de notificación se deriva de otro acto legislativo, el Reglamento de servicios de identificación y la confianza electrónicos (eIDAS) (Parlamento Europeo y del Consejo, 2014). El artículo 19 de este Reglamento establece que los proveedores de servicios fiduciarios deben informar de «cualquier violación de seguridad o pérdida de integridad que tiene un impacto significativo en el servicio de confianza proporcionado o en los datos personales» a los órganos de control pertinentes (por ejemplo, una autoridad de seguridad o de protección de datos) y, en algunos casos, a ENISA. Dado que el Reglamento es directamente aplicable en los Estados miembros sin necesidad de transposición, la regla de notifi-

tor de las comunicaciones electrónicas (directiva sobre la privacidad y las comunicaciones electrónicas).

² Directiva 2002/21/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas.

³ Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

cación consagrada en el presente acto legislativo (el Reglamento eIDAS) se aplica directamente a nivel nacional.

España

La primera iniciativa a analizar es la Estrategia de Ciberseguridad Nacional (ECSN), aprobada en diciembre de 2013. Incluye como uno de sus cuatro principios rectores la Responsabilidad Compartida, estableciendo que: «todos los agentes públicos y privados con responsabilidad en esta materia, incluyendo también a los propios ciudadanos, han de sentirse implicados con la ciberseguridad. Para ello, se hace precisa una intensa coordinación de los diferentes organismos de las Administraciones públicas y una adecuada cooperación público-privada capaz de compatibilizar iniciativas y propiciar el intercambio de información».

Este principio se desarrolla, posteriormente, en dos líneas de acción en las que se establece el marco estratégico que facilita el desarrollo de iniciativas para el intercambio de información. En concreto, la línea de acción 1, «Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas» establece la necesidad de garantizar la coordinación, la cooperación y el intercambio de información entre la Administración General del Estado, las Comunidades Autónomas, las Entidades Locales, el sector privado y los organismos competentes de la Unión Europea e internacionales para asegurar la permanente concienciación, formación y capacidad de respuesta a través del Sistema de Intercambio de Información y Comunicación de Incidentes. Esta aproximación se refuerza, posteriormente, a través de la línea de acción 8, «Compromiso Internacional» que, con el objetivo de promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales, facilita la promoción de las mejores prácticas en el conocimiento de la situación, la alerta y la respuesta ante incidentes cibernéticos.

La ECSN fue desarrollada a través del Plan Nacional de Ciberseguridad (PNCS) aprobado en 2014 que, a su vez, se concretó en nueve «planes derivados». El plan derivado 9, «Intercambio de Información sobre Amenazas», se ha dedicado específicamente a desarrollar esta actividad, desarrollando e implantando los procedimientos, mecanismos y herramientas que permitan llevar a cabo el intercambio de información sobre ciberamenazas entre los órganos y organismos con competencia en materia de ciberseguridad de la Administración General del Estado (AGE), las Comunidades Autónomas, las Entidades Locales y el sector privado nacional, así como con los correspondientes organismos competentes de la Unión Europea, OTAN e internacionales; contribuyendo con ello a lograr una coordinación y cooperación eficaces en la ejecución de las necesarias acciones de prevención, detección, reacción y respuesta frente a las ciberamenazas.

El segundo instrumento analizado es el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), el organismo que se encarga de impulsar, coordinar y supervisar todas las actividades que tiene encomenda-

das la Secretaría de Estado de Seguridad del Ministerio del Interior en relación con la protección de las infraestructuras críticas españolas, conforme a la Ley 8/2011⁴, en la que se Establecen las Medidas para la Protección de las Infraestructuras Críticas, posteriormente desarrollada a través del Real Decreto 704/2011⁵. La revisión en 2015 del *Plan Nacional para la Protección de las Infraestructuras Críticas*, de 7 de mayo de 2007, permitió incluir la obligación de que los Operadores de Infraestructura Crítica reporten al CERT de Seguridad e Industria (CERT/CSIRTSI) incidentes de ciberseguridad conforme al nivel de alerta establecida en cada momento. Para facilitar el cumplimiento de este requisito se desarrolló la *Guía de Reporte de Incidentes de Ciberseguridad*⁶, que establece el procedimiento a seguir por los operadores y los niveles de atención y respuesta por parte del CERT/CSIRTSI en función del nivel de alerta existente.



Figura 4.3. Niveles de Alerta del PNPIC (Fuente CNPIC).

El tercer instrumento es la Ley 9/2014, General de Telecomunicaciones⁷, que incluyó en una disposición adicional, la «disposición adicional novena. Ges-

⁴ Ley 8/2011, de 28 de abril, por la que se Establecen Medidas para la Protección de las Infraestructuras Críticas.

⁵ Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas.

⁶ Instrucción pendiente de publicación.

⁷ Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

ción de incidentes de ciberseguridad que afecten a la red de internet», la obligación y necesidad de que los prestadores de servicios de la Sociedad de la Información, los registros de nombres de dominio y los agentes registradores que estén establecidos en España presten su colaboración con el *CERT* competente en la resolución de incidentes de ciberseguridad que afecten a la red de internet. Para el ejercicio de las funciones y obligaciones anteriores, el punto 2 de dicha disposición establece que los prestadores de servicios de la Sociedad de la información, respetando el secreto de las comunicaciones, suministrarán la información necesaria al *CERT* competente y a las autoridades competentes, para la adecuada gestión de los incidentes de ciberseguridad, incluyendo las direcciones IP que puedan hallarse comprometidas o implicadas en los mismos.

Por último, se recoge la necesidad de informar a la Agencia Española de Protección de Datos de las brechas de ciberseguridad que supongan la filtración de información de carácter personal. La Directiva 2002/58/CE ⁸ establece que los proveedores de servicios de comunicaciones electrónicas disponibles para el público están obligados a notificar las quiebras de seguridad que puedan afectar a datos personales a las autoridades nacionales competentes y, en algunos casos, también a los abonados y particulares afectados. El 25 de agosto de 2013 entró en vigor el Reglamento Europeo 611/2013⁹, de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE. El reglamento se aplica a los proveedores de servicios de comunicaciones electrónicas disponibles para el público y, en ciertos casos, a abonados y particulares afectados, y en España lo ha incorporado la reforma de la Ley General de Telecomunicaciones (LGT), en vigor desde el 11 de mayo. En el caso español, la competencia para recibir estas comunicaciones por parte de los proveedores de servicios corresponde a la Agencia Española de Protección de Datos.

La AEPD puso en marcha un sistema para que los proveedores de servicios de comunicaciones electrónicas notifiquen las eventuales quiebras de seguridad que se hayan producido en sus sistemas y que puedan afectar a los datos personales que tratan. El procedimiento está disponible a través del apartado «Notificación preceptiva de quiebras de seguridad» de la Sede Electrónica de la Agencia.

⁸ Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

⁹ Reglamento (UE) n.º 611/2013 de la Comisión de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, sobre la privacidad y las comunicaciones electrónicas.

No se han incluido en este capítulo otras obligaciones derivadas de reglamentos sectoriales que exigen la notificación o compartición de información relacionada con brechas de ciberseguridad.

Además del sector público en España con INCIBE, CCN, Ministerio de Defensa o CNPIC, entre otros, hay empresas privadas que publican constantemente informes y datos sobre ciber amenazas, ejemplos como 11PATHS (Teléfono) o BLUELIV. Cabe destacar también la labor de organismos como CCI, ISMS FORUM o SIC, que fomentan el intercambio de información, generación de reportes así como foros para la compartición de conocimiento. En líneas generales se ha producido un avance muy significativo en los últimos años en materia de compartición de información y conocimiento.

Áreas para una cooperación efectiva en el intercambio de amenazas

Compartir información sobre amenazas de seguridad supone un gran beneficio siempre que recoja contenido de valor y se difunda de forma estructurada. Respecto al contenido, la información útil debe incluir avisos de seguridad sobre vulnerabilidades, informes y estudios sobre protocolos, sistemas y prácticas de seguridad, pero, sobre todo, información preventiva y reactiva para enfrentar ciberamenazas e incidentes de seguridad.



Figura 4.4. Áreas de intercambio de información (fuente CERT/CSIRTSI).

A continuación se describe la información que, potencialmente, se va a compartir de forma colaborativa entre distintos CERT públicos o privados y con sus comunidades:

Avisos de seguridad

Los CERT/CSIRT aglutinan un volumen muy alto de información relacionada con eventos de seguridad asociados a la actividad que desarrolla y que

puede complementar en colaboración con otros actores públicos o privados relacionados con la ciberseguridad. Estos eventos, tratados y procesados de forma adecuada pueden dar lugar a la identificación de incidentes de forma proactiva que luego son comunicados dentro y fuera de la comunidad (*constituency*) de actuación del CERT para provocar una acción de mitigación.

De forma adicional las vulnerabilidades, puntos débiles de seguridad en productos o servicios, son identificadas y reportadas por los propios fabricantes o por investigadores para que puedan corregirse con los correspondientes parches de seguridad. Los CERT evalúan y valoran la información recibida sobre estas vulnerabilidades y emiten avisos que contienen la descripción, la criticidad, los sistemas afectados y las posibles soluciones destinadas a mitigar o minimizar el problema durante el periodo en el que el fabricante elabora el parche.

Informes

Uno de los elementos que utilizan los CERT para fomentar la cultura de la seguridad y la generación de conocimiento especializado en la materia es la creación de guías y estudios sobre temas relacionados con la ciberseguridad. Estas guías y estudios tienen como finalidad aportar tanto valor práctico como teórico para fomentar y mejorar la seguridad digital en todos los ámbitos de la sociedad y para los administradores de sistemas y técnicos en ciberseguridad. En su elaboración, los CERT se basan en su experiencia práctica en la neutralización de una determinada amenaza, en la gestión de un determinado tipo de incidente, en su conocimiento en relación a cómo configurar una determinada tecnología con el objetivo de minimizar la probabilidad de que se pueda ver afectada por un ciberataque...



Figura 4.5. Publicaciones del CERT/CSIRTSI (fuente CERT/CSIRTSI).

Estudios y herramientas

Los CERT ponen a disposición de su comunidad herramientas de ciberseguridad enfocadas a la prevención, detección y respuesta a incidentes de ciberseguridad que, en muchos casos, han sido desarrolladas por el propio CERT en

base a la necesidad de responder a una amenaza concreta, posiblemente de alto impacto, para la que el mercado de productos de ciberseguridad no tiene respuesta en ese momento concreto. En otras ocasiones, estas herramientas facilitadas por el CERT tienen como objetivo mejorar el nivel de concienciación respecto a los riesgos generales o asociadas a una tecnología específica.



Figura 4.6. Estudios y herramientas de «Protege tu Empresa» (fuente INCIBE).

Indicar que también se difunden guías y manuales con instrucciones técnicas para la configuración segura de servidores, sistemas y aplicativos¹⁰.

Incidentes y ciberamenazas

Una de las tareas más importantes de los CERT es proporcionar información sobre nuevas ciberamenazas de forma que la información proporcionada sea relevante y tenga validez y permita que su comunidad u otros CERT/CSIRT puedan protegerse de forma adecuada, facilitando el aprendizaje y la mejora efectiva de los niveles de seguridad.



Figura 4.7. Qué podemos compartir (fuente: plataforma ICARO-INCIBE).

¹⁰ Pueden consultarse en <https://www.incibe.es/protege-tu-empresa/guias>

Uno de los principales problemas para facilitar toda esta información, de forma que pueda ser procesada por el receptor e integrada en su arquitectura de ciberseguridad, es el formato adoptado. A continuación se analizará esta problemática.

Los problemas de la normalización: iniciativas privadas vs estándares de facto

La siguiente dificultad a superar para el intercambio de información es establecer un formato común y reconocido entre los beneficiarios de la información. En este sentido, el uso de estándares posibilitará un uso y una distribución eficiente y rápida de la información.

Con este objetivo, la IETF da los primeros pasos hacia la estandarización en 2007 publicando el RFC 5070 que define *IODEF*, acrónimo para *Incident Object Description Exchange Format*. Esta especificación recoge una serie de pautas dirigidas a los *CISRT* (*Computer Security Incident Response Team*) que son deseables a la hora de documentar los indicadores significativos en incidentes de seguridad. Se basa en esquemas XML para la gestión de los datos y será un punto de referencia para posteriores adaptaciones.

El camino hacia la adopción de un estándar no siempre es único y rápido, y tras la especificación *IODEF* surgen múltiples aproximaciones que pugnan por convertirse en el estándar *de facto*. Entre los estándares que han cobrado mayor protagonismo y aceptación podemos destacar por un lado *OpenIOC* (de la compañía *FireEye*) y las propuestas más colaborativas *Cybox*, *STIX* y *TAXII* (iniciativa del Gobierno estadounidense a través de *MITRE*, *DHS* y *US-CERT*).

Datos a intercambiar

Existen múltiples datos a intercambiar, que van desde simples *HASH* de ficheros maliciosos, *IP* registradas, dominios y elementos de red, hasta las

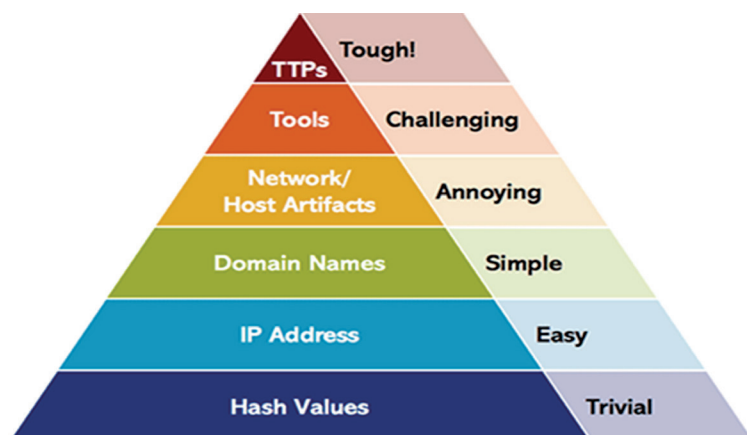


Figura 4.8. «Pirámide del dolor» de David J. Bianco.

herramientas, tácticas y procedimientos de los atacantes. Existen múltiples referencias a los beneficios de la compartición de información para los actores, siendo una de las más conocidas la llamada «Pirámide del dolor» de David J. Bianco (dolor provocado a los atacantes como consecuencia de la acción de compartir).

Métodos de intercambio

Existen tradicionalmente tres métodos de conexión con el objetivo de intercambiar información, además del evidente intercambio uno a uno:

- HUB (Un ente centraliza la información de los productores y la transmite a los consumidores N:1-1:M).
- SOURCE (una repositorio central al que los usuarios se suscriben 1:M).
- P2P (Relaciones que tienen toda la casuística posible 1:1 ,1:M, N:1 o N:M).

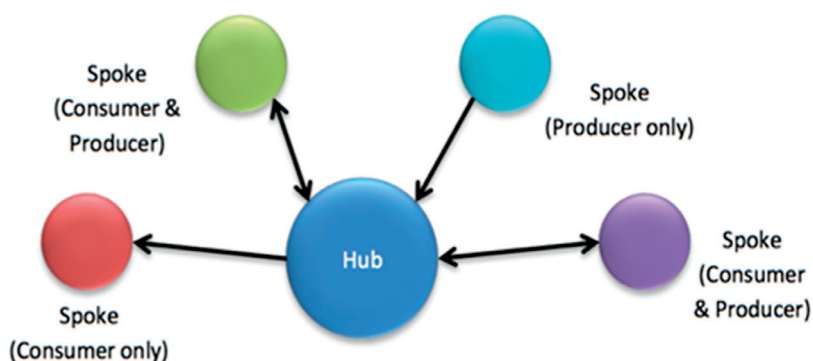


Figura 4.9. HUB.

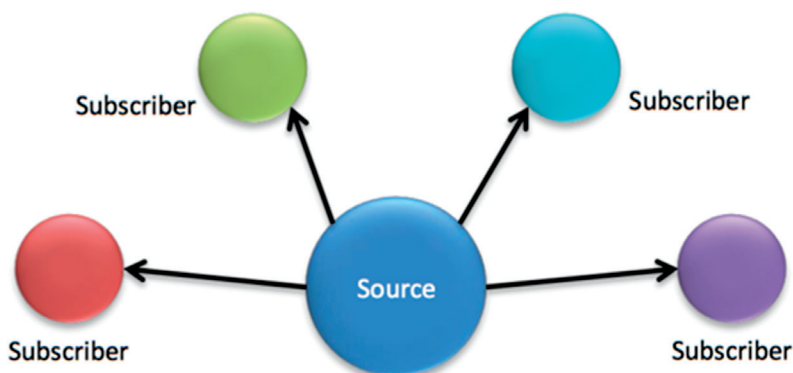


Figura 4.10. SOURCE.

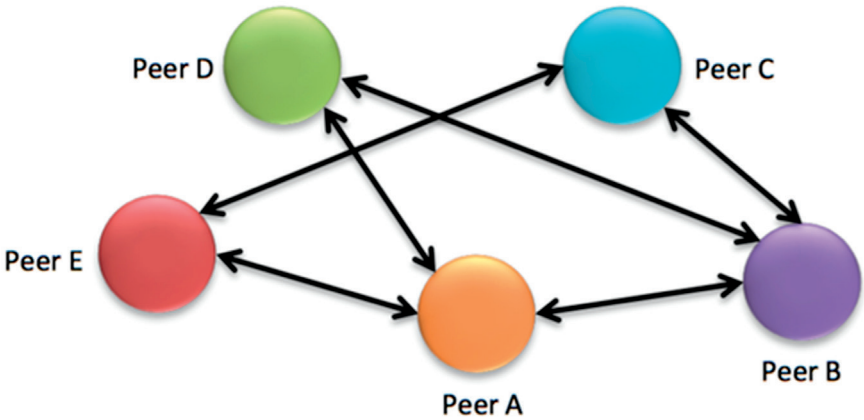


Figura 4.11. PEER to PEER.

Formatos de intercambio de datos de amenazas

Existen múltiples formatos que estandarizan los mecanismos de intercambio de información: STIX, CIF, OPENIOC, CybOX, VERIS, IODEF, TAXII o TLP.

Standard/Framework	2015	2016
Open Threat Exchange (OTX)	50.8%	40.0%
Structured Threat Information Expression (STIX)	45.9%	29.2%
Collective Intelligence Framework (CIF)	39.3%	26.2%
Open Indicators of Compromise (OpenIOC) Framework	32.8%	16.9%
Other	6.6%	13.8%
Cyber Observable eXpression (CybOX)	26.2%	11.5%
Vocabulary for Event Recording and Incident Sharing (VERIS)	19.7%	9.2%
Incident Object Description and Exchange Format (IODEF)	23.0%	8.5%
Trusted Automated eXchange of Indicator Information (TAXII)	32.8%	N/A
Traffic Light Protocol (TLP)	27.9%	N/A

Figura 4.12. Formatos de intercambio de datos de amenazas.

Se distinguen dentro de los estándares varios tipos: los distintos lenguajes formales para la descripción de los indicadores de compromiso (OpenIOC, IODEF o STIX), las definiciones para el intercambio de información (TAXII o RID), las plataformas de gestión de la misma (CDXI, MISP o CIF) y los mecanismos de manejo de incidentes (RT o RTIR).

OpenIOC

Es una iniciativa liderada por la compañía MANDIANT perteneciente a la multinacional FireEye que ha estado presente de manera pionera en la definición y establecimiento del concepto *IoC* (*Indicator of Compromise*)¹¹ en la gestión de incidentes. Un *IoC* es un ente que describe una evidencia forense para identificar una intrusión en un sistema o red.

OpenIOC se distribuye abiertamente bajo licencia Apache2¹² y se basa en un esquema XML para definir *IoC* y permite la extensión con información propia. Cuenta con un alto grado de madurez, simplicidad y reconocimiento, si bien en la parte crítica se trata de una implementación libre apoyada principalmente por una empresa y se le acusa de falta de flexibilidad, dado que en gran medida sigue directrices de un único fabricante orientando su uso hacia productos propios. Esta desventaja, asimismo, tiene su parte positiva, pues hay más de quinientas descripciones de entornos completos desarrollados por MANDIANT, lo cual genera una base de datos de adversarios muy completa.

CybOX, STIX, TAXII

Por otro lado, la organización norteamericana MITRE, organización sin ánimo de lucro y mucho más orientada hacia desarrollos colaborativos en múltiples disciplinas tecnológicas que incluye la ciberseguridad, ha puesto grandes esfuerzos en la estandarización de esquemas de *Information Sharing*. MITRE, en conjunción con el Department of Homeland Security, el National Cyber Security Communications, Integration Center y el US-CERT de Estados Unidos ha dirigido el desarrollo de los estándares: STIX, TAXII y CybOX. Este desarrollo ha transicionado hacia el consorcio de estándares OASIS. Los esfuerzos de estandarización de MITRE están siendo ampliamente respaldados por la industria y AAPP, por lo que múltiples herramientas lo soportan como estándar *de facto*.

Cyber Observable eXpression (CybOX)

El primer borrador de este estándar es de 2010 e incorpora formatos JSON para la caracterización de información sobre *malware*, detección de intrusiones, respuesta y gestión de incidentes y forense digital. En su estructura se definen más de setenta objetos (ficheros, sesión HTTP, conexión de red, etcétera) caracterizados por tipos base de datos, propiedades y relaciones, utilizando un vocabulario predefinido.

¹¹ Back to Basics Series: OPENIOC BY Will Gibb.

¹² www.openioc.org, licencia de contenidos abiertos que fomenta la compartición de la información.

Structured Threat Expression (STIX)

Este estándar es relativamente reciente y presenta un lenguaje estructurado para describir las ciberamenazas en un formato que puede ser compartido, almacenado y analizado de forma consistente. Aparece para aportar una organización de la información de manera altamente estructurada e interrelacionada para lograr una alta legibilidad y fácil comprensión.



A language for modeling and
representing cyber threat
intelligence.



A protocol for exchanging cyber threat intelligence.

Figura 4.13.

STIX serializa los datos en formato JSON y adopta un formato basado en grafos para ofrecer una representación muy intuitiva de los objetos y relaciones entre los mismos. Los objetos se agrupan en nueve dominios clave: observables, indicadores, incidentes, procedimientos, objetivos de explotación, acciones de respuesta, campañas, actores y reportes.

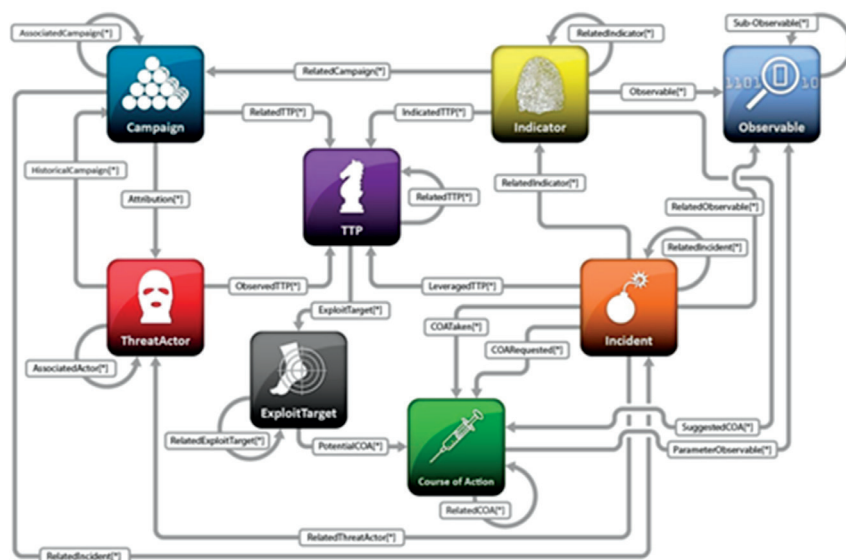


Figura 4.14. Detalle de elementos en STIX. «Detect, SHARE, Protect Solutions for Improving Threat Data Exchange among CERT». ENISA. Octubre de 2013.

Los objetos STIX son indicadores que se encuadran en los referidos dominios y comparten una serie de propiedades para presentar los datos existiendo además objetos de relación que sirven para establecer enlaces entre los dominios (nodos). Es un modelo que está ganando fuerza por su consistencia y usabilidad. Aunque principalmente integra el esquema CybOX, tiene extensiones para incluir otros estándares e indicadores como TLP, OpenIOC, reglas de Snort y YARA.

TAXII, cuya especificación inicial viene de 2012 y fue consolidada en 2014, proporciona unas especificaciones orientadas a conformar un mecanismo flexible de transporte de información de ciberamenazas. TAXII se centra en los mecanismos de distribución de información y adopta otros estándares para el formato de la misma. Así, a través de los servicios definidos por TAXII, las organizaciones pueden intercambiar información de forma segura y automatizada con soporte para múltiples formatos de representación de información de ciberamenazas, especialmente STIX y CybOX. Soporta diversas arquitecturas de comunicación (Hub and Spoke, Peer to Peer y cliente/servidor).

Versión STIX	Información
1.2	Publicada por DHS/MITRE. Esquemas XML.
1.2.1	Publicada por OASIS. Esquemas UML y XML.
2.0	Publicada por OASIS. Basada en JSON y esquema UML.

Tabla 4.1. Estándares de arquitecturas de comunicación.

Estos tres estándares, con el respaldo del consorcio de estándares OASIS, empiezan a consolidarse como opción preferida por múltiples fabricantes para dar formato a la información en sus productos de inteligencia. Entre ellos están importantes multinacionales como IBM (IBM QRadar), Splunk (Splice), Intel Security (McAfee Advanced Threat Defense), VeriSign (iDefense), etcétera.

Múltiples estándares para intercambio de información, un mismo objetivo

ESTÁNDAR	VENTAJAS	DESVENTAJAS
IODEF	Estándar IETF definido por CERT/CSIRTS- Independiente de fabricantes- Formato flexible XML-	Adopción limitada- Orientada a incidentes, puede contener información sensible difícil de compartir. Alta granularidad que dificulta implementaciones.
OpenIOC	Licencia libre (Apache 2). Esquema XML. Herramientas libres de gestión: IOC Editor, IOC finder.	Adopción limitada. Menor flexibilidad de integración. No soporta descripción de tácticas, técnicas y/o procedimientos de intrusión.

ESTÁNDAR	VENTAJAS	DESVENTAJAS
CybOx	Proporciona amplia lista de objetos detallados. Integración con STIX. Independiente de fabricante.	Alta granularidad que dificulta implementaciones.
STIX	Legibilidad. Representación global de objetos con grafos, incluyendo relaciones. Integración de esquema CybOx. Flexibilidad para integrar otros esquemas.	Adopción relativamente reciente.

Tabla 4.2. Múltiples estándares para intercambio de información.

Aunque no se pueda decir que exista un único procedimiento universalmente aceptado en *Information Sharing*, sí podemos concluir que los métodos descritos en este artículo se perfilan como los más utilizados. Estos estándares cuentan cada uno con sus pros y sus contras, siendo en última instancia una decisión del emisor de la información escoger entre uno u otro.

Respecto a los repositorios para la compartición, cabe destacar *CIF* y *MISP*. Mediante *CIF* (*Collective Intelligence Framework*) se detalla el marco para el almacenamiento de la inteligencia en un repositorio central, donde la información es guardada según *IODEF*.



Figura 4.15. «Detect, SHARE, Protect Solutions for Improving Threat Data Exchange among CERTs». ENISA. Octubre de 2013.

OTX

Open Threat Exchange es la apuesta lanzada por ALIEN VAULT; fabricante conocido por sus sistemas USM (Gestión Unificada de la Seguridad) y desarrolladores originales del proyecto OpenSource OSSIM. OTX es una plataforma para el intercambio en la nube, que funciona con su propio formato + OpenIOC + STIX, que facilita la compartición de amenazas. La plataforma describe tanto el intercambio de información, el metalenguaje y el API para su conexión. La principal ventaja es la posibilidad de suscripción a los distintos *PULSES* (IOC de una fuente/s) así como la creación de nuevos, así como una lista de IP con su reputación. Gracias a toda la información almacenada, no solo se define el intercambio sino que la existencia de un repositorio alimentado en tiempo real por ALIENVAULT y diversos aliados (empresas y particulares) otorga un valor diferencial a este sistema.

El repositorio soporta incluir información en formato OPEN IOC o ficheros STIX, por lo que representa en la actualidad una fuente de indicadores de compromiso ampliamente utilizada.

MISP

MISP es una plataforma de intercambio de amenazas basado en un *software* libre de código abierto y orientado a facilitar la compartición de información de indicadores de compromiso (IOC) y de amenazas cibernéticas. MISP puede almacenar IOC de una manera estructurada, simplificando el proceso



Figura 4.16. Formas de utilización de MISP.

de correlación, las exportaciones hacia sondas de detección de intrusiones (IDS) o sistemas de correlación de eventos de seguridad (SIEM), ya sea en formatos STIX o en OpenIOC.

Inicialmente fue construido para ser utilizado en el ámbito del NATO Computer Incident Response Capability (NIRC), MISP permite compartir características técnicas de las amenazas dentro de una comunidad de confianza, sin tener que incluir información sobre el contexto del incidente. Esto facilita la preservación de la confidencialidad de información sensible relacionada con un incidente de ciberseguridad, como el activo afectado y el grado de impacto o de afectación.

MISP combina un repositorio de búsqueda de información multidireccional con mecanismos para su distribución dentro de la comunidad. También proporciona automatización para la importación y exportación de datos de forma automática y una interfaz para conectar con otros entornos y sistemas.

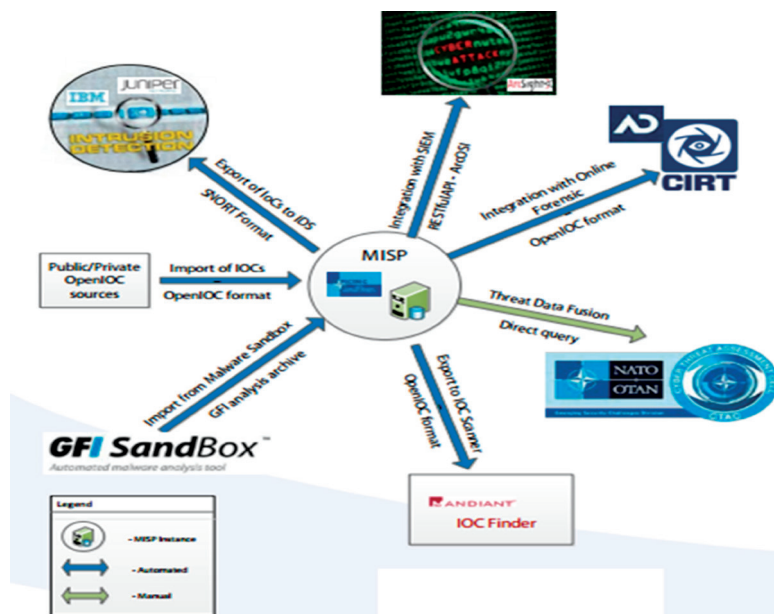


Figura 4.17. Uso de MISP en NCIRC.

Otra ventaja de la plataforma es la posibilidad de establecer una arquitectura federada entre comunidades. Esto permite que el intercambio de información entre comunidades que representan, por ejemplo, países, se haga de forma segura y controlada en base a los criterios que se hayan establecido dentro de esa comunidad, y facilita la configuración de plataformas «de segundo nivel» que representan necesidades específicas de los distintos ámbitos en los que se pueda estructurar esa comunidad, por ejemplo, los distintos sectores productivos: energía, transporte, finanzas, etcétera. De esta

manera, la información es relevante en cada nivel y no se comparte fuera de ese colectivo de confianza de forma no controlada.

Análisis de requisitos de los actores del ecosistema público-privado para el intercambio de amenazas

En la actualidad existen numerosos ecosistemas para el intercambio de información que pueden dividirse en según múltiples atributos:

- Alcance: nacionales, regionales y mundiales.
- Tipología: privados, Administraciones públicas o acceso universal.
- Acceso: gratuitos, membresía o pago.
- Ámbito: B2B (empresas), B2C (particulares), G2G (Estados) o G2C (ciudadanos).
- Sectores: industriales, operadores críticos, banca, universales, etcétera.

Empresas, Administraciones y usuarios/ciudadanos

Una vez vistos los métodos de descripción de las posibles amenazas, es importante reseñar cómo se genera la inteligencia por los diversos actores así como, cómo se produce el consumo de la misma. Normalmente la inteligencia es generada desde:

- Administraciones: locales (ejemplo: CESICAT o GVA CERT), nacionales (CCN o INCIBE) o regionales (ENISA, OAS o USCERT)
- De empresas: normalmente con ámbito global (Telefonica, Karspersky, Mandiant-FEYE, ThreatConnect, ThreatStream, Symantec, McAfee o Digital Shadows entre otras).
- Organizaciones: principalmente englobadas en los distintos grupos de FS-ISAC (SOLTRA) o bajo organizaciones sin ánimo de lucro tipo FIRST-TERENA, APWG o ISMS.
- Particulares: con el auge de las tecnologías sociales, cada vez se comparte más información en *blogs*, Twitter o simplemente repositorios creados por personas con el ánimo de compartir información. El rol que normalmente tienen los particulares/ciudadanos en la compartición de información de este tipo, es el de receptores de la inteligencia. Organismos como INCIBE dedican gran parte de sus programas a la concienciación y sensibilización de los ciudadanos en materias de ciberseguridad.

ISAC vs ISAO

El ecosistema formado por los centros de análisis y compartición de información (*Intelligence Sharing and Analysis Centers, ISAC*) y su unión con los diversos actores forma uno de los mecanismos más ágiles para la distribución

de la información. El Gobierno americano ha fomentado la creación de estos organismos para la compartición de información con especial énfasis en la protección de operadores críticos.

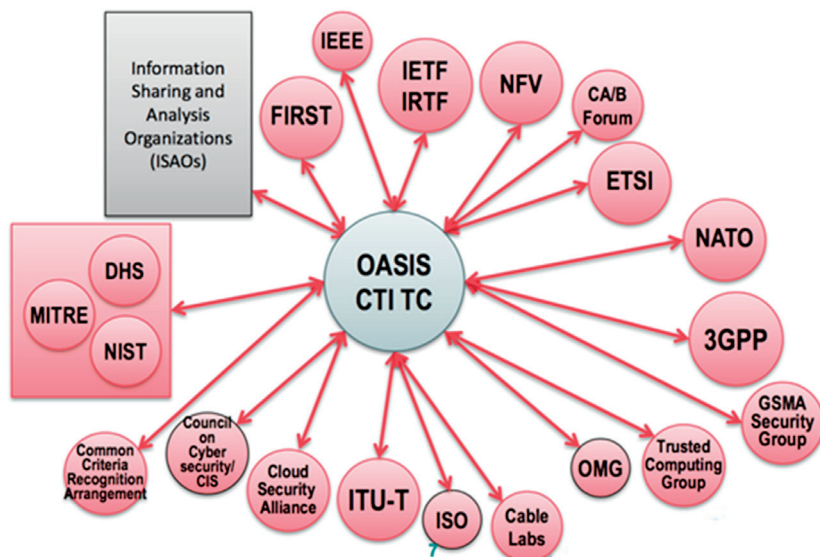


Figura 4.18. Fuente www.oasis-open.org.

En España cabe recalcar que la protección de las infraestructuras críticas está bajo el CNPIC, el cual gestiona alertas y compartición del conocimiento en dicho ámbito.



Figura 4.19. Sistema PIC.

Enisa define en Europa los operadores críticos como: energía, agua, alimentación, salud, finanzas, orden público, transporte, espacio, nuclear-química y tecnología-comunicaciones.

Fabricantes y proveedores de servicios de inteligencia

En la actualidad existen cientos de empresas que proveen servicios de inteligencia. Dentro de la cadena de valor existen principalmente cuatro enfoques:

Generadores de información, inteligencia estándar y accionable. Asimismo, se produce desde información básica, pasando por inteligencia de fuentes abiertas OSINT hasta la que requiere de intervención manual HUMINT.

Herramientas para la gestión de la inteligencia y gestión de incidentes: aparecen desde simples plataformas para la gestión de la información hasta mega *suites* que gestionan todo el ciclo de la inteligencia así como su aplicación en la organización y el enriquecimiento constante de la información.

Servicios de acción sobre la inteligencia: normalmente prestados por MSSPs o compañías especialistas en seguridad que, tras la recolección de la inteligencia, son especialistas en aplicarla sobre elementos de red (por ejemplo, para evitar un ataque de denegación de servicio) o sobre un incidente existente (por ejemplo, realizar un análisis forense completo y poder atribuir las causas, origen y atribución completa).

Fabricantes de tecnología: permiten el uso automático o semiautomático de la inteligencia para mejorar la prevención y detección en materia de seguridad.

Organismos oficiales (CERT, CSIRT y agencias públicas)

La compartición de información en Europa ha evolucionado en los últimos años de manera drástica. En base a los informes de 2013, donde básicamente el email (seguro o estándar) era la principal fuente de intercambio no estructurado, en la actualidad numerosos CERT/CSIRT intercambian información mediante STIX/TAXII.

Los datos recolectados provienen de un estudio de ENISA¹³ sobre dieciocho CERT gubernamentales, cinco universitarios y cuatro de empresas.

En el informe realizado se destacan los puntos que inhiben el intercambio, con su clasificación en: legal, técnica, procedimientos, confianza o interés.

¹³ *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*. ENISA. Diciembre de 2015.

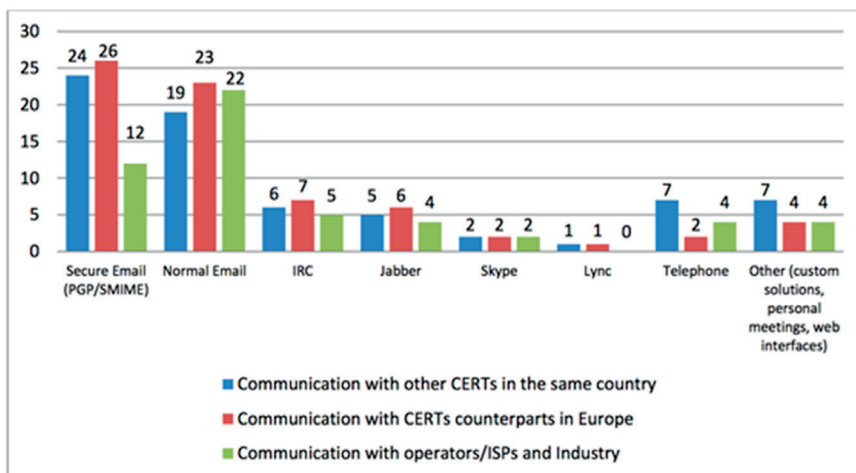


Figura 4.20.

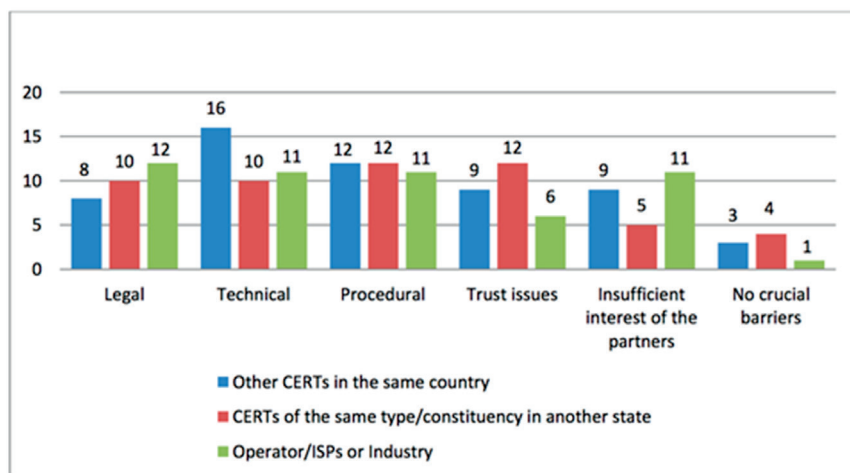


Figura 4.21.

El caso norteamericano: Cyber Threat Intelligence Integration Center (CTIIC)

CTIIC¹⁴ nace en febrero del año 2015 a través de un Memorando Presidencial¹⁵ con el objetivo de proporcionar análisis de inteligencia de todas las fuentes integradas relacionadas con las amenazas informáticas extranjeras e incidentes cibernéticos que afectan a los intereses nacionales, apoyando

¹⁴ www.dni.gov/index.php/about/organization/ctiic-who-we-are

¹⁵ Presidential Memorandum-Establishment of the Cyber Threat Intelligence Integration Center.

a los centros responsables de la seguridad cibernética y de la defensa de la red del Gobierno de Estados Unidos y facilitar y apoyar los esfuerzos para contrarrestar las amenazas cibernéticas.

El *CTIIC* no es un centro operativo y, por tanto, no gestiona incidentes pero apoya a distintos organismos federales con sus funciones operativas, proporcionando a estas entidades, además de a otros departamentos y organismos, la inteligencia necesaria para llevar a cabo sus misiones de seguridad cibernética.

Estructura organizativa

El *CTIIC* apoya al Consejo Nacional de Seguridad en el cumplimiento de sus responsabilidades de seguridad cibernética y tienen una estrecha colaboración con todos los departamentos y organismos que realizan funciones de seguridad cibernética en el Gobierno.



Figura 4.22. Escudo oficial del CTIIC (Fuente DNI).

Responsabilidades del Centro

Proporciona análisis de todas las fuentes de la inteligencia integrada en relación con amenazas informáticas extranjeras o relacionadas con incidentes cibernéticos que afectan a los intereses nacionales de Estados Unidos.

Apoya al Centro de Integración Nacional de Seguridad Cibernética y Comunicaciones, al Mando Conjunto de Ciberdefensa, a la Fuerza Conjunta de Investigación Cibernética y a otras entidades gubernamentales de Estados Unidos correspondientes a proporcionar acceso a la inteligencia necesaria para llevar a cabo sus respectivas misiones.

Supervisa el desarrollo y aplicación de las capacidades de inteligencia compartida (incluidos los sistemas, programas, políticas y estándares) para mejorar el conocimiento de la situación de la inteligencia relacionada con las

amenazas informáticas extranjera o relacionados con incidentes cibernéticos que afectan a los intereses nacionales.

Se asegura que los indicadores de la actividad maliciosa y los informes de amenazas se puedan distribuir a las agencia de los Estados y a las entidades del sector privado.

Facilita y apoya los esfuerzos para desarrollar e implementar planes para contrarrestar amenazas informáticas contra los intereses nacionales de Estados Unidos.

Conclusiones y Recomendaciones

Como se ha descrito en el capítulo, el proceso de recolección de datos y su conversión en información para poder llegar a generar inteligencia sobre la misma no es un proceso trivial. Asimismo, la capacidad de «accionar» dicha inteligencia es diversa, dependiendo de la calidad de la misma, su naturaleza o capacidad del receptor. Los avances en estandarización en los últimos cinco años han sido espectaculares, por lo que desde OASIS a buen seguro se generara un estándar que será usado ampliamente por la industria *de facto*.

Cabe destacar la necesidad de mejorar los incentivos para la compartición, dado que la complejidad existente en el ecosistema actual (origen de la información, receptores, privacidad, confidencialidad o la propia integridad) genera una complejidad que inhibe la distribución de información por problemas políticos, económicos, socioculturales, técnicos o legales.

Las distintas administraciones locales, nacionales o regionales disponen de equipos para fomentar la creación y distribución de inteligencia en cibermenazas (ejemplos desde los *CERT* locales de administraciones públicas, *CERT* de Seguridad e Industria, el *CCN-CERT* o el *CERT* de las Fuerzas Armadas (ESPCERTDEF) y organismos europeos como *EUROPOL EC3* o *ENISA*). Asimismo, los distintos Ejércitos cuentan en la mayoría de los países *NATO* con un quinto dominio (CyberSpace) donde se genera información y se coopera para la mitigación de las distintas cibermenazas existentes. En el caso de España, esas funciones son realizadas por el Mando Conjunto de Ciberdefensa, responsable del planeamiento y la ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa y otras que pudiera tener encomendadas.

Por otro lado en el sector privado se consumen ampliamente las informaciones generadas para operadores críticos así como la inteligencia generada por las múltiples empresas existentes, si bien cada vez es más frecuente el uso de la información desde los líderes del mercado y organizaciones *FSISAC*.

En materia de capacidades, en la actualidad, tanto Estados Unidos como China e Israel llevan la delantera en los modelos públicos, por todo ello desde

los distintos organismos y empresas europeas englobados bajo ECSO, se ha priorizado la ciberseguridad en el horizonte 2016-2019 con 450 millones de euros en ayudas, lo cual a buen seguro ayudará a la creación de datos de ciberinteligencia de calidad y su compartición óptima.

Bibliografía de consulta

INCIBE (2016). León, julio de 2016. www.incibe.es

Bitácora: <https://www.certs.es/alerta-temprana/bitacora-ciberseguridad/threatexchange>

blog de ciberseguridad:

§ <https://www.certs.es/blog/unidos-las-ciberamenazas-information-sharing>

Servicio ICARO:

§ <https://www.certs.es/servicios-operadores/icaro>

Plataforma MISP.

<http://www.misp-project.org/>

<https://circl.lu/services/misp-malware-information-sharing-platform/>

HiTrust. 2016.

Intercambio de información sobre amenazas:

<https://blog.hitrustalliance.net/threat-information-sharing-an-increasingly-effective-weapon-for-fighting-ransomware-and-other-cybercrime/>

ENISA, European Union Agency for Network and Information Security

(2014) Detect, SHARE, Protect. *Solutions for Improving Threat Data Exchange among.*

(2015) *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches.*

OTAN, Organización del Atlántico Norte.

<https://www.ncia.nato.int/Documents/Agency%20publications/Malware%20Information%20Sharing%20Platform%20%28MISP%29.pdf>

Libros y todo J: <http://dl.acm.org/citation.cfm?id=2994544>

The White House (2015). *Fact Sheet Cyber Threat Intelligence Integration Center.*

<https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center>

Office of the Director of National Intelligence (2015).

<https://www.dni.gov/index.php/about/organization/ctiic-who-we-are>

<https://www.dni.gov/index.php/about/organization/ctiic-what-we-do>

Capítulo quinto

Cooperación público-privada en la protección de infraestructuras críticas

Fernando Sánchez Gómez

Director del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). Es teniente coronel de la Guardia Civil y diplomado de Estado Mayor por el Centro Superior de Estudios de la Defensa Nacional

Justo López Parra

Responsable de Prevención y Respuesta a la Ciberamenaza en Endesa. Es Ingeniero Informático por la Universidad de Castilla La Mancha, certificado CISM y está homologado como director de Seguridad Privada por el Ministerio del Interior

Resumen

Este capítulo se inicia mostrando las nuevas amenazas que han surgido contra el sistema de sectores estratégicos, tratando, asimismo, la colaboración entre las empresas privadas y los organismos públicos para su protección. Como ejemplos de estas amenazas se estudian los ciberataques Blackenergy, que consiguió dejar sin electricidad a una población de 1,5 millones de habitantes, y Stuxnet, primer ciberataque que de forma masiva consiguió la destrucción física de su objetivo.

El contenido de este trabajo está basado en la intensa colaboración que el CNPIC (Centro Nacional para la Protección de las Infraestructuras Críticas) y Endesa han desarrollado, en el marco de la protección de las infraestructuras críticas, durante los últimos años, aprovechando así la experiencia adquirida en el tratamiento conjunto de las ciberamenazas. Actualmente, las herramientas que el CNPIC, en colaboración con el INCIBE, pone al servicio de las organizaciones que proveen servicios esenciales son: apoyo frente a incidentes, equipo de respuesta a incidentes cibernéticos (CERTSI_), servicios de alerta temprana, planificación y desarrollo de ciberejercicios y acuerdos de colaboración. Al mismo tiempo, la Oficina de Coordinación Cibernética del Ministerio del Interior ejerce la tarea de llevar a cabo la coordinación operativa entre los elementos tecnológicos ya reflejados y las capacidades de investigación y de persecución del delito propias de las Fuerzas y Cuerpos

de Seguridad del Estado, constituidas por las unidades tecnológicas de la Guardia Civil y de la Policía Nacional.

Para finalizar este capítulo, se da cuenta de distintas herramientas previstas para continuar potenciando la colaboración público-privada que tan satisfactorios resultados están dando para mejorar la seguridad de nuestros servicios esenciales.

Palabras clave

Ciberataque, amenaza, stuxnet, blackenergy, normativa, colaboración público-privada, *CERT* (equipo de respuesta a emergencias informáticas), infraestructuras críticas, servicios esenciales, planificación.

Abstract

This chapter begins by describing the latest threats that have emerged against the system of strategic sectors. It is also highlighted the need of seeking cooperation among all actors and building a robust public-private partnership scheme. Some examples of these new threats are *BlackEnergy*, which managed to leave without electricity a population of 1.5 million, and not so recently, *Stuxnet*, first known cyberattack which achieved a massively physical destruction of its target.

The content of this work is based on the intensive collaboration developed in the last few years between CNPIC (National Centre for the Protection of Critical Infrastructure) and Endesa, taking advantage of the experience already acquired in the joint treatment of cyberthreats.

Currently, the tools that the CNPIC, in collaboration with the INCIBE, makes available to those organizations that provide essential services include: support against incidents, a devoted cyberincidents response team (*CERTSI*), early warning services, planning and development ciberejercices, and non disclosure agreements for information sharing. At the same time, the Cyber Coordination Office, of the Ministry of the Interior, is entitled to carry out operational coordination between all these actors and the Law Enforcement Agencies, whose capabilities of investigation and crime pursuit are provided by the technological units of the Civil Guard and the National Police.

Finally, this chapter ends accounting for a number of tools that could be useful to further enhance the public-private partnership.

Keywords

Cyberattack, threat, stuxnet, blackenergy, regulation, public-private partnership, *CERT* (computer emergency response team), critical infrastructures, essential services, planification.

Introducción

Tras los últimos ciberataques conocidos contra los servicios esenciales de diferentes países de nuestro entorno, con distintos grados de afección sobre los que se conocen como infraestructuras críticas y sus redes de comunicaciones, cabe, en buena lógica, hacerse la pregunta de cómo de resistente y adaptable es la sociedad moderna e hipertecnificada de hoy a, por ejemplo, la dependencia del suministro de energía, agua o medios de pago.

Si una gran ciudad, o una extensa zona de un territorio cualquiera, sufriese un ciberataque, dirigido por otro Estado o por terroristas, que lograse eventualmente una caída del servicio eléctrico, del transporte público o de las telecomunicaciones durante, digamos, veinticuatro horas ¿cómo respondería la población?, ¿cómo responderían los mercados?, ¿cómo responderían nuestros sistemas de emergencia?, ¿cuándo se restituirían los servicios?, es más, ¿a qué otros servicios podría arrastrar un posible «efecto dominó»? y, sobre todo ¿cuáles serían sus consecuencias?

Preguntas como estas podrían repetirse *ad eternum* pero lo que parece claro es que nuestra sociedad, la sociedad postmoderna, no solo no está aún preparada, sino que ni siquiera contempla un posible fallo generalizado de los servicios esenciales sobre los que pivotan nuestra vida económica, política, social y nuestra propia supervivencia como individuos. Esto mismo es lo que ha convertido a los servicios esenciales y a las infraestructuras críticas que los sustentan en un objetivo de primer nivel y es lo que ha provocado que las naciones modernas se hayan puesto manos a la obra para proteger estos activos que suponen la columna vertebral del mismísimo estado del bienestar.

El estudio de los ataques realizados contra infraestructuras estratégicas nos sirve para confirmar que una empresa privada no puede defenderse por sí misma de ataques cada vez más sofisticados y agresivos. La desproporción entre los medios con los que cuenta el atacante y el defensor hace que solo sea cuestión de tiempo el que aquel consiga el objetivo planteado. Por otra parte, el paradigma de la globalización ha hecho posible que, por primera vez en la historia de la humanidad, las grandes amenazas contra los Estados no tengan por qué provenir de otros Estados, sino que han entrado en juego otra serie de actores cuyas capacidades pueden poner en jaque o desestabilizar países enteros. De la misma manera, la participación del sector privado en la seguridad nacional, dados los recursos y la información que maneja, no es ya un factor meramente deseable sino que se ha convertido en una verdadera necesidad.

La colaboración público-privada viene a dar algunas de las claves y también algunas de las herramientas apropiadas para que las empresas privadas y los propios Estados puedan defenderse con mayores garantías contra estas amenazas de nuevo cuño.

En España esta colaboración es ya un hecho, sin perjuicio de que aún queda mucho camino por recorrer. Varios de los sectores estratégicos de nuestro

país, si bien es verdad que en diferentes escenarios de madurez, trabajan de forma coordinada y regular con el Centro Nacional para la Protección de las Infraestructuras Críticas y, a través de este, con el CERT de Seguridad e Industria (CERTSI_) en la protección de los sistemas informáticos que dan soporte a las infraestructuras críticas del país. Muestra objetiva de ello es que, tan solo en la primera mitad de 2016, este CERT había trabajado ya sobre doscientos sesenta y dos incidentes reportados sobre activos críticos de nuestro país. Más del doble que en todo 2015 (ciento treinta y cuatro). Y más del cuádruple que en todo 2014 (sesenta y tres)¹.

Como indicaba en el párrafo anterior, el trabajo que el CNPIC viene realizando contempla varios escenarios de madurez. Uno de los más satisfactorios, en cuanto a los resultados y en cuanto a la obtención de la sinergia necesaria, viene llevándose a cabo con el sector eléctrico español, de los que ENDESA, que ha tenido a bien colaborar con nosotros en este artículo, es uno de sus mejores representantes. El camino recorrido por el momento en este modelo de colaboración público-privada es un posible caso de éxito que estamos intentando replicar en muchos otros proyectos que ahora estamos iniciando.

Un poco de historia

Con el inicio del siglo XXI aparece una nueva tipología de ciberataques muy sofisticados, llevados a cabo por grupos organizados apoyados por Estados o directamente por esos Estados. El objetivo inicial era robar información estratégica que sirva a los intereses del atacante. Con el tiempo, ese objetivo inicial se amplía a otros más ambiciosos como el bloqueo de servicios públicos o la toma de control de sistemas industriales, que permitan manejar en remoto infraestructuras estratégicas para el funcionamiento del país.

Este tipo de ataques suponen un nuevo tipo de amenaza llamada APT (*Advanced Persistent Threat* o Amenaza Persistente Avanzada). Las amenazas persistentes avanzadas² suelen manifestarse como un *malware* (*software* malicioso) en el que se invierten millones de dólares, que persigue objetivos muy concretos, tras el que, en un buen número de casos, se pueden encontrar Estados u organizaciones terroristas o criminales y que está especialmente diseñado para mantenerse oculto en el sistema atacado y que aprovechan vulnerabilidades de *software* desconocidas hasta ese momento o usan técnicas de ingeniería social muy concretas con las que infectar al personal de la empresa objetivo.

En este tipo de amenazas, las medidas de seguridad habituales no son efectivas ya que el *malware* se ha diseñado para que las herramientas de segu-

¹ Fuente: CERTSI_. *Informe Situación Ciberseguridad*. Septiembre de 2016.

² Fuente: CNPIC. *Ciberdelincuencia, ciberterrorismo, y protección de infraestructuras críticas*. Documento PIC_8_1.pdf

ridad no las detecten y por lo tanto no actúe contra él. Los sistemas de seguridad utilizados actualmente en las empresas como antivirus, *IPS* (Sistemas de Protección de intrusiones) o *firewalls* (cortafuegos), basan la detección de *malware* en el uso de bases de datos de firmas de *malware* conocido. Es decir, de *software* que sabemos que es malicioso. Pero si es la primera vez que se usa este *software* los sistemas de seguridad no lo detectarán. Esto provoca la dificultad para identificar el *malware* y por lo tanto para tratarlo de forma eficaz.

Actualmente, los sistemas informáticos ocupan un lugar central en nuestra vida, dando soporte a multitud de procesos industriales, procesos ligados a nuestra actividad económica y social, como los ligados a la energía, el agua o el transporte. Como activos importantes de un país, dentro de un conflicto internacional, estos sistemas se han convertido en objetivos atacables y, por supuesto, en potenciales objetivos terroristas. El concepto de guerra informática o ciberguerra hace referencia al desplazamiento de un conflicto que toma el ciberespacio y las tecnologías de la información como campo de operaciones. Podemos definir la guerra cibernética como «el conjunto de acciones llevadas a cabo por un Estado para penetrar en los ordenadores o en las redes de otro país con la finalidad de causar perjuicio o alteración».

La ciberguerra ya ha sido empleada en diversos conflictos, tanto en ofensivas militares de un país contra otro como de un grupo terrorista en contra de un gobierno.

Estos son algunos de los ataques más importantes que se han realizado en los últimos años:

- BlackEnergy, Ucrania 2015. Este *malware* de tipo «troyano», programa malicioso que permanece oculto en el equipo infectado y ofrece al atacante acceso remoto al mismo, infectó a varias compañías eléctricas ucranianas y provocó apagones de varias horas en la ciudad ucraniana de Ivano-Frankivsk.
- Stuxnet, Irán 2010. Stuxnet es un el primer gusano (*software* malicioso que se duplica a sí mismo) conocido dedicado a espiar y manipular sistemas industriales. El ataque tuvo como objetivo los sistemas de centrifugado de las plantas de enriquecimiento de uranio de Irán, logrando retrasar el programa nuclear iraní durante al menos dos años.
- Ciberataque a Estonia, 2007. El traslado en Tallin del Soldado de Bronce, monumento a los soviéticos caídos durante la II Guerra Mundial, provocó un ciberataque el 27 abril de 2007 que consiguió bloquear el acceso a sitios web de organizaciones públicas y privadas de Estonia, incluidos el Parlamento, bancos, ministerios y periódicos. En el momento álgido de los ataques, los teléfonos móviles y las tarjetas bancarias dejaron de funcionar.
- Titan Rain, EEUU 2003. «Titan Rain» fue el nombre en clave que se le asignó a una serie de ataques coordinados sobre sistemas de información de Estados Unidos llevados a cabo desde 2003 hasta 2006, con posi-

ble origen en China. Los atacantes lograron acceso a las redes corporativas de empresas que gestionaban información sensible, como Lockheed Martin, Redstone Arsenal y la NASA, entre otros.

En este tipo de ataques debemos tener en cuenta que las medidas de seguridad habituales no son suficientes. La amenaza ha cambiado, el atacante está muy preparado y cuenta con el personal y los recursos adecuados para atacar cualquier sistema. Tradicionalmente, las empresas trabajan en un perímetro de seguridad donde se mantienen seguros sus equipos informáticos, utilizando programas de formación y concienciación para que su personal sepa actuar frente a las nuevas amenazas. Sin embargo, esto no es suficiente, hoy en día es necesaria la existencia en las empresas de equipos de respuesta especializados en la prevención y gestión de este tipo de incidentes. Estos equipos especializados deben trabajar junto a los *CERT (Computer Emergency Response Team)* nacionales en el tratamiento de los ataques y en mantener información actualizada de las amenazas y ataques que puedan afectar a su sector. La información obtenida deben transmitirla dentro de sus organizaciones a las distintas áreas afectadas y muy especialmente a aquellas que proporcionan los servicios esenciales a la sociedad, de la forma más ágil posible, estableciéndose una relación de confianza que permita el trabajo conjunto y transparente frente a cualquier amenaza entre el *CERT* y los equipos especializados existentes en las empresas.

Para entender mejor estas amenazas vamos a profundizar en estos casos por su carácter de referente en este tipo de ataques.

BlackEnergy

En 2013 se inició un conflicto entre Ucrania y Rusia provocado por el acercamiento de la primera a la Unión Europea. Como consecuencia de este conflicto, la península de Crimea, con una población mayoritariamente prorusa, se independizó de Ucrania para adherirse a la Federación Rusa.

Enmarcado en este conflicto se produce el ciberataque BlackEnergy, ejecutado el 23 de diciembre de 2015, con el objetivo de sabotear los sistemas de control de infraestructuras públicas ucranianas. En él varias distribuidoras eléctricas fueron comprometidas por el troyano BlackEnergy dejando a los hogares de la región ucraniana de Ivano-Frankivsk (con una población de alrededor de 1,5 millones de habitantes) sin electricidad.

Sin embargo, este no ha sido el único caso de ataque ocurrido a sistemas de control en Ucrania ya que a comienzos de 2016 se produjo un ataque a los sistemas informáticos del aeropuerto de Kiev con la intención de provocar el caos y el desconcierto tras la afección del servicio aéreo. Las noticias coinciden en que el *malware* detectado es similar a BlackEnergy, aunque en este caso se detectó en sus estados iniciales y pudo ser eliminado sin tener con-

secuencias. En noviembre de 2015 también se produjo otro ataque a cadenas de televisión y medios con características similares a los descritos.

BlackEnergy es un troyano, programa malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado. El objetivo del programa es, obviamente, poder controlar en remoto el equipo infectado.

La vía de infección utilizada en el caso que nos ocupa fue el envío de correos electrónicos con documentos adjuntos infectados, suplantando al emisor. Estos correos se enviaban a personas seleccionadas de las compañías eléctricas afectadas.

El vector de ataque utilizado para la infección es la explotación de vulnerabilidades de los programas Microsoft Word, Excel y Powerpoint.

El funcionamiento de BlackEnergy³ puede resumirse en tres funciones:

- Comunicación con el servidor de comando y control que lo dirigirá. Es una de las primeras acciones que intenta realizar BlackEnergy para, a continuación, poder descargarse nuevos componentes y llevarse la información sustraída.
- Escaneos de red que buscan generalmente servicios abiertos relacionados con protocolos del sector de la energía como ICCP o IEC-104 para obtener información de la red.
- Envío de comandos para la ejecución de órdenes que incluyen múltiples aperturas y cierres de interruptores de circuitos, más comúnmente conocidos como *breakers*, en un espacio limitado de tiempo.
- Borrado de archivos de sistema para que el rearranque sea lo más difícil posible.
- Borrado de los eventos/registros de Windows para borrar las evidencias de las actuaciones realizadas.

El objetivo buscado con estas actuaciones es provocar el mayor daño posible y la incapacidad para arrancar de nuevo los sistemas. Precisamente, al ser estos los sistemas que gestionan la infraestructura eléctrica, su inhabilitación tiene como consecuencia provocar primero la caída del sistema eléctrico y después dificultar la restitución del servicio.

Stuxnet

En 2006 Irán retomó su programa nuclear con la puesta en marcha de un grupo de centrifugadoras para el enriquecimiento de uranio en la planta de enriquecimiento de combustible de Natanz. Ante la sospecha de que se pudiera hacer un uso militar del uranio enriquecido, aumentaron las presiones

³ Fuente: CERTSI. <https://www.certs.es/blog/blackenergy-sistemas-criticos> y <https://www.certs.es/blog/protegiendose-blackenergy-detectando-anomalias>

de la comunidad internacional, lideradas por la ONU y Estados Unidos, para que Teherán abandonase estas actividades.

Ante esta hipotética amenaza nuclear iraní surgió Stuxnet, con el objetivo de retrasar o paralizar el programa nuclear iraní. El origen del *malware* parece encontrarse en una colaboración entre la National Security Agency de Estados Unidos e Israel.

Stuxnet es un gusano informático, programa malicioso que se duplica a sí mismo y que afecta a equipos con Sistema Operativo Windows que tienen instalado *software* de Siemens para el control de plantas industriales. Con Stuxnet se infectó la planta de combustible de Natanz, consiguiendo que se modificaran periódicamente las condiciones de funcionamiento de las centrifugadoras (necesarias para el enriquecimiento de uranio, que a su vez es el combustible usado para provocar una reacción nuclear) causando un gran estrés a los rotores y provocando roturas en los mismos. Se calcula que en el momento más álgido del ataque fueron afectadas unas mil centrifugadoras.

El primer ataque fue en 2008, consiguiendo dejar fuera de control las primeras centrifugadoras afectadas que al mismo tiempo enviaban parámetros de funcionamiento normal al Centro de Control de Natanz. Esto provocó un importante daño físico a las centrifugadoras pero también una falta de confianza por parte de las autoridades iraníes en sus técnicos y sistemas de control, que acabaron solicitando ayuda a técnicos internacionales para tratar de entender la situación.

La vía de infección utilizada fueron dispositivos de memoria USB distribuidos entre personal seleccionado del programa nuclear Iraní y el personal con acceso a la planta de Natanz.

El vector de ataque utilizado para la infección fue la explotación de vulnerabilidades aún no conocidas, llamadas vulnerabilidades de día 0, de Microsoft y Siemens.

Stuxnet⁴ es el primer ciberataque que de forma masiva consiguió una destrucción física de su objetivo, en este caso las centrifugadoras. Esta puede haber sido la primera vez que una potencia haya utilizado armas cibernéticas para paralizar la infraestructura de otro país, logrando, con un *software* informático lo que hasta entonces solo se podía lograr mediante el bombardeo de un objetivo o el sabotaje mediante explosivos. Según la Administración estadounidense⁴ el ataque provocó un retraso de entre dieciocho meses y dos años en el desarrollo del programa nuclear iraní.

Aunque el ataque consiguió su objetivo, también provocó problemas importantes al extenderse a otras infraestructuras vulnerables, fundamentalmente de Irán, pero también de otros países como Indonesia, India, Paquistán,

⁴ Fuente: *New York Times*. <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>

Rusia, Cuba e incluso los propios Estados Unidos. Seguramente, gracias a esta infección masiva y no prevista en otros países, se ha conocido y podido estudiar el ataque que de otra forma podría haber pasado inadvertido.

Ciberataque a Estonia 2007

En 2007 se iniciaron una serie de protestas en Estonia como consecuencia del traslado del Soldado de Bronce (monumento soviético homenaje a los soldados caídos en la II Guerra Mundial) desde el centro de Tallin a un cementerio. En Rusia este traslado se consideró una ofensa.

Estonia era ya entonces un país con una alta dependencia de las tecnologías de la información, donde muchos servicios públicos eran ofrecidos mayoritariamente por dichas nuevas tecnologías. Esto originó que las protestas derivasen pronto en ataques cibernéticos, provocando la caída de los sistemas objetivo y por lo tanto la falta de disponibilidad de los servicios ofrecidos por estos. En el momento álgido de los ataques, además de numerosos servicios públicos, los teléfonos móviles y las tarjetas bancarias dejaron de funcionar.

Este tipo de ataques es conocido como *DDoS*, acrónimo en inglés de Denegación de Servicio Distribuida, haciendo alusión a un ataque realizado simultáneamente desde muchos equipos que lanzan multitud de peticiones contra el servidor objetivo. Este es uno de los ataques más populares en internet, por su eficacia y sencillez.

Los principales objetivos fueron las páginas web del presidente de Estonia, del Parlamento, de las instituciones de gobierno, de los medios de comunicación y de los bancos del país. El país finalmente se aisló del internet exterior, para poner fin a los ataques.

El ataque provocó la respuesta de la OTAN que ayudó a Estonia desde el Centro de Ciberdefensa, desde donde se realiza el seguimiento de este tipo de incidentes. Este ataque se considera el primer ciberataque por denegación de servicio organizado contra un país del que se tiene noticia.

Titan Rain

Este ataque se inició en 2003 y duró al menos tres años. Se relaciona con el Gobierno chino y su necesidad de tecnología para el crecimiento de un país que se estaba convirtiendo en una nueva potencia mundial.

El Gobierno estadounidense acusó al Gobierno chino de estar detrás del ataque, lo que provocó enfrentamientos diplomáticos entre ambos gobiernos. Adam Paller, director del Instituto SANS (especializado en Seguridad de Sistemas), indicó que el ataque fue realizado por personal con una «intensa disciplina» y que «ninguna organización puede hacer esto a menos que sea un ejército», apuntando la autoría al Ejército chino.

Titan Rain atacó múltiples objetivos gubernamentales y empresariales de Estados Unidos y de Gran Bretaña. Entre los gubernamentales se encontraban: la NASA, el FBI, o el Departamento de Defensa, así como el Foreign Office británico. Respecto a las empresas afectadas, destacaron las relacionadas con proyectos de defensa como Lockheed Martin o el Laboratorio Nacional Sandia, dependiente del Departamento de Energía de los Estados Unidos, cuyos proyectos tienen por objetivo la prueba de componentes en armas atómicas, el desarrollo de los programas de energía y del medio ambiente, así como la protección de las infraestructuras nacionales.

Los *hackers* usaron ordenadores y páginas web chinas, con un bajo nivel de seguridad, utilizándolos como vía de infección para llevar a cabo el ataque, protegiendo de esta forma su origen.

Pilares de la colaboración en la protección de las infraestructuras críticas

Las infraestructuras críticas dan servicio a amplias extensiones de territorio y a un número muy elevado de personas, empresas e industrias. Por lo tanto, por definición, el impacto de la caída de una de ellas debe ser necesariamente global y extenso. Y ello convierte en dependientes tanto los servicios que proporcionan estas infraestructuras como las propias infraestructuras entre sí.

Hay que recordar, precisamente, que por «dependencia» se entiende la relación entre dos productos o servicios en la cual un producto o servicio es necesario para la generación del otro. En el caso que nos ocupa, las dependencias incluyen tanto los servicios esenciales como las infraestructuras que los soportan. De esta manera, para que las infraestructuras funcionen de manera adecuada se necesita de los servicios suministrados por otras infraestructuras o segmentos del mismo sector o de otros sectores diferentes y esto es lo que se conoce como interdependencias⁵.

Lo que sí es cierto es que, ya sea a través de la conectividad, las políticas y procedimientos directos o la proximidad geoespacial, los sistemas críticos de infraestructuras interactúan y de forma cada vez más acusada. Estas interacciones crean a menudo complejas relaciones que se cruzan entre sí. Sin embargo, el modelado y el análisis de las interdependencias entre las infraestructuras y sus elementos críticos es un fenómeno relativamente nuevo y tremendamente complejo.

Los propietarios y gestores de infraestructuras, históricamente interesados en el correcto funcionamiento de sus propias instalaciones, a menudo muy

⁵ Parlamento de España: Ley 11/2011, de 28 de abril, por la que se Establecen Medidas para la Protección de las Infraestructuras Críticas (artículo 2.j). <https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf>

bien acotadas, deben ahora lidiar con los problemas provocados por la ilimitada conectividad de las redes y de la tecnología.

Hay una necesidad creciente de analizar y comprender mejor la influencia que tienen entre sí múltiples sectores, que pueden inducir efectos secundarios potencialmente imprevistos sobre los demás, ya sea directa o indirectamente, y que pueden derivar, en casos extremos, en la generación de efectos cascada, o dominó, de consecuencias difícilmente previsibles⁶.

En España, de acuerdo a nuestra legislación vigente, se entiende la Protección de las Infraestructuras Críticas (PIC) como el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de los servicios esenciales con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra las infraestructuras que los soportan y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia⁷. Así, en nuestro país, las políticas sobre PIC se sustentan en cinco principios básicos, todos ellos alineados con la Estrategia Nacional de Seguridad de 2013, que dotan de cohesión y coherencia a todo el sistema⁸. Estos son:

1. Coordinación.
2. Responsabilidad compartida y cooperación público-privada entre los diferentes agentes.
3. Equilibrio y eficiencia.
4. Planificación escalonada.
5. Resiliencia⁹.

En nuestro país, la mayoría de las infraestructuras críticas pertenecen o están operadas por compañías privadas, como ya se ha apuntado. Esta situa-

⁶ En el ensayo de Duddenhoeffer, Perman y Manic, publicado por el *Idaho National Laboratory*, los autores establecen el concepto de «nodo» y de «borde», para clarificar las diferentes relaciones de dependencia existentes entre las infraestructuras de servicios esenciales. De esta manera, para Duddenhoeffer «un nodo de infraestructura es una entidad que actúa como fuente, produce, consume o transforma un recurso (...) de la misma manera, sin embargo, un nodo puede representar factores políticos o sociales de influencia que no se manifiestan en forma física, pero que pueden afectar físicamente a la propia infraestructura». Por otra parte, el «borde es una entidad física o virtual que actúa como un conducto para el flujo para una cantidad física, información o influencia. Por lo tanto, un borde (o arco) entre dos nodos representa un nivel directo de dependencia». <https://inldigitallibrary.inl.gov/sti/3578215.pdf>

⁷ *Ibidem*, 5.

⁸ De la Corte, Luis, *et al. Seguridad nacional, amenazas y respuestas*. Madrid, Editorial LID (2014).

⁹ El completo trabajo de John D. Moteff, realizado en agosto de 2012 para el Servicio de Investigación del Congreso de Estados Unidos efectúa una primera aproximación al término resiliencia desde el punto de vista de la pérdida y recuperación de los niveles de operación habituales de un proveedor determinado. Más interesante es la propia medida del término, su combinación con los factores de riesgo y las medidas y políticas esbozadas para mejorar los niveles de resiliencia existentes.

<https://www.fas.org/sgp/crs/homesec/R42683.pdf>

ción hace imprescindible que tanto las Administraciones Públicas como los operadores privados trabajen, asumiendo la responsabilidad que a cada uno les corresponda y de forma coordinada, en la protección de las infraestructuras críticas antes, durante y después de un eventual evento negativo. La plasmación de esta idea invoca el segundo de los principios arriba reflejados: el de la responsabilidad compartida y la cooperación público-privada¹⁰.

Independientemente de la manera de obtenerlo, el éxito de cualquier modelo de cooperación público-privada debe estar basado en todas o algunas de las siguientes premisas:

- **Confianza.** Dado que la materia PIC aborda cuestiones muy sensibles, es esencial crear una atmósfera de confianza en la que ambas partes sean conscientes de la necesidad de cada uno de ellos de actuar con la discreción debida. Mantener una relación de confianza entre la Administración y las empresas privadas es fundamental para hacer crecer la colaboración¹¹. Por la experiencia adquirida, se puede constatar que para fomentar la confianza son necesarios puntos de contacto únicos en ambas partes, con capacidad de decisión dentro de su organización, que tengan conocimiento de las posibilidades que tiene la otra parte para obtener el máximo partido de la relación. Además, es clave fomentar la colaboración en otras actividades de ciberseguridad, como ciberejercicios, cuestionarios, gestión de incidentes menores, participación en foros... de forma que sean naturales y automáticos los procedimientos de colaboración frente a cualquier tipo de actuación que deba realizarse conjuntamente en un futuro entorno real. La creación de mecanismos de cooperación informal entre el personal de ambas entidades es también una faceta indispensable para mejorar la confianza entre la Administración competente y la empresa. La confianza entre ambas partes permitirá, además, una mayor agilidad en la compartición de la información y la rapidez en la toma de decisiones que permitan gestionar el incidente eficazmente. Un ejemplo significativo del trabajo conjunto en España en esta materia se produjo precisamente en el marco del ataque BlackEnergy, ya comentado en páginas anteriores. Desde el CERT de Seguridad e Industria (CERTSI_), operado conjuntamente por el INCIBE y el CNPIC, se informó puntualmente sobre el ataque a las empresas del sector energético español como posibles objetivos de un ataque similar. La información que se compartió incluía un nivel ejecutivo, necesario para ayudar

¹⁰ Conceptos ambos introducidos en el estudio de la Comisión Europea *Inventory of Crisis Management Capacities in the European Commission and Community Agencies*, mayo de 2010. Documento no público.

¹¹ Esta necesidad fue planteada como una de las conclusiones principales en el *Manual de Buenas Prácticas para las Políticas PIC* (RECIPE), publicado por la Dirección General de Interior de la Comisión Europea en marzo de 2011. http://www.oaip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/FINAL_RECIPe_manual.pdf

a entender la amenaza a la Alta y Media Dirección¹², y, obviamente, un nivel técnico dirigida a los operadores especializados de cada organización que desvelaba, entre otros parámetros, el origen del *malware*, la vía de transmisión, las vulnerabilidades explotadas, los indicadores de compromiso y las medidas necesarias para prevenirlo. Esto permitió a las empresas del sector implantar en sus organizaciones las medidas planteadas, permitiendo adelantarse a una repetición de ese mismo ataque y reforzando el sistema, en este caso eléctrico, de nuestro país.

- **Intercambio de información.** Que debe ser en ambas direcciones, válido para ambas partes y basado en presupuestos de confidencialidad y explotabilidad¹³.
- **Respeto.** Ambas partes deben reconocer el valor añadido que supone la participación de la otra parte en la colaboración.
- **Transparencia.** Tanto en los procedimientos generales como en la información que se pone a disposición de la otra parte. La transparencia permite generar el ambiente necesario para que la colaboración sea fructífera pero para que tenga continuidad debe darse en ambos sentidos. La transparencia por parte de la Administración pública competente (en este caso, el CNPIC) permitirá compartir con las empresas privadas la información de incidentes que puedan afectar a estas, así como los medios con los que cuenta para poder ayudarles. Todo ello les ofrece a las empresas privadas un tiempo fundamental para preparar la respuesta a estos incidentes. Por su parte, la transparencia desde la empresa privada hacia la Administración, tanto en incidentes como en lo relativo a medios disponibles, permite una valoración del incidente por el órgano competente y posibilita una compartición de la información del incidente con otras entidades del sector que les permitirá tomar las medidas adecuadas para anticiparse al incidente.
- **Marco regulatorio claro.** Los operadores quieren saber claramente a qué se deben atener. Es recomendable tener pocas leyes y simples y, sobre todo, evitar duplicidades¹⁴.
- **Neutralidad.** En el marco en el que se desarrolla la colaboración PIC no pueden existir intereses partidistas ni económicos¹⁵.

¹² La implicación de la Alta Dirección en las políticas de seguridad a implantar por la organización es una condición *sine qua non* exigida por el CNPIC a la hora de plasmar los diferentes planes derivados de la Ley 8/2011. Fernando Sánchez, en el libro *Marco legal y de gestión de la protección de las infraestructuras críticas*, coordinado por Francisco J. Vanaclocha, asegura que «es preferible una aproximación voluntaria a la imposición, pero de alguna manera debe instarse a la cooperación de los operadores. El establecimiento de marcos de gobierno y la obtención del compromiso de la alta dirección es esencial para ello».

¹³ *Ibíd.* 11. Esta necesidad de intercambio de información es precisamente lo que subyace tras la Propuesta de decisión del Consejo de 27 de octubre de 2008 relativa a una Red de información sobre alertas en infraestructuras críticas (CIWIN) [COM(2008) 676 final]. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52008PC0676>

¹⁴ *Ibíd.* anterior.

¹⁵ La labor de «árbitro» del Sistema, como uno de los objetivos específicos de la legislación española sobre protección de infraestructuras críticas viene justificada por Fernando

- **Interés común.** Los resultados obtenidos deben beneficiar a ambas partes, de forma que exista el necesario *quid pro quo*.
- **Conciencia de las posibilidades y restricciones de cada uno.** Esto implica que cada parte debe conocer qué es lo que hace el otro y qué se le puede pedir.
- **Expectativas realistas.** En línea con lo anterior. Hay que tener en cuenta cuáles son los recursos, capacidades y limitaciones de cada uno para diseñar objetivos alcanzables. Algunas de las acciones que se pueden desarrollar, como ejemplo, podrían ser:
 - Conocimiento mutuo.
 - Participación en estrategias e iniciativas comunes.
 - Elaboración de guías, estándares o buenas prácticas.
 - Ejercicios y simulacros sectoriales
 - Empleo operativo: basado en una correcta capacidad de interlocución y reacción.

Lo que parece claro es que los pilares de la colaboración público-privada, más allá del cumplimiento de la legislación en curso, deben ser conceptos como los que se acaban de citar. Es únicamente sobre estas bases sobre las que se podrá construir una relación sólida que permita el intercambio fluido de información y el trabajo conjunto en aquellos incidentes que así lo necesiten. Y más, si el «campo de batalla» donde se va a operar debe hacer frente a una amenaza virtual cada vez más agresiva y sofisticada.

El sistema de planificación PIC y su encaje con la ciberseguridad

Normativa PIC, colaboración público-privada y ciberseguridad

La protección de las infraestructuras que aseguran el mantenimiento de los servicios esenciales se ha convertido en una prioridad para las diferentes naciones, teniendo en cuenta la dependencia que la sociedad tiene de los mismos y que incrementa exponencialmente año a año.

Por este motivo, en el ámbito de la Unión Europea, se aprobaron primero el Programa Europeo de Protección de Infraestructuras Críticas (PEPIC)¹⁶ y, más tarde, la Directiva 2008/114 del Consejo de la Unión Europea, de 8 de diciembre¹⁷. Ambos documentos vinieron precedidos en el tiempo por sendas Comunicaciones de la Comisión al Consejo y al Parlamento Europeo, donde

Sánchez en el artículo «Las políticas de protección de infraestructuras críticas en España», publicado en la *Revista Seguridad y Ciudadanía* n.º 11, de junio de 2014 (pp. 33 y ss.).

¹⁶ <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52006DC0786>. El PEPIC se basó de manera muy especial en el *Libro Verde de 17 de noviembre de 2005, sobre un Programa Europeo para la Protección de Infraestructuras Críticas* [COM (2005) 576 final (no publicado en el Diario Oficial)].

¹⁷ <https://www.boe.es/doue/2008/345/L00075-00082.pdf>

se pedía la puesta en marcha de medidas urgentes en la lucha contra el terrorismo, tanto en su prevención, prevención y respuesta, como en la preparación y gestión de las posibles consecuencias¹⁸.

A nivel nacional, las políticas sobre protección de infraestructuras críticas empezaron a ver la luz de forma temprana respecto a otras naciones de nuestro entorno. Ya en 2007 se aprobó, en mayo, un primer Plan Nacional para la Protección de las Infraestructuras Críticas que fue seguido en noviembre por la creación del Catálogo Nacional de Infraestructuras y la aprobación de un Acuerdo sobre Protección de Infraestructuras Críticas, que tuvo como primera consecuencia el nacimiento del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)¹⁹.

El CNPIC, actor central desde ese momento en el campo que nos ocupa, se configura de este modo como el órgano ministerial encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior (Autoridad competente en esta materia) en relación con la protección de las infraestructuras críticas en el territorio nacional²⁰.



Figura 5.1. Logo CNPIC.

El complejo carácter que la seguridad nacional ha adquirido en los últimos años, unido todo ello a la ya mencionada enorme dependencia que la sociedad actual tiene del sistema de infraestructuras que asegura la prestación de los servicios esenciales, evidenció, ya entonces, la necesidad de poner en práctica estrategias y políticas en esta materia para garantizar la seguridad en la normal prestación de los servicios esenciales frente a amenazas derivadas de posibles ataques deliberados²¹.

¹⁸ <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52004DC0701>

<http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52004DC0698>

¹⁹ <http://www.cnpic.es/index.html>

²⁰ Parlamento de España: Ley 11/2011, de 28 de abril, por la que se Establecen Medidas para la Protección de las Infraestructuras Críticas (artículo 7). <https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf>

²¹ La prestación de los servicios esenciales y la disponibilidad de los mismos tiene un enlace claro con el concepto de continuidad de negocio aplicado por la mayoría de las com-

En España, se consideró prioritario desde aquel momento integrar en estas estrategias a las amenazas provenientes del ciberespacio como un potencial elemento disruptivo del normal funcionamiento de las infraestructuras críticas. El tiempo, vistos los acontecimientos que han tenido lugar en la última década, ha dado la razón a esa decisión estratégica que entonces adoptó el Ministerio del Interior a la hora de apostar por un concepto de seguridad integral, entonces muy incipiente a nivel internacional, que aunase las políticas, metodologías y operaciones concernientes a la seguridad física de los activos y las relativas a la seguridad lógica, o cibernética, de las redes y sistemas²².

El panorama de seguridad internacional, la irrupción del terrorismo internacional y el auge del crimen organizado, como se acaba de mostrar, no han hecho sino poner de manifiesto los efectos que podrían tener sobre la salud pública, la industria o la economía nacionales determinados ciberataques dirigidos contra los sistemas de supervisión, control y adquisición de datos (sistemas SCADA) o los complejos sistemas informáticos que rigen el funcionamiento de los procesos de negocio y servicios de nuestras empresas estratégicas.

La legislación española, cuyo máximo exponente es la Ley 8/2011, de 28 de abril, por la que se Establecen Medidas para la Protección de las Infraestructuras Críticas (comúnmente conocida como Ley PIC) introdujo como figura clave en las políticas del Gobierno el conocido como «Sistema de Protección de Infraestructuras Críticas»²³.

pañías privadas. De forma muy especial, el sector financiero tiene una notable madurez en la aplicación de políticas de continuidad de negocio que han arraigado con gran fuerza en la aplicación, por parte de las entidades de este sector estratégico, de la legislación sobre protección de infraestructuras críticas. Para mayor información sobre ello, consultar el artículo escrito por César Pérez-Chirinos en 2009, *Critical Financial Institutions: Business Continuity Scenarios and Costs*, en *European CIIP Newsletter*.

<http://www.irriis.org/ecn/ECN%20issue%2012%20v1%2001.pdf>

²² El estudio *Protecting Critical Infrastructure in the EU* llevado a cabo por el CEPS (*Centre for European Policy Studies*) Task Force Report en 2010 (<https://www.ceps.eu/system/files/book/2010/12/Critical%20Infrastructure%20Protection%20Final%20A4.pdf>) efectúa, en este sentido, una clara recomendación al mencionar (p. 28-29): «the CEPS Task Force strongly recommends that a coordinated, holistic approach be adopted, encompassing both CIP and CIIP. An early recognition of the need for a coordinated approach between these two policy domains came in 2003 from the "G8 Principles for Protecting Critical Information Infrastructures" adopted by the G8 Justice & Interior Ministers, which clearly state that: In order effectively to protect critical infrastructures ... countries must protect critical information infrastructures from damage and secure them against attack ... Effective protection also requires communication, coordination, and cooperation nationally and internationally among all stakeholders – industry, academia, the private sector, and government entities, including infrastructure protection and law enforcement agencies».

²³ El trabajo publicado en 2016 por la Fundación Borredá en el libro dirigido por César Álvarez, *El modelo de protección de infraestructuras críticas en España-Guía PIC*, desglosa los componentes del Sistema PIC y el esquema de planificación emanado de la Ley 8/2011.

Según dicha ley, el Sistema de Protección de Infraestructuras Críticas se compone de todos aquellos agentes (instituciones, órganos y empresas procedentes tanto del sector público como del privado) con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos. El Sistema se asienta, a su vez, en un sistema escalonado de planeamiento compuesto por los siguientes planes, ordenados de mayor a menor nivel: Plan Nacional de Protección de las Infraestructuras Críticas, Planes Estratégicos Sectoriales, Planes de Seguridad del Operador, Planes de Protección Específicos y Planes de Apoyo Operativo.

La piedra angular sobre la que se basa este Sistema, del cual su cúspide es la Comisión Nacional PIC, no es otra que un robusto esquema de cooperación en el que los diferentes agentes (y de forma muy particular los operadores críticos, sean estos públicos o privados) se encuentren representados y donde tengan capacidad de decisión a la hora de definir dichas políticas.

La forma de promocionar el Sistema PIC por el Gobierno de España, a través del Ministerio del Interior y del CNPIC, responde, en todo caso, a un delicado equilibrio en el que, por una parte, se requiere acceder a la cooperación mediante procesos de diálogo y colaboración genuina y, por otra, es preciso marcar una serie de reglas, de obligado cumplimiento, a las que todos los participantes han de acogerse. Todo ello es aún más importante en tanto en cuanto entran en juego aspectos cada vez más importantes, como es el



Figura 5.2. Esquema del Sistema PIC.

caso de la ciberseguridad, donde es fundamental contar con mecanismos ágiles e inmediatos de cooperación e intercambio de información entre todos los agentes implicados de alguna u otra manera en la securización del ciberespacio.

Por este motivo, se podría concluir en esta primera aproximación que la Ley PIC y el reglamento que la desarrolla (el Real Decreto 704/2011, de 20 de mayo)²⁴, han configurado un marco legal y una estructura organizativa que aporta un aire innovador para implantar una nueva política de seguridad, necesaria por otra parte, donde se establece la necesidad de garantizar la adecuada prestación de los servicios esenciales a través de mecanismos que posibiliten la seguridad integral de este tipo de infraestructuras. Para ello, la participación del sector privado es esencial y el modelo de colaboración público-privada, basado en preceptos de confianza y confidencialidad, la clave del mismo.

Nos detendremos a continuación brevemente sobre los cinco planes que conforman el esquema de planificación del Sistema PIC.

El Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC)

El Plan Nacional de Protección de las Infraestructuras Críticas (en adelante, PNPIC) representa la cúspide del complejo esquema de planificación integrada del que se ha dotado el Sistema PIC. Como ya se sabe, el PNPIC es elaborado por la Secretaría de Estado de Seguridad y tiene como objetivo establecer los criterios generales y las directrices precisas para movilizar las capacidades operativas del Ministerio del Interior, en coordinación con los operadores críticos y con el apoyo, en su caso, de las Fuerzas Armadas para articular las medidas preventivas necesarias para asegurar la protección permanente, actualizada y homogénea del conjunto de infraestructuras nacionales frente a aquellas amenazas de carácter deliberado que tengan como objetivo las mismas.

Este Plan, vigente desde mayo de 2007 y obsoleto en su mayor parte, se actualizó en febrero de 2016 mediante la instrucción número 1/2016 de la Secretaría de Estado de Seguridad. De este modo, se demuestra que la Secretaría de Estado de Seguridad, máximo órgano responsable del impulso y coordinación de las distintas medidas de seguridad de las infraestructuras críticas nacionales no es ajena, entre otras cosas, a las amenazas derivadas de este entorno digital en el que nos encontramos. En particular, consciente del auge de los incidentes contra activos digitales y lo que esto supone para el normal funcionamiento de los sectores estratégicos nacionales, el PNPIC garantiza la presencia de mecanismos de seguimiento de las labores de prevención, detección, respuesta y recuperación ante ciberincidentes.

²⁴ <http://www.boe.es/boe/dias/2011/05/21/pdfs/BOE-A-2011-8849.pdf>

El PNPIC se encuentra en su desarrollo operativamente vinculado con el Plan de Prevención y Protección Antiterrorista, también de reciente actualización (mayo de 2015). De este modo, el PNPIC complementa al anterior mediante el establecimiento de una serie de procedimientos de actuación asociados a cada uno de los niveles presentes en el conocido como «Nivel de Alerta en Infraestructuras Críticas» (NAIC). Para cada uno de los cinco niveles de los que consta el NAIC se determina un incremento gradual de las medidas de protección y vigilancia de las infraestructuras críticas nacionales. Como no podía ser de otra forma, en cada nivel NAIC se determinan una serie de medidas de seguridad, vigilancia y protección de carácter exclusivamente cibernéticas, medidas que afectan tanto a los órganos pertenecientes a Secretaría de Estado de Seguridad, al CERT de Seguridad e Industria (CERTSI) y a los operadores críticos nacionales.

Una de las principales novedades que presenta el PNPIC es la integración de todos los agentes del Sistema de Protección de Infraestructuras Críticas, entre los que cabe destacar, en materia de ciberseguridad, el rol que juegan los operadores críticos en el desarrollo de medidas de autoprotección, siendo fundamental el reporte de incidentes que afecten a su operativa diaria. Este nuevo requisito va acompañado de la necesidad de identificar en cada operador crítico la figura del Responsable de Seguridad TI corporativo (o CISO), como interlocutor natural en el ámbito de la ciberseguridad, con objeto de agilizar los intercambios de información específicos en la materia.



Figura 5.3. PNPIC.

Contenidos. Rasgos principales del nuevo PNPIC.

El PNPIC se estructura en un cuerpo principal y en un anexo, donde se recogen las medidas a implantar en cada nivel de activación del mismo por los diferentes agentes participantes. Al igual que el Plan de Prevención y Protección Antiterrorista, con el que está alineado, el PNPIC está clasificado como «Difusión Limitada», y su anexo como «Confidencial».

El PNPIC supone la culminación del Sistema de Protección de Infraestructuras Críticas emanado de la Ley 8/2011, PIC, y la implantación de todas las herramientas de planificación previstas en dicha norma. Asimismo, introduce como principal novedad la puesta en marcha de medidas operativas concretas sobre dos presupuestos fundamentales:

- La inclusión de la figura del operador crítico como partícipe del sistema de seguridad nacional.
- La inclusión de medidas de ciberseguridad, dando contenido al concepto de «seguridad integral».

La figura del Operador Crítico en el PNPIC.

Los principales actores participantes en el PNPIC son:

- Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). Órgano ministerial encargado del impulso, la coordinación y la supervisión de cuantas actividades tiene encomendadas la Secretaría de Estado de Seguridad en relación con la Protección de las Infraestructuras Críticas, por lo que asume las funciones de coordinación del PNPIC.
- Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO). Órgano directivo de la Secretaría de Estado de Seguridad competente en la recepción, integración y análisis de la información estratégica disponible en la lucha contra todo tipo de terrorismo y radicalismo violento, encargado en lo respectivo a este Plan de la evaluación de la amenaza terrorista contra el Sistema de Protección de Infraestructuras Críticas (Sistema PIC).
- Fuerzas y Cuerpos de Seguridad del Estado (FCSE). Responsables de la protección a través de dispositivos preventivos y reactivos de las infraestructuras críticas que se encuentran ubicadas en su área de responsabilidad.
- Fuerzas Armadas (FAS). Encargadas de reforzar la protección a través de dispositivos preventivos y reactivos de las infraestructuras críticas que previamente se designen por el Ministerio del Interior.
- Operadores Críticos (OC). Los propietarios y/o gestores de las infraestructuras críticas que prestan servicios esenciales a la sociedad.

De todos ellos, la única figura que no está presente en el vigente Plan de Prevención y Protección Antiterrorista (PPPA) es la del operador crítico. El PNPIC prevé que este agente, emanado de la Ley 8/2011, sea responsable en la seguridad común en la parte que le afecta. Por ello, determina una serie de obligaciones y medidas operativas (que aparecen relacionadas tanto en el cuerpo como en el anexo del Plan) para su cumplimiento, estando además en coordinación con el propio PPPA. En este sentido, al operador crítico se le requiere entre otras cosas que:

- Designe obligatoriamente un responsable de Seguridad y Enlace que será a todos los efectos el punto de contacto natural entre el CNPIC y su organización.

- Los Planes de Protección Específicos (documentos de carácter operativo que se podrán ver en las siguientes páginas) tengan una graduación de medidas, donde se recojan los diferentes niveles de activación del PNPIC, y que deberán estar coordinados con los planes de los cuerpos policiales competentes.
- Acceda al intercambio de información y la actualización de datos de sus activos a una plataforma facilitada por el CNPIC (PI3), donde se centraliza la información disponible.
- Active los protocolos que se deriven del nivel de alerta declarado, en coordinación con las FCSE. Estos protocolos vienen recogidos en el anexo del Plan (cuatro medidas para el nivel 1, cinco para el nivel 2, otras cinco para el 3, cuatro para el nivel 4 y cuatro para el 5), siendo todas ellas, obviamente, acumulables.
- Participe en una mesa sectorial donde se evalúen los procedimientos de colaboración y comunicación existentes y se efectúe el seguimiento y coordinación de las medidas de protección activadas. Esta mesa se convocó el pasado día 15 de junio de 2016 por vez primera.

Igualmente, en el anexo del Plan vienen recogidos las responsabilidades y cometidos de los diferentes órganos del Ministerio del Interior (FCSE, CITCO y CNPIC) en cada uno de los niveles.

Las medidas de ciberseguridad en el PNPIC²⁵.

La ciberseguridad se incluye como complemento necesario a las medidas existentes tradicionalmente en el marco de la seguridad física. De esta forma, por primera vez se considera este aspecto en una instrucción operativa dictada por el Secretario de Estado de Seguridad. Entre otras medidas, destacan en el PNPIC:

- El rol del CERTSI_ y la Oficina de Coordinación Cibernética como interlocutores necesarios con los operadores en los diferentes niveles de alerta que se declaren.
- La obligación, por parte de los operadores críticos, de llevar a cabo labores de vigilancia digital y de reportar incidentes a los anteriores organismos. Para ello, se está trabajando en la definición de unos umbrales de seguridad (a partir de los cuales se debe comunicar el incidente) y en unos procedimientos concretos de intercambio de información.
- La designación de los responsables de Seguridad de la Información de los operadores críticos (CISO/responsables seguridad TI) para reportar incidentes y coordinarse con el Ministerio del Interior.

Como resumen, hay que apuntar que el PNPIC, al mismo tiempo que completa la batería legislativa que deriva de la Ley PIC, homogeniza las medidas operativas que contiene el Plan de Prevención y Protección Antiterro-

²⁵ *El modelo de protección de infraestructuras críticas en España-Guía PIC*, Editorial Borrmar S.A. dirigido por César Álvarez (pp. 37 y ss.).

rista, identificándose con los niveles de alerta consignados en este último. Finalmente, extiende responsabilidades y cometidos en ambos ámbitos a un nuevo actor, el operador crítico (en su mayoría organizaciones privadas), estableciendo un enlace operativo vinculante con la Secretaría de Estado de Seguridad y con las unidades de las FCSE a nivel territorial.

Los Planes Estratégicos Sectoriales (PES)

Los Planes Estratégicos Sectoriales tienen como misión principal conocer «cuáles son los servicios esenciales proporcionados a la sociedad, el funcionamiento de estos, las infraestructuras estratégicas sobre las que se asientan, los operadores, propietarios o gestores de las mismas, las vulnerabilidades del sistema, las consecuencias potenciales de su inactividad y las medidas estratégicas necesarias para su mantenimiento»²⁶. En definitiva, tiene por objeto obtener una idea global y completa de los diferentes sectores o subsectores estratégicos, de modo que se facilite y agilice tanto la identificación de operadores e infraestructuras críticas como las medidas necesarias para su protección, por lo que se puede decir sin temor a equivocarnos que estos planes son la base sobre la que se edifica todo el Sistema PIC. En lo que respecta a la ciberseguridad, los Planes Estratégicos Sectoriales permiten obtener información veraz de cuál es el nivel de dependencia del sector para con las tecnologías de información y comunicaciones.

Cabe destacar que el proceso de elaboración de un Plan Estratégico Sectorial es una tarea eminentemente técnica y multidisciplinar, de manera que es necesario el concurso de expertos tanto de la rama en cuestión como en seguridad. La mecánica de redacción de este tipo de planes exige la creación de grupos de trabajo complejos donde participan expertos de los diferentes ministerios competentes, otros organismos públicos y privados, empresas, operadores, consultoras y asociaciones profesionales.

A nivel global, el Plan Estratégico Sectorial (PES) se basa en un análisis general de riesgos donde se contemplan las vulnerabilidades y amenazas potenciales, tanto de carácter físico como lógico, que afectan al sector o subsector en cuestión en el ámbito de la protección de las infraestructuras.

Su elaboración, como ya se ha explicado, se lleva a cabo en el seno de un grupo de expertos incardinado dentro del Grupo de Trabajo (GTIPIC) y coordinado por el CNPIC. En estos trabajos, principalmente en el desarrollo del análisis de riesgos general y estratégico del sector, se cuenta con la participación activa y el asesoramiento técnico de aquellos operadores estratégicos identificados en cada sector. Un Plan Estratégico Sectorial tipo se

²⁶ José Ignacio Carabias, en su artículo «Protección de infraestructuras críticas y planificación». *Revista Seguritecnia*, n.º 409, junio de 2014.

estructura en cuatro capítulos, cuyo contenido se muestra sucintamente a continuación²⁷:

1. En primer lugar, se elabora un estudio y análisis de la normativa sectorial a nivel comunitario y nacional que es de aplicación específica a dicho sector. Su objetivo estriba en poder conocer toda la base normativa que regula el funcionamiento sectorial para determinar aquella que puede ser de mayor interés desde el ámbito PIC para que el desarrollo y el resultado de los trabajos del Plan no vayan en contraposición de los criterios, reglas y normas que regulan dicho sector.
2. En segundo lugar, se dirige un estudio del funcionamiento y de la organización del sector, identificando cuáles son los servicios esenciales que se prestan en el mismo y que deben ser objeto de protección. Del funcionamiento y estructura de los servicios esenciales se obtendrá una segmentación del sector compuesta por los diferentes ámbitos de actividad que se desarrollan y la tipología de infraestructuras o segmentos sobre los que se sustentan los ámbitos de actividad. A modo de ejemplo, el Sector de la Energía, se subdivide en varios subsectores como son la electricidad, el gas y el petróleo. Dentro del subsector de la electricidad existirían los ámbitos de la generación, transporte, distribución y operación-control. Siguiendo con la segmentación del subsector de la electricidad, el ámbito del transporte de electricidad estaría compuesta por los segmentos o tipología de las infraestructuras siguientes: líneas de transporte (400 y 200 kV) y subestaciones de transporte. Una vez determinado y realizado el estudio del funcionamiento de los servicios esenciales prestados a nivel sectorial, se está en condiciones de identificar cuáles son aquellas infraestructuras estratégicas sobre las que se asientan los diferentes servicios esenciales. A su vez, se localizan los operadores más relevantes, en función de la titularidad y de la gestión de las tipologías de infraestructuras ya identificadas como fundamentales para el correcto funcionamiento de los servicios esenciales. Del estudio del funcionamiento y organización del sector, se establecen además las diferentes interdependencias intrasectoriales (con otros ámbitos del mismo sector) e intersectoriales (con otros sectores estratégicos). El objetivo es diseñar un mapa de interdependencias que ayude a identificar a nivel sectorial, por cada una de las tipologías de infraestructuras definidas, sus dependencias de entrada (de quién depende la infraestructura) y de salida (quién depende de la infraestructura).
3. El tercer capítulo aborda la realización de un análisis de riesgos general y estratégico en el que se contemplan las vulnerabilidades y ame-

²⁷ La estructura, organización y contenido de un Plan Estratégico Sectorial tipo aparece desarrollada en mayor detalle en el artículo de Fernando Sánchez, «Protección de infraestructuras críticas: El Sistema de planeamiento como herramienta de implantación (I)», publicado en la *Revista Seguridad y Ciudadanía* n.º 12, de diciembre de 2014 (pp. 31 y ss.).

nazas potenciales, tanto de carácter físico como lógico, que puedan afectar al sector o subsector en cuestión, estimando el impacto que tendría en la sociedad. Para ello se cuenta con unas tablas de estimación (basadas en los criterios horizontales de criticidad derivados de la Directiva 2008/114, sobre protección de infraestructuras críticas europeas) donde se parametrizan los daños/impacto sobre las personas, económico y medioambiental y, finalmente, la incidencia sobre el servicio prestado. Estas tablas, eminentemente técnicas y de una extrema complejidad, son elaboradas *ad hoc* para cada uno de los Planes Estratégicos Sectoriales por equipos de trabajo especializados.

4. Finalmente, el capítulo cuarto, de carácter más organizativo, aborda las propuestas necesarias para la implantación de medidas de diferente tipo, a saber:

- Organizativas y técnicas, necesarias para prevenir, reaccionar y, en su caso, paliar, las posibles consecuencias de los diferentes escenarios que se prevean.
- Preventivas y de mantenimiento.
- De coordinación con el Plan Nacional de Protección de las Infraestructuras Críticas.

Cada uno de los Planes Estratégicos Sectoriales deberá ser aprobado por la Comisión Nacional de Protección de las Infraestructuras Críticas, presidida por el secretario de Estado de Seguridad y compuesta por representantes de diez ministerios y organismos. Los planes, de carácter clasificado, son gestionados y custodiados en un registro central por el CNPIC, sin perjuicio de que cada ministerio y organismo del Sistema dispongan de una copia de estos, siempre y cuando cuenten con las medidas de seguridad previstas por la Ley para la custodia, archivo y manejo de material clasificado. A su vez, el CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o parte de la información contenida en dichos planes.



Figura 5.4. Planes Estratégicos Sectoriales aprobados en 2016.

Durante el año 2014 se acometió el desarrollo y posterior aprobación por parte de la Comisión Nacional de Protección de las Infraestructuras Críticas de los planes referentes al Sector Energía (electricidad, gas y petróleo), Industria nuclear y Sistema Financiero. Posteriormente, se hizo lo propio en 2015 con el Sector Agua y el Sector Transporte (marítimo, aéreo, carreteras y ferroviario). En 2016 se aprobaron los correspondientes a los sectores Espacio e Industria Química y se está actualmente redactando el relativo al sector de las Tecnologías de la Información y Comunicaciones (TIC).

Los Planes de Seguridad del Operador (PSO)²⁸

El Plan de Seguridad del Operador es aquel documento de carácter estratégico en el que el operador crítico, una vez designado oficialmente a través de Resolución del secretario de Estado de Seguridad, ha de recoger cuáles son las políticas generales de seguridad de su organización para garantizar la protección y la seguridad del conjunto de activos de los que es titular o gestor.

Como se ha podido ver en el epígrafe anterior, referido a los Planes Estratégicos Sectoriales, una vez se ha procedido al nombramiento de operador crítico tras su identificación, se inicia un proceso marcado en el artículo 13 de la Ley PIC. Entre las obligaciones a las que se enfrenta, se destaca como primera de ellas la de elaborar un PSO en el plazo de seis meses a partir de la notificación de la resolución de su designación. Este Plan (solo uno por operador crítico designado) se presentará al CNPIC para su evaluación y, si procede, su aprobación por el secretario de Estado de Seguridad u órgano en el que este delegue. El Plan de Seguridad del Operador tiene la finalidad, así, de integrar todos aquellos criterios de seguridad integral que los operadores críticos aplican al conjunto de las infraestructuras de las que son propietarios o gestores.

El Plan de Seguridad del Operador, como instrumento de planificación del Sistema de Protección de Infraestructuras Críticas, contendrá al menos los siguientes aspectos:

1. La política general de seguridad del operador y su marco de gobierno.
2. La relación de servicios esenciales prestados por el operador.
3. La metodología de análisis de riesgo (amenazas físicas y lógicas) que aplica.
4. Los criterios de aplicación de las medidas de seguridad integral.

²⁸ La estructura y contenido de un Plan de Seguridad del Operador tipo aparece desarrollada en mayor detalle en el artículo de Fernando Sánchez, «Protección de infraestructuras críticas: El Sistema de planeamiento como herramienta de implantación (II)», publicado en la *Revista Seguridad y Ciudadanía* n.º 13, de junio de 2015 (pp. 22 y ss.).

Para marcar el camino a seguir y asesorar al operador en su redacción, el CNPIC elabora una guía en la que se recogen los contenidos mínimos sobre los que se debe de apoyar el operador a la hora del diseño y elaboración de su Plan. A su vez, se establecen algunos puntos explicativos sobre aspectos recogidos en la normativa de referencia. En dicha guía, igualmente, se pretende orientar a aquellos operadores que hayan sido o vayan a ser designados como críticos en el diseño y elaboración de su respectivo Plan, con el fin de que estos puedan definir el contenido de su política general y el marco organizativo de seguridad, que encontrará su desarrollo específico en los Planes de Protección Específico (objeto del próximo epígrafe) de cada una de sus infraestructuras críticas. La Guía de Contenidos Mínimos es públicamente accesible y fue aprobada mediante Resolución de 8 de septiembre de 2015 de la Secretaría de Estado de Seguridad (BOE n.º 224, de 18 de septiembre)²⁹.

Dado que el desarrollo de estos planes está condicionado por la aprobación de los respectivos PES que aplican a cada operador crítico, hasta el momento se han podido completar aquellos relativos al Sector Energía, Industria Nuclear, Sistema Financiero, Agua y Transporte, Espacio e Industria Química, estando en fase de iniciación los correspondientes a los sectores TIC, Alimentación y Salud.

Los Planes de Protección Específicos (PPE)³⁰

Del sistema de planificación hasta ahora esbozado se deriva una responsabilidad compartida entre el operador crítico (propietario y/o gestor de las infraestructuras críticas que presta servicios esenciales) y el Gobierno de España, representado por la Secretaría de Estado de Seguridad del Ministerio del Interior, como garante de que los servicios esenciales sean proporcionados en condiciones de seguridad, integridad y calidad, en beneficio de la población civil, las instituciones públicas y el sistema empresarial del país.

Para ello, las dos primeras piezas de dicho sistema de planificación ya han sido, en su mayor parte, como se ha visto en estas líneas, diseñadas por el Estado (Plan Nacional de Protección de las Infraestructuras Críticas y Planes Estratégicos Sectoriales), mientras que la redacción de los Planes de Seguridad del Operador es una responsabilidad de los operadores críticos. Todos estos documentos son de carácter estratégico, elaborados, revisados y, en su caso, aprobados, en el ámbito de la Administración General del Estado por los departamentos u organismos competentes.

²⁹ <http://www.boe.es/boe/dias/2015/09/18/pdfs/BOE-A-2015-10060.pdf>

³⁰ La estructura y contenido de un Plan de Protección Específico tipo aparece desarrollada en mayor detalle en el artículo de Fernando Sánchez, «Protección de infraestructuras críticas: El Sistema de planeamiento como herramienta de implantación (II)», publicado en la *Revista Seguridad y Ciudadanía* n.º 13, de junio de 2015 (pp. 50 y ss.).

Tras estos planes de carácter superior, la implantación del Sistema PIC tiene su continuación en el marco territorial y operativo a través de los Planes de Protección Específicos y de los Planes de Apoyo Operativo, sobre los cuales las Administraciones Públicas tienen responsabilidad en la aprobación y revisión de los primeros y en la elaboración, aprobación y revisión de los segundos.

El Plan de Protección Específico es aquel documento operativo donde el operador crítico debe definir las medidas concretas ya adoptadas y las que se vayan a adoptar para garantizar la seguridad integral (física y lógica) de aquellas infraestructuras que sean catalogadas como críticas. Es decir, el operador ha de elaborar un Plan por cada uno de los activos identificados como críticos.

El Plan de Protección Específico de cada infraestructura deberá contemplar la adopción tanto de medidas permanentes de protección como de medidas de seguridad temporales y graduadas, que vendrán en su caso determinadas por la activación del Plan Nacional de Protección de las Infraestructuras Críticas, o bien como consecuencia de las comunicaciones que las autoridades competentes puedan efectuar al operador crítico en relación con una amenaza concreta sobre una o varias infraestructuras por este gestionadas. Al igual que en el caso de los Planes de Seguridad del Operador, los operadores cuentan con una guía de Contenidos Mínimos (igualmente aprobada por Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad) para el desarrollo de los Planes de Protección Específicos³¹.

Cabe destacar en este caso que, dado el elevado número de planes existentes, en el desarrollo del sistema de planificación e implantación territorial de los mismos se requiere la intervención de las distintas Delegaciones de Gobierno y Fuerzas y Cuerpos de Seguridad del territorio donde se encuentran enclavadas las diferentes infraestructuras críticas identificadas.

Por todo ello, y con el fin de culminar el establecimiento del sistema de planificación establecido en la Ley 8/2011 a nivel territorial, en atención a las especiales obligaciones que exige la citada Ley a las Administraciones públicas competentes, y teniendo en cuenta los numerosos agentes que participan en su implantación (Delegaciones del Gobierno, Comunidades Autónomas y Fuerzas y Cuerpos de Seguridad) se dictó por parte del Secretario de Estado de Seguridad una Instrucción, de fecha 10 de septiembre de 2015, dirigida a todos los agentes responsables, donde se termina de definir el marco de actuación de estos. Dicha instrucción tiene como objeto contribuir a agilizar la implantación del citado sistema de una manera eficaz, ágil, homogénea y armonizada en las diferentes Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía, desde el punto de vista de la seguridad y protección de las infraestructuras.

³¹ Ibíd. 29.

Los Planes de Apoyo Operativo (PAO)

La Ley PIC prevé que, sobre cada infraestructura crítica, las Fuerzas y Cuerpos de Seguridad competentes, para llevar a cabo su protección, desarrollarán un Plan de Apoyo Operativo en el que se diseñará un plan de reacción e intervención en apoyo de los mecanismos de seguridad implementados por cada organización en sus respectivos Planes de Protección Específicos. Esto supone, por tanto, un trato «preferencial» sobre las instalaciones críticas en caso de incremento del nivel de alerta previsto por el PNPIC.

El Cuerpo policial competente deberá redactar, tras serle notificada la aprobación del Plan de Protección Específico por la Secretaría de Estado de Seguridad, un Plan de Apoyo Operativo para dicha infraestructura, donde se establecerán las medidas planificadas de vigilancia, prevención, protección y reacción que deberá adoptar dicho Cuerpo policial y, en su caso, su coordinación con otras Fuerzas y Cuerpos de Seguridad.

El Plan de Apoyo Operativo deberá contemplar las medidas preventivas y reactivas a desarrollar en función del nivel de riesgo establecido en el Plan de Prevención y Protección Antiterrorista y/o el Plan Nacional de Protección de las Infraestructuras Críticas o de confirmarse la existencia de una amenaza inminente.

Las medidas propuestas en el Plan de Apoyo Operativo serán complementarias a aquellas de carácter gradual previstas por el operador crítico en su Plan de Protección Específico, el cual deberá servir como base para la redacción del primero. Para ello, el Cuerpo policial competente deberá tener acceso al contenido del citado Plan de Protección Específico y podrá requerir la colaboración del Delegado de Seguridad de dicha infraestructura crítica. Por su parte, el operador deberá poder tener acceso, de forma limitada, al contenido de dichos planes para armonizarlos con los Planes de Protección Específicos de sus propias instalaciones. De la misma manera, las unidades operativas de las Fuerzas y Cuerpos de Seguridad competentes deberán coordinarse con los servicios de seguridad de los operadores para la protección de las instalaciones afectadas.

El Plan de Apoyo Operativo, cuya elaboración será supervisada por la Delegación del Gobierno o, en su caso, por el órgano de la Comunidad Autónoma con competencia en materia de seguridad, se ajustará a los contenidos mínimos establecidos por la Secretaría de Estado de Seguridad que se adjuntan como anexo a la Instrucción de 10 de septiembre de 2015, ya mencionada en el anterior epígrafe.

Finalmente, una vez elaborado un Plan de Apoyo Operativo, el Cuerpo policial competente lo remite a la Delegación del Gobierno que, a su vez, lo cursa al CNPIC para su aprobación y validación por la Secretaría de Estado de Seguridad.

De esta manera, el ciclo planificador, iniciado con el PNPIC, se ve cerrado con la aprobación de los diferentes Planes de Apoyo Operativo con la intervención y delimitación de responsabilidades de todos los agentes responsables en materia de protección de infraestructuras críticas. Obviamente este es un proceso largo, que será culminado a principios de 2017 en lo respectivo a los sectores de la Energía y Sistema Financiero y Nuclear. Una vez esté rematado se puede decir que el Sistema PIC que emane de dicho proceso tendrá la robustez y agilidad necesarias para abordar la problemática de la protección de nuestras infraestructuras y servicios esenciales con garantías de éxito, con los controles necesarios y con la cooperación público-privada como eje conductor de las actividades e iniciativas que se desarrollen.

Herramientas para la colaboración

Como ya se ha visto, el Sistema de Protección de Infraestructuras Críticas integra una serie de planes de seguridad en los que la ciberseguridad tiene un papel fundamental, como complemento a aquellas medidas de seguridad de carácter más tradicional que se contemplaban hasta el momento de crear este sistema holístico. Sin embargo, la ciberseguridad requiere en algunas ocasiones el establecimiento de otra serie de medidas particulares que garanticen la comunicación, cooperación y colaboración entre los distintos agentes con capacidad de actuación. En el ámbito de la protección de las infraestructuras críticas, se considera fundamental no solo el asegurar una adecuada protección cibernética de las infraestructuras³², sino además el garantizar que se implementan herramientas relativas a la participación e integración de todos los agentes responsables de una u otra manera en la ciberseguridad. A continuación se detallan las medidas implantadas al efecto hasta el momento por el CNPIC.

Apoyo frente a incidentes

Las tecnologías empleadas por las infraestructuras críticas no difieren de aquellas empleadas en otro tipo de entornos, por lo que las amenazas a las que se ven expuestas son las mismas, si bien el impacto de su materialización sí que puede amplificarse en entornos críticos. Por lo tanto, los operadores críticos deben protegerse frente a ataques que puedan afectar a

³² La Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 30 de marzo de 2009, sobre protección de infraestructuras críticas, «Protegiendo a Europa de ciberataques a gran escala e interrupciones: mejora de la preparación, la seguridad y la respuesta» [COM (2009) 149 final], hace por primera vez, a nivel europeo, un llamamiento a la convergencia de la seguridad física y la seguridad lógica, ante la evidencia de la utilización de la red por criminales y terroristas como medio de llevar a cabo sus acciones contra las infraestructuras críticas.

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF>

la confidencialidad, integridad o disponibilidad de sus activos tecnológicos, siendo conscientes de que la interconectividad, que predomina en este tipo de entornos, puede facilitar la propagación de un incidente hacia todo el entorno tecnológico de la organización.

De forma adicional, cabe destacar el hecho de que cuando se tiene conocimiento de un incidente, es muy difícil asignar *a priori* una tipología concreta. De hecho, incidentes en los que todo apunta a que van dirigidos exclusivamente hacia el robo de información pueden formar parte de un ataque más complejo que tenga por objeto inhabilitar el servicio o afectar al correcto funcionamiento de la infraestructura. Los intereses de los atacantes pueden diferir por tanto en cada ataque y, siendo compleja su identificación, suelen estar referidos a la obtención de un beneficio económico, a la publicidad de sus acciones o propaganda de determinadas ideologías o, en casos extremos, a causar terror en la población.

Como se ha reseñado repetidamente a lo largo de este artículo el CNPIC plantea, además de ser uno de sus precursores en España, el concepto de seguridad integral³³, trabajando de forma dinámica y continua para garantizar la seguridad a los sistemas de información y telecomunicaciones que soportan las infraestructuras. En este campo se han fortalecido las capacidades de prevención, detección, respuesta y recuperación para hacer frente a las ciberamenazas, desarrollando:

- Un Equipo de Respuesta a Incidentes Cibernéticos (CERT de Seguridad e Industria–CERTSI_), con sede en León, operado por el Instituto Nacional de Ciberseguridad (INCIBE), en conjunción con el CNPIC y que se ha erigido en el punto de referencia nacional para la resolución técnica de incidentes de ciberseguridad que puedan afectar a la prestación de los servicios esenciales³⁴.

³³ Exigible a los operadores críticos, entre otras, por la *Guía de Contenidos Mínimos* aprobada mediante Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad (BOE n.º 224, de 18 de septiembre).

<http://www.boe.es/boe/dias/2015/09/18/pdfs/BOE-A-2015-10060.pdf>

³⁴ El CERT de Seguridad e Industria (CERTSI_) es, entre otras acciones, consecuencia del *Acuerdo Marco de Colaboración en materia de Ciberseguridad entre la Secretaría de Estado de Seguridad del Ministerio del Interior y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo*, de fecha 4 de octubre de 2012 (actualizado con fecha 21 de octubre de 2015).

El mencionado acuerdo fijó las bases de la colaboración entre la SES y la SETSI para impulsar en España los aspectos de seguridad en el ámbito de la Sociedad de la Información en general, la protección de las infraestructuras críticas y la lucha contra los delitos informáticos (también conocidos como «ciberdelitos») y el ciberterrorismo, dando respuesta a los objetivos planteados por la Estrategia Española de Seguridad de 2011 y la Agenda Digital para España. Dicha colaboración fue planteada sobre la base de un mecanismo de coordinación entre el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) y el entonces INTECO (hoy INCIBE) en la resolución de incidentes y mitigación de sus efectos, así como en el intercambio de información de interés.

- Una Oficina de Coordinación Cibernética (OCC) en el seno del CNPIC, como punto de contacto nacional de coordinación operativa 7 × 24 para el intercambio de información.

En lo que respecta a la gestión de incidentes de ciberseguridad, es importante resaltar que por parte del CNPIC y el CERTSI_ se ha desarrollado la *Guía de reporte de ciberincidentes para operadores críticos*, con objeto de establecer una clara delimitación de la tipología de ciberincidentes que deben de ser reportados, así como la forma y momento de hacerlo en cada caso.

De este modo, esta guía tiene por objeto dar cumplimiento a lo dispuesto en el PNPIC, desarrollando en detalle cuál es el tipo de acciones que debe de llevar a cabo el operador crítico según el Nivel de Alerta sobre infraestructuras críticas que se encuentre activo en un momento determinado (a la hora en que se escribe este artículo nos encontramos en nivel 4, coordinado con el Nivel de Alerta Antiterrorista). Cabe destacar que el aumento gradual de medidas asociadas en materia de ciberseguridad conlleva una serie de obligaciones no solo para los operadores críticos, sino también, muy especialmente, para el CNPIC y el CERTSI_ como responsables de la administración de la ciberseguridad de las infraestructuras críticas nacionales, con la adquisición de un compromiso para la intervención y resolución de las incidencias en un marco temporal variable, según escale el nivel de la amenaza.

El equipo de respuesta a incidentes cibernéticos de seguridad e industria (CERTSI_)

El CERT de Seguridad e Industria (CERTSI_) es el CERT Nacional competente, por Acuerdo del Consejo Nacional de Ciberseguridad de 29 de mayo de 2015, en la prevención, mitigación y respuesta ante incidentes cibernéticos en el ámbito de las empresas, los ciudadanos y los operadores de infraestructuras críticas³⁵.

Creado en octubre de 2012 a través de un Acuerdo Marco de Colaboración en materia de ciberseguridad entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, recientemente actualizado el pasado 21 de octubre de 2015, el CERTSI_ se configura como la entidad tecnológica encargada de la gestión de incidentes de naturaleza cibernética que afecten a los operadores de los servicios esenciales en España.

Este equipo de respuesta es el resultado de la suma de capacidades y competencias del Instituto Nacional de Ciberseguridad (INCIBE) y del Centro

³⁵ El Consejo Nacional de Ciberseguridad (Comité especializado) es un órgano colegiado de apoyo al Consejo Nacional de Seguridad con la finalidad de informar y asesorar a aquel en el ámbito de la ciberseguridad, de acuerdo con lo previsto por la Estrategia de Seguridad Nacional de junio de 2013.

Nacional para la Protección de las Infraestructuras Críticas (CNPIC) y, por consiguiente, añade a las responsabilidades ya existentes sobre empresas y ciudadanos, previas a la firma del Acuerdo SES-SETSI, aquellas que se derivan de la necesidad de mejorar la protección de las infraestructuras críticas y la provisión de los servicios esenciales³⁶.

En este sentido, cabe destacar que habitualmente los *CERT* no se encargan únicamente de la gestión de incidentes, sino que ofrecen de forma habitual otro tipo de servicios de utilidad para su público objetivo. En el caso particular del CERTSI, el inicio de las actividades en el ámbito PIC se diseñó sobre la base de la identificación y definición de un catálogo de servicios en el ámbito de la prevención, detección y respuesta ante incidentes, que se ha ido mejorando y complementando aprovechando la experiencia y madurez del propio centro a lo largo de estos últimos tiempos³⁷.

En la actualidad, dicho catálogo contempla servicios adicionales de valor añadido, como son la realización de ciberejercicios con periodicidad anual o la compartición de información acerca de vulnerabilidades «día cero» (vulnerabilidades que aún no han sido publicadas por el fabricante). De este modo, se pretende dotar a los operadores críticos de información y capacidades privilegiadas con objeto de complementar la, sin duda necesaria, gestión autónoma de la ciberseguridad.

La Oficina de Coordinación Cibernética del Ministerio del Interior

En el año 2014, mediante la Instrucción 15/2014, de la Secretaría de Estado de Seguridad, se creó dentro del CNPIC la Oficina de Coordinación Cibernética (OCC) que se configuró desde ese instante como el órgano técnico de coordinación de la Secretaría de Estado de Seguridad en materia de ciberseguridad. Su objetivo es conseguir una mayor eficiencia en la gestión de aquellos aspectos de la Estrategia de Ciberseguridad Nacional que se encuentran

³⁶ Algunas de las actuaciones acordadas en el ámbito de la protección de las infraestructuras críticas son:

1. La respuesta a Incidentes de Seguridad TIC en las infraestructuras críticas y los operadores de servicios esenciales.

2. La puesta en marcha de auditorías de seguridad y esquemas de acreditación sobre sistemas de información que dan soporte a las infraestructuras críticas.

Dichas medidas, recogidas en los Contenidos Mínimos publicados por Resolución del Secretario de Estado de Seguridad en relación a los Planes de Seguridad del Operador y a los Planes de Protección Específicos, serán actualizadas de forma periódica por el CNPIC, y contarán con la colaboración del INCIBE en la variable de ciberseguridad.

3. La realización de simulacros y ciberejercicios sobre infraestructuras críticas.

³⁷ De acuerdo con lo determinado en el Acuerdo SES-SETSI, el equipo técnico del CERTSI atenderá los incidentes de acuerdo con las prioridades definidas en los umbrales y procedimientos fijados por ambas entidades. Asimismo, el servicio se desempeñará en horario continuado (24 x 7 x 365) con un acuerdo de nivel de servicio (SLA) que permita dar una respuesta ágil a los incidentes de los que se tenga constancia.

bajo la competencia del Ministerio del Interior, siendo además el punto natural de interlocución del Ministerio con el CERTSI_ en materia tecnológica³⁸.

En este sentido, las actuaciones que lleva a cabo la OCC se refieren normalmente al intercambio de información en materia de ciberdelincuencia y ciberterrorismo; a la coordinación de acciones de respuesta ante incidentes, integrando las capacidades de las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado cuando sea necesario; a la emisión de información de alerta temprana sobre ciberamenazas; a la supervisión en materia de ciberseguridad de los planes de seguridad que conforman el PNPIC y a la participación en proyectos de I+D.

Por otra parte, el PNPIC contempla en determinadas situaciones el establecimiento de Dispositivos Extraordinarios de Ciberseguridad. Para su diseño e implementación, la OCC se ha erigido como el órgano responsable de efectuar la coordinación técnica entre los responsables de seguridad de los sistemas y tecnologías de la información de los operadores críticos, las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado y el CERTSI_.

Recientemente, en virtud de otra instrucción de la Secretaría de Estado de Seguridad (2/2016 de 10 de febrero) la OCC se constituyó también en punto de contacto del Estado Español en el marco de lo prescrito por la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información³⁹.

³⁸ En noviembre de 2014, mediante Instrucción 15/2014 del Secretario de Estado de Seguridad, se crea la Oficina de Coordinación Cibernética (OCC). De manera específica, la OCC es identificada como la unidad responsable de la coordinación técnica entre la SES y sus organismos dependientes y el CERTSI_. Para ello, se le ha dotado de los mecanismos de intercambio de información seguros necesarios para comunicarse tanto con dicho CERT como con las distintas unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado, agilizando la difusión de información que pueda ser de interés para cualquiera de las partes.

³⁹ La Directiva 2013/40/UE determina en su artículo 13 que los Estados miembros deberán garantizar la existencia de un punto de contacto nacional operativo a efectos del intercambio de información sobre ciberataques. Asimismo, establece la necesidad de que estos cuenten con procedimientos para que, en caso de solicitud de ayuda urgente, la autoridad competente pueda indicar, en un plazo máximo de ocho horas a partir de la recepción de la solicitud de ayuda, si la misma podrá ser atendida y la forma y el plazo aproximado de ello. La instrucción 2/2016 tiene por objeto la designación de la Oficina de Coordinación Cibernética como punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros. De esa manera, la OCC se constituyó, desde febrero de 2016, en el punto de contacto nacional operativo en el marco de lo establecido en el artículo 13 de la Directiva 2013/40/UE. Esta Oficina dispondrá de las necesarias capacidades de operación veinticuatro horas al día, siete días a la semana, con el fin de responder a las solicitudes de ayuda en el plazo máximo marcado por la citada Directiva. Para ello contará, también, con un enlace permanente con las unidades responsables de las Fuerzas y Cuerpos de Seguridad del Estado y con aquellos otros órganos de esta Secretaría de Estado con competencias en la materia.



Figura 5.5. Logo de la Oficina de Coordinación Cibernética del Ministerio del Interior.

Alerta temprana e intercambio de información

En los últimos años se ha podido observar que, en materia de ciberseguridad, se está asistiendo a un cambio de paradigma en lo referente al intercambio de información sobre ciberincidentes y a las acciones de alerta temprana derivadas del conocimiento de las amenazas que presenta el entorno en el que desarrollan su actividad los operadores de servicios esenciales. Este cambio de paradigma se basa en el paso de los viejos usos y costumbres de un mundo poco conectado, en el que el acceso a la información disponible era restringido y normalmente referido a sistemas propietarios, a un escenario en el que la hiperconectividad y el acceso instantáneo a todo tipo de información es omnipresente; escenario en el que, por supuesto, se ven inmersos los sectores estratégicos nacionales.

En este nuevo escenario, un potencial ciberdelincuente o ciberterrorista cuenta con una multiplicidad de recursos de los que antes no disponía: información sobre sistemas de control industrial, información sobre los protocolos que usan esos sistemas, sobre sus vulnerabilidades, sobre quiénes los administran, sobre su pertenencia, así como cuantiosas herramientas para poder vulnerar la seguridad de dichos sistemas de control industrial...

Ahora bien, en este nuevo escenario hiperconectado que puede ser aprovechado por quienes buscan obtener algún beneficio a través de la disrupción de la confidencialidad, la disponibilidad o la integridad de los sistemas, también se está empezando a utilizar como recurso indispensable a la hora de

luchar contra las amenazas que presenta la operativa de sistemas de control industrial en un entorno conectado y global. Los dos pilares de este nuevo paradigma son la alerta temprana y el intercambio de información, que funcionan sobre la base de unos principios muy sencillos:

- Cuanto antes se tenga conocimiento de una amenaza y su naturaleza, antes se podrán dedicar recursos para evitar que llegue a materializarse o, si esto ocurre, a mitigar el impacto producido. En el mundo hiperconectado, conocer que tus sistemas pueden ser comprometidos y difundir este conocimiento sobre la base de una red colaborativa de usuarios mutuamente interesados es técnicamente posible.
- La información sobre incidentes reales y cómo han sido mitigados es de gran utilidad a la hora de elaborar contramedidas, mejorar los sistemas y protocolos así como publicar guías de buenas prácticas a fin de evitar que un incidente de similares características vuelva a reproducirse. La tendencia de ocultar la información de resolución de incidentes se está abandonando progresivamente y ahora prima la difusión y obtención de información sobre aquellos incidentes que pueden afectarnos. Esto es una consecuencia lógica del nivel de avance tecnológico de la sociedad industrializada: la cantidad de conocimiento sobre las vulnerabilidades de nuestros sistemas que se genera en un entorno hiperconectado supera a aquel conocimiento que pueda ser generado por equipos individuales en la gestión de sus sistemas y su seguridad, por lo que estratégicamente es más ventajoso el unirse a comunidades de intercambio de información que aislarse de estas redes.

Por todo ello, una de las principales líneas de acción del CNPIC, junto con el INCIBE, es precisamente el impulso, desarrollo e implantación de proyectos que tienen como claro objetivo ofrecer soporte tecnológico a los responsables de la administración de la ciberseguridad en operadores de servicios esenciales y sus infraestructuras y redes, para que puedan establecer estas redes de intercambio de información y alerta temprana. Este soporte se realiza en dos niveles distintos: a nivel individual, con aplicativos adaptados a las características del operador crítico y, a un nivel más amplio, mediante plataformas o proyectos dirigidos al conjunto de operadores de los distintos sectores estratégicos.

Como ejemplo del nivel individual de acción, y enmarcado en la Estrategia de Ciberseguridad Nacional⁴⁰, se ofrece el servicio Detector de Incidentes, que es una plataforma tecnológica de alerta temprana y vigilancia tecnológica, por la que el CERTSI_ lleva a cabo el despliegue y operación de servicios de inteligencia en ciberseguridad mediante el establecimiento de acuerdos con entidades de referencia internacional en materia de ciberseguridad, a fin

⁴⁰ Línea de acción n.º 3: *Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas* (pp. 34 y ss.).
<http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional>

de obtener información actualizada que se utiliza en las labores de investigación para la detección proactiva de amenazas. Mediante este servicio se puede analizar, en las propias instalaciones del operador, el tráfico de internet entrante y saliente, contrastando la información obtenida con las listas de recursos maliciosos conocidos y de indicadores de compromiso que suministra en tiempo real el servidor de gestión centralizada del INCIBE. Esta funcionalidad permite al operador crítico reducir de forma drástica el tiempo de detección de compromiso de sus activos tecnológicos al contar en sus propias instalaciones con la información actualizada de amenazas en curso.

En el plano de la acción colectiva, el servicio ÍCARO ofrece a los operadores críticos una plataforma en la que intercambiar información acerca de ciberamenazas. ÍCARO es una plataforma que centraliza la información aportada por los operadores de servicios esenciales de los distintos sectores estratégicos, de tal forma que el CERTSI_ puede contrastar y verificar dicha información para posteriormente ofrecérsela a todos los operadores que conforman la comunidad de intercambio de información. Un aspecto muy importante de este sistema es la utilización de estándares internacionales para estructurar dicha información y posteriormente intercambiarla, de tal forma que las labores pueden automatizarse. De esta forma, el operador puede desplegar en sus instalaciones una instancia de ICARO que se sincroniza automáticamente con la plataforma central y puede tanto obtener información como aportar nuevos datos para complementar los que ya se encuentren analizados por el CERT. La información sobre una amenaza concreta puede ser muy diversa, llegando a incluir muestras de *malware*, listados de IPs con actividad maliciosa, indicadores de compromiso, reglas de *firewall*, guías de mitigación y buenas prácticas, etcétera.

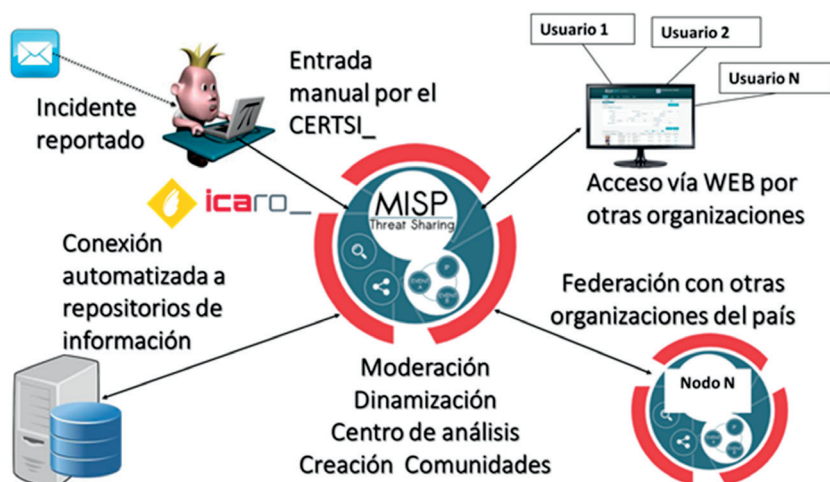


Figura 5.6. Funcionamiento plataforma ÍCARO.

Ciberejercicios

La realización de ciberejercicios es una pieza fundamental en la estrategia del Gobierno en materia de ciberseguridad, por ello, desde el año 2012, el CNPIC, junto con el INCIBE, a través del CERTSI⁴¹, se ha involucrado en la organización de los ejercicios CyberEX⁴². En las primeras convocatorias de CyberEX (2012 y 2013) el objetivo principal a alcanzar para las entidades participantes era la evaluación de las capacidades técnicas y organizativas, por lo que el ejercicio se basó en la simulación de ataques técnicos a servicios perimetrales. En 2014, el público objetivo fueron operadores de servicios esenciales y también se procedió a la ejecución de simulaciones generalistas, al tener un carácter multisectorial. La última convocatoria, en 2015, enfocado en el negocio, se centró ya en operadores del sector estratégico financiero.

Para la actual convocatoria de 2016⁴³ se ha apostado de nuevo por una visión multisectorial; siguiendo el plan previsto, se comienza la alternancia entre las ediciones sectoriales y multisectoriales, que permitirán mantener un contacto cercano con los operadores de nuestros servicios esenciales. Además, en la actual edición se pasará de dieciocho participantes a treinta.

En cuanto a las pruebas a realizar durante la fase de ejecución, se llevarán a cabo tres, que buscarán entrenar distintos aspectos de la seguridad de las entidades. Estas son: un ataque/defensa para tratar de entrenar las capacidades de reacción frente a ataques, una prueba para entrenar las capacidades de coordinación y toma de decisiones técnicas y estratégicas en una crisis y, finalmente, una prueba de análisis para entrenar las capacidades de análisis técnico de un incidente.

⁴¹ La realización de simulacros y ciberejercicios sobre infraestructuras críticas es uno de los objetivos del Acuerdo SES-SETSI en materia de ciberseguridad. En dicho documento, se coincide en que la realización de simulacros y ejercicios que sean capaces de probar el nivel de protección corporativa con el que cuentan los operadores de infraestructuras críticas, la resistencia de las infraestructuras críticas y de los sistemas de información que las soportan y la capacidad de coordinación real entre los agentes implicados en caso de ciberataques constituye un mecanismo efectivo y de alto valor, no solo para el CNPIC como órgano competente, sino también para los propios operadores críticos.

Basados en la experiencia desarrollada en la realización de los ciberejercicios Ciberex y buscando su continuidad y consolidación, el CNPIC e INCIBE diseñan y coordinan conjuntamente ciberejercicios que permiten la mejora de los procedimientos de actuación, las técnicas, las capacidades, la preparación y la concienciación de los operadores de infraestructuras críticas y de otros prestatarios de servicios esenciales, a partir de su entrenamiento y del mejor conocimiento de los riesgos y amenazas en el ámbito de las tecnologías de la información y las comunicaciones.

⁴² <https://www.cyberex.es/international/es/inicio>
<https://www.certs.es/servicios-operadores/cyberex>

⁴³ <https://www.incibe.es/sala-prensa/notas-prensa/comienzan-los-ciberejercicios-nacionales-cyberex-2016-destinados-mejorar>

Se prevé que durante la ejecución de las pruebas otras entidades públicas como Fuerzas y Cuerpos de Seguridad del Estado o entidades reguladoras puedan adquirir el rol de observador.

Como novedad en 2016, se procederá a la ejecución de los ciberejercicios a partir de un entorno tecnológico estable (plataforma) que permite la realización de competiciones y entrenamiento de conocimientos sobre ciberseguridad de los participantes, con el diseño de escenarios que se puedan desplegar en la plataforma. Se contará con cuatro tipos de escenarios que pueden ser implementados en esta plataforma: ataque/defensa, descargables, *Capture The Flag (CTF)* y didácticos. En el empleo de esta plataforma, con cada ciberejercicio, el CERTSI_ determinará si se llevará a cabo el ciclo de vida completo de desarrollo de un ciberejercicio o únicamente la fase de ejecución. Esto permitirá reutilizar ciberejercicios, amortizando su coste con cada iteración.

Además de CyberEX, el CNPIC ha participado como coorganizador y jugador en otros cuatro tipos de ciberejercicios en los últimos meses, tanto nacionales como internacionales, como las Jornadas PSCIC, en el marco del proyecto *CIISC-T2 (Critical Infrastructure: Improvement of Security Control Against the Terrorist Threat)*. CIISC-T2 es un proyecto ya finalizado y cofinanciado por la Comisión Europea a través del programa CIPS en el que CNPIC, junto con el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), Isdefe y Kemea (autoridad griega) son cobeneficiarios. Dentro del paquete de trabajo WP3 «Cyberexercise to protect critical infrastructures», la OCC y el CERTSI_ han participado como coordinador y jugador, respectivamente, y la ejecución de este paquete se ha visto materializada en el ciberejercicio de las II Jornadas PSCIC⁴⁴. Es importante destacar que dentro del paquete de trabajo WP4 «Cyberexercise to protect potencial european critical infrastructures» el CNPIC participó como líder en la planificación de un ciberejercicio a nivel europeo en 2015 como continuación del llevado a cabo en el 2014.

Por otro lado, la Administración española, como país miembro de la OTAN, ha participado como planificador y jugador en el ejercicio CMX-16, teniendo el CNPIC un rol relevante en la recreación de los escenarios. *CMX (Crisis Management Exercise)* son ejercicios organizados por OTAN con la participación de los países aliados. A nivel nacional, estos ejercicios son liderados por el CESEDEN y para la convocatoria de este año se han recreado dos eventos nacionales, un altercado en un buque en aguas nacionales y un ataque a una infraestructura crítica portuaria. Además, como cada año, el CNPIC ha participado en el ciberejercicio Locked Shields, organizado por el Centro de Excelencia de Ciberdefensa de la OTAN.

Finalmente, en el ámbito europeo, la OCC está participando como jugador en el ejercicio paneuropeo Cyber-Europe 2016, coorganizado, a nivel nacional, por

⁴⁴ <https://www.jornadaspsbic.isdefe.es/?lang=es>

el Departamento de Seguridad Nacional (DSN) de Presidencia del Gobierno. En este mismo ámbito europeo, se organizó en Madrid en febrero de 2016, conjuntamente por la Unidad de Acción contra el Terrorismo (UAT) de OSCE (Organización para la Seguridad y Cooperación en Europa) y el CNPIC, un taller internacional consistente en un ejercicio de simulación (*table-top exercise*) sobre protección de infraestructuras críticas energéticas contra ataques informáticos, siguiendo el modelo de colaboración público-privada, con presencia de hasta quince grandes entidades del sector energético nacional.

Acuerdos de colaboración

La eficaz y eficiente colaboración entre el sector público y el sector privado en el ámbito de la protección de las infraestructuras críticas debe sustentarse sobre los siguientes pilares:

- Intercambio de información. El CNPIC asegura, mediante las plataformas de comunicación incluidas en el sistema informático de gestión del Catálogo Nacional de Infraestructuras, la comunicación y el intercambio de información tanto con las Fuerzas y Cuerpos de Seguridad y con los organismos competentes para la seguridad de los distintos sectores estratégicos como con los operadores críticos. En materia de ciberseguridad, a través del CERTSI_ circula cualquier tipo de información relevante que pueda mejorar el conocimiento del entorno, ya sea a nivel sectorial, organizativo o individual.
- Responsabilidad compartida. No se puede cargar al Estado con la responsabilidad exclusiva del aseguramiento del correcto funcionamiento de los servicios esenciales, al estar cerca del 80 % de las infraestructuras críticas que los suministran en manos del sector privado. En este sentido, los servicios ofrecidos por el CNPIC de forma general y por la OCC y el CERTSI_ de forma particular, en materia de ciberseguridad, tienen como uno de sus objetivos mejorar la concienciación de los operadores, con el fin de que sean capaces de responder autónomamente ante incidentes cibernéticos. Con todo, el CERTSI_ y la OCC siempre estarán como soporte de aquellos operadores críticos que requieran una ayuda excepcional.
- Confianza mutua. Las colaboraciones público-privadas se basan fundamentalmente en el establecimiento de relaciones sólidas entre los participantes. Se da por hecho que, si bien la participación en colaboraciones público-privadas es voluntaria, una vez se forma parte de una de ellas se asume que las conclusiones son vinculantes. La confianza mutua es la única manera de salvar la barrera del natural recelo a informar sobre incidentes, sobre todo cuando esta información pueda ser aprovechada por la competencia.

Sin embargo, no basta con la definición de esos tres pilares para garantizar una adecuada cooperación público-privada. Más si cabe cuando el intercam-

bio de información se lleva a cabo mediante medios tecnológicos para los que es necesario asegurar la confidencialidad de la información transmitida. Por este motivo fundamentalmente, los servicios del CERTSI_ se ofrecen siempre bajo la suscripción de un acuerdo de confidencialidad en materia de ciberseguridad que obliga a las partes suscriptoras (actualmente alrededor de cien, lo que supone una «bolsa» de un centenar de beneficiarios de lo que puede ser considerado como uno de los mayores foros de intercambio de información de nuestro país). De forma adicional, los operadores críticos firman igualmente otro acuerdo de confidencialidad con el CNPIC para garantizar que la información disponible en el Catálogo de Infraestructuras se maneja de forma apropiada y con las garantías necesarias. No obstante, los operadores que firman acuerdos deben garantizar igualmente que manejan adecuadamente la información aportada desde el CNPIC, el CERTSI_ o la OCC, de modo que se ratifique la confianza mutua mencionada anteriormente.

Controles recomendados

Además de las herramientas tratadas durante este capítulo, que ya se están utilizando para potenciar la colaboración público-privada, existen otras que nos permitirán seguir fomentando la colaboración y con ella la ciberseguridad. Un claro ejemplo es la adopción de controles o medidas de seguridad internacionalmente reconocidos para la protección de los sistemas de un determinado sector. De esta forma se garantiza la estandarización de los mismos y la personalización para el sector, siguiendo criterios de eficacia y facilidad para su implantación.

Al tener controles comunes, es posible comparar el nivel de seguridad de las empresas del sector y por lo tanto detectar si existe un problema de seguridad en alguna de ellas. Igualmente, frente a una nueva amenaza sería sencillo conocer la vulnerabilidad del sector y tomar las medidas necesarias para minimizar el riesgo lo antes posible.

Estos controles deberían fijarse conjuntamente entre la autoridad pública y las empresas del sector afectado, aportando la primera las amenazas existentes en el sector y las segundas el conocimiento de sus sistemas y su criticidad. Partiendo de esta información se determinarán los controles que son más eficaces, así como el nivel de implantación necesario. Debido a que las amenazas varían, también deben hacerlo los controles; esto nos obliga a mantener una gestión de los controles activos y una comunicación con las empresas afectadas por los mismos.

En el caso del sector de la energía y concretando en las infraestructuras esenciales de este sector, se podrían utilizar algunos de los siguientes estándares para definir los controles más apropiados:

- ISO 27019, guía para la gestión de la Seguridad de la información en sistemas de control del sector de la energía.

- Instituto SANS, instituto especializado en la formación e investigación en ciberseguridad.
- NIST que depende del Departamento de Comercio de Estados Unidos.

Estos estándares tienen un reconocimiento internacional importante, necesario para poder alcanzar un consenso sobre su necesidad y eficacia, así como para encontrar personal formado en los mismos, o bien para facilitar la formación del personal necesario. A continuación hacemos una pequeña descripción de los mismos.

ISO 27019

La Organización Internacional de Normalización (ISO) tiene como objetivo la creación de estándares internacionales y está formada por diversas organizaciones nacionales de estandarización. La serie de normas ISO 27000 son estándares de seguridad publicados por ISO que contiene las mejores prácticas en seguridad de la información para desarrollar, implementar y mantener controles para los sistemas de gestión de la seguridad de la información (SGSI o *ISMS*, acrónimo en inglés de *Information Security Management System*). Dentro de esta familia de estándares se encuentra la ISO 27019, enfocada a extender la seguridad a los procesos de sistemas de control (sistemas usados en procesos de producción industriales para controlar equipos o máquinas) del sector de la energía, permitiéndole implementar un sistema de gestión de la seguridad de la información.

La ISO 27019 es un documento técnico que, basado en la ISO 27002 (centrada en la implantación de los controles para la gestión de la seguridad de la información) se centra en su aplicación a los sistemas de control usados en el sector de la energía. El objetivo del documento es extender los estándares ISO 27000 a los procesos de sistemas de control y automatización de forma que permita al sector de la energía implementar un sistema de gestión de la seguridad de la información acorde con la ISO 27001.

SANS Institute

El Instituto *SANS* (*SysAdmin Audit, Networking and Security*) es una organización educativa que desde 1989 trabaja en la formación y certificación de especialistas en seguridad de la información, así como en documentos de investigación relacionados con esta especialidad. El Instituto genera y mantiene una gran colección de documentos de investigación sobre diversos aspectos de la seguridad de la información. De las publicaciones realizadas por el *SANS* Institute, podemos destacar la publicación periódica de los veinte controles críticos de seguridad para una ciberdefensa efectiva. Estos controles resumen de una forma práctica las medidas de seguridad más efectivas para implementar la seguridad en una empresa.

NIST

NIST son las siglas del *National Institute of Standards and Technology*, que depende del Departamento de Comercio de Estados Unidos y es responsa-

ble de desarrollar estándares de ciberseguridad, guías, test y métricas. Entre sus objetivos se encuentra el aumento de la fiabilidad y la capacidad de recuperación de las infraestructuras de sistemas. Esta tarea requiere una inversión sustancial en el diseño y el desarrollo de los sistemas y redes informáticas. Los documentos son desarrollados de forma conjunta por expertos de todo el mundo y revisados en un proceso público por expertos de la industria afectada por el documento, profesores especializados y personal del propio *NIST*. El *NIST* trabaja para conseguir un conjunto estructurado de procesos de sistemas de seguridad que, basándose en las normas internacionales ya establecidas, ofrece un importante punto de partida para realizar la documentación. Dentro de los documentos publicados destaca la Publicación 800-160, Ingeniería de Seguridad de Sistemas (*Systems Security Engineering*) que, publicado en mayo de 2014, ofrece un enfoque integrado para la construcción de sistemas resistentes, ayudando a las organizaciones a desarrollar una infraestructura de sistemas resistentes frente a los ataques cibernéticos y otras amenazas. Otra publicación a destacar realizada por el *NIST* es la *Guía para la seguridad de los sistemas de control industrial (Guide to Industrial Control Systems)*: esta guía define controles de seguridad para los sistemas SCADA (*Supervisory Control and Data Acquisition*), equipos PLC (*Programmable Logic Controllers*) y sistemas DCS (*Distributed Control Systems*).

Ámbito internacional

La colaboración público-privada, al igual que la ciberseguridad, no conocen fronteras y por tanto es inútil restringir sus actividades a ámbitos delimitados geográficamente. Teniendo esto presente, el Sistema de Protección de Infraestructuras Críticas en España facilita el encaje de las actividades llevadas a cabo a nivel nacional con aquellas que se emprenden internacionalmente. Muchos de los ciberejercicios presentados en este artículo se diseñan y planifican desde una perspectiva global, pero existen otro tipo de actividades que tienen por objeto fomentar la colaboración público-privada.

En particular, cabe destacar que a nivel de la Unión Europea, el CNPIC es miembro de diversos Grupos de Trabajo enmarcados en el ámbito de la ciberseguridad y de la Protección de las Infraestructuras Críticas. Dentro del Programa Europeo de Protección de Infraestructuras Críticas (PEPIC) existen una serie de iniciativas en las que el CNPIC participa asiduamente, como son: la red de Información para Infraestructuras Críticas (*C/WIN*), el Grupo de Protección Civil- Subgrupo PIC (Comisión Europea) y el Grupo de Expertos sobre PIC Estados Unidos-Unión Europea-Canadá. En este ámbito europeo, se celebró en mayo de 2016 en Ámsterdam, ejerciendo Países Bajos la Presidencia del Consejo de la Unión Europea, una reunión de alto nivel sobre ciberseguridad con participación de altos funcionarios de los Estados miembros encargados de la seguridad cibernética y directivos de empresas de telecomunicaciones, así como responsables de la seguridad de infraestructuras críticas, donde estuvo igualmente representado este Centro.

En lo que respecta al marco de las relaciones con Iberoamérica, y de la mano de la Organización de Estados Americanos (OEA), el CNPIC ha coorganizado con el INCIBE (en Chile, julio de 2015 y en Paraguay, noviembre de 2015) sendos talleres sobre «Protección de Infraestructuras Públicas y Ciberseguridad» con el objetivo de formar en la materia a entidades públicas y privadas de los países de la zona, con la asistencia de once Gobiernos latinoamericanos.

Con un marcado carácter de intercambio de experiencias internacionales en materia de la Protección de Infraestructuras Críticas y la Ciberseguridad, se creó el conocido como *Proceso Meridian* en el año 2005. Ese año se llevó a cabo una primera Conferencia celebrada en Londres. A día de hoy se ha conformado como un foro internacional de gran prestigio, formado por cerca de cuarenta países de los cinco continentes, donde participan exclusivamente gobiernos y cuya presidencia rotatoria es otorgada a países con reconocido prestigio y experiencia en este campo. España ha venido participando en todas las Conferencias Meridian desde el año 2007, a través del CNPIC, y desde el 2012 es miembro de pleno derecho del Comité Directivo, habiendo ostentado durante 2015 la presidencia del Proceso Meridian. Por este motivo el CNPIC organizó en León, entre los días 21 y 23 de octubre de 2015, la 11.ª Conferencia Meridian. Esta se combinó con otro evento global de ciberseguridad, dedicado a empresas y ciudadanos, que se celebró también en León entre los días 19 y 21 y que lideró el Instituto Nacional de Ciberseguridad (INCIBE). Todo ello ha supuesto conjuntamente una de las iniciativas de ciberseguridad de mayor entidad puestas en marcha por un Gobierno a lo largo de 2015.

Bibliografía

Legislación y Normativa Nacional

Ley 8/2011, de 28 de abril, por la que se Establecen Medidas para la Protección de las Infraestructuras Críticas. Boletín Oficial del Estado n.º 102, de 29 de abril de 2011.

Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. Boletín Oficial del Estado n.º 121, de 21 de mayo de 2011.

Plan Nacional de Protección de Infraestructuras Críticas, de 7 de mayo de 2007. Modificado por Instrucción 1/2016, de 10 de febrero, de la Secretaría de Estado de Seguridad. No publicado en el Boletín Oficial del Estado.

Estrategia de Seguridad Nacional. Catálogo de Publicaciones de la Administración General del Estado. Gobierno de España, junio de 2013.

Estrategia de Ciberseguridad Nacional. Catálogo de Publicaciones de la Administración General del Estado. Gobierno de España, diciembre de 2013.

Plan Nacional de Ciberseguridad. Aprobado por el Consejo de Seguridad Nacional en octubre de 2014. No publicado en el Boletín Oficial del Estado.

Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se establecen los contenidos mínimos de los planes de seguridad del operador y planes de protección específicos conforme a lo dispuesto en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de infraestructuras críticas. Boletín Oficial del Estado n.º 225, de 19 de septiembre de 2015.

Instrucción número 15/2014, de 19 de noviembre, de la Secretaría de Estado de Seguridad, por la que se crea la Oficina de Coordinación Cibernética del ministerio del Interior. No publicado en el Boletín Oficial del Estado.

Instrucción número 3/2015, de 25 de mayo, de la Secretaría de Estado de Seguridad, por la que se actualiza el Plan de Prevención y Protección Antiterrorista. No publicado en el Boletín Oficial del Estado.

Instrucción número 10/2015, de 10 de septiembre, de la Secretaría de Estado de Seguridad, por la que se regula el proceso de implantación del Sistema de Protección de Infraestructuras Críticas a nivel territorial. No publicado en el Boletín Oficial del Estado.

Instrucción número 2/2016, de 20 de mayo, de la Secretaría de Estado de Seguridad, por la que se regula la coordinación en materia de ciberseguridad en el ámbito del Ministerio del Interior. No publicado en el Boletín Oficial del Estado.

Acuerdo Marco de Colaboración en materia de ciberseguridad entre la Secretaría de Estado de Seguridad del Ministerio del Interior y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo. Actualizado con fecha 21 de octubre de 2015. No publicado en el Boletín Oficial del Estado.

Legislación y Documentación Oficial Comunitaria

Directiva 2008/114, sobre la identificación y designación de infraestructuras críticas europeas y la necesidad de evaluar su protección. Diario Oficial de la Unión Europea, Ley 345/75, de 23 de diciembre de 2008.

Directiva 2013/40, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión 2005/222/JAI del Consejo. Diario Oficial de la Unión Europea, Ley 218/8, de 14 de agosto 2013.

Directiva 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Diario Oficial de la Unión Europea, Ley 194/1, 19 de julio de 2016.

Programa Europeo de Protección de Infraestructuras Críticas (PEPIC). Comunicación de la Comisión de 12 de diciembre de 2006 sobre un Programa Europeo para la Protección de Infraestructuras Críticas [COM (2006) 786 final-Diario Oficial C. 126 de 7 de junio de 2007].

Propuesta de decisión del Consejo de 27 de octubre de 2008, relativa a una red de información sobre alertas en infraestructuras críticas (CIWIN) [COM(2008) 676 final-no publicada en el Diario Oficial].

Libro Verde de 17 de noviembre de 2005 sobre un Programa Europeo para la Protección de Infraestructuras Críticas [COM (2005) 576 final].

Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 20 de octubre de 2004, «Lucha contra el terrorismo: preparación y gestión de las consecuencias» [COM (2004) 701 final-Diario Oficial C 52 de 2.3.2005].

Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 20 de octubre de 2004, «Prevención, preparación y respuesta a los ataques terroristas» [COM (2004) 698 final-Diario Oficial C 14 de 20.1.2005].

Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 30 de marzo de 2009, sobre protección de infraestructuras críticas, «Protegiendo a Europa de ciberataques a gran escala e interrupciones: mejora de la preparación, la seguridad y la respuesta» [COM (2009) 149 final].

CEPS (*Centre for European Policy Studies*) Task Force Report: «Protecting Critical Infrastructure in the EU», marzo de 2010.

Comisión Europea: «Inventory of Crisis Management Capacities in the European Commission and Community Agencies», mayo de 2010.

Comisión Europea: «Manual de Buenas Prácticas para las Políticas PIC (RECIPE)», marzo de 2011.

Publicaciones

ÁLVAREZ, César, *et al.* (2016), «El modelo de protección de infraestructuras críticas en España». Madrid, Editorial Borrmar S.A.

CARABIAS, José Ignacio, «Protección de infraestructuras críticas y planificación», *Revista Seguritecnia*, n.º 409, junio de 2014.

DE LA CORTE, Luis *et al.* (2014), «Seguridad nacional, amenazas y respuestas». Madrid, Editorial LID.

DUDENHOEFFER, D. D. *et al.* (2006), «Critical Infrastructure Interdependency Modelling», trabajo publicado para el Idaho National Laboratory, ref. INL/EXT-06-11464.

MOTEFF, John D. (2012), «Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress». Trabajo publicado por el *Congressional Research Service*, Washington.

PÉREZ-CHIRINOS, César, *Critical Financial Institutions: BusinessContinuity Scenarios and Costs*, en *European CIIP Newsletter*, agosto-septiembre de 2009, Volumen 5, n.º 2.

SÁNCHEZ, Fernando J., «Las políticas de protección de infraestructuras críticas en España», *Seguridad y Ciudadanía*, revista del Ministerio del Interior, n.º 11, junio de 2014.

SÁNCHEZ, Fernando J., «Protección de infraestructuras críticas: el Sistema de planeamiento como herramienta de implantación (I)», *Seguridad y Ciudadanía*, revista del Ministerio del Interior, n.º 12, diciembre de 2014.

SÁNCHEZ, Fernando J., «Protección de infraestructuras críticas: el Sistema de planeamiento como herramienta de implantación (II)», *Seguridad y Ciudadanía*, revista del Ministerio del Interior, n.º13, junio de 2015.

VANACLOCHA, Francisco J. *et al.* (2013), «Marco legal y de gestión de las infraestructuras críticas». Madrid, Editorial McGraw-Hill.

Capítulo sexto

La cooperación público-privada en el fomento de la cultura de ciberseguridad

Gregorio Miguel Pulido Alonso

*Teniente Coronel del Ejército de Tierra DIM
Jefe de la Sección de Preparación del MCCD*

Rafael Rosell Tejada

Director Comercial de S2Grupo

Resumen

En una sociedad avanzada como la nuestra, es capital conseguir una cultura de ciberseguridad global que nos haga más resilientes. La concienciación en esta materia, parte de la cultura de ciberseguridad, es clave en la consecución de este objetivo. Sin embargo, llegar a todos los ciudadanos requiere que los principales actores del sector público y privado en ciberseguridad hagan un esfuerzo en la misma dirección. La consecución de un objetivo como este, unido a la velocidad a la que evolucionan unas amenazas sin precedentes, obliga a todos a alinear sus esfuerzos, puesto que de otra forma no será posible alcanzar un estado de madurez en nuestra cultura de ciberseguridad que garantice un bajo nivel de riesgo.

Para que la cooperación entre ambos sectores sea efectiva esta debe materializarse en forma de «asociación» (*partnership*), con unas normas de constitución y funcionamiento bien establecidas. El instrumento legal, en el caso español, que serviría para articular dicha alianza, podría tomar la forma de convenio. En cualquier caso, será necesario que los asociados principales dediquen, en la forma que se acuerde, suficientes recursos humanos y materiales a este esfuerzo.

Actualmente, nos encontramos en un escenario en el que los diversos actores han puesto diferentes iniciativas en marcha, generalmente orientadas a resolver sus propios problemas y, en muchos casos, divergentes unas de otras.

Palabras clave

concienciación, resiliencia, cultura de ciberseguridad, ciberdefensa, cooperación público privada, incidente, ciberincidentes, programa.

Abstract

In an advanced society like ours, it is capital to achieve a comprehensive cybersecurity culture which enable us to be more resilient. Cybersecurity awareness, as a part of the cybersecurity culture, is a key element to achieve this goal. In order for this awareness to reach all of the citizens, it is necessary that both, public and private sectors, join efforts in the same direction. This partnership will benefit, not only the nation, but also the organizations involved.

To be effective, this cooperation shouldn't rest as a simple declaration of intent. On the contrary, this Public Private Partnership should be created with a clear mandate and well defined rules. The legal framework, in the Spanish case, could be on the basis of a formal agreement signed by the partners. In any case, it will be necessary that the stakeholders involved commit enough resources to this common effort.

Nowadays, we find a scenario where different actors have started several initiatives conducting in general terms to resolve their own issues, but in some cases diverging the ones from the others.

Keywords

Awareness, resilience, cybersecurity culture, cyberdefence, public private partnership, incident, cyberincident, program.

Introducción

El mundo en el que vivimos y en el mundo que vamos a vivir marca la creciente e incesante necesidad de la ciberseguridad. Nos enfrentamos a cambios muy rápidos en la sociedad determinados por una serie de «megatendencias» que lo están transformando todo: la hiperconectividad, la aceleración tecnológica y el incremento de población conectada a la Red, impulsada por el crecimiento continuo de la población que habita el planeta.

Cada una de estas megatendencias tiene la capacidad de cambiar el mundo por sí mismas. Juntas tienen una capacidad transformadora sin precedentes en la historia de la humanidad.

Los cambios exponenciales que se están produciendo en las tecnologías de la información y las comunicaciones son la base de ese gran efecto transformador de la sociedad. Gartner habla de un «nexo de fuerzas»¹, una convergencia de lo social, la movilidad, la nube y el acceso a enormes volúmenes de información y su procesamiento mediante técnicas de *Big Data*, impulsado por la aparición de múltiples tipos de dispositivos con precios cada vez menores, que nos permiten un acceso ubicuo y universal a «todo». En definitiva, un nexo de fuerzas que allanan el camino hacia una sociedad completamente digital.

La aceleración tecnológica descrita por el fundador de Intel y conocida como la Ley de Moore tiene un impacto directo en muchos campos de la ciencia y la tecnología, no solo en el campo de las TIC. Campos como la salud, la energía, la industria, la inteligencia artificial, el transporte, la defensa, etcétera, también están experimentando este proceso de transformación exponencial.

La hiperconectividad también está jugando un papel clave en la transformación digital de la sociedad. La conexión de «todo» en red conlleva la aparición de nuevos productos y servicios inimaginables hace tan solo unos años y el desarrollo, en consecuencia, de un modelo económico completamente nuevo y diferente basado en el concepto de *IoT*, *Internet of Things*, o *IoE*, *Internet of Everything*².

Hablamos en términos generales de la «caída de las fronteras». Desde el punto de vista de la seguridad la identificación del perímetro de protección ha sido siempre, en todos los ámbitos, la primera fase para determinar el despliegue de defensas en una organización. Hoy por hoy, las fronteras han caído por la hiperconectividad. No sabemos dónde está la frontera digital de una organización y, por tanto, no podemos determinar el perímetro de protección. Se habla en términos generales de que «la frontera somos las personas» y esta es la razón por la que el éxito de los programas de concienciación es esencial y se debe basar en un cambio de cultura de ciberseguridad.

¹ <http://www.gartner.com/it-glossary/nexus-of-forces/>

² https://en.wikipedia.org/wiki/Internet_of_things

La Real Academia Española, entre otras acepciones, define cultura como «el conjunto de conocimientos que permite a alguien desarrollar su juicio crítico». Por extensión, se puede definir la cultura en ciberseguridad como el conjunto de conocimientos y habilidades que permiten a un ser humano desenvolverse en el ciberespacio de una manera segura.

El ciberespacio se define, en la Estrategia de Ciberseguridad Nacional³, como el dominio global y dinámico compuesto por las infraestructuras de tecnología de la información —incluida internet—, las redes y los sistemas de información y de telecomunicaciones. En otras palabras, el ciberespacio está compuesto por internet y el resto de redes a las que accedemos con nuestros nuevos dispositivos.

Esta cultura de seguridad global es, en esencia, lo que necesitamos madurar para conseguir un estado de ciberriesgo nacional asumible. Sin embargo, no todo el mundo requiere un mismo nivel de seguridad, dependerá, fundamentalmente, de la relación, personal o profesional, que el individuo tenga con el ciberespacio. Así, por ejemplo, una persona que accede de manera ocasional con su *smartphone* a una red social y un directivo de una organización que maneja información sensible con multitud de dispositivos tienen, sin duda, requisitos de seguridad diferentes. Lógicamente, esta situación conlleva niveles de madurez distintos en sus culturas de seguridad.

En cualquier caso, todos los usuarios del ciberespacio deben tener un mínimo conocimiento, claro y reflexivo, del riesgo real que suponen las amenazas a las que se enfrentan en él, así como la manera de hacerles frente. En otras palabras, los ciudadanos digitales deben estar concienciados en esta materia. Para proteger la sociedad es, por tanto, necesario que todo ciudadano o empleado de una organización pública o privada tome conciencia de los riesgos a los que se enfrenta la sociedad en su conjunto.

La Escuela de Altos Estudios de la Defensa, en septiembre de 2013, publicó un completo monográfico que abordaba en profundidad la necesidad de crear una conciencia nacional de ciberseguridad⁴. El objeto del presente artículo es presentar datos, teorías e iniciativas existentes en esta materia, para concluir en cómo la cooperación entre el sector público y privado se constituye, dada la magnitud del problema, en la mejor forma de abordar la concienciación en ciberseguridad a nivel nacional y de situar la cultura global de ciberseguridad en un nivel que minimice el riesgo en esta materia.

El eslabón más débil de la cadena

En este entorno —hiperconectado, hipertecnológico, universal y con acceso ubicuo a todo— se están diseñando los nuevos modelos económicos de la

³ <http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional>

⁴ Escuela de Altos Estudios de la Defensa, Monografías 137. «Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario». 2013.

sociedad digital y nadie se quiere quedar atrás. La Unión Europea, en su documento «Estrategia de Ciberseguridad»⁵, afirma que el uso de la tecnología está directamente relacionado con el incremento de la productividad y el incremento del PIB de los países hasta el punto que el Mercado Único Digital supone un incremento de 500.000 millones de euros anuales de su producto interior bruto (en torno a un 5 % del PIB de la zona euro).

Los Gobiernos están impulsando, a través de sus Agendas Digitales, la adopción de las TIC a todos los niveles a través de sus políticas de «tracción» porque son evidentes los efectos positivos que estos avances producen en la sociedad a todos los niveles. No obstante, este desarrollo tecnológico sin precedentes no está exento de riesgos. Uno de ellos es la necesidad de conseguir que esta nueva sociedad digital sea un espacio seguro y de confianza para todos. No en vano, todas las agendas digitales que se están desarrollando tienen en común su apuesta por la seguridad y el desarrollo de la confianza en la Red.

La Agenda Digital Europea es una de las siete iniciativas emblemáticas en la Estrategia Europa 2020 y se diseña en torno a siete campos de actuación principales y dieciséis acciones clave. El tercer campo de acción es «Fomento de la confianza y seguridad en Internet» con la línea de acción AC6, «Conseguir una política de seguridad reforzada y de alto nivel», y la AC7, «Medidas incluyendo legislativas para combatir los ciberataques».

En nuestro caso, la Agenda Digital Española, alineada con la europea, pretende impulsar con acciones concretas la sociedad digital en toda su amplitud. Para conseguirlo se estructura en torno a seis grandes objetivos con sus respectivas líneas de acción. El cuarto es «Reforzar la confianza en el ámbito digital», donde se apuesta claramente, entre otras iniciativas, por la concienciación y sensibilización de la sociedad en esta materia con un enfoque claro hacia las personas. En el ámbito de actuación de la agenda se desarrolla el «Plan de confianza en el ámbito digital» con cinco ejes estratégicos:

- Experiencia digital segura.
- Oportunidad para la industria TIC.
- Nuevo contexto regulatorio.
- Capacidades para la resiliencia.
- Programa de excelencia en ciberseguridad.

Este interés unánime en la seguridad y la confianza en la Red responde al enorme crecimiento que están teniendo cualitativa y cuantitativamente los incidentes de seguridad. El número de amenazas se multiplica y cada vez son más complejas y esto está creando una sensación de inseguridad que puede frenar el desarrollo tecnológico si no se toman cartas en el asunto. En

⁵ http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

su informe «Global Risk»⁶ del año 2014, el World Economic Forum llegaba a plantear un escenario plausible al que llamaba «Cybergedon».

El «Special Eurobarometer 423» sobre ciberseguridad, publicado en 2015, pone cifras a este problema de inseguridad y desconfianza en el mundo digital y, en su introducción, lo cuantifica en miles de millones de euros de pérdidas anuales en Europa, con más de 150.000 tipos de virus en libre circulación y más de un millón de víctimas diarias del cibercrimen. En cuanto a los datos en España, el eurobarómetro refleja el 62 % de los ciudadanos que no se sienten bien informados sobre los ciberdelitos (frente a un 50 % en Europa). Asimismo, el 89 % de los ciudadanos cree que el riesgo de ser víctima de un ciberdelito está aumentando y al 87 % (un 85 % en Europa) le preocupa que las autoridades públicas no mantengan segura su información personal en internet (frente a un 67 % en Europa).

Por lo que la situación en España es, si cabe, incluso peor que en Europa en términos generales de desconfianza.

En 2015, la compañía de seguros británica Lloyd's estimó que el coste anual de los ciberataques rondaba los 400 billones de dólares al año, incluyendo los daños directos producidos más los daños derivados de las tareas de recuperación. El presidente de la compañía, Stephen Catlin, con más de cuarenta y dos años de experiencia, llegó a decir en Londres en febrero de 2015: «los balances de las aseguradoras no son lo suficientemente grandes para cubrir los riesgos de ciberseguridad. Es, sin duda, el mayor y el más sistémico de los riesgos que he afrontado en toda mi carrera»⁷.

Para IBM, en 2014, el 95 % de los ciberincidentes fueron causados por errores humanos, entre ellos introducir información sensible o incluso clasificada en sistemas conectados a internet⁸. Solamente el 45 % de los ataques fueron realizados por *outsiders* (personal ajeno a la empresa). Según Kaspersky⁹, la cifra es aproximadamente del 80 %. Coincidiendo en el dato, el Gobierno de los Estados Unidos especifica que sobre el 80 % de los ciberincidentes suceden por tres factores: pobres prácticas de los usuarios, pobres prácticas en la gestión de las redes y los datos, y pobre implementación de la arquitectura de red¹⁰.

En 2013 el principal objetivo de los ciberdelincuentes eran los sistemas de las empresas. En 2014 pasaron a ser las personas¹¹. En esa misma línea, Deloitte afirma que, aunque los ciberdelincuentes reinvierten una parte de

⁶ <http://reports.weforum.org/global-risks-2014/>

⁷ http://internacional.elpais.com/internacional/2015/02/06/actualidad/1423257712_728999.html

⁸ IBM 2015, Cyber Security Intelligence Index, *Analysis of cyber attack and incident data from IBM's worldwide security services operations*.

⁹ Kaspersky, Cybersecurity Awareness Brochure.

¹⁰ The DoD Cybersecurity Culture and Compliance Initiative.

¹¹ Check Point, 2015 Security Report.

sus beneficios en desarrollar nuevas capacidades técnicas para sobrepasar las barreras de seguridad, el procedimiento que más emplean para acceder al usuario final es la ingeniería social a través de internet¹². Una muestra, según Symantec¹³, es que las campañas de *spear-phishing* se incrementaron en un 55 % en 2015 y las técnicas de ingeniería social llegaron a un nivel de sofisticación elevado, dirigido incluso a sobrepasar los sistemas con doble factor de autenticación. También se han observado ataques realizados con *malware* con la finalidad de robar datos personales para su uso posterior.

El perfil profesional de las personas elegidas como objetivo es muy amplio. Por ejemplo, durante la campaña de ataque conocida como «Witchcoven» los adversarios recogieron una ingente cantidad de datos de ejecutivos, diplomáticos, funcionarios gubernamentales y personal militar, especialmente en Europa y Estados Unidos¹⁴. Sin embargo, en los últimos años se ha observado un crecimiento regular en ciberataques a empresas de menos de doscientos cincuenta empleados, llegando incluso a suponer un 43 % de todos los ataques.

Finalmente, y como muestra de la forma de trabajo de los ciberdelincuentes, Checkpoint insistía en que en 2014, habían observado en los sistemas investigados por ellos, un nivel de ciento seis descargas por hora de ficheros infectados con *malware* desconocido. El 52 % de este *malware* venía dentro de un .pdf mientras que el 3 % eran ficheros correspondientes al paquete Office. En el ciberataque contra el sector energético ucraniano conocido como «Black Energy» el medio empleado para insertar el *malware* fue un fichero de extensión doc¹⁵.

Ante esta situación, que se agrava día a día, es necesario fomentar una cultura de ciberseguridad global adecuada a través de estrategias de concienciación, tal y como se recoge en la «Estrategia de Ciberseguridad para la Unión Europea» que afirma de manera clara que «los usuarios finales contribuyen de forma decisiva a garantizar la seguridad de las redes y los sistemas de información: es preciso que sean conscientes de los riesgos que corren en línea y sean capaces de adoptar medidas sencillas para protegerse de ellos».

Ciberresiliencia y concienciación en ciberseguridad

No existe a nivel nacional o multinacional una definición acordada sobre el término ciberresiliencia. Sin embargo, basándonos en los trabajos de MITRE¹⁶

¹² Deloitte, Cyber crime: a clear and present danger. Combating the fastest growing cyber security threat.

¹³ Symantec, Internet Security Threat Report, volume 21, April 2016.

¹⁴ Special Report FIREEYE Threat Intelligence pinpointing targets: Exploiting Web Analytics to Ensnare Victims, Jonathan Wrolstad Barry Vengerik.

¹⁵ Kaspersky, IT Threat evolution in Q1 2016, Alexander Gostev, Roman Unuchek, Maria Garnaeva, Denis Makrushin, Anton Ivanov.

¹⁶ MITRE Corporation, Cyber Resilience Metrics: Key Observations, Deborah Bodeau, Richard Graubart.

la podemos definir como «la capacidad de anticiparse, resistir, recuperarse y adaptarse a condiciones hostiles consecuencia de condiciones ambientales adversas, estrés de los sistemas por distintas causas o ciberataques».

Symantec ha desarrollado un modelo para mejorar la ciberresiliencia en una empresa basado en cinco pilares¹⁷. El primero de ellos es la «preparación/ identificación», que se basa en gran medida en el conocimiento de los riesgos a los que se enfrenta la empresa y en el que una de las acciones clave es la concienciación de los usuarios. Los otros pilares de este modelo son la protección, detección, respuesta y recuperación.

El modelo de gestión de resiliencia de un equipo de respuesta ante emergencias informáticas (CERT *Resilience Management Model* (CERT-RMM))¹⁸, desarrollado bajo los auspicios del Departamento de Defensa de Estados Unidos por el Instituto de Ingeniería del Software (SEI) de la Universidad Carnegie Mellon, contempla como una de las áreas que componen dicho modelo la formación y concienciación de la organización [*Organizational Training and Awareness* (OTA)].

Así pues, basados en estos dos modelos dirigidos al ámbito empresarial fundamentalmente, vemos cómo la mejora de los niveles de ciberresiliencia de una organización pasa, indefectiblemente, por impulsar la cultura de ciberseguridad y la concienciación. Este hecho es extrapolable al ámbito nacional como veremos posteriormente, aunque no vamos a profundizar más en la ciberresiliencia, ya que se trata más profundamente por el Instituto de Estudios Estratégicos en un gran artículo de opinión firmado por el profesor Salvador Carrasco¹⁹:

Iniciativas existentes

Vista pues la necesidad de una concienciación en ciberseguridad, de manera sucinta vamos a repasar distintas iniciativas para extraer claves que nos sirvan para acometer esta tarea.

En España

A nivel nacional y dentro del sector público, el objetivo IV de la Estrategia de Ciberseguridad Nacional (ECSN) es «sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio». Asimismo, especifica claramente que «la gestión

¹⁷ SYMANTEC, *The Cyber Resilience Blueprint: A New Perspective on Security*.

¹⁸ CERT® *Resilience Management Model*, Version 1.2, Richard A. Caralli, Julia H. Allen, David W. White.

Lisa R. Young, Nader Mehravari, Pamela D. Curtis, February 2016, CERT Program.

¹⁹ «Ciber-resiliencia», Luis de Salvador Carrasco, IEEEs Cuaderno de opinión.

eficaz de los riesgos derivados del ciberespacio debe edificarse sobre una sólida cultura de ciberseguridad. Ello requiere de los usuarios una sensibilización respecto de los riesgos que entraña operar en este medio, así como el conocimiento de las herramientas para la protección de su información, sistemas y servicios».

Derivado directamente de la ECSN, se ha aprobado el Plan de cultura de ciberseguridad, concienciación, sensibilización y educación, cuyo objetivo es «promover la cultura de ciberseguridad entre ciudadanos, profesionales, empresas y Administraciones Públicas españolas mediante el desarrollo de actividades y mecanismos para la sensibilización, concienciación, formación y educación que renueven y doten de nuevos conocimientos sobre los riesgos derivados del ciberespacio y el uso seguro y responsable de las TIC».

El Plan se articula en tres ejes de acción: sensibilización, concienciación y conocimiento; normativa y buenas prácticas. Cada eje tiene asignado un organismo de la Administración pública como responsable y otros como colaboradores. Asimismo, se contemplan unos recursos financieros y humanos para poderlo llevar a cabo.

En cuanto a las acciones concretas que se derivan de dicho Plan, algunas de ellas son: desarrollar actividades de sensibilización para asegurar que los ciudadanos, empresas, profesionales, red académica, operadores estratégicos y operadores de infraestructuras críticas tienen acceso a información relativa a vulnerabilidades, ciberamenazas e información para proteger mejor su entorno tecnológico; proponer contenido específico de sensibilización en ciberseguridad para incluirlos en los módulos educativos dirigidos a todos los niveles de la enseñanza en cumplimiento a lo establecido en el convenio de Lanzarote²⁰; proponer contenido específico de sensibilización en ciberseguridad para incluirlos en los programas de administración de las Administraciones Públicas; desarrollar programas de concienciación en ciberseguridad, en colaboración con agentes del sector público y privado potenciando, a través de los organismos con competencias en la materia, la necesaria coordinación y racionalización de esfuerzos; desarrollo de un catálogo de buenas prácticas; detección de necesidades y difusión de herramientas y servicios de ciberseguridad.

En línea con todo lo anterior, los principales actores públicos y privados en el ámbito de la ciberseguridad han ido desarrollando diferentes modelos e iniciativas basadas en el establecimiento de marcos de buenas prácticas.

El Centro Criptológico Nacional CCN-CERT ha sido uno de los pioneros y uno de los más activos y eficientes en definir una fuerte estrategia de generación de información de valor que sirva fundamentalmente a las Administraciones

²⁰ [http://www.fapmi.es/imagenes/subsecciones1/1de5_Doc_03_Convenio %20Lanzarote_Parlamentarios.pdf](http://www.fapmi.es/imagenes/subsecciones1/1de5_Doc_03_Convenio_%20Lanzarote_Parlamentarios.pdf)

Públicas —que es su ámbito de actuación— pero también a empresas para protegerse frente a los ciberriesgos.

Dicho centro ha desarrollado una fuerte actividad de generación de Guías²¹ que cubren la inmensa mayoría de aspectos relevantes, desde políticas o procedimientos hasta guías técnicas de configuración de entornos. Se trata de guías de enorme valor que sirven de marco de referencia a los equipos técnicos para desarrollar el trabajo de protección de sus perímetros.

Por otro lado, ha realizado una intensa labor en el desarrollo de informes del estado²² de las amenazas y las previsiones que, desde el CCN-CERT, tienen del desarrollo futuro de las mismas. Así mismo, dicho centro ha organizado diversos cursos de formación.

Por otro lado, también participa en el Mes Europeo de la Ciberseguridad²³, organizado por *ENISA* (Agencia Europea de las Redes y de la Información), cuyo principal objetivo es «concienciar a los ciudadanos de la necesidad de preservar la información y abogar por un cambio en la percepción de las ciberamenazas mediante la promoción de la seguridad de los datos y la información, la educación, el intercambio de buenas prácticas y la competencia».

Otra institución muy activa es el Instituto de Ciberseguridad Nacional (INCIBE) que, por su parte, ha desarrollado diferentes iniciativas orientadas tanto a empresas como ciudadanos. En el ámbito específico del programa de sensibilización, concienciación, educación y formación definido por el Plan de Confianza Digital y la Estrategia de Ciberseguridad Nacional 2013, desde el año 2015 INCIBE lleva a cabo el proyecto Servicio de Creación, mejora y soporte de contenidos de ciberseguridad y confianza digital de INCIBE dirigidos a las empresas y ciudadanos. La Oficina de Seguridad del Internauta (OSI)²⁴ es una de sus principales iniciativas en este ámbito. Es una oficina que ofrece materiales, herramientas y buenas prácticas. Cabe destacar, por ejemplo, por su interés, el «kit de concienciación»²⁵ que INCIBE ha desarrollado y ha puesto a disposición de las empresas. Dicho kit propone una serie de prácticas y materiales a distribuir. La primera fase, por ejemplo, consistiría en lanzar un ciberataque dirigido, dentro de la empresa, con un fichero infectado con *malware* inocuo y cuyo vector de infección sería el correo electrónico o una memoria USB. INCIBE incluso propone los mensajes y ficheros a utilizar. Una vez realizada esta primera fase, ya se pasaría una fase formativa en la que se distribuyen materiales como pósteres o trípticos, que también han sido preparados por INCIBE. Se daría continuidad posteriormente a esta tarea mediante consejos de ciberseguridad de periodicidad mensual.

²¹ <https://www.ccn-cert.cni.es/pdf/guias/1297-indice-series-ccn-stic/file.html>

²² <https://www.ccn-cert.cni.es/informes.html>

²³ <https://www.enisa.europa.eu/news/enisa-news/ecsm>

²⁴ <https://www.osi.es>

²⁵ INCIBE, Kit de concienciación, manual de implantación.

Por otro lado, los CERT de ámbito autonómico (CSIRT-CV, CESICAT, ANDALUCIA-CERT), en el ámbito de sus funciones, también han desarrollado programas de concienciación basados en portales donde se puede encontrar información relativa a riesgos y buenas prácticas. Merece la pena destacar la gran labor desarrollada por el CSIRT-CV en este ámbito. Es un centro muy activo que cuenta con numerosos cursos²⁶ e informes²⁷ que han tenido muy buena aceptación en la Comunidad Valenciana.

En general, las distintas experiencias que se han ido implementando en el panorama nacional se orientan hacia:

- Plan de seguridad, gestión de la seguridad en los procesos de la empresa.
- Cultura de seguridad o todo lo relativo a la sensibilización de ciudadanos y empleados, y de cómo prepararlos.
- Protección de la información, copias de seguridad, protección contra la fuga de información, cifrado, borrado seguro, destrucción de soportes, etcétera.
- Puesto de trabajo, para garantizar la seguridad desde cada puesto.
- Movilidad y conexiones inalámbricas o cómo proteger las comunicaciones en un entorno móvil e inalámbrico.
- Contingencia y continuidad de negocio, para estar preparado para recuperar la actividad del negocio en caso de un incidente.
- Cumplimiento legal, fundamentalmente desde el aspecto de protección de datos personales (LOPD) y de la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI).
- Buenas prácticas de los departamentos de informática. Engloba la seguridad en sistemas y redes, la protección ante intrusiones, las auditorías internas y consideraciones de seguridad en desarrollo del *software* y mantenimiento de sistemas.
- Fraude y gestión de identidad, cómo detectarlo y evitarlo, concienciación sobre técnicas de ingeniería social, timos más frecuentes, etcétera.
- Contratación de servicios, es decir, los aspectos que el empresario ha de considerar cuando contrata servicios en internet o externaliza parte de su actividad.

Otras iniciativas diferentes han sido las que, durante años, han desarrollado la Policía Nacional y la Guardia Civil, tratando de concienciar a los niños en los colegios sobre los peligros que encierra la red.

Por su parte, el Mando Conjunto de Ciberdefensa tiene como misión, entre otros, el definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de ciberdefensa del propio Ministerio de Defensa. En base a ese cometido ha coordinado y puesto en marcha, como veremos posteriormente, el Plan de Concienciación en Ciberdefensa

²⁶ <https://www.csirtcv.gva.es/es/paginas/formación.html>

²⁷ <https://www.csirtcv.gva.es/es/paginas/descargas-informes-csirt-cv.html>

(CONCIBE) y ha explorado interesantes programas dirigidos a su ámbito de actuación y basados en cursos de sensibilización en la plataforma e-learning del MINISDEF, que incluso incorporan técnicas de *gamificación* orientadas a mejorar los resultados prácticos.

Según Hairol Romero Sandí y Elvin Rojas Ramírez, en su trabajo sobre «La gamificación como participante en el desarrollo del B-learning»²⁸ definen la *gamificación* como una técnica de aprendizaje basado en las mecánicas y dinámicas de juego para alentar o motivarlo, colaborando en la construcción de nuevas experiencias convirtiendo algunas actividades consideradas aburridas en innovadoras e interesantes para los participantes.

En el ámbito privado hay muchas iniciativas lideradas por las diferentes compañías especializadas en ciberseguridad para implementar planes de concienciación en sus clientes. En general, se han ido diseñando planes de concienciación basados tanto en culturas de procesos con la transmisión de políticas y buenas prácticas a los empleados, como en culturas de *compliance* para el cumplimiento de normativas o legislaciones. Así, se han puesto en práctica numerosas iniciativas basadas en el bombardeo continuo de mensajes relacionados con las políticas o buenas prácticas o con las normativas a cumplir, con un impacto generalmente bajo.

No se ha tenido en cuenta, por lo general, que la cultura de seguridad de una compañía y, por tanto, cómo se comporta la misma en términos de seguridad, está fuertemente ligada a las creencias, valores y asunciones de los empleados o personas que la conforman.

Un cambio cultural para adaptar la cultura de seguridad de una organización a las realidades actuales de la ciberseguridad supone una labor increíblemente dura a menos que se empiece desde cero. Normalmente las organizaciones tienen ya establecida su cultura de seguridad e incluso los individuos aportan ya una cultura de ciberseguridad preestablecida.

Hasta principios de 2013, los equipos de IT trataban de imponer estrategias de seguridad ortodoxas. La creación de estrictas reglas y controles que se esperaba que fueran seguidas por todos los empleados. Por ello, se hacía necesario un fuerte apoyo de la dirección y la comunicación era vital para vencer las objeciones de algunos y para mantener la fuerza de la estrategia.

El mundo de la seguridad (de la información) lleva muchos años trabajando en la gestión de riesgos como eje central de estudio para la protección de la información y las infraestructuras de las organizaciones. Sin embargo, en lo que a la implicación del empleado se refiere, el enfoque suele ser «no toques nada». Con el objetivo de proteger aquello que gestiona, se ha metido durante años al empleado en una burbuja de sobreprotección, lo que se traduce en limitar al máximo sus permisos y su capacidad de acción.

²⁸ <http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP118.pdf>

Pero es de sobra conocido que la mejora de la seguridad de las organizaciones, tanto cuando hablamos de la información como de los propios medios físicos, no depende «solo» de la implantación de medidas técnicas de seguridad o la definición de procedimientos; es fundamental la implicación de las personas. No se repite suficiente que el factor humano es un pilar fundamental en la seguridad y, por tanto, es necesario desarrollar técnicas efectivas y eficientes para desarrollar al máximo este potencial. Las últimas experiencias más exitosas van en esta línea.

Así, según el NIST (113)²⁹, existen diferentes niveles de aprendizaje a la hora de aplicarlos a los diferentes miembros de la empresa según los roles y responsabilidades en ciberseguridad que desempeñan dentro de ella, que son:

Concienciación: es un proceso de aprendizaje destinado a todos los miembros de la empresa y se enfoca en cambiar las actitudes individuales y colectivas para comprender la importancia de la seguridad y las consecuencias adversas de su fracaso.

Su objetivo es que los empleados reconozcan y retengan la información que se les proporciona.

Ejemplos de canales para proporcionar este aprendizaje son los folletos, pósteres, videos, comunicados por *email*, *banners*, etcétera. Se busca alcanzar un impacto en un corto espacio de tiempo.

Formación: es un proceso que se centra en trasladar a los empleados de la empresa los conocimientos y habilidades que les permitan realizar su trabajo con mayor eficacia. Se centra en dar a conocer y hacer que se dominen las habilidades necesarias para desempeñar adecuadamente un rol determinado. Ejemplos de canales para proporcionar este aprendizaje son los cursos, las prácticas, las demostraciones, los talleres, etcétera. Se busca alcanzar un impacto temporal a medio plazo.

Educación: es el proceso de formación en ciberseguridad más avanzado y se centra en el desarrollo de la capacidad y la visión para llevar a cabo actividades complejas y multidisciplinarias, así como las habilidades necesarias para promover el desarrollo profesional en ciberseguridad. Se centra en hacer que se desarrolle un entendimiento profundo y la capacidad de gestionar el conocimiento en la materia. Las actividades para proporcionar este tipo de aprendizaje incluyen la investigación y desarrollo, los seminarios y grupos de trabajo, los cursos monográficos avanzados, etcétera. Se busca alcanzar un impacto temporal a largo plazo.

Según ENISA³⁰, los programas de concienciación se deben desarrollar en tres fases: planificar, estimar y diseñar. Los programas de formación y concienciación deben ser diseñados teniendo siempre en cuenta la misión,

²⁹ <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf>

³⁰ <http://www.enisa.es/>

visión y objetivos de cada empresa. Es muy importante que apoyen las necesidades de negocio y que influyan en la cultura de la empresa y, también, en las arquitecturas que soportan sus servicios TI. Los programas más exitosos son aquellos en los que los usuarios consideran que son relevantes para los problemas que se tratan de resolver. En esta etapa se identifican las necesidades de formación y concienciación, se diseña un plan eficaz que cubra dichas necesidades, se busca y se asegura la disponibilidad de los servicios de formación necesarios y se establecen las prioridades para llevarlas a cabo.

Desarrollar y gestionar: en esta fase se incluye cualquier actividad necesaria para implementar el programa de formación y concienciación sobre ciberseguridad. Las acciones del programa, que ejecuta la estrategia establecida para cubrir las necesidades de formación identificadas, solo se podrán gestionar y llevar a cabo una vez haya sido desarrollado el correspondiente material formativo.

Evaluar y ajustar: los mecanismos de evaluación y de retroalimentación son componentes críticos para cualquier programa de concienciación sobre la ciberseguridad. La mejora continua solo se puede alcanzar si podemos conocer cómo está funcionando el programa actual. Es particularmente importante, a nuestro modo de ver, desarrollar sistemas de medición que sean lo más realistas posible, es decir, que nos permitan medir claramente el riesgo que introduce el factor humano. Una vez que se han alcanzado los requisitos iniciales básicos de concienciación, se puede diseñar y empezar a aplicar una estrategia de mejora continua.

Todos los referenciales se hacen eco de la necesidad de considerar el factor humano como un componente esencial de la seguridad.

No obstante, además de todo esto, lo que está claro es que el comportamiento de la organización ante las ciberamenazas depende esencialmente de la cultura de seguridad de la organización. Si queremos cambiar el comportamiento ante ellas, esencialmente, estamos ante un problema de cambio cultural.

De forma general, las culturas de ciberseguridad que nos podemos encontrar en las organizaciones se pueden agrupar bajo cuatro paradigmas diferentes, que, en diferentes momentos, cuentan con aspectos que son beneficiosos para nuestra cultura de seguridad:

- Cultura de Procesos, donde todo es formal y burocrático, el valor central es el control y se crean numerosas políticas y procedimientos formales.
- Cultura de *Compliance*, donde las preocupaciones frente a la legislación vigente establecen las prioridades.
- Cultura de Confianza, en el que trasladamos al empleado los conocimientos y las herramientas adecuadas para gestionar los riesgos a los que, inexorablemente, se tiene que enfrentar.

- Cultura de Autonomía, en el que se fomenta la capacidad de reacción. Es esencial cuando se está materializando un ataque.

A pesar del mencionado plan nacional y de los muchos proyectos de los diferentes organismos, todavía no se ve una acción concertada a nivel global en marcha, probablemente debido a la falta de recursos derivados del momento económico que hemos vivido todos estos años.

Dentro del sector privado

Después de algunos años tratando de implementar estrategias de concienciación corporativas, podríamos decir que nos hemos olvidado de que lo que tenemos que formar y concienciar es a las personas, y por tanto los programas deben ir enfocados a concienciar a las personas para que desarrollen todas sus actividades, tanto en su vida privada como en la profesional, con un nivel adecuado de seguridad. Es decir, se debe fomentar en las personas una cultura de gestión del riesgo adecuada y proporcionarles las herramientas necesarias para realizar estas tareas.

Esta falta de conocimientos y cultura de seguridad no pasa desapercibida para los ciberdelincuentes que aprovechan descuidos, prácticas inseguras de comportamiento y, en general, la falta de formación en materia de seguridad por parte de los empleados para poner en riesgo la seguridad de cualquier organización.

Aunque, en teoría, un modelo basado en impedir al usuario realizar operaciones suena francamente bien, la realidad es que el empleado, nos guste o no, tiene que tocar cosas. Dicho de otra forma, la práctica nos ha demostrado que las paredes de la burbuja en la que intentamos meter al empleado son muy delgadas y este se enfrenta de manera continua a situaciones de riesgo sin tener la información, los conocimientos y las herramientas necesarias para protegerse.

Ante esta situación, no se puede seguir reforzando el papel de la tecnología y los procesos, manteniendo al mínimo imprescindible el de las personas ya que los sistemas de protección y los procedimientos no son infalibles. Hay que apostar, necesariamente, por fortalecer también las capacidades defensivas de las personas en busca de una posición de equilibrio y solidez sobre la que implantar una gestión eficaz de la seguridad.

Para conseguir este objetivo es necesario abordar el problema desde su origen, convirtiendo al empleado en parte de la defensa: *human firewall*³¹. De esta forma, el empleado juega un papel activo y relevante en la gestión de la información que maneja, lo que da lugar a una estrategia de seguridad mucho más robusta.

³¹ Término acuñado por S2 Grupo en sus sesiones de concienciación.

El primer paso es capacitar al empleado por medio de acciones continuadas de concienciación, formación y prueba en entornos de simulación.

Mediante la concienciación se involucra e implica al empleado en la protección de las tecnologías e información que gestiona, a través del conocimiento y aplicación de las normativas, procedimientos y buenas prácticas en seguridad. Para conseguirlo hay que mostrar al empleado las amenazas a las que se enfrenta y su posible impacto, haciéndole entender por qué debe realizar una gestión adecuada de la seguridad.

A través de la formación se traslada a la persona el conocimiento necesario para llevar a la práctica una gestión adecuada de la seguridad. Se le forma en cómo hacerlo, dotándole de los conocimientos y herramientas necesarias.

Por último, con el objetivo de mantener actualizados los conocimientos adquiridos dentro de un ciclo de mejora continua, se pone al empleado a prueba mediante ciberejercicios en entornos de simulación.

Una vez capacitado es cuando se puede dotar al empleado de la responsabilidad en la gestión de la seguridad de la información y los medios digitales que maneja, teniendo en cuenta las particularidades de los distintos colectivos que componen una organización, convirtiéndoles en parte activa de la estrategia de defensa.

La creación de una cultura de confianza digital que permita reforzar la protección de los organismos y estimule la implicación de los ciudadanos en el entorno digital, resulta vital para impulsar el pleno desarrollo de la sociedad conectada; para lo cual, el sector de la ciberseguridad se configura como un elemento habilitador clave.

Es esencial, por tanto, promover esta cultura de seguridad en las organizaciones que enfatice todos los aspectos que son esenciales en la gestión de la misma.

La seguridad centrada en las personas es una aproximación estratégica que enfatiza la responsabilidad y la confianza y desenfatisa el control restrictivo y preventivo de la seguridad.

Hay diferentes estadios o niveles en los que hay que avanzar hasta llegar a una cultura de ciberseguridad totalmente centrada en las personas para que el riesgo sea bajo.

Un primer nivel de madurez que podríamos llamar instintivo. En este nivel el riesgo es alto, los comportamientos se memorizan y transmiten informalmente entre empleados y no están documentadas las políticas. Las emociones individuales son los principales criterios de decisión, son intuitivas.

A continuación vendría un nivel más consciente de la necesidad de avanzar en mejorar la cultura de ciberseguridad. Es un nivel de conciencia. En él existe la necesidad de analizar, identificar y cambiar aquellos comportamientos

tos que pueden comportar un riesgo para la organización. Se establecen los primeros intentos para formalizar y estimular comportamientos deseados. Se determinan las políticas y se empiezan a llevar a cabo entrenamientos/formaciones.

Mucho más avanzado, y por ello el factor humano comporta en esta situación un riesgo bastante menor, está el nivel de visibilidad. En este estado los comportamientos y las características culturales se miden y analizan. Se correlacionan los procesos de decisión con los patrones culturales y de comportamiento. Los riesgos culturales que impactan en los objetivos fundamentales son identificados y documentados. Existen ya estrategias formales para bajar el riesgo cultural.

Avanzando en el estado de madurez de la cultura de ciberseguridad subiríamos a un nivel en el que toda la organización está orientada e involucrada en la transformación cultural, es el nivel de conversión. Todos están totalmente orientados, en su conjunto, hacia el esfuerzo global que supone el cambio de los comportamientos y hábitos. La cultura y el comportamiento se miden de forma continua para detectar defectos en los esfuerzos en marcha. Todos los empleados son evaluados y rinden cuentas de las actuaciones culturales.

Por último, un grado de madurez muy alto se corresponde con una conciencia global de la compañía de los diversos ciberriesgos y, por tanto, un grado de riesgo mucho más bajo. La cultura de la organización está formalmente gestionada como un proceso y la medición de todo lo relativo a ella está completamente automatizada. Es el nivel de dominio.

Fuera del entorno laboral

Las estrategias de concienciación pasan, en la práctica, por entender que las personas somos en esencia eso, personas. Todos los planes de concienciación, en general, están orientados a los empleados o a los ciudadanos. No nos damos cuenta que, en realidad, son los mismos. Cualquier persona, en esencia, establece unos parámetros de comportamiento que afectan tanto a su vida personal como a la profesional. En este sentido, es imprescindible hacer que las personas entiendan el problema y adopten unos estándares de comportamiento que mejoren su nivel general de ciberseguridad y, con ello, el de las organizaciones en las que trabajan.

Por otro lado, es necesario que las políticas de seguridad de las organizaciones contemplen que, en realidad, los perímetros de protección hoy en día son completamente difusos y se maneja en muchos casos información corporativa y sensible en equipos que están fuera de ese perímetro, en muchos casos en casa.

La tecnología de los hogares conectados en la actualidad es cada vez más compleja. Las previsiones con el despliegue masivo de *IOT* es que se multi-

pliquen los dispositivos útiles gestionados por cada unidad familiar, llegando incluso según previsiones recientes a tener que manejar cientos de direcciones IP en una red de un hogar avanzado. Las previsiones hablan de 500 IP.

Actualmente, de manera intuitiva y a nivel casero, uno de los miembros de la unidad familiar ejerce labores que ejercería un jefe de la información y un jefe de la seguridad (CIO y CISO), desplegando la tecnología que el hogar necesita y «vigilando» de la forma que puede y sabe la seguridad de su entorno tecnológico. Ese CIO y CISO en funciones no tiene especial formación tecnológica y, si bien puede ser un usuario de la tecnología, actualmente no tiene suficiente formación o conocimiento para ejercer de responsable de seguridad de su hogar. Muchas veces no sabe realmente a lo que se enfrenta.

Si estas personas, con sus unidades familiares, son ejecutivos de compañías que directa o indirectamente trabajan en entornos sensibles el escenario de riesgo se complica.

Por lo tanto, algunas acciones públicas deben ir encaminadas a fomentar el conocimiento y las herramientas que el CISO de la casa puede utilizar para proteger su entorno. Tener un hogar protegido, sin duda, redundará en fortalecer la seguridad del sistema en su conjunto, puesto que es uno de los eslabones más débiles de toda la cadena de seguridad.

A nivel multinacional

La Autoridad Australiana de Telecomunicaciones y Medios de Información³² publicó un trabajo sobre las diversas campañas de concienciación hechas en diversos países. De este estudio se dedujeron algunos aspectos que dichas campañas tenían en común, entre los cuales destacamos: las herramientas dominantes en la mayoría de las campañas eran páginas web y publicaciones; los juegos y test eran bastante escasos; la mayoría de las campañas no incluían un servicio de asesoramiento; el patrocinador de las campañas era normalmente el Gobierno, aunque en algunos casos se incluía al sector privado; los temas cubiertos eran muy diversos y no se cubrían todos los aspectos que hubieran sido necesarios; las audiencias objetivo en muchas campañas estaban muy diversificadas; la evaluación sobre el éxito de las campañas era bastante; la difusión de folletos, *websites* y otros medios pasivos tienen un impacto limitado si no vienen seguidas de prácticas, y los mensajes difundidos vía televisión han demostrado ser muy efectivos.

Dentro del marco de la OTAN, esta ha desarrollado un Programa de Implementación de Concienciación en Ciberdefensa. Dicho programa está basado en tres principios: la coherencia de los mensajes, la coordinación entre sus

³² An overview of international cyber-security awareness raising and educational initiatives. Research report commissioned by the Australian Communications and Media Authority, May 2011.

agencias y la sostenibilidad del mismo. Incluye una serie de actividades, incluyendo el *branding* (creación de una imagen corporativa, en este caso para ciberseguridad), objetivos, medidas de los efectos y normas de gobernanza del programa. Dentro de estas actividades el Centro de Excelencia en Ciberdefensa (CCD COE) de Tallin (Estonia) ha lanzado un curso *online* orientado a los usuarios de las redes OTAN y cuya finalidad es ayudarles a familiarizarse con la terminología, los tipos de ciberataque y las técnicas defensivas.

Dentro de la Unión Europea ya hemos visto cómo la propia estrategia contempla la concienciación como un factor necesario a contribuir a la resiliencia. ENISA ha desarrollado varios estudios y materiales en este sentido y los ha puesto a disposición de las naciones miembro. Una de estas actividades es el Mes de la Ciberseguridad.

Una iniciativa muy interesante es el acuerdo firmado recientemente por los ministros de Defensa de Letonia, Lituania, Estonia, Holanda, Finlandia, Austria y la Unión Europea³³. Este documento supone un «compromiso para mitigar los riesgos en el ciberespacio debidos al factor humano mediante una iniciativa en ciberhigiene». Esta iniciativa está abierta a todos los Estados miembros e instituciones de la Unión Europea. Los que se adhieran a ella se comprometen a adoptar unas buenas prácticas y se implementará una plataforma de *e-learning*. Como resultado ya se ha publicado una guía en ciberhigiene³⁴ dirigida por un grupo de expertos de la Universidad de Tallin y el ministerio leton de Defensa, aunque han contribuido otros expertos.

En este documento se categoriza al personal en grupos (usuarios, directivos y especialistas IT) y los comportamientos que dan origen a ciberincidentes (negligencia, intenciones maliciosas, falta concienciación, falta conocimiento sobre la organización). No todos los comportamientos son aplicables a todos los usuarios

En la Estrategia Internacional para el Ciberespacio de los Estados Unidos³⁵, y dada la globalidad de este dominio, esta nación asume como finalidad el ayudar a otros Estados para, entre otras acciones, desarrollar e implementar programas dirigidos a elevar el nivel de concienciación y construir así una cultura de ciberseguridad.

Como parte de la ciberdefensa

No existe una definición acordada sobre el término ciberdefensa, pero parece estar claro que entre sus objetivos fundamentales se encuentra la pro-

³³ Pledge of the Cyber Hygiene Initiative.

³⁴ Guidelines for Responsible IT-related Practices in Modern Organizations (Cyber Hygiene).

³⁵ International, Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. May 2011.

tección de las redes y sistemas TIC de los departamentos o ministerios de defensa de las naciones, y que es responsabilidad fundamentalmente de las Fuerzas Armadas.

Puesto que los programas de concienciación deben ser diseñados teniendo siempre presente la misión de la organización y teniendo en cuenta la cultura o idiosincrasia de la misma, la concienciación en ciberdefensa podría ser considerada como un caso particular, si tenemos en cuenta primeramente las misiones de las Fuerzas Armadas (FAS) y consideramos otros factores como: la sensibilidad de la información procesada en las TIC de los ministerios de defensa, la debida seguridad de las operaciones militares (OPSEC) y la dispersión geográfica de las unidades y la movilidad del personal, sometido a frecuentes cambios de destino.

Es necesario definir unos programas diferenciados de los que pueda tener otro organismo nacional o una empresa. La diferencia fundamental se centraría en unos contenidos adicionales destinados a sensibilizar al personal sobre los riesgos que para las operaciones militares pueden tener unas malas prácticas en el ciberespacio. Así, por ejemplo, el militar debe ser muy precavido con los contenidos (fotos, comentarios, etcétera) que cuelga en las redes sociales, puesto que puede dar claves al adversario sobre equipamiento, localización de unidades, movimiento de fuerzas, estado de moral, etcétera.

Otra particularidad debe ser la derivada de la dispersión (despliegues en zonas de operaciones, dispersión de unidades, etcétera) que obligará a contemplar métodos de difusión de mensajes de concienciación que permitan llegar a todo el personal. Un ejemplo sería el uso de aplicaciones para dispositivos móviles (apps).

Finalmente, muy importante, hacer llegar los mensajes a las personas que conforman el entorno personal cercano de los profesionales de las Fuerzas Armadas. Los adversarios pueden utilizar técnicas de ingeniería social para, a través de amigos o familiares, hacerles llegar un *software* malicioso.

En este sentido y como ya habíamos avanzado, desde su creación por la Orden Ministerial 10/2013³⁶, y en desarrollos sucesivos de la estructura de las Fuerzas Armadas, se ha asignado al Mando Conjunto de Ciberdefensa (MCCD) el cometido de definir, dirigir y coordinar la concienciación en materia de ciberdefensa. El MCCD, en coordinación con los distintos ámbitos del Ministerio de Defensa elaboró un Plan de Concienciación en Ciberdefensa (CONCIBE) que fue aprobado por el jefe del Estado Mayor de la Defensa en diciembre de 2015.

³⁶ Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

El CONCIBE determina unas audiencias objetivo, niveles a alcanzar, acciones a realizar, recursos, prioridades, cronograma y responsabilidades. Una de las particularidades de este Plan con respecto a otros programas de concienciación es que en la audiencia objetivo se incluye personal que no es usuario de las TIC del Ministerio de Defensa, pero que pertenece a él. No todos los puestos de trabajo de las Fuerzas Armadas acceden a las TIC, sin embargo es muy raro encontrar personal que no tenga un ordenador personal o dispositivo móvil. Incluyendo a este personal, se está reconociendo que el comportamiento privado entraña riesgos cuando se interactúa en el ciberespacio. También y por las razones que hemos expuesto anteriormente, es objeto del CONCIBE el entorno cercano de los militares, como pueden ser familiares o amigos próximos, lo cual no solo contribuye de manera indirecta a la seguridad de las operaciones, sino que además se contribuye al esfuerzo de concienciación de todos los ciudadanos previsto a nivel nacional.

Este Plan está en ejecución desde su aprobación a finales de 2015 y se han desarrollado acciones que han involucrado a diversas unidades y organismos de las Fuerzas Armadas, habiéndose incluso contratado algunos productos a empresas privadas. El CONCIBE contempla unas métricas que deben ayudar en un futuro próximo a hacer una revisión del propio Plan.

Otro ejemplo de plan específico en el ámbito de la defensa es la Iniciativa de Cultura y Cumplimiento de Ciberseguridad (CD3I)³⁷ del Departamento de Defensa (*DoD*) de los Estados Unidos. Liderada por el Mando Estratégico (USSTRATCOM) y el Mando Cibernético (USCYBERCOM), establece de manera clara la responsabilidad individual de los usuarios y operadores de proteger las redes del *DoD*, así como la de los jefes de unidad de impulsar la cultura de ciberseguridad.

Esta iniciativa establece una serie de principios directores de comportamiento individual (integridad, adecuado nivel de conocimientos, correcta aplicación de los procedimientos, respaldo, y actitud inquisitiva ante los incidentes) y agrupa a los usuarios en cuatro niveles (usuarios, directivos, especialistas IT y ciberguerreros). También especifica que debe haber un sistema de inspecciones, un sistema de comunicación y unos recursos para llevarla a cabo y afirma de manera contundente que «la ciberseguridad debe convertirse en una parte integral de las operaciones, de la misma manera que lo es un esquema de maniobra».

Programas, planes, campañas de concienciación

Aparte de las campañas o planes que ya hemos analizado, existe mucha información y documentación disponible en internet para servir a ayudar a

³⁷ The DoD Cybersecurity Culture and Compliance Initiative.

definir programas, planes o campañas de concienciación. Vamos a repasar algunos que nos han parecido interesantes.

Entre ellas, de gran valor es la Guía sobre Programas de Formación y Concienciación en ciberseguridad del Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST)³⁸. Merece la pena analizar un poco este documento ya que es una completísima guía que no solo sirve para los programas de concienciación, sino también para formación. Esta guía define responsabilidades dentro de una empresa y los pasos críticos a dar para acometer una tarea de concienciación: diseño de un programa, la preparación del material, la implementación del programa y el seguimiento del mismo.

Dentro del diseño del programa, primero especifica acciones a seguir para estructurar la actividad, desarrollar un análisis de necesidades, desarrollar el plan de concienciación, establecer prioridades y definir un nivel a alcanzar. Estructurar la actividad es crítico y propone tres posibles modelos partiendo de la base de que siempre debe existir una autoridad central en formación y concienciación: centralizado, en el que la política, la estrategia a seguir y la implementación son dirigidas por una entidad central; parcialmente distribuido, de manera que la política y la estrategia a seguir están centralizadas y la implementación descentralizada; solo la definición de la política a seguir queda centralizada. La elección de un modelo u otro estará basado en consideraciones como el presupuesto, la organización, el tamaño de la misma y su dispersión geográfica.

La guía también expone cómo hacer métricas de concienciación, cómo puede ser el porcentaje de usuarios que han participado en sesiones de concienciación, los ciberincidentes que sufre la organización a causa del usuario o entrevistas con el personal responsable.

Dado que los recursos siempre serán limitados, será necesario establecer unas prioridades para difundir mensajes. Estas prioridades vendrán dadas fundamentalmente por el nivel de exposición a ciberataques a la que puede estar sometida una parte de la audiencia de adiestramiento.

En cuanto al desarrollo del material de concienciación, el documento propone varias opciones: desarrollado por la propia organización; utilizar alguno desarrollado por alguna organización profesional o contratar a una empresa especializada. También dependerá de la misión y capacidad de la organización definirse por un medio u otro. *A priori* da la impresión que solo las grandes organizaciones pueden ser capaces de desarrollar sus propios materiales.

Con respecto a los temas a incluir en las campañas, el NIST 800-50 propone, por ejemplo: uso y gestión de contraseñas, incluyendo su creación, frecuen-

³⁸ NIST Special Publication 800-50, «Building an Information Technology Security Awareness and Training Program».

cia de cambios y protección; protección contra código malicioso; políticas; correos electrónicos; seguridad en la web; copia de seguridad de los datos; ingeniería social; *shoulder surfing*; responsabilidades de los usuarios, etcétera.

Otros documentos de utilidad para la redacción de un plan de concienciación son la Guía Suplementaria de Recursos del Modelo de Ciberresiliencia³⁹ y la Guía de Autoevaluación de Ciberresiliencia⁴⁰, ambos derivados del ya mencionado CERT-RMM.

En la primera guía se deja claro que las organizaciones deben dedicar recursos a la concienciación como son: instalaciones, personal, materiales de concienciación, etcétera. También tienen la opción de contratar la concienciación a proveedores ajenos. Ahora bien, en este caso hay que hacer un esfuerzo para definir bien las necesidades de la organización y hacer que el proyecto responda a las mismas. Por otra parte, habrá una parte relacionada con los procedimientos propios de la organización que difícilmente podrá ser subcontratada.

Con respecto la guía de autoevaluación, esta es muy interesante ya que se establecen una serie de aspectos que sirven para evaluar, en general, el nivel de madurez de la resiliencia de una organización. Uno de esos aspectos es la concienciación y en ese particular se pueden sintetizar en dos: que exista un programa dentro de la organización y que este se esté ejecutando.

Por otra parte, el Consejo de Estándares de Seguridad de Tarjetas de Pago (PCI SCC), que es un foro responsable del desarrollo, educación y concienciación de los estándares para incrementar la seguridad de los pagos electrónicos, hace algunas propuestas interesantes en materia de concienciación en ciberseguridad⁴¹. Entre ellas destacamos: la necesidad de crear un equipo para concienciación compuesto de personal con diversos perfiles; definir el mínimo nivel de conocimientos a alcanzar por todo el personal de la organización; incluir diversos modos de difundir los conocimientos, como pueden ser la formación clásica, aprendizaje basado en el ordenador, *emails*, circulares, boletines; difundir los materiales adecuados en los momentos oportunos y de manera eficiente; ajustarse a la idiosincrasia de la organización y definir unas métricas que sirvan para medir el éxito de las campañas.

Asimismo el Instituto SANS en noviembre de 2015 llevó a cabo una encuesta⁴² sobre este tema. Este estudio ha puesto en relieve dos hechos clave: en general los equipos de concienciación no tienen el apoyo, tiempo y recursos

³⁹ Carnegie Mellon University, Cyber Resilience Review (CRR) Supplemental Resource Guide, volume 9, Training and Awareness, Version 1.1.

⁴⁰ Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide February 2016.

⁴¹ PCI Security Standards Council. Best Practices for Implementing a Security Awareness Program, October 2014.

⁴² SANS, Awareness is hard: a tale of two challenges, 2016.

que necesitarían para tener éxito; y segundo, los equipos de concienciación suelen tener buenas habilidades técnicas pero les suelen faltar habilidades de comunicación interpersonales.

Basados en las propuestas del PCI SCC y SANS podemos llegar a la conclusión de que los equipos de concienciación ideales deberían estar compuestos por un buen comunicador y un buen técnico. El primero para hacer llegar los mensajes clave y el segundo para apoyarle y poder realizar demostraciones técnicas que tengan el impacto necesario.

En la misma línea y según Kaspersky hay empresas que gastan millones en campañas de concienciación pero realmente pocos responsables de la seguridad de las TIC (CISO) están contentos con los resultados. El motivo aparentemente es que la mayor parte de los programas llevan mucho tiempo, son muy técnicos y esencialmente basados en mensajes negativos. Por tanto, propone aproximarse al problema con una visión más sofisticada con técnicas de *gamificación*, ataques simulados e instrucción interactiva en profundidad de las destrezas en ciberseguridad⁴³.

Cooperación público-privada para la concienciación en ciberseguridad

A la vista de todo lo comentado hasta el momento podemos ver que definir un plan de concienciación para una organización o empresa nunca es sencillo, pues aunque existen guías disponibles y muchas experiencias y buenas prácticas, en muchos casos lo verdaderamente difícil para acometer con éxito y garantías un proyecto de concienciación reside en el cambio cultural que es necesario realizar. Asimismo, es necesario dedicar recursos materiales, humanos y financieros, y para ello hay que convencer de la necesidad a la dirección de las organizaciones.

La tarea se complica aún más si la concienciación la queremos llevar a un ámbito superior, como es el nacional. En este caso la audiencia objetivo es muy amplia: afecta a todos los ciudadanos de la nación. Sin duda, para la consecución de un objetivo de esta naturaleza la Administración debe jugar un papel clave a la hora de dinamizar este trabajo, aportando los recursos necesarios. Sin embargo, los organismos públicos con responsabilidades en la materia son diversos, cada uno con diferente organización, responsabilidades y recursos.

Teniendo en cuenta que el concienciar a los ciudadanos redunda en beneficio de ambos, nación y empresas, quizá la solución esté en abordar este tema de una manera global mediante la creación de una asociación de cooperación entre ambos sectores [*Public-Private-Partnership (PPP)*]. ENISA ha estudia-

⁴³ Kaspersky. Cybersecurity Awareness Brochure.

do cómo articular una *PPP*⁴⁴ en ciberseguridad y ofrece algunas recomendaciones que pueden ser de utilidad y que pasamos a analizar.

Participar en una *PPP* trae beneficios para ambos sectores. El Gobierno de la nación cumple con lo expresado en la ECSN relativo a la mejora de la resiliencia, que a su vez es un mandato expresado en la Estrategia de Ciberseguridad de la Unión Europea, que indica que «para impulsar la ciberresiliencia en la Unión Europea, tanto las Administraciones Públicas como el sector privado deben desarrollar capacidades y cooperar efectivamente».

Para los socios del sector privado el pertenecer a una asociación de este tipo les reporta también otros beneficios. Entre ellos se pueden destacar los siguientes: acceso a información privilegiada y especializada, acceso al conocimiento no disponible en ningún sitio más, oportunidad de contribuir a una dirección estratégica y a políticas nacionales, y la posibilidad de intercambiar lecciones aprendidas, buenas prácticas y ver distintos puntos de vista sobre cómo afrontar el problema.

Pero si hay un beneficio importante para que una empresa participe en un *PPP* este es el prestigio que supone participar en una iniciativa de estas dimensiones. Para otras compañías el prestigio viene dado por la confiabilidad que ofrecen a sus clientes de que sus transacciones electrónicas y privacidad quedan protegidas por su compromiso con la ciberseguridad.

Una *PPP*, según *ENISA*, queda definida como una relación organizada entre organizaciones públicas y privadas, en la que se establece un ámbito y objetivos en común y define unos cometidos y metodología de trabajo para alcanzar la finalidad compartida.

Esta definición es muy interesante pues supone que una asociación de este tipo no debe ser una entelequia, un simple deseo político de armonía entre ambos sectores. Una *PPP* debe estar perfectamente estructurada y definida y por supuesto esta asociación debe ir más allá de la mera contratación de servicios a empresas. Debe suponer una aportación común de esfuerzos a un fin común que redunde en beneficio de todos los participantes en ella.

En primer lugar, debe existir un organismo de coordinación o regulador. Dicho organismo puede ser el que impulse la iniciativa y, en general, debe ser visto como un socio más en disposición de apoyar. En ningún caso debe dar la impresión de que se establece una relación de mando y subordinación entre los asociados en la *PPP*. A esta *PPP* en este documento nos referiremos también como consorcio o asociación.

Es fundamental definir con claridad las relaciones entre miembros de la asociación y los procesos que se van a desarrollar en el marco de la asociación y entre esta y el exterior. Entre ellos es vital la definición de la gobernanza

⁴⁴ Cooperative Models for Effective Public Private Partnerships food Practice Guide.

de la *PPP*, así como una clara definición de los cometidos a desempeñar por cada socio participante.

Es importante animar a los socios a compartir información y a que tengan en cuenta la información que reciben. Como mecanismos de relación dentro del grupo, estos deben quedar claramente establecidos en los estatutos y deberían basarse en reuniones regulares presenciales, reuniones por videoconferencia, difusión electrónica (*email*, portales web, etcétera) o una combinación de todas ellas.

Habrà también que definir el tipo de asociación que se quiere crear teniendo en cuenta la misión y que puede ser de varios tipos: comunidades a largo plazo, cuya razón fundamental es el intercambio de información; grupos de trabajo, son aquellos que se constituyen con un fin muy concreto; grupos de repuesta rápida, se constituyen por un corto periodo de tiempo y para ocuparse de algún asunto urgente; o grupo de actividad combinada, es una comunidad a largo plazo que puede reunirse para planear y practicar estrategias y, si hay una emergencia, un pequeño comité constituye un grupo de respuesta rápida o equipo de trabajo.

Este tipo de asociación debe canalizar la inversión pública necesaria en esta materia. El punto de partida para que se pueda dar una cooperación público-privada efectiva es la necesidad de orientar la inversión para conseguir una serie de objetivos. En este sentido en la *PPP* estarán representados todos los estamentos implicados en la resolución de estos problemas: Administración, empresas y ciudadanos.

De cualquier manera, al definir una asociación de este tipo, será fundamental considerar el marco legal. En el caso español este es la Ley 40/2015 que regula el régimen jurídico del sector público. En dicha ley se definen los convenios como aquellos «acuerdos con efectos jurídicos adoptados por las Administraciones Públicas, los organismos públicos y entidades de derecho público vinculados o dependientes o las universidades públicas entre sí o con sujetos de derecho privado para un fin común» (artículo 47, apartado 1, de la Ley 40/2015). Esta definición incluye tanto los convenios interadministrativos (artículo 6 de la Ley 30/1992) como los convenios suscritos entre Administraciones Públicas y particulares.

En dicha ley se establecen los requisitos para la celebración de convenios. Por ser de especial aplicación a la definición de una *PPP* destacamos los siguientes: «La suscripción de convenios deberá mejorar la eficiencia de la gestión pública, facilitar la utilización conjunta de medios y servicios públicos, contribuir a la realización de actividades de utilidad pública y cumplir con la legislación de estabilidad presupuestaria y sostenibilidad financiera. Los convenios que incluyan compromisos financieros deberán ser financieramente sostenibles, debiendo quienes los suscriban tener capacidad para financiar los asumidos durante la vigencia del convenio, y las aportaciones financieras que se comprometan a realizar los firmantes no podrán ser superiores a los gastos derivados de la ejecución del convenio».

En cuanto al contenido mínimo de un convenio, la Ley 40/2015 expresa que este será el siguiente: «a) Sujetos que suscriben el convenio y la capacidad jurídica con que actúa cada una de las partes. b) La competencia en la que se fundamenta la actuación de la Administración pública, de los organismos públicos y las entidades de derecho público vinculados o dependientes de ella o de las universidades públicas. c) Objeto del convenio y actuaciones a realizar por cada sujeto para su cumplimiento, indicando, en su caso, la titularidad de los resultados obtenidos. d) Obligaciones y compromisos económicos asumidos por cada una de las partes, si los hubiera, indicando su distribución temporal por anualidades y su imputación concreta al presupuesto correspondiente de acuerdo con lo previsto en la legislación presupuestaria. e) Consecuencias aplicables en caso de incumplimiento de las obligaciones y compromisos asumidos por cada una de las partes y, en su caso, los criterios para determinar la posible indemnización por el incumplimiento. f) Mecanismos de seguimiento, vigilancia y control de la ejecución del convenio y de los compromisos adquiridos por los firmantes. Este mecanismo resolverá los problemas de interpretación y cumplimiento que puedan plantearse respecto de los convenios. g) El régimen de modificación del convenio. A falta de regulación expresa la modificación el contenido del convenio requerirá acuerdo unánime de los firmantes. h) Plazo de vigencia del convenio».

Vemos, pues, cómo un convenio puede ser el mecanismo ideal para definir una PPP.

Experiencias y buenas prácticas

En junio de 2012, cuarenta y cinco representantes de la Unión Europea y de los Estados Unidos, del sector público y privado, se reunieron en Bruselas para discutir cómo involucrar intermediarios para «elevar la concienciación en ciberseguridad»⁴⁵. Los participantes expusieron algunas ideas y compartieron experiencias y buenas prácticas. Algunas de las conclusiones de dicha reunión son las siguientes:

- Para las empresas el cooperar en campañas de concienciación crea una buena imagen de la marca, generando así buenas oportunidades de negocio. Sin embargo, convencer a los directivos de la importancia de participar en un proyecto de este tipo es una gran dificultad, a pesar de que merece la pena a largo plazo el financiarlo.
- La ciberseguridad supone un reto cultural pues debe ir encaminada a ciertos cambios en el comportamiento de los usuarios.
- Los ciudadanos son conscientes de alguna manera de que hay medios técnicos para protegerse, pero en muchos casos no saben cómo aplicarlos.

⁴⁵ Involving Intermediaries in Cyber-security Awareness Raising.

- Es importante no asustar a los usuarios pero sí animarlos a conectarse y estar seguros al mismo tiempo.
- Para concienciar no es necesario dar excesiva información técnica.
- Los mensajes de concienciación deben estar cuidadosamente estudiados para que vayan dirigidos a una audiencia concreta.
- Los usuarios de las TIC más jóvenes puede ser buenos promotores y llegando a ellos se puede llegar a los padres. Cuanto antes comience la educación, mayores serán los efectos en el comportamiento adecuado de los usuarios en el ciberespacio.

Los medios de comunicación social deberían ser considerados como el principal canal para difundir los mensajes clave. Así, por ejemplo, la televisión tiene un papel clave. También debe tenerse en cuenta la popularidad de las redes sociales.

Los participantes en una PPP deben estar involucrados en todas las etapas del proceso.

También la OTAN ha definido una Asociación Industria-OTAN en Ciberdefensa (*NATO Industry Cyber Partnership, NCIP*). Este agrupa a distintas entidades de la OTAN, equipos de respuesta ante incidentes de ciberseguridad y un amplio espectro de representantes de las industrias de los países, incluyendo también representantes de las universidades y centros de enseñanza⁴⁶.

Un ejemplo concreto

En Estados Unidos se han lanzado algunas iniciativas interesantes en cuanto a concienciación en ciberseguridad, como son: el mes de la concienciación en ciberseguridad, la campaña *Stop. Think. Connect*, el día de la privacidad de los datos (*Data Privacy Day*) y la campaña *Re: Cyber* para directivos.

En 2001 se fundó la Alianza Nacional de Ciberseguridad (*National Cyber Security Alliance, NCSA*). Fue conformada por un grupo de líderes visionarios de la industria que se dieron cuenta de que no se había hecho lo suficiente para formar al público sobre cómo protegerse en las redes. Desde el principio los principios reguladores incluían que, aunque en algunas esferas los socios miembros podían competir, sin embargo, todos tenían un interés compartido en un internet más seguro y confiable y el éxito final vendría garantizado si trabajaban juntos y próximos al Gobierno, quien también compartía este interés.

Hoy en día la misión de la *NCSA* es educar una sociedad digital de tal manera que puedan utilizar internet de manera segura en la casa, el trabajo y la escuela, protegiendo la tecnología que utilizan las personas, las redes a las que se conectan y los medios compartidos. Sus actividades están financiadas por los miembros asociados y por el Departamento de Seguridad.

⁴⁶ <http://www.nicp.nato.int/news/index.html>

Algunas empresas asociadas a esta iniciativa son: ADP, AT & T, Bank of America, Comcast, EMC, ESET, Facebook, Google, Intel, Leidos, McAfee, Microsoft, Symantec, Verizon and VISA.

En el año 2009 la política del ciberespacio del presidente Obama recomendaba que «El Gobierno Federal, en cooperación con educadores e industria, debería conducir un esfuerzo común de concienciación pública en ciberseguridad y esfuerzo en educación». Como respuesta, en una iniciativa sin precedentes, la NCSA junto con el grupo de trabajo Anti Phising trajeron consigo veinticinco empresas y siete agencias gubernamentales para explorar la posibilidad de una campaña nacional de concienciación. El grupo rápidamente tomó la tarea y en los siguientes catorce meses trabajando en estrecha cooperación y por consenso investigó y desarrolló un conjunto de mensajes que deberían estar disponibles y ser usados por todos.

Este es el origen del programa clave desarrollado por la NCSA y conocido como *Stop.Think.Connect* (Para. Piensa. Conecta). El trabajo desarrollado ha sido reconocido al proclamar el presidente Obama *Stop. Think.Connect* como la campaña nacional de concienciación durante su anuncio del Mes Nacional de Ciberseguridad en 2010.

Algunos de los beneficios de esta campaña incluyen:

- Más de ciento cincuenta socios firmaron la campaña para utilizar el mensaje de la campaña. Grandes y pequeñas empresas, departamentos de policía e instituciones educativas y del Gobierno entre ellas.
- La campaña se ha expuesto en transportes públicos de importantes ciudades de Estados Unidos como Washington, Boston y Chicago.
- Se han desarrollado pequeñas campañas en torno a mensajes clave de la campaña.
- Muchas empresas lo han utilizado para demostrar al público su política interna de seguridad en las redes.
- Mucho material ha sido desarrollado para escuelas.

Aunque esta campaña inicialmente solo iba dirigida a los Estados Unidos, esta campaña creció internacionalmente y se ha expandido hacia otras organizaciones regionales e incluso otros países.

Conclusiones

La concienciación en ciberseguridad es una actividad permanente que debe empezar desde las etapas iniciales de la enseñanza y que debe alcanzar a todos los ciudadanos. Sin duda, supone un claro beneficio para el individuo y su ámbito laboral, lo que redundará finalmente en una nación más resiliente en el ciberespacio.

El Gobierno de España a través del Plan de Cultura de Ciberseguridad, Concienciación, Sensibilización y Educación intenta que se alcance el objetivo

último de garantizar la resiliencia nacional en la primera etapa del proceso. Y esto lo hace involucrando a los diversos actores del sector público.

Sin embargo, las dimensiones de dicho proyecto son muy amplias y echamos de menos a empresas y organizaciones que también pueden participar y cuya contribución es significativa. Esta cooperación público-privada no debería ser una simple postura política o declaración de intenciones. Debería ir más allá utilizando el marco legal disponible, mediante la celebración en un convenio que diera cabida a diversos actores del sector público como del sector privado, que oriente la necesaria inversión por parte del sector público.

A nadie se le escapa la dificultad de la creación de un ente de estas características. En primer lugar para la Administración dedicar recursos especialistas con experiencia en diversas materias (comunicación pública, ciberseguridad, asesores legales, etcétera). En segundo lugar, el llegar a un acuerdo y materializarlo. Finalmente, destinar la inversión necesaria para tener éxito en esta tarea.

A pesar del esfuerzo a realizar, creemos que a nadie se le escapan tampoco los beneficios a largo plazo. Un ejemplo en esta línea es la fórmula seguida por la Unión Europea para enfocar la inversión en I+D+i que se va a realizar en el marco del Horizonte 2020. Se han definido diversas *PPP*; en particular en el ámbito de la ciberseguridad, con el objeto de canalizar la inversión hacia los intereses y necesidades de los sectores productivos.

En cualquier caso, no basta con que el individuo esté concienciado en ciberseguridad. Hay que conseguir que la persona tenga un compromiso real con su empresa y con su nación. Para ello, a nivel laboral, las empresas y organizaciones deben ofrecer a los trabajadores un plan de vida, una seguridad, un sentimiento de grupo, en algunos casos un ideal, y proporcionar una serie de valores añadidos que vayan más allá del estímulo económico directo. A nivel nacional es importante hacer saber al ciudadano que con su ciberseguridad personal contribuye a la de la nación.

En definitiva, para tener éxito y mejorar nuestra cultura global de ciberseguridad hay que (1) pensar que trabajamos con personas (2), disponer del apoyo institucional y los recursos para desarrollar todos los planes que son necesarios y alinearlos con los intereses del Estado y (3) Aglutinar en una *PPP* a todos los interesados (empresas, Administración, empresas de ciberseguridad) para definir las líneas de trabajo más apropiadas para garantizar el éxito.

Capítulo séptimo

I+D+i y ciberseguridad: análisis de una relación de interdependencia

Aurelio Hinarejos Rojo

Capitán del Cuerpo de Ingenieros Politécnicos del Ejército DGAM/SDGPLATIN

José de la Peña Muñoz

Director de la Revista SIC

Resumen

Los autores analizan la relación de interdependencia entre la I+D+i y la ciberseguridad, reivindicando el alineamiento de lo expresado en las Estrategias Españolas de Ciencia y Tecnología e Innovación (EECTI) y de Ciberseguridad Nacional (ECSN). Al tiempo exponen algunos de los frentes de I+D+i proyectados para sumergirse posteriormente en un análisis genérico que permite hacerse una idea razonable del esfuerzo internacional en I+D+i. En el capítulo se brinda también una visión de la colaboración público-privada y se exponen iniciativas significativas de alcance internacional y supranacional para finalizar con una aportación en la que se mencionan materias prometedoras para su tratamiento en los ecosistemas de CPP en I+D+i sobre ciberseguridad.

Palabras clave

investigación y desarrollo, innovación, ciberseguridad, ciberdefensa militar, resiliencia, independencia tecnológica, autonomía estratégica, ecosistemas de colaboración público-privada.

Abstract

The authors analyse the relationship of interdependence between research, development and innovation, and cybersecurity, while claiming the convergence of Spanish strategies for Science, Technology and Innovation (EECTI) and National Cyber Security (ECSN). At the same time, some of the hottest R&D&I areas are exposed just before delving into a generic analysis of the subject matter, which allows a reasonable picture of the international effort into cyber R&D&I to be provided. In addition, a perspective on public-private partnership in this realm, as well as significant initiatives at supra- and international level are exposed. Finally, an overview of promising matters on public-private partnership ecosystems focused on R&D&I on cybersecurity is also depicted.

Keywords

Research and development, innovation, cybersecurity, military cyberdefence, resilience, technological independence, strategic autonomy, public-private partnership ecosystems

Introducción

«Politics is about crafting and picking alternatives. Politics matters, therefore, only if choices can be made and if making them has real consequences».

—Dan Breznitz—

A principios del mes de enero de 2016, el Departamento de Seguridad Interior de los Estados Unidos (*DHS, Department of Homeland Security*) informaba acerca de la manipulación ilícita de vehículos aéreos no tripulados (*UAV*) del servicio de protección de fronteras¹. Por medio del envío de señales GPS falsas que aparentaban ser genuinamente procedentes de los satélites NAVSTAR, lo que se conoce como *GPS spoofing*, narcotraficantes mejicanos lograban manipular la misión de los drones a fin de poder cruzar libremente la frontera entre Estados Unidos y México y así conseguir libertad de acción en su actividad criminal. Hoy por hoy no es posible acabar con esta vulnerabilidad, ya que la incorporación de un módulo anti-*spoofing*, tal como se hace en los sistemas militares, comprometería la autonomía de vuelo del *UAV*, por no mencionar el impacto económico que ello supondría. Sin embargo, se espera que la innovación tecnológica posibilite en el futuro inmediato la implantación de este tipo de módulos de forma asequible y con unas características físicas que no impidan su eficacia operativa. Este es solo un ejemplo, entre muchos otros que podrían mencionarse, de la confianza existente en que las actividades de investigación y desarrollo en curso conduzcan a innovaciones que permitan una mejora significativa en las condiciones de ciberseguridad actuales.

Más recientemente, el 16 de agosto de 2016, el diario *The New York Times* se hacía eco de la publicación en Internet por parte del grupo autodenominado *The Shadow Brokers*, de fragmentos de código fuente de *software* clasificado como «*Top secret*» aparentemente proveniente de la *National Security Agency* (*NSA*) de los Estados Unidos y que supuestamente habría formado parte del arsenal de ciberarmas atribuido a esta agencia². Los *Shadow Brokers* afirmaban no obstante que el *software* pertenecía al *Equation Group*, nombre en clave con que la firma rusa Kaspersky Labs se refiere a la *NSA*. De hecho, Kaspersky Labs había identificado en el ciberespacio un grupo caracterizado por la complejidad de sus actividades y su apego al empleo de criptografía fuerte, imputándoles el desarrollo de *malware* como STUXNET³. Con

¹ Cimpanu, Catalin. «Drug Cartels are Hacking US Border Patrol Drones», Softpedia, Jan 1 2016, <http://news.softpedia.com/news/drug-cartels-are-hacking-us-border-patrol-drones-498312.shtml>

² Sanger, David E. «"Shadow Brokers" Leak Raises Alarming Question: Was the N.S.A. Hacked?», The New York Times, http://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html?_r=0. Fecha de la consulta: 20 de agosto de 2016.

³ GReAT, «A Fanny Equation: "I am your father", Stuxnet», Kaspersky Labs, February 17 2015, <https://securelist.com/blog/research/68787/a-fanny-equation-i-am-your-father-stuxnet/>. Fecha de la consulta: 24 de septiembre de 2016.

su anuncio, los *Shadow Brokers* aseguraban haber logrado golpear al hasta entonces invulnerable *Equation Group*. Lo que es importante resaltar en este contexto es que, recíprocamente, en el lado de las amenazas, se puede entrever que las más sofisticadas proceden de décadas de investigación y desarrollo de ciberarsenales por parte de actores supuestamente vinculados a entidades estatales.

Visto que, como ha venido ocurriendo a lo largo de miles de años de historia militar, el I+D está detrás de cada innovación, tanto en la vertiente ofensiva como en la defensiva, convendría, antes de entrar en materia, establecer una mínima clarificación terminológica con la intención de hacer más inteligible lo que más adelante se expondrá en este capítulo.

Por un lado, existe una frecuente confusión en la literatura especializada con los conceptos de ciberseguridad y ciberdefensa, cuestión abordada por Feliú⁴. En el ámbito de este capítulo sostendremos que la misión de la ciberdefensa es garantizar la ciberseguridad⁵. Igualmente, procede también diferenciar entre investigación y desarrollo (I+D) e innovación (i). Mientras que el I+D es el trabajo creativo emprendido sistemáticamente para incrementar el conocimiento científico, así como para utilizar este conocimiento con el fin de proyectar aplicaciones prácticas del mismo, la innovación tecnológica será el resultado de la transformación de una idea en un producto nuevo o mejorado que es introducido en un mercado y diseminado de manera que produzca un efecto en la sociedad o bien de un servicio nuevo o mejorado que ha sido insertado dentro de un proceso de producción⁶. De aquí que el objetivo del I+D+i en ciberdefensa será disponer de una capacidad defensiva avanzada que permita establecer de manera eficaz en cuanto a su coste las medidas de prevención, disuasión, protección y reacción necesarias para alcanzar el estado de ciberseguridad deseado.

Entendido que un proceso de I+D+i eficaz es necesario para dotarnos de mayor ciberseguridad, veremos que no es suficiente. Hasta la década de los ochenta del siglo pasado la mayoría de los avances tecnológicos procedían de la industria militar y aeroespacial, generosamente financiada con dinero público (en cierta medida como subproducto del complejo militar-industrial

⁴ Feliú Ortega, Luis. «La ciberseguridad y la ciberdefensa». En: *El ciberespacio: nuevo escenario de confrontación*. Monografías del CESEDEN 126. CESEDEN, Madrid, febrero de 2012.

⁵ En este trabajo se enfocará la seguridad en el dominio ciberespacial con una doble perspectiva: por un lado, estática, en la que la ciberseguridad es un estado a alcanzar y mantener; y, por otro lado, dinámica, en la que la ciberdefensa, activa o pasiva, será un proceso conducente al estado de ciberseguridad deseado. En síntesis, la ciberdefensa será el medio y la ciberseguridad el fin.

⁶ Organisation for Economic Cooperation and Development. *Main definitions and conventions for the measurements of Research and Experimental Development (R&D). A summary of the Frascati Manual*. 1993. París: 1994, p. 4.

del que advirtió el presidente Eisenhower)⁷, pero hoy día las innovaciones proceden mayoritariamente de la industria civil. Es por ello que las Administraciones Públicas se ven en cierta forma obligadas a llegar a acuerdos con operadores económicos no institucionales con el fin de acceder a los beneficios de una tecnología novedosa sin asumir los riesgos derivados de su investigación y desarrollo. Es decir, en este contexto, toma forma la colaboración público-privada (CPP) en I+D+i, aunque con el matiz de que será más exitosa en materia de innovación que en el puro aspecto de la investigación y desarrollo. Si bien lo descrito es aplicable a múltiples tecnologías, será la colaboración público-privada, por sus características específicas y que veremos en este capítulo, especialmente indicada en el caso del I+D+i en ciberseguridad. En este sentido, la creación en los Estados Unidos de *Defense Innovation Unit Experiment (DIUx)* supone una apuesta por la colaboración público-privada como medio para mantener el liderazgo tecnológico del Departamento de Defensa norteamericano en el ciberespacio, y constituye un nítido ejemplo de las iniciativas que en esta dirección se están impulsando en otros países⁸.

Por otro lado, el asunto que se plantea no es trivial. Nos movemos en un espacio tridimensional en el que los ejes son el I+D+i, el nivel de ciberseguridad y el grado de colaboración público-privada, siendo necesario encontrar la zona de equilibrio donde se produce la sinergia suficiente como para sostener el sistema, produciendo al mismo tiempo beneficios para las partes.

Por lo que respecta a la dimensión de la ciberseguridad, partimos de la base de que esta presenta tres aspectos: el personal que la gestiona, los procesos que permiten garantizar su eficacia y los productos (tecnología) que soportan a estos últimos mejorando la eficiencia⁹. En cuanto a la colaboración público-privada, claramente existirá una diferencia de enfoque por parte del sector privado, que aspira a un legítimo retorno de inversión cuanto más generoso mejor, y un sector público que ha de atender en primer lugar a colmar las necesidades de seguridad y defensa de la población. En la práctica, ocurre que la colaboración público-privada no es una panacea y suscita suspicacias entre las partes. Existen numerosas ventajas y desventajas en su puesta en práctica. ¿Qué espera el sector público de una colaboración en I+D+i en ciberseguridad (transferencia de conocimien-

⁷ Discurso del mensaje de despedida del presidente norteamericano Dwight Eisenhower, donde divulgó el concepto de «complejo militar-industrial», 17 de enero de 1961. Véase también: «The Military-Industrial Complex: The Farewell Address of President Eisenhower», Basements Publications, 2006.

⁸ Creada en abril de 2015 por el secretario de Estado Ashton Carter, la *DIUx* es fruto de la *Defense Innovation Initiative*, cuyo objetivo es la generación de nuevas capacidades militares, así como del *Long Range Research and Development Plan*. Su finalidad es apoyar las propuestas tecnológicas de la industria civil estadounidense para madurarlas e integrarlas en el armamento y material, incluido el destinado a operaciones en el ciberespacio.

⁹ Informe mensual de ciberseguridad CIBERelcano n.º 13, Real Instituto Elcano de Estudios Internacionales y Estratégicos, Madrid, abril de 2016, p. 12.

tos, acceso a tecnología novedosa, etcétera? Y qué puede esperar el sector privado de una cooperación con el público (financiación, ventajas fiscales, etcétera). ¿En qué aspectos debería ceder el sector público (relajación de las exigencias en materia de cesión de derechos de propiedad intelectual o flexibilidad en las relaciones contractuales) y en qué otros el sector privado (apuesta por el largo plazo en lugar de beneficios a corto)? Es necesario investigar dónde se encuentran los intereses comunes y dónde los particulares, de manera que el esfuerzo se centre en potenciar precisamente el logro de los intereses comunes. Cabe preguntarse también si existen casos documentados donde esa colaboración en I+D+i haya dado o esté dando resultados positivos.

Para abordar sistemáticamente el tema analizaremos progresivamente los diferentes planos definidos por cada pareja de ejes de este espacio: CPP y ciberseguridad, I+D+i y ciberseguridad y CPP e I+D+i. No nos detendremos mucho en el primer plano de la colaboración público-privada en ciberseguridad por ser el ámbito más general y cuyos pormenores se hallan exhaustivamente tratados en otros capítulos de este volumen. En cuanto al segundo plano, constituido por la I+D+i y la ciberseguridad, explicaremos someramente la diferencia entre investigación y desarrollo, y la innovación propiamente dicha, que será en lo que estemos más interesados en ciberseguridad. Presentaremos la necesidad y justificación de una estrategia de I+D+i en ciberseguridad plenamente en línea con la Estrategia Española de Ciencia y Tecnología y de Innovación y con la Estrategia de Tecnología e Innovación de la Defensa, por una parte, y con la Estrategia de Ciberseguridad Nacional, por otra. También repasaremos los retos actuales planteados al I+D en ciberseguridad, tales como el logro de la ansiada resiliencia de los sistemas en lugar de limitarnos a la mera protección de estos, avanzar en la capacidad de análisis forense para, entre otras cosas, lograr la atribución de los ciberataques, la gestión de identidades, innovación en productos, procesos y personas, etcétera.

El tercer plano, formado por la confluencia entre la colaboración público-privada y la I+D+i, en términos generales nos lleva a intentar responder las cuestiones antes formuladas. El papel general del Estado en los procesos de innovación ha sido ampliamente debatido por autores como Gerschenkron¹⁰ y Breznitz¹¹. En este sentido el resultado esperado de una exitosa colaboración público-privada será la transformación del conocimiento y experiencia generados a nivel académico e industrial (I+D) en productos innovadores aptos para un mercado abierto y competitivo.

¹⁰ Gerschenkron, A. «Economic Backwardness in Historical Perspective: A Book of Essays». Belknap Press of Harvard University Press, Cambridge, 1962.

¹¹ Breznitz, Dan. «Innovation and the state: political choice and strategies for growth in Israel, Taiwan, and Ireland», Yale University Press, New Haven, 2007.

Investigación, desarrollo e innovación en ciberseguridad

La rápida evolución de las amenazas exige una inversión continua en I+D e innovación tecnológica para no quedarse atrás. Antes de examinar en detalle la especificidad de la I+D+i en ciberseguridad, procede volver a hacer hincapié en la diferencia entre I+D e innovación.

La investigación y desarrollo (I+D) es definida por Christopher Freeman como «el trabajo creador que, emprendido sobre una base sistemática, tiene por objeto el aumento del conocimiento científico y técnico, y su posterior utilización en nuevas aplicaciones»¹². Por su parte, la innovación es, ante todo, un hecho fundamentalmente económico consistente en la aplicación comercial de una idea. Para el propósito de este capítulo, la innovación en ciberseguridad/ciberdefensa consistirá en la transformación de ideas y conocimiento en productos, procesos o servicios nuevos, o significativamente mejorados, que tendrán difusión y aceptación entre los actores comprometidos en la protección del ciberespacio. Así, una ciberdefensa eficaz se nutrirá de innovación procedente en gran parte del esfuerzo inversor en I+D.

La importancia actual de la investigación y desarrollo en ciberseguridad descansa, entre otras razones, en el hecho de que existe suficiente evidencia de la falta de eficacia de los métodos tradicionales de ciberdefensa. Estos se basan principalmente en el empleo de métodos heurísticos, detección de *software* dañino mediante reconocimiento de determinadas secuencias de código, protección mediante cortafuegos o medidas de prevención de pérdida de datos como las copias de seguridad, que no se encuentran ya a la altura de poder contrarrestar las modernas amenazas a la ciberseguridad¹³. Es por ello que urge adoptar una aproximación más científica al problema, que habrá de centrarse en tres áreas de actuación donde se concentran los principales desafíos: productos (tecnología), procesos y personal (PPP).

En cuanto a la primera de estas áreas, objetivo importante de la innovación tecnológica será la obtención de productos resilientes, así como el desarrollo y puesta en explotación de métodos de defensa más sofisticados, tales como el aprendizaje en profundidad (*deep learning*), que se van a basar en la inteligencia artificial y en el aprendizaje automático (*machine learning*) y que puede resultar de gran valor en la detección temprana de amenazas. Por su parte, la criptología, el análisis forense o la gestión de identidades continuarán constituyendo objetivos que también merecerán atención preferente. En todo caso, la ciberdefensa deberá ser efectiva en cuanto a su coste. Esto es, deberá centrarse en conseguir protección a un coste permisible, proporcionando defensas que sean capaces de, o bien impedir los ataques, o bien

¹² Freeman, Christopher. «The Economics of Industrial Innovation», The MIT Press, Cambridge, 1982.

¹³ Greengard, Samuel. «Cybersecurity Gets Smart». En: *Communications of the ACM*, vol. 59, n.º 5, May 2016, p. 29.

hacerlos extremadamente difíciles, de manera que resulten muy costosos a los perpetradores. Sin embargo, según el investigador Daniel Genki y otros «el problema de crear *hardware* o *software* económicos que mitiguen adecuadamente toda clase de ataques, incluidos los ataques de canal lateral¹⁴ sigue sin resolver»¹⁵. De aquí que aún quede un largo camino por recorrer en investigación en ciberseguridad.

La innovación en procesos es un concepto que lleva la innovación más allá de la transición tecnológica entre el espacio de la I+D y el de su uso práctico, al tratar de involucrar a los operadores en el proceso de cambio desde el principio. Ello es especialmente aplicable al ámbito de la ciberseguridad debido a la naturaleza cambiante de las tácticas empleadas por las amenazas.

Finalmente, área de especial atención de la innovación es la de los recursos humanos, el personal, por cuanto su disponibilidad con la adecuada formación, cualificación técnica y adiestramiento específico es clave tanto para mantener el estado deseado de ciberseguridad como para enfrentarse con éxito a las amenazas a la seguridad nacional en el ciberespacio.

La investigación y el desarrollo

Las ciberamenazas explotan en su favor la complejidad de las arquitecturas de los sistemas de información y telecomunicaciones existentes hoy día, que mediante sofisticadas técnicas informáticas como la computación en la nube y la virtualización proporcionan servicio a millones de dispositivos móviles y fijos. El carácter dinámico y distribuido de estas arquitecturas dificulta las actividades de ciberdefensa elementales como son la prevención, detección y respuesta en tiempo útil ante ciberataques. De aquí que resulte imprescindible un esfuerzo inversor en investigación y desarrollo de soluciones que permitan afrontar este desafío. Es de destacar en este sentido que la Agencia de Defensa Europea (EDA) ha identificado noventa y nueve proyectos de investigación y desarrollo de acuerdo con su *Agenda de investigación en ciberdefensa* (CDRA, *Cyber Defence Research Agenda*), que abordan asuntos tan variados como el aseguramiento del *software*, el establecimiento de repositorios de datos de investigación, la protección de sistemas móviles y empotrados, y la lucha contra la falsificación de identidades en el ciberespacio, entre otros.

¹⁴ Conocidos en inglés como *side-channel attacks*, un «ataque de canal lateral» es un ataque criptológico a un criptosistema basado en la información obtenida de la implementación física del mismo, en lugar de explotar una debilidad algorítmica o de efectuar un ataque por fuerza bruta. Por ejemplo, las emanaciones electromagnéticas del criptosistema, su consumo de energía o incluso los sonidos que produzca podrían aportar información susceptible de ser explotada para romper el sistema.

¹⁵ Hewitt, Carl. «Future Cyberdefenses Will Defeat Cyberattacks on PCs», en: *Communications of the ACM*, vol. 59, n.º 8, Aug 2016, p. 8.

A continuación efectuaremos un repaso de los temas prioritarios en investigación y desarrollo en ciberseguridad: resiliencia, consciencia situacional del entorno en cuanto a ciberseguridad, criptología, sistemas de detección de intrusiones y código dañino e intercambio de información sobre ciberseguridad.

Resiliencia

Últimamente se ha extendido el uso del término resiliencia en multitud de contextos diferentes. Entre otras definiciones, la Directiva de Política Presidencial de la Casa Blanca define resiliencia como «la capacidad de prepararse para y adaptarse a condiciones cambiantes, y resistir y recuperarse rápidamente de las disrupciones», incluyendo «la capacidad para resistir y recuperarse de ataques deliberados, accidentes, incidentes y amenazas procedentes de la naturaleza»¹⁶.

En ciberseguridad, la resiliencia tiene que ver con la robustez de los sistemas y su capacidad de recuperación frente a acciones hostiles. Asumiendo que los ataques a redes y sistemas de información, así como las entradas ilegítimas en los mismos, son inevitables, constituye todo un reto encontrar cómo lograr mantener inalteradas un conjunto mínimo predeterminado de funciones críticas, lo que denominaremos «resiliencia». Si hasta ahora se ha oído principalmente hablar de la protección de los sistemas, a partir de ahora el siguiente objetivo es disponer de sistemas resilientes, es decir, capaces de recuperarse frente a ciberataques. También se puede argumentar que la ciberresiliencia trata de la gestión, que no la eliminación, de los riesgos, una vez fijado un nivel de riesgo aceptable para el entorno considerado.

Imponer un requisito operativo de resiliencia a los sistemas implica que las nuevas tecnologías habrán de posibilitar el cumplimiento de la misión para la que han sido diseñados dichos sistemas, aun cuando se encuentren bajo ataque. De aquí que la investigación aplicada resulte fundamental para el desarrollo de estas tecnologías, sin olvidar que una resiliencia efectiva en cuanto al coste se logra, de nuevo, como conjunción óptima de tres factores: técnicos, humanos y procedimentales.

Consciencia situacional

La mejora de la consciencia situacional¹⁷ del entorno en cuanto a ciberseguridad es uno de los objetivos más importantes que se fijan a la

¹⁶ Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21), The White House, Washington DC, 2013.

¹⁷ Conocida en inglés como *situation awareness* o *situational awareness* (SA), la consciencia situacional es el conocimiento inmediato del entorno mediante la percepción de los sucesos y elementos del mismo en relación con el tiempo o el espacio, la comprensión de su significado y la posibilidad de inferir su estado futuro tras el cambio de alguna variable como puede ser la ocurrencia de un suceso predeterminado o bien el mero transcurso del tiempo.

hora de adquirir una capacidad de ciberdefensa. Se trata de uno de los temas difíciles en la investigación en ciberseguridad y ciberdefensa, y abarca materias tan variadas como: métricas de consciencia situacional, valoración dinámica del riesgo para el aseguramiento de la misión, monitorización continua y análisis del tráfico de red, técnicas de visualización y análisis de las visualizaciones y evaluación de la efectividad de la consciencia situacional en ciberdefensa. Al igual que con la resiliencia, será necesario disponer de las herramientas, *hardware* y *software*, apropiadas, el personal adecuadamente formado y los procedimientos adaptados.

Existen numerosas iniciativas para fomentar la investigación y desarrollo en esta materia. Como botón de muestra mencionaremos las llevadas a cabo por dos organizaciones multinacionales comprometidas con el I+D en ciberseguridad: la Alianza Atlántica y la Agencia de Defensa Europea (EDA).

Por un lado, la Organización para la Ciencia y la Tecnología (STO) de la OTAN aprobó en 2015 una actividad denominada, no sorprendentemente, *Cyber Defence Situation Awareness* (IST-148), con la finalidad de investigar de manera colaborativa a escala internacional los temas antes citados para dar respuesta a esta apremiante necesidad operativa¹⁸.

Y por el otro lado, también la Agencia de Defensa Europea ha identificado la consciencia situacional en ciberdefensa como una carencia que ha de ser abordada, a fin de proporcionar a las autoridades una visión clara del escenario de amenazas realmente existente, de manera que estas puedan dimensionar adecuadamente los recursos para combatirlas, así como para gestionar eficazmente los riesgos en ciberseguridad durante las fases de planeamiento y de conducción de las operaciones. Con este propósito la EDA está impulsando el proyecto *Cyber Situation Awareness Package* (CySAP)¹⁹.

Criptología

Los productos criptológicos seguirán desempeñando un papel muy destacado en los métodos de ciberdefensa, por cuanto son esenciales para autenticar sujetos, mantener la confidencialidad y la integridad de la información, evitar el repudio y registrar las acciones ejecutadas en el sistema a efectos de imputación de responsabilidades. Al fin y al cabo, estos productos serán esencialmente implementaciones de funciones criptológicas emanadas de un proceso de investigación. Sin embargo, resulta curioso descubrir que, a pesar de que la criptología se encuentra latente en casi cualquier producto

¹⁸ https://www.cso.nato.int/ACTIVITY_META.asp?ACT=8921. Fecha de la consulta: 10 de agosto de 2016.

¹⁹ <https://www.eda.europa.eu/info-hub/press-centre/latest-news/2016/02/24/business-case-on-cyber-situation-awareness-package-agreed>. Fecha de la consulta: 10 de agosto de 2016.

o proyecto relativo a ciberseguridad, es difícil encontrar programas de investigación y desarrollo específicamente dedicados al avance de esta disciplina (investigación básica) o al desarrollo de nuevos sistemas o protocolos criptológicos propios²⁰. Se puede considerar una excepción, no obstante, la iniciativa CriptoRed²¹.

Volviendo al asunto de la protección contra los «ataques de canal lateral», que introducíamos anteriormente, en Estados Unidos, el experto Carl Hewitt ha defendido que sea el Departamento de Defensa quien inicie un programa de investigación y desarrollo de ciberdefensas potentes y económicas para ordenadores personales utilizando tecnologías como las jaulas de Faraday para procesadores, acopladores ópticos, filtros para las fuentes de alimentación eléctrica o el etiquetado de memoria²².

Y para finalizar esta breve pincelada, quedaría reseñar que la introducción del concepto *Internet of Things* en el mundo militar hace especialmente importante y necesaria la continuación de la investigación en criptología.

Computación confiable

Un sistema confiable es aquel del que se tiene la seguridad de que puede hacer valer una política de seguridad especificada con un determinado nivel de confianza. La computación confiable²³ será pues aquella en la que el sistema informático se comportará consistentemente de la forma esperada. Una forma de lograr este objetivo consiste en la integración de un subsistema criptográfico conocido como *Trusted Platform Module (TPM)* cuyo *hardware* ha de ser capaz de almacenar una clave de cifrado de manera inaccesible al resto del sistema.

La protección de sistemas de mando y control militar, y de sistemas empujados en plataformas como vehículos, equipos de radio y sistemas de armas es extremadamente importante para salvaguardar las misiones militares y la vida e integridad física de los participantes en las mismas. El empleo de técnicas de computación confiable proporciona en estos casos una garantía de seguridad difícilmente alcanzable por otros medios.

La implantación de la computación confiable basada en los *TPM* en plataformas computacionales ordinarias (ordenadores personales o dispositivos móviles) ha sido, no obstante, fuertemente criticada por voces prominentes

²⁰ DÁVILA MUÑOZ, Jorge. «Criptología y Seguridad». Cuadernos Cátedra ISDEFE-UPM n.º 4, ETSI de Telecomunicación, Madrid, 2008.

²¹ Criptored es una red temática iberoamericana de criptografía y seguridad. <http://www.criptored.upm.es>

²² HEWITT, Carl. «Future Cyberdefenses Will Defeat Cyberattacks on PCs», en: «Communications of the ACM», vol. 59, n.º 8, Aug 2016, p. 8.

²³ *Trusted computing*.

dentro de la comunidad científica²⁴ y del activismo en la Red²⁵, por considerarlo una amenaza contra la privacidad de los consumidores y una forma de encadenar a estos a los fabricantes de *hardware* y *software*. Es por ello necesario proseguir la investigación en computación confiable de manera que se pueda alcanzar una solución que incremente la ciberseguridad general en la sociedad sin socavar derechos considerados irrenunciables por los ciudadanos.

Sistemas de detección de intrusiones, código dañino y amenazas persistentes avanzadas.

La detección de amenazas persistentes avanzadas (*APT*, *Advanced Persistent Threats*) es otro asunto necesitado de investigación, ya que los productos comerciales alcanzan como mucho un 80 % de detecciones positivas de código dañino y ello no es suficiente. Además, es imperativo detectar estas *APT* en una escala de tiempos significativamente más baja: horas en vez de días o semanas.

Por otra parte, debido a que los métodos tradicionales de protección contra estas amenazas (prevención de pérdida de datos mediante copias de seguridad, uso de herramientas defensivas como los cortafuegos, detección de código dañino en función de su firma digital o, simplemente, la heurística) resultan hoy día poco eficaces, la investigación está centrándose en adoptar nuevas técnicas basadas en inteligencia artificial y en aprendizaje automático con el fin de construir modelos defensivos radicalmente diferentes. El objetivo es mejorar la identificación de comportamientos y patrones sospechosos, y así poder construir entornos de seguridad auto-adaptativos con el fin de ganar resiliencia con la mínima intervención humana. Las técnicas empleadas se basan en tecnologías como *Big Data*, correspondencia de patrones, computación cognitiva y métodos de aprendizaje profundo que intentan simular la forma de funcionamiento de la mente humana²⁶.

Como muestra de la importancia que se concede a la mejora de la efectividad en la detección de las *APT*, la Agencia de Defensa Europea, al amparo del programa *Pooling & Sharing*, está impulsando el proyecto *MASFAD* (*Multi-agent System for Advanced Persistent Threat Detection*) consistente en un sistema de detección de amenazas persistentes avanzadas a integrar en sistemas de información para el mando y control militar²⁷. Actualmente se

²⁴ Anderson, Ross. «Trusted Computing' Frequently Asked Questions. TC/TCG/LaGrande/NGSCB/Longhorn/Palladium/TCPA. Version 1.1 (August 2003)», disponible en: <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>. Fecha de la consulta: 1 de agosto de 2016.

²⁵ Stallman, Richard. «Can You Trust Your Computer?», disponible en: <https://www.gnu.org/philosophy/can-you-trust.en.html>. Fecha de la consulta: 1 de agosto de 2016.

²⁶ Greengard, Samuel. «Cybersecurity Gets Smart». En: *Communications of the ACM*, vol. 59, n.º 5, May 2016, p. 29.

²⁷ MEES, Wim, y DEBATTY, Thibault. «Multi-agent System for APT Detection». En: «Proceedings of the 2014 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW'14)», IEEE Computer Society, Washington DC, USA, 2014, pp. 401-406.

dispone de un demostrador tecnológico de *MASFAD* y se está trabajando en una segunda fase del proyecto denominada *MASFAD II*.

Intercambio de información sobre ciberseguridad.

Un reto importante que encara la comunidad de ciberdefensa a escala global es la adquisición, integración e intercambio de información sobre amenazas y ataques en tiempo real. Es más, este intercambio de información dentro de las propias organizaciones no suele estar automatizado, dependiendo en gran medida de la intervención de operadores humanos, siendo por ello que existe un margen para la mejora de la calidad y eficiencia de esta comunicación donde juega su papel la automatización de los intercambios de información. Por ejemplo, resulta muy ineficiente que la implementación de contramedidas frente a determinadas amenazas se haga de manera redundante por diferentes organizaciones que funcionan aisladamente, cuando podrían trabajar colaborativamente si dispusieran de un marco de trabajo normalizado.

Por ello existe la necesidad operativa de conseguir la integración coherente de representaciones normalizadas y estructuradas de la información relevante, incluyendo análisis de patrones de ciberataque. En este sentido encontramos dos iniciativas dignas de mención: *CYBEX* y *STIX*.

CYBEX (*Cybersecurity Information Exchange Framework*), como su propio nombre indica, es un marco de intercambio de información sobre ciberseguridad que está siendo estandarizado por la Unión Internacional de Telecomunicaciones (*ITU*). Este marco de trabajo describe la forma en que la información sobre ciberseguridad ha de ser intercambiada entre las entidades de ciberdefensa²⁸ a escala global y cómo se asegura este intercambio. Los proponentes de este estándar sostienen que la implementación de *CYBEX* a escala mundial minimizaría la dispersión de la información y posibilitaría una respuesta más rápida y eficaz contra las amenazas²⁹.

STIX (*Structured Threat Information eXpression*) es esencialmente un lenguaje estructurado para definir información e inteligencia sobre ciberamenazas³⁰. Sus casos de uso incluyen el análisis, la especificación de patrones de indicación, la gestión de actividades de prevención y respuesta, así como la compartición de información sobre estas amenazas. Se trata de un producto resultante de I+D llevado a cabo por MITRE³¹, entidad que, no obstante, lo

²⁸ Por ejemplo los CERT y CIRT.

²⁹ Rutkowski, Anthony, *et al.* «CYBEX: the cybersecurity information exchange framework (x.1500)». En: *SIGCOMM Computer Communications Review*, n.º 40, 5 de octubre de 2010, pp. 59-64.

³⁰ <https://makingsecuritymeasurable.mitre.org/docs/stix-intro-handout.pdf>. Fecha de la consulta: 17 de septiembre de 2016.

³¹ La Corporación MITRE es una empresa pública estadounidense sin ánimo de lucro que gestiona centros de investigación y desarrollo financiados con fondos del Gobierno Federal de los Estados Unidos. Véase: <http://www.mitre.org>

licencia sin restricciones de uso³². Lo interesante de este proyecto es que, una vez iniciado por MITRE, es continuado en forma de esfuerzo colaborativo por los usuarios pertenecientes a la comunidad de interés en inteligencia de amenazas en el ciberespacio.

Innovación

La innovación en ciberseguridad se ha de abordar de manera coherente en tres áreas de actuación: tecnologías (productos), procesos y recursos humanos (personas).

Innovación en productos

La innovación tecnológica en ciberseguridad debe ser la consecuencia directa del esfuerzo en investigación y desarrollo. La gran ventaja de la que disfrutan estos productos es que se basan en tecnologías de uso dual y ello debería suponer un incentivo para que los distintos actores implicados en la seguridad del ciberespacio (Gobiernos y Administraciones Públicas, industrias y organismos de investigación) decidan compartir los riesgos y beneficios de encarar juntos los retos que se presentan en este terreno. Según Michael Sieber, antiguo jefe de la Unidad de Superioridad en la Información del Área de Capacidades y Armamento de la Agencia de Defensa Europea, el carácter dual de estas tecnologías brinda la oportunidad de compartir el esfuerzo de enfrentarse a los desafíos en ciberseguridad³³.

Detección de amenazas, análisis forense, plataformas de adiestramiento en ciberdefensa, así como de mando y control de operaciones en el ciberespacio son algunas de las áreas donde aún existe un gran espacio abierto para la innovación.

Innovación en procesos

En ciberdefensa, este tipo de innovación está relacionada con cambios en la dirección y organización bajo la que se desarrollan las actividades defensivas; se trata en esencia, de una innovación doctrinal que ha de posibilitar una mayor inteligencia de la situación y un mejor aprovechamiento de los recursos disponibles, humanos, financieros y materiales. En general, se distinguen dos tipos de innovaciones de procesos: a nivel externo y a nivel interno. En el contexto de la ciberdefensa, las de nivel externo se refieren a la constitución de redes de cooperación con otros agentes nacionales e internacionales empeñados en el esfuerzo ciberdefensivo y al intercambio real de información entre los mismos. A nivel interno se identifican las innovaciones dirigidas a mejorar el rendimiento del trabajo en equipo, de manera

³² Se encuentra libremente disponible en: <https://stixproject.github.io>

³³ —, «Bricks to build a cyber shield», EuropeanDefenseMatters, issue 9, European Defense Agency, Brussels, 2015, p.10.

que resulte más eficiente la ciberdefensa (reducción de escalas de tiempo, de horas a minutos, por ejemplo).

Según MITRE, una ciberdefensa eficaz depende en gran medida de la rápida respuesta a las tácticas cambiantes de las amenazas³⁴. Para su implementación se introduce la idea de «innovación en las operaciones», que no es más que una variante de la innovación en procesos. Es un concepto que lleva la innovación más allá de la transición tecnológica entre el espacio de la I+D y el de su uso práctico, al intentar involucrar a todos los participantes en el proceso defensivo: operadores, administradores de sistemas, desarrolladores o analistas de amenazas, de manera que todos deben ser innovadores con el fin de llevar la delantera a los creadores de ciberamenazas.

Innovación en recursos humanos

El hombre sigue siendo el elemento fundamental de la acción también en el ciberespacio. Las más avanzadas tecnologías son virtualmente inútiles si no son utilizadas por personal adecuadamente adiestrado en su manejo. En Estados Unidos el Consejo Asesor de Seguridad Interior considera que una amenaza de seguridad apremiante es la escasez de personal especializado en ciberseguridad, por el consecuente vacío defensivo que se produce y que aparece como una invitación al ataque y a la materialización de las amenazas³⁵.

Las políticas innovadoras en recursos humanos son muy variadas y van desde la incentivación de la profesionalización de la ciberseguridad a las que simplemente impulsan la capacitación del personal o promueven la captación de personal especializado a través de la organización de cibercompeticiones que atraigan a los más capaces y motivados. Tampoco se pueden olvidar las que promueven la educación y mentalización sobre riesgos de todos los usuarios del ciberespacio, trabajen o no en ciberseguridad.

Resulta, pues, imperativo atender este aspecto y desarrollar políticas innovadoras en relación con el personal especializado en ciberseguridad. Ello no es sencillo si se tiene en cuenta el elenco de ocupaciones que contempla esta disciplina, desde las tecnológicas, altamente especializadas, hasta las de carácter gerencial, enfocadas en la administración, dirección y control de las actividades.

En conclusión, la implantación con éxito de una idea novedosa implica una creación de valor, pero será solo la puesta en práctica de una política de innovación coherente en las tres dimensiones (productos, procesos y personas) la que sea capaz de crear la sinergia necesaria para afrontar con éxi-

³⁴ <https://www.mitre.org/capabilities/cybersecurity/operational-innovation>. Fecha de la consulta: 20 de septiembre de 2016.

³⁵ Homeland Security Advisory Council, «Cyber Skills Task Force Report», Department of Homeland Security, Washington, DC, 2012.

to retos de la talla de los planteados por organizaciones como *The Shadow Brokers* o el *Equation Group*.

Necesidad de una actuación específica de I+D+i en ciberseguridad

La defensa en el nuevo escenario de confrontación que constituye el ciberespacio³⁶ exige la disponibilidad de una capacidad ciberdefensiva, en cuya obtención la innovación continua en productos, procesos y recursos humanos desempeña un papel crucial. A su vez, esta capacidad de innovación vendrá principalmente determinada por la apropiada transición de productos y tecnología de ciberseguridad desde el espacio de la I+D al de su empleo operativo.

La adopción de una adecuada estrategia de investigación, desarrollo e innovación en materia de ciberseguridad deviene, pues, en una necesidad insoslayable. España cuenta con la Estrategia Española de Ciencia y Tecnología y de Innovación (EECTI)³⁷, en el marco de la cual se sitúa el planeamiento de la I+D+i en ciberseguridad, sin perjuicio de que, dado su carácter transnacional, también es abordada a nivel de Unión Europea. Por otro lado, circunscrita al ámbito exclusivo de los equipos y sistemas con finalidad específicamente militar, la Estrategia de Tecnología e Innovación de la Defensa (ETID) del Ministerio de Defensa contempla actuaciones en ciberdefensa, en línea con la EECTI.

Asimismo, la actuación en I+D+i específica para la ciberseguridad nacional debe ser coherente no solo con la estrategia global del Estado en tecnología e innovación, la EECTI, sino también con las estrategias de seguridad y ciberseguridad en vigor. A continuación repasaremos estos planteamientos, enfocados desde la perspectiva de la I+D+i.

La Estrategia de Seguridad Nacional

La Estrategia de Seguridad Nacional (ESN)³⁸ concibe la seguridad aplicando un enfoque integral, de manera amplia e interdisciplinar, a nivel nacional, europeo e internacional extraeuropeo, involucrando también a la sociedad civil en los ámbitos de interés prioritario de la Seguridad Nacional. Precisamente la ESN identifica el ciberespacio como uno de estos ámbitos de actuación preferente, al ser considerado un escenario accesible, poco regulado y de difícil control, donde pueden tener lugar amenazas contra la seguridad nacional³⁹.

³⁶ —, «El ciberespacio: Nuevo escenario de confrontación», Monografías del CESEDEN n.º 128, CESEDEN, Madrid, 2012.

³⁷ —, «Estrategia Española de Ciencia y Tecnología y de Innovación (2013-2020)», Ministerio de Economía y Competitividad, Madrid, 2013.

³⁸ —, «Estrategia de Seguridad Nacional: un proyecto compartido», Presidencia del Gobierno, Madrid, 2013.

³⁹ ESN, p. 26.

La ESN señala la relación de dependencia entre innovación y seguridad en el marco de la seguridad económica de la nación, de suerte que, para garantizar esta, propugne, entre otras medidas, la incentivación de un modelo de crecimiento económico sostenible que «potencie la productividad, el tejido empresarial, la innovación y la competitividad»⁴⁰. En este sentido, es pertinente reseñar que ya la anterior Estrategia Española de Seguridad de 2011 (EES) declaraba explícitamente que «quedarse por detrás de nuestros competidores en capacidad de innovación tendrá un serio impacto en nuestra competitividad y desarrollo y, por tanto, en nuestra seguridad»⁴¹.

También identifica la ESN la ciberseguridad no como un mero aspecto técnico de la seguridad sino como un eje fundamental de nuestra sociedad y sistema económico, ya que «España está expuesta a los ciberataques, que no solo generan elevados costes económicos, sino también, y lo que es más importante, la pérdida de confianza de los ciudadanos en unos sistemas que, en la actualidad, resultan críticos para el normal funcionamiento de la sociedad»⁴².

En relación con la I+D+i, una de las actuaciones que propone la ESN para afianzar la seguridad en el ciberespacio a nivel nacional es la «promoción de la capacitación de profesionales en ciberseguridad» y el «impulso a la industria española a través de un Plan de I+D+i»⁴³, aunque sin abordar el asunto de la independencia tecnológica, como sí lo hiciera su antecesora, la Estrategia Española de Seguridad de 2011, al propugnar el apoyo al desarrollo de empresas privadas nacionales en un sector estratégico como el de la ciberseguridad, «en el que puede ser peligrosa la dependencia de empresas extranjeras»⁴⁴.

La Estrategia de Ciberseguridad Nacional

La Estrategia de Ciberseguridad Nacional (ECSN) constituye un segundo escalón de desarrollo sectorial de la Estrategia de Seguridad Nacional⁴⁵. Constituye una línea de respuesta a las ciberamenazas, una de las circunstancias que la EES identifica en su capítulo 4, sobre amenazas, riesgos y respuestas, como potencialmente atentatoria contra la seguridad nacional⁴⁶. Como objetivo global, la ECSN se plantea «lograr que España haga un uso seguro de los sistemas de información y telecomunicaciones, fortaleciendo las capaci-

⁴⁰ ESN, p. 44.

⁴¹ —, «Estrategia Española de Seguridad: una responsabilidad de todos», Gobierno de España, Madrid, 2011, p. 38.

⁴² ESN, p. 27.

⁴³ ESN, p. 42.

⁴⁴ EES, p. 68.

⁴⁵ —, «Estrategia de Ciberseguridad Nacional», Presidencia del Gobierno, Madrid, 2013, p. 3.

⁴⁶ EES, p. 65.

dades de prevención, defensa, detección y respuesta a los ciberataques»⁴⁷, para lo cual, entre otras medidas, establece que «será necesario potenciar, impulsar y reforzar las capacidades nacionales de investigación y desarrollo en ciberseguridad de las TIC⁴⁸». En el caso de la defensa, la ECSN indica también que «además de mejorar las capacidades de los sistemas militares de defensa y de inteligencia es necesario reforzar la seguridad de los sistemas de información y comunicación estratégicos, adaptándolos a los nuevos riesgos y amenazas del ciberespacio»⁴⁹.

En lo que se refiere al I+D+i, la ECSN es explícita. Detalla que para alcanzar soluciones nacionales confiables «se requiere fomentar y mantener una actividad de I+D+i en materia de ciberseguridad de manera efectiva»⁵⁰. En particular, la ECSN contempla una línea de acción, la sexta, que se ocupa precisamente del tema que nos interesa (conocimientos, competencias e I+D+i), con la intención de «promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad»⁵¹. Merece la pena analizar esta línea de acción pues es donde convergen las diferentes estrategias: por un lado, la de seguridad nacional, de la que la estrategia de ciberseguridad nacional es solo una especialización sectorial, y, por otro lado, la estrategia española de ciencia, tecnología e innovación. Entre otras medidas, esta línea de acción contempla las siguientes actuaciones⁵²:

1. Extender y ampliar los programas de captación de talento, investigación avanzada y capacitación en ciberseguridad en cooperación con universidades y centros especializados.
2. Fomentar el desarrollo industrial de productos y servicios en materia de ciberseguridad por medio de instrumentos, entre otros, como el Plan Estatal de Investigación Científica y Técnica y de Innovación e iniciativas de apoyo a su internacionalización.
3. Impulsar la coordinación nacional y la dinamización del sector industrial y de servicios de ciberseguridad para la mejora de la competitividad, la internacionalización, la identificación de oportunidades, la eliminación de barreras y la orientación normativa, entre otras actividades.
4. Impulsar las actividades de certificación de ciberseguridad de acuerdo con las normas y estándares de reconocimiento internacional, incluyendo estos criterios en los procesos de desarrollo y adquisición de productos o sistemas.

⁴⁷ —, «Estrategia de Ciberseguridad Nacional», Presidencia del Gobierno, Madrid, 2013, p. 21.

⁴⁸ ECSN, p. 22.

⁴⁹ ECSN, p. 23.

⁵⁰ ECSN, p. 26.

⁵¹ ECSN, p. 37.

⁵² *Idem. Ibid.*

5. Impulsar modelos y técnicas de análisis de ciberamenazas y medidas de protección de productos, servicios y sistemas, así como su especificación, evaluación y certificación.

Como vemos, esta línea de acción es ambiciosa, está bien trazada, define adecuadamente el qué y apunta en algunos casos el cómo (Plan Estatal de Investigación Científica y Técnica y de Innovación), pero no han faltado voces críticas respecto a la misma. Por ejemplo, el investigador Dávila Muro considera que, declaraciones de intenciones aparte, los resultados permitirán evaluar si la ECSN tiene vocación de proporcionar soluciones al futuro cibernético de nuestra sociedad o si por el contrario, en sus propias palabras, este documento se trata tan solo de «un puente hasta la redacción del siguiente»⁵³. Es decir, la sexta línea de acción de la ECSN delinea un conjunto de intenciones a nivel estratégico, pero es necesario pasar de la estrategia a la táctica: cómo, cuándo y con qué recursos acometer en la práctica todas esas iniciativas determinarán el éxito o el fracaso de la acción estratégica. Como mínimo, una financiación específica y adecuada a la magnitud del empeño sería condición necesaria, aunque no suficiente, para el éxito.

La Estrategia Española de Ciencia, Tecnología e Innovación.

La Estrategia Española de Ciencia, Tecnología e Innovación 2013-2020 (EECTI)⁵⁴ recoge en su objetivo general cuarto la necesidad de orientar la investigación hacia los grandes desafíos del futuro⁵⁵, y, más concretamente, hacia la ciberseguridad como parte del objetivo específico sobre seguridad, protección y defensa⁵⁶. Además, prescribe que el I+D+i en ciberseguridad debe alinear la política española en esa materia con los objetivos perseguidos por la Unión Europea a través del programa Horizonte 2020, de manera que se facilite el acceso de los agentes españoles a las fuentes de financiación comunitarias.

En cuanto a su implementación, corresponde a los planes estatales de ciencia y tecnología y de innovación el desarrollo y financiación, por parte de la Administración General del Estado, de las actuaciones contenidas en la EECTI. El Plan Estatal de Investigación Científica y Técnica y de Innovación

⁵³ Dávila Muro, Jorge. «La estrategia de ciberseguridad nacional y otros buenos deseos». En: *Revista SIC*, n.º 108, febrero de 2014.

⁵⁴ —, «Estrategia Española de Ciencia, Tecnología e Innovación 2013-2020», Ministerio de Economía y Competitividad, Madrid, 2013. Disponible en: http://www.idi.mineco.gob.es/st-fls/MICINN/Investigacion/FICHEROS/Estrategia_espanola_ciencia_tecnologia_Innovacion.pdf

⁵⁵ EECTI, p. 26. El apartado 4.4 formula el objetivo general IV: Investigación orientada a los retos de la sociedad.

⁵⁶ EECTI, p. 31. El apartado 4.4.8 plantea el objetivo específico 8: Seguridad, protección y defensa.

(PEICTI) para el periodo 2013-2016⁵⁷ contempla la ciberseguridad como un reto para «la economía y la sociedad digital»⁵⁸, así como para «la seguridad, protección y defensa»⁵⁹.

La Estrategia de Tecnología e Innovación de Defensa

La Estrategia de Tecnología e Innovación de Defensa (ETID)⁶⁰ es el marco general en el que se deben situar los distintos planes y actividades de los agentes dedicados a la I+D+i de la defensa, y nace con la intención de «mejorar la gestión de la I+D+i del Ministerio de Defensa, de forma que se tenga un mayor aprovechamiento de las oportunidades para potenciar su situación dentro del marco nacional e internacional de la innovación aplicable a la defensa»⁶¹.

La I+D+i de la defensa, como parte de la I+D+i nacional, debe ser plenamente consistente con los objetivos de la EECTI. Por un lado, la ETID se encuentra alineada con las acciones programáticas y los objetivos tecnológicos del reto en seguridad, protección y defensa del Plan Estatal de Investigación Científica, Técnica y de Innovación⁶². Por otro lado, la ETID limita la ciberdefensa al ámbito de los sistemas de información y comunicaciones para el mando y control militar, para los que define dos metas tecnológicas: la automatización de las acciones ante ciberataques⁶³ y la inteligencia cibernética y disminución de la cibermovilidad del enemigo⁶⁴.

Estrategia de Ciberseguridad de la Unión Europea.

La Estrategia de Ciberseguridad de la Unión Europea (ECSUE)⁶⁵ se centra en dos áreas: tecnología y capacitación del personal. En lo referente a tecnología, la ECSUE identifica los siguientes temas abiertos a la innovación: criptología, protección de sistemas militares (plataformas y sistemas empujados), sistemas autónomos y capacitación mediante adiestramiento y formación.

⁵⁷ —, «Plan Estatal de Investigación Científica y Técnica y de Innovación 2013-2016», Ministerio de Economía y Competitividad, Madrid, 2013. Disponible en: http://www.idi.mineco.gob.es/stfls/MICINN/Investigacion/FICHEROS/Plan_Estatal_Inves_cientifica_tecnica_innovacion.pdf

⁵⁸ PEICTI, p. 38.

⁵⁹ PEICTI, p. 39.

⁶⁰ —, «Estrategia de Tecnología e Innovación de Defensa», Ministerio de Defensa, Madrid, 2015. Disponible en: [http://www.tecnologiaeinnovacion.defensa.gob.es/Lists/Publicaciones/Attachments/205/ETID %202015.pdf](http://www.tecnologiaeinnovacion.defensa.gob.es/Lists/Publicaciones/Attachments/205/ETID%202015.pdf)

⁶¹ ETID, presentación del secretario de Estado de Defensa.

⁶² PEICTI, p. 39; ETID, p. 22.

⁶³ Meta tecnológica 6.5.1, ETID, anexo I, p. 62.

⁶⁴ Meta tecnológica 6.5.2, ETID, anexo I, p. 62.

⁶⁵ —, «Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN(2013) 1 final», European Commission, Brussels, 7/2/2013. Disponible en: https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

Prioridades clave de esta estrategia son la ciberdefensa en el marco de la política común de seguridad y defensa de la Unión Europea, la necesidad de un marco de política de ciberdefensa de la Unión Europea, la mejora de las capacidades ciberdefensivas de los Estados miembros, sinergias cívico-militares y cooperación con otras partes interesadas, incluso más allá de las fronteras comunitarias. Como actuación derivada de la puesta en práctica de esta estrategia el Consejo de Europa adoptó en 2014 un marco para la definición de una política de ciberdefensa⁶⁶ que esboza principios generales para facilitar la cooperación con el sector privado en lo que se refiere al desarrollo de una capacidad de ciberdefensa, con un especial enfoque en el fortalecimiento de la investigación y el desarrollo tecnológico, así como de la base tecnológica e industrial europea de defensa⁶⁷. Por último, cabría reseñar que la Unión Europea, por medio de la Comisión Europea, tiene prevista comenzar la financiación directa del I+D en ciberdefensa a través de la Acción Preparatoria del próximo programa marco de investigación y desarrollo, ya que la ciberseguridad es uno de los cuatro temas principales de dicha acción.

Consideraciones sobre el camino a seguir en I+D+i en ciberseguridad

La actuación en I+D+i en ciberseguridad ha de articularse en torno a los ejes prioritarios marcados en la EECTI y, a su vez, debe estar alineada con una política de ciberseguridad nacional, de manera que se oriente al logro del objetivo global de la Estrategia de Ciberseguridad Nacional, que no es sino «lograr que España haga un uso seguro de los sistemas de información y telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques»⁶⁸.

En lo que respecta a la I+D de defensa se advierte que aún queda camino por recorrer. Por un lado, se observa que su carácter eminentemente finalista puede constituir en ocasiones un lastre en materia específica de ciberdefensa, por cuanto no promueve la investigación básica, que es un aspecto crítico en ciberseguridad. Por otro lado, la I+D de defensa está enfocada en las aplicaciones con un fin específicamente militar, mientras que los productos y tecnologías en seguridad cibernética tienen un carácter dual. Luego es imperativo atraer a la I+D+i militar a nuevos agentes que antes dirigían sus actividades hacia el mundo comercial civil, por lo que una actuación en este sentido solo puede tener éxito si se dan los suficientes incentivos para que ambas partes obtengan beneficios. A título de ejemplo, encontrar un adecuado equilibrio en términos de propiedad intelectual entre empresas y Administración es clave para incentivar la innovación.

En todo caso será preciso de nuevo diferenciar entre I+D (confinado a la comunidad investigadora tanto académica como industrial, tanto en el sector

⁶⁶ EU Cyber Defence Policy Framework, noviembre de 2014.

⁶⁷ *European Defence Technological and Industrial Base (EDTIB)*.

⁶⁸ ECSN, p. 21.

público como en el privado) e innovación, proceso en el que es necesario involucrar a mayor número de actores. Ambos deben ser abordados en sus respectivos contextos, debiendo identificar de manera temprana necesidades presentes y futuras en materia de ciberseguridad, tanto provenientes del sector público como del privado. Igualmente importante será también saber realizar la transición de productos y tecnología de ciberseguridad desde el espacio de la I+D hasta el mercado⁶⁹.

La inversión en I+D+i en ciberseguridad

Habida cuenta de que el escenario de la ciberdefensa es relativamente nuevo, que todavía se están conformando sus estructuras organizativas (algunas cambiarán en los Estados miembros de la Unión Europea con la transposición de la Directiva NIS a más tardar en 2018) y que algunos países no tienen su modelo presupuestario preparado para reflejar las inversiones en ciberseguridad (menos todavía I+D+i en ciberseguridad), no existe mucha información identificable y contrastada sobre esta materia.

Sin embargo, sí hay datos suficientes en diversas esferas y partidas que permiten hacerse una idea razonable de la situación, tanto en algunos Estados como en organizaciones supranacionales e internacionales (por prudencia, y más a la velocidad a la que avanza la preocupación por la inseguridad digital, es pertinente señalar aquí que algunos de estos datos están sometidos a posible modificación).

En Europa, por ejemplo, se espera destinar cerca de 1.800 millones de euros de aquí al año 2020 para financiar la I+D+i en tecnologías, productos y servicios de ciberseguridad. El mecanismo utilizado ha sido la firma en 2016 de un acuerdo entre la Comisión Europea con la *European Cyber Security Organization (ECS)*, un instrumento de CPP al que más tarde se aludirá.

Sin salir de Europa, es de obligada mención la carta que en octubre de 2016 remitieron los ministros de Defensa de Francia, Alemania, Italia y España a sus colegas del resto de países de la Unión Europea para, tras el *Brexit*, fortalecer la defensa europea, dotarla de autonomía estratégica y estudiar la creación de un Consejo de Ministros de Defensa europeos.

El movimiento tendrá consecuencias positivas para la ciberdefensa militar, la I+D+i y la CPP, por cuanto se apuesta por «consolidar una base tecnológica e industrial europea de defensa capaz de gestionar tecnologías clave, proveer las necesarias capacidades militares en el futuro y reforzar nuestra autonomía de decisión»⁷⁰.

⁶⁹ En Estados Unidos, la DHS S&T Cyber Security Division tiene por misión precisamente esto.

⁷⁰ González, Miguel. «Los cuatro grandes de la Unión Europea apuestan por una defensa común con "autonomía estratégica"», *El País*, 15 de octubre de 2016, http://internacional.elpais.com/internacional/2016/10/14/actualidad/1476449123_095969.html

Durante el desarrollo de la conferencia NITEC 2016 en el verano de 2016, la OTAN anunció la inversión de 3.000 millones de euros en ciberseguridad para reforzar capacidades frente a posibles ciberataques.

Como es sabido, la OTAN dispone del Centro de Excelencia de Ciberseguridad en Tallin (Estonia), del que España es miembro fundador. Precisamente dicho Centro se ubicó allí por el ciberataque que sufrió hace años este país europeo, un suceso que marcó el inicio de la toma de conciencia por los Gobiernos y Estados occidentales de la importancia de la ciberdefensa.

El Centro de Excelencia de Ciberseguridad tiene información actualizada y precisa del estado de la ciberseguridad a gran escala.

En la Cumbre de Varsovia en julio de 2016, la OTAN expuso el estado del arte de su incubadora de proyectos en el ámbito de la ciberseguridad, que se desarrolla en el contexto de la relación de la propia OTAN con actores de la industria a través de la OTAN *Industry Cyber Partnership (NICP)*⁷¹, y eje de sus espacios colaborativos orientados a la innovación.

La *NATO Industry Cyber Partnership* es una iniciativa formal, aprobada por los veintiocho países aliados durante la Cumbre celebrada en Gales (2014) y presentada días después en el encuentro de ciberseguridad celebrado en Mons (Bélgica). A través de *NICP* la Alianza busca impulsar la cooperación con el sector privado en base a los siguientes principios: mejorar la ciberseguridad en la cadena de suministro de defensa de la OTAN; aumentar la comprensión y el conocimiento sobre las ciberamenazas y riesgos mutuos, incluyendo el intercambio de información; contribuir a los esfuerzos de la Alianza en educación, formación y realización de ciberejercicios; mejorar el intercambio de las mejores prácticas y conocimientos sobre la preparación y recuperación; ayudar a la OTAN y aliados a aprender de la industria.

El acercamiento al sector privado establecido se guía por tres principios; a saber: cooperar con el sector privado con el objetivo principal de reforzar la protección de las propias redes de la OTAN; dar la bienvenida a la cooperación con las empresas más innovadoras de los países de la OTAN de forma abierta, transparente e inclusiva; y crear sinergias a través de la construcción, el esfuerzo y la garantía de una coherencia en las iniciativas existentes con la industria.

Estados Unidos⁷², el país en el que se gestó y desarrolló Internet, y en el que la Administración Obama nombró en 2016 a un *CISO (Chief Information Security Officer)* Federal, viene destinando desde hace años ingentes cantidades de recursos para atender la ciberseguridad y perfeccionar en un ciclo continuo sus capacidades de ciberdefensa en prevención, explotación y ataque.

⁷¹ <http://www.nicp.nato.int>

⁷² <https://whitehouse.gov>

El aumento de la tensión en la campaña presidencial durante 2016 por la exfiltración de información de servidores del Partido Demócrata y posterior filtración masiva llevó a una escalada de ciberguerra fría, en la que Estados Unidos indicó públicamente que la autoría de estos hechos (ciberataque) era responsabilidad de Rusia, reservándose el derecho a responder mediante un ciberataque proporcionado. Al hecho, le sucedió —esté o no relacionado— un ciberataque de denegación de servicio de significativas proporciones a entidades privadas de Estados Unidos.

Para el año 2017 Estados Unidos ha presupuestado una inversión en ciberseguridad de 19.000 millones de dólares (17.183 millones de euros), lo que supone un incremento de 5.000 millones de dólares (alrededor de 4.520 millones de euros) respecto al presupuesto de 2016. De los 19.000 millones de dólares, 3.100 millones de dólares (2.804 millones de euros) se destinarán a la modernización tecnológica en varias agencias federales y 62 millones de dólares (algo más de 56 millones de euros) a la ampliación de esfuerzos para atraer y retener a profesionales cualificados en ciberseguridad que trabajen para la Administración estadounidense.

Por su parte, el Cyber Command de Estados Unidos está reforzando su fuerza cibernética con la estructuración de ciento treinta y tres equipos montados a partir de seis mil doscientos militares, civiles y personal de apoyo de todos los departamentos militares y componentes del área de defensa. Este cibercomando estaría plenamente operativo en 2018, aunque ya se están empleando mecanismos al servicio de los objetivos de la Administración en todo el espectro de sus operaciones cibernéticas.

Las operaciones en el ciberespacio motivadas por la amenaza del islamismo radical violento ha provocado que en abril de 2016 el secretario de Defensa, Ash Carter, afirmara que el Pentágono planeaba invertir 35.000 millones de dólares —alrededor de 32.000 millones de euros— en ciberseguridad para reforzar las capacidades militares ofensivas y defensivas.

Estados Unidos destina a I+D+i notables recursos, sabedor de que tales inversiones se traducen en ventajas a corto, medio y largo plazo. Su ecosistema le permite no solo alinear las sinergias del sector privado y del público, sino mantener continuamente engrasada la maquinaria de la innovación y su encaje en el mercado, nutriéndose, además, de iniciativas foráneas a las que metaboliza vía inversiones de capital-riesgo.

Canadá⁷³ dispone de un Plan de Acción en materia de ciberseguridad para el periodo 2015-2020. Como parte de este Plan, se prevé la inversión de 2.009 millones de dólares (1.393 millones de euros), de los cuales 1.513 millones de dólares (1.049 millones de euros) se destinarán a la defensa y 439 millones de dólares (304 millones de euros) al aumento de la seguridad nacional.

⁷³ <http://budget.gc.ca>

Otros Estados del continente americano también están planeando su esfuerzo para invertir en ciberseguridad, incluido el capítulo de alguna línea de I+D+i. Prácticamente todos manifiestan interés por este frente, aunque el estado de madurez en Latinoamérica y Caribe no es homogéneo.

Hay que reseñar que la Organización de Estados Americanos (OEA), con la que las estructuras de la ciberseguridad nacional española, particularmente a través de INCIBE, mantienen una creciente colaboración, tiene en su hoja de ruta acciones al respecto, aunque muy vinculada con la protección de infraestructuras críticas y la persecución del ciberdelito y no tanto en lo referente a la ciberdefensa militar. Los países de la «vieja Europa» también están realizando esfuerzos en varios frentes.

Reino Unido⁷⁴, hoy más de actualidad que nunca por el *Brexit*, es un Estado que considera la buena gestión de su ciberseguridad como un valor diferencial en lo social y lo económico. Invertirá, entre 2015 y 2020, 1.900 millones de libras esterlinas (2.225,5 millones de euros) en su protección frente a ciberataques y en el desarrollo de capacidades soberanas en el ciberespacio. Espera generar por ello más de cien mil empleos directos.

En abril de 2016, el Gobierno británico anunció una inversión de 40 millones de libras (46,8 millones de euros) para el *Cyber Security Operations Centre (CSOC)*, como parte de sus planes para referenciar las capacidades de ciberseguridad operativa de su Ministerio de Defensa. Y en octubre de ese mismo año, el secretario de Defensa, Michael Fallon, asignó 265 millones de libras (293,4 millones de euros) a este Ministerio para fines de ciberseguridad.

Reino Unido dispone de un ramo industrial orientado a la ciberseguridad, que es un ingrediente esencial para gozar de una razonable independencia tecnológica en algunos frentes de la ciberdefensa.

En junio de 2016, Francia⁷⁵ anunció una inyección de 1,5 millones de euros para aumentar sus capacidades de defensa en la «guerra cibernética», algo señalado como estratégicamente prioritario por el ministro de Defensa del país galo. El presupuesto francés de 2016 para la defensa alcanza los 32.000 millones de euros, manifestándose un fuerte compromiso con la modernización.

Alemania⁷⁶ es otro Estado nuclear de la Unión Europea. Su ministra de defensa dio a conocer en abril de 2016 los planes para establecer una nueva fuerza cibernética para mejorar la eficacia de defensa de las Fuerzas Armadas, el *Kommando Cyber- und Informationsraum (KdoCIR)*. Este Comando para la Ciberseguridad y la Información tendrá acceso a unos fondos de inversión de más de 1.000 millones de euros y sus operaciones tendrán el centro de mando en Bonn para supervisar las tareas operativas como la cibernética,

⁷⁴ <http://blog.rielcano.org>

⁷⁵ <http://www.defense.gouv.fr>

⁷⁶ <http://faz.net>

informática, de comunicaciones militares e información geológica. A tal fin, las capacidades TI existentes de la *Bundeswehr* (Fuerzas Armadas) se agruparán a partir de abril de 2017 dentro de la nueva rama de la cibernética e información espacial (CIR) y se asignará un total de trece mil quinientos puestos de otras ramas CIR, que será dirigida por un inspector con el grado de teniente general.

Para proveer de personal a este «ciberejército» se tiene previsto crear en 2018 un grado específico en la Universidad del Ejército alemán en Munich, donde se aspira a formar también un *cluster* de ciberdefensa con participación de empresas del sector privado.

Estas iniciativas se unen a la campaña de reclutamiento de efectivos en el campo de la ciberseguridad, que cuenta con un presupuesto de 3,6 millones de euros, y a la creación del Departamento Cyber/TI (CIT) dentro del Ministerio de Defensa con un director de la Información al frente que asumirá la responsabilidad.

Italia⁷⁷ destina menos recursos a TIC que Francia y Alemania. Su presupuesto en I+D+i orientado a la ciberdefensa y a la ciberdefensa en sí es limitado. En 2015 el presupuesto general militar alcanzó los 1.000 millones de euros y en 2016, según las informaciones disponibles, tiene presupuestados 2.000 millones para ciberseguridad, defensa y cultura. En abril de ese mismo año se presentó el «Framework Nazionale per la Cyber Security».

Si vamos a otro rincón del globo, llegamos a Australia⁷⁸. En abril de 2016 se anunció el desarrollo de una nueva estrategia contra ciberataques para el periodo 2016-2017, que contará con un presupuesto de 230 millones de dólares (157,4 millones de euros) para la creación de cien nuevos puestos de trabajo y aumentar las capacidades gubernamentales de ciberseguridad. Esta inversión complementa la que se deduce de las medidas para la próxima década centradas en la mejora de las capacidades cibernéticas y de inteligencia de defensa, contenidas en el Libro Blanco de Defensa 2016.

La nueva estrategia también incluye el fortalecimiento de las ciberdefensas, la creación del ciberembajador y la designación de un especialista para asistirlo en la materia.

El esfuerzo en ciberseguridad de otros países, como Turquía o Japón, no es fácilmente cuantificable, y menos en I+D+i. Sí, ciertamente, puede afirmarse que el segundo mencionado, Japón, país altamente tecnificado y con un potente sector industrial de TIC, seguramente atenderá a través de su Plan Nacional del Ministerio de Defensa a diez años (dividido en dos periodos de cinco, 2014-2018 y 2019-2023) la potenciación de las capacidades de ciber-

⁷⁷ <http://www.cybersecurityframework.it> ; <http://sicurezzanazionale.gov>

⁷⁸ <http://www.zdnet.com>

defensa en el contexto de nuevas capacidades de guerra y la creación de una «Fuerza Dinámica Conjunta de Defensa» (*Dynamic Joint Defense Force*).

Rusia es una potencia que utiliza la fuerza militar. No es conocido su nivel de inversión en ciberseguridad y ciberdefensa; sin embargo, fuentes cercanas a su Ministerio de Defensa han declarado a una publicación especializada en ciberseguridad⁷⁹ que podría estar entre los 200 y 250 millones de dólares USA (entre 180 y 225 millones de euros) al año.

Sobre China tampoco hay demasiados datos contrastables. Este país dispone de un gran sector de TIC y los analistas no dudan en afirmar que sus inversiones en I+D+i en ciberseguridad son considerables y crecientes. China dispone de estructuras en consonancia con el tamaño del país.

En marzo de 2016, anunció la puesta en marcha de su primera organización pública para la ciberseguridad, *The Cyber Security Association of China*, compuesta por instituciones académicas, expertos y empresas de Internet. La organización se centra en promover la autodisciplina en la industria, a fin de acelerar el establecimiento de estándares en ciberseguridad y promover la cooperación internacional. El objetivo último es salvaguardar la ciberseguridad del país y la conversión de China como una gran potencia en Internet, atrayendo además a empresas de ciberseguridad vanguardistas y talento.

Ya en febrero de 2016, China aprobó una inversión destinada a ciberseguridad con un capital inicial de 300 millones de yuanes (alrededor de 41 millones de euros)⁸⁰.

Irán es mención obligada. Cuando en 2013 Hasan Rohani asumió el cargo de presidente de Irán, según un informe de la organización británica *Small Media*, titulado «Iranian Internet Infrastructure and Policy Report»⁸¹, los fondos para ciberseguridad de este país para el bienio 2013-2014 alcanzaron los 42.073 millones de riales iraníes (algo más de 1 millón de euros). Al año siguiente se disparó hasta los 178.800 millones de riales iraníes (algo más de 5 millones de euros); y en 2015-2016 llegó a los 550.000 millones de riales iraníes (aproximadamente 15,5 millones de euros), lo que supone un incremento del 1.200 % en solo tres años.

Muy posiblemente, los ataques de Stuxnet (2010) y Flame (2012), y los escándalos de las filtraciones de la NSA en Estados Unidos, hayan jugado un papel relevante en la fortificación de las ciberdefensas iraníes frente a ciberrataques, específicamente cibersabotajes. Y no es de dudar que hayan sido un estímulo para sentar las bases de una capacidad ofensiva, rasgo que hoy hay que entender como un indicador del grado de avance de un Estado. Sea

⁷⁹ <http://ieee.es>

⁸⁰ <http://www.gadgetsnow.com/tech-news/China-launches-first-cybersecurity-organization-report/articleshow/51561355.cms> ; <http://www.scmagazineuk.com>

⁸¹ <http://europe.newsweek.com>

con los productos, herramientas y servicios mediante una I+D+i propia o de terceros.

Y si Irán es cita obligada, también lo es Arabia Saudí⁸², que en el año 2015 detectó más de 160.000 ataques al día, convirtiéndose en el país más atacado de Oriente Medio, según las cifras disponibles. La mayoría de los objetivos se concentraron en los sectores de las telecomunicaciones, el petróleo, el gas y la banca.

Se espera que el mercado de ciberseguridad de Arabia Saudí pase de los 1.510 millones de dólares de 2013 hasta los 3.480 millones de dólares en 2019, con una tasa de crecimiento anual del 14,50 %. Esta es una señal inequívoca del esfuerzo inversor de las agencias gubernamentales y Gobiernos locales de este país.

India es otro país que presta una extraordinaria atención a la ciberseguridad. En 2014-2015, su departamento de TI destinó 1.160 millones de rupias indias (15,7 millones de euros) a la seguridad cibernética. Además se ha propuesto establecer un Centro Nacional de Coordinación Cibernética (CNCC) con un presupuesto separado de 10.000 millones de rupias indias, más de 136 millones de euros⁸³.

De acuerdo con el informe del Consejo de Seguridad de Datos de la India (*SDIC*), el tamaño del mercado de la ciberseguridad de este país es de aproximadamente 4.000 millones de dólares (más de 3.500 millones de euros), y se espera que crezca hasta los 35.000 millones de dólares (32.000 millones de euros) en el año 2025⁸⁴.

Asimismo, India ha estado buscando ayuda para formarse en las mejores prácticas en seguridad cibernética. A principio de 2016, una delegación oficial encabezada por funcionarios del Gobierno indio y empresarios del país visitó Londres, La Haya e Israel. Según diversos medios, Israel ha ofrecido colaboración a la India para preparar un plan de ciberseguridad integral⁸⁵.

India, considerado por las multinacionales como un país atractivo para la deslocalización del desarrollo de aplicaciones, dispone de una ingente cantidad de profesionales muy bien formados en matemáticas y en ciencias de la computación. Su industria de ciberseguridad destaca en no pocos frentes, uno en especial es el de las herramientas IRM con seguridad de grado militar.

No sería de recibo concluir sin mencionar a Israel, el Estado que desde poco antes de la explosión del uso comercial de Internet es el símbolo del éxito del fomento estatal de la I+D+i en ciberseguridad y del triunfo comercial de

⁸² <http://www.think-progress.com> ; <http://www.mcit.gov.sa>

⁸³ <http://articles.economictimes.indiatimes.com>

⁸⁴ <http://www.enterpriseinnovation.net>

⁸⁵ <http://economictimes.indiatimes.com>

empresas especializadas, hoy multinacionales sólidamente asentadas y/o adquiridas por las grandes multinacionales de la industria TIC.

En el ejemplo de Israel trasciende el hecho de la I+D+i, porque ha sabido construir un ecosistema que ha culminado en un modelo de CPP digno de elogio, motivo por el que se estudiará su caso en el siguiente apartado.

Conclusión

La inversión de los Estados, las organizaciones internacionales y las supranacionales en I+D+i orientada a la ciberseguridad y a la ciberdefensa no es, en líneas generales, un capítulo presupuestario asentado. Al menos no lo es como en otros frentes más experimentados en el contexto de los complejos industriales de las defensas y los centros de investigación y universidades.

Las estructuras públicas de la ciberseguridad y la ciberdefensa tienen pocos años de vida y en la mayoría de países todavía están sometidas a cambio y no han empezado a engranarse de modo óptimo en las maquinarias de I+D+i.

Si a ello le sumamos que el ciberespacio es especialmente dinámico, sus fundamentos no estuvieron orientados a la seguridad de la información (salvedad hecha de la disponibilidad de las comunicaciones) y al uso comercial generalizado, y que la criticidad de la ciberseguridad todavía no ha sido completamente metabolizada ni por los Estados ni por las industrias y los centros de conocimiento, y convertida en procesos ágiles que permitan a unos prever y saber qué quieren en grano fino y a otros servirlo y proponer avances en una suerte de mercado estable y creciente, la conclusión está a la vista: queda casi todo por hacer en una sociedad inmersa en un proceso imparable de transformación digital que traerá, sin duda, cambios en el proceso clásico de I+D+i, en la localización y aprovechamiento de las canteras de talento y en la forma en la que se manifiesten las amenazas y ataques, porque en un futuro no muy lejano casi cualquier persona tendrá medios a su disposición para ciberatacar, configurándose un escenario de asimetría extrema.

El papel de la colaboración público-privada en el proceso de I+D+i

La colaboración público-privada (CPP) está ligada a las sociedades que aspiran a lograr cotas crecientes y sostenibles de bienestar, guardando un equilibrio entre el alcance de los poderes del Estado y las capacidades de la iniciativa privada.

La base del modelo es, por tanto, la colaboración leal entre las estructuras públicas y las organizaciones que operan en el sector privado.

Las sociedades más evolucionadas son aquellas que se han dotado de un ecosistema sostenible para la CPP; es decir, uno en el cual ambas partes obtienen ventajas y beneficios directos e indirectos conforme a derecho y

a buenas prácticas. Este ecosistema, además, se extiende al escenario de relaciones exteriores y al de las organizaciones supranacionales e internacionales, como no puede ser de otra manera en la era de la globalización.

La CPP es un mecanismo nuclear en la ya mencionada Estrategia Española de Ciencia y Tecnología e Innovación 2013-2020. Y en lo que toca a la ciberseguridad, forma parte de la doctrina de la Estrategia de Ciberseguridad Nacional-ECSN, que el Gobierno de España define como «... El marco de referencia de un modelo integrado basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado, en la colaboración público-privada y en la participación de la ciudadanía». Algo similar expresó la Unión Europea en su Estrategia Europea de Ciberseguridad, y lo mismo han hecho numerosos países en sus documentos correspondientes.

Si hay un frente de la ciberseguridad en el que la CPP adquiera una especial significancia, ese es el de la I+D+i. Así se expresa en el Objetivo V de la ECSN, centrado en «Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad», al indicar que «... Se requiere fomentar y mantener una actividad de I+D+i en materia de ciberseguridad de manera efectiva». Y que para ello «... «Será necesaria una adecuada coordinación del conjunto de agentes implicados en las TIC, facilitando la colaboración entre empresas y organismos públicos de investigación...».

Más adelante, en la Línea de Acción 5, «Seguridad y resiliencia de las TIC en el sector privado», se resalta la necesidad de impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.

Esta Línea de Acción está íntimamente ligada a la Línea de Acción 6, «Conocimientos, Competencias e I+D+i», en la que se expresa la necesidad de promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad.

También hay referencias a la CPP y la I+D+i, ya directas ya indirectas, en la Agenda Digital para Europa, la Agenda Digital para España y el Plan de Confianza en el Ámbito Digital.

Por tanto, y en el caso de España, está sobradamente justificada la obligación de poner a punto un ecosistema de CPP para alcanzar una buena posición en I+D+i en la ciberseguridad a efectos generales y también en la defensa y en las operaciones militares. Y no hay que olvidar aquí que, al igual que la mayoría de las infraestructuras críticas existentes en España se gestionan por multinacionales cotizadas, también el mayor porcentaje de la inversión y el gasto en I+D+i en ciberseguridad la realizan compañías de ciberseguridad y de TIC (en general, también multinacionales cotizadas), cuyo beneficio mercantil no proviene de las adquisiciones de productos y servicios por la defensa, aunque el germen del ciberespacio fuera, en origen, una solución

académica para minimizar riesgos asociados con la indisponibilidad de la red de comunicaciones académico-militar ARPANET, y por mucho que ciertos desarrollos de fabricantes destacados de TIC y de ciberseguridad de la llamada «era Internet», hoy liberados para uso civil, hayan tenido su génesis en la cobertura de necesidades de la inteligencia y de la defensa militar.

En la actualidad, se tiene la sensación de que el llamamiento por parte de las áreas no civiles de los Estados al sector civil para que se propongan soluciones a necesidades de las defensas no es el motor principal que mueve la I+D+i y que, a la postre, se traduce en avance social. Quizá esta circunstancia, que pudiera ser no coyuntural, deba interpretarse como un rasgo de la transformación digital.

Iniciativas foráneas

Hay algunos ejemplos ilustrativos de iniciativas de CPP en I+D+i, o en los que la I+D+i encuentra acomodo. El más significativo por su dimensión, y en el que nos centraremos, es el emprendido por el Estado de Israel en el desierto del Neguev, en el que se ha creado un parque especializado en ciberseguridad, denominado CyberSpark⁸⁶, que aúna en una misma localización geográfica a instituciones académicas (la Universidad Ben Gurion), la industria tecnológica y las Fuerzas de Defensa de Israel (FDI).

La intención del Gobierno israelí es trasladar a las inmediaciones del Parque, inaugurado en 2016, a unos treinta mil soldados de la Unidad 8200 —incluidas las unidades de seguridad cibernética— que, a su vez, trabajarán estrechamente con la Autoridad Nacional de Seguridad Cibernética.

CyberSpark ya ha atraído a numerosas empresas multinacionales, con las que las instituciones públicas israelíes mantienen una relación *win to win*. Además, en el Parque se han instalado tres incubadoras y existen seis *startups* que dan empleo a unas mil doscientas personas.

Israel es un país que lleva a gala su potencial en ciberseguridad, una industria que se constituye en uno de los motores de su economía: genera más de 6.000 millones de dólares al año, exporta por valor de 3.500 millones de dólares y cuenta con unas cuatrocientas treinta empresas instaladas y cuarenta centros de ciberseguridad y de I+D de multinacionales extranjeras.

CyberSpark encuentra sitio en el Parque de Tecnologías Avanzadas (ATP), inaugurado en 2013 por el primer ministro Benjamin Netanyahu.

Esta experiencia es actualmente una de las más avanzadas a nivel mundial en lo que respecta a la CPP en I+D+i en ciberseguridad y ofrece notables ventajas a Israel, ya que potencia su industria de ciberseguridad en el circuito internacional y, al tiempo, la integra con otras áreas de las TIC, como las

⁸⁶ <http://cyberspark.org.il>

vinculadas con la *IoT*, las infraestructuras críticas, el sector financiero, el de telecomunicaciones o el espacio exterior.

En principio, «CyberSpark no está comprometido con cualquier operación o desarrollo ofensivo»⁸⁷.

Iniciativas supranacionales

En Europa se ha creado la Organización Europea de Ciberseguridad (European Cyber Security Organization, *ECS*)⁸⁸, una entidad autofinanciada y sin ánimo de lucro en la que participan asociaciones empresariales, grandes compañías y pymes, centros de investigación y universidades, que se cataloga como asociación público-privada sobre ciberseguridad europea.

La Comisión Europea firmó en julio de 2016 un acuerdo CPP con la *ECS* orientado a la promoción, la investigación y la innovación en seguridad cibernética. Para guiarse en los objetivos marcados se ha formado un órgano, denominado *Partnership Board*, integrado por miembros de la Comisión Europea y miembros de la *ECS*, que llevará a cabo un análisis exhaustivo del programa de trabajo en ciberseguridad del plan Horizonte 2020, la ejecución del gasto total y todas las materias relacionadas con la I+D, además de acomodar las actualizaciones necesarias del plan de trabajo plurianual y de realizar un seguimiento de los compromisos contraídos en el acuerdo público-privado firmado. La inversión total comprometida podría alcanzar los 1.800 millones de euros hasta 2020.

El Instituto Nacional de Ciberseguridad, INCIBE, se ha adherido a *ECS* como punto de contacto oficial de España junto a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI) y el Centro para el Desarrollo Tecnológico Industrial (CDTI), en esta asociación en la que hay entidades españolas participantes que han trabajado, trabajan o pueden trabajar en la ciberdefensa española.

INCIBE también ha promovido la creación en España de RENIC, la Red de Excelencia Nacional de Investigación en Ciberseguridad, que ya es miembro de pleno derecho de la *ECS*.

La *ECS* articulará sus acciones en base a las siguientes líneas de acción:

- Colaborar con la Comisión Europea y las Administraciones Públicas nacionales para promover la investigación y la innovación (I+I) en ciberseguridad.
- Desarrollar e invertir en proyectos piloto de demostración y de impulso al mercado para facilitar llevar la innovación al mercado de ciberseguridad.
- Favorecer la competitividad y el crecimiento de la industria de la ciberseguridad en Europa (grandes empresas y pymes) para facilitar a los

⁸⁷ Declaraciones a *SIC* (n.º 120) de Roni Zehavi, *CEO* de CyberSpark.

⁸⁸ *ECS*: www.ecs-org.eu

usuarios finales/operadores tecnologías innovadoras, aplicaciones, servicios y soluciones.

- Apoyar la implantación en el mercado de las mejores tecnologías innovadoras y servicios de ciberseguridad para su uso profesional y privado.
- Promover y ayudar en la definición e implementación de una política industrial de ciberseguridad para fomentar el uso de soluciones de ciberseguridad, así como soluciones TIC seguras y confiables a escala europea para aumentar la autonomía digital.
- Apoyar el desarrollo y los intereses de todo el ecosistema de la ciberseguridad y la seguridad de las TIC.

La financiación de esta iniciativa de CPP se hará del siguiente modo: por parte de la Unión Europea se fija una inversión de 450 millones de euros. Por parte de los actores representados en la ECS se liberarán tres euros por cada euro invertido por la Unión Europea. Se espera, por tanto, que este mecanismo desencadene una inversión total, como ya hemos comentado, de 1.800 millones de euros de aquí al año 2020.

España

La inversión en ciberdefensa es baja —y manifiestamente mejorable— para un país con la posición de España, al igual que la dedicada a I+D+i, no registrándose además iniciativas evolucionadas de CPP. Por decirlo de alguna manera: si se destinara a la ciberseguridad militar las decenas de millones de euros que cuesta adquirir un solo cazabombardero o un tanque o los elementos no ciber de un barco de guerra, España sería una potencia francamente destacada; hecho que es extrapolable a muchos otros países, incluso europeos. Aunque semejante decisión hoy debería estar avalada por un cálculo de riesgos en el que se analizaran las ciberamenazas, la probabilidad de materialización, el valor de los activos (entre los que está la información) que pudieran verse afectados, el impacto y el problema que pudiera causar a España, directa o indirectamente, disponer de un cazabombardero, un tanque o un barco menos (si es que el momento actual fuera propicio para las adquisiciones).

No obstante lo dicho, el Mando Conjunto de Ciberdefensa (MCCD) firmó en 2016 un acuerdo a tres años con opción de prórroga con INCIBE para, entre otras acciones, colaborar en la generación de conocimiento científico y tecnológico mediante el concurso de equipos de investigación del ámbito académico, apoyar la transferencia de los resultados de la I+D+i a las Administraciones y llevar a cabo iniciativas conjuntas de formación de profesionales en ciberseguridad y ciberdefensa.

Igualmente, el MCCD firmó en 2016 un acuerdo con el Centro Criptológico Nacional (CCN) por el que estableció un marco de colaboración en varios frentes, uno de ellos centrado en el desarrollo de proyectos tecnológicos.

El MCCD ha activado acuerdos con algunas universidades españolas para dotarse de algunos instrumentos esenciales para el cumplimiento de su misión. Hay dos iniciativas que podemos referenciar, una centrada en el desarrollo de una herramienta *software* de generación de escenarios de ciberdefensa, que se integre en el campo de maniobras del MCCD, y la otra enfocada al desarrollo de una solución orientada a la visualización completa de la situación de la ciberdefensa en un momento dado. Ambos proyectos fueron presentados en las II Jornadas del MCCD en mayo de 2016.

De otro lado, INCIBE, que ha lanzado diversas acciones para estimular el crecimiento de la I+D+i, y está potenciando la conformación de un Polo Tecnológico Nacional de Ciberseguridad, a modo de *atractor* de los distintos agentes involucrados, para apoyar la industrialización, I+D+i en la ciberseguridad, y conectarla con rutas de internacionalización, terreno en el que colabora ICEX España Exportación e Inversiones.

A estas iniciativas mencionadas se suman otras estrictamente privadas, llevadas a cabo por algunas multinacionales de origen español, principalmente centradas en promover y/o adquirir *startups* en nuevos frentes de la ciberseguridad. Estas iniciativas, aunque no se enmarquen en la CPP estrictamente, tienen implicaciones en parte del ecosistema en el que encuentra sitio esta y la I+D+i, puesto que algunas toman forma en el marco de la colaboración entre la industria privada usuaria de TIC, la industria proveedora de TIC y servicios, la universidad y la investigación, tratando de estimular nuevas ideas y enfoques que puedan cristalizar en futuras líneas de desarrollo industrial, principalmente en el control de ciberfraude, la identificación y autenticación enfocadas al *scoring*, la minimización de riesgos intencionales, la ingeniería de datos y la analítica predictiva.

Las multinacionales de sectores estratégicos (también las de origen español) están invirtiendo en I+D+i para ir dominando su transformación digital. Y en sus enfoques han incorporado la gestión de riesgos de ciberseguridad.

Estos movimientos, en principio ajenos en el momento presente a la ciberdefensa militar, quizá deban ser analizados por especialistas en la ciberseguridad militar porque van a delimitar el ecosistema digital de la sociedad a la que nos dirigimos, en la que la manifestación de conflictos ciberespaciales y ciberfísicos no entenderá de barreras conceptuales y postestativas, ni de la naturaleza de las organizaciones que han de defenderse y atacar en un marco de acuerdos intersupranacionales y cualquier investigación, disciplina, técnica o tecnología que facilite información y ventaja ha de valorarse.

Retos, riesgos y oportunidades

Las estructuras de la defensa están inmersas en el proceso de transformación digital que afecta a toda la sociedad y que trae consigo la analítica

avanzada de macrodatos, la robótica aplicada a casi todos los escenarios, la inteligencia artificial, la computación cognitiva, las tecnologías de comunicaciones avanzadas que soporten servicios de misión crítica incompatibles con la indisponibilidad y resilientes.

Por otro lado, gran parte de las estructuras de la defensa, a efectos generales, son usuarias de tecnologías de la información y comunicaciones de uso civil que padecen defectos de diseño en materia de seguridad, debido principalmente a los tiempos de mercado y la presión de los inversores.

En España (y a buen seguro también en otros países) la industria de la defensa en su conjunto no fue muy madrugadora a la hora de enarbolar la bandera de la ciberseguridad, que se configuró como ramo específico gracias a algunas pequeñas compañías especializadas muy competitivas y a algunos grupos pioneros de departamentos y áreas de grandes empresas. La facturación en 2015 de este ramo oferente en España supera los 1.000 millones de euros. Podemos formularnos la siguiente pregunta a modo de reflexión: ¿qué porcentaje de esa cifra se debe a inversiones de las estructuras del Ministerio de Defensa ampliamente entendidas y de la ciberdefensa militar en concreto?

El reto aquí es conformar en la industria de la defensa un ecosistema viable de empresas de ciberseguridad o con línea de ciberseguridad gestionadas por personas y equipos de personas que estén interesados en innovar y no en mantener el *status quo*. Tal ecosistema debería estar preparado para renovarse completamente (como el ave Fénix) sin empezar de cero. Y aquí juegan un papel esencial las empresas completamente establecidas, que son capaces de dar garantías financieras, continuidad a las líneas de industrialización, diagnosticar con una orientación a la mejora y la modernización, ayudar en la prescripción, facilitar la identificación de nuevos productos prometedores que aparecen en el mercado, realizar investigación y desarrollo... pero que hace ya tiempo dejaron de ser organizaciones punteras en innovación.

La oportunidad que se abre brinda la posibilidad de enfocar la fortaleza de la ciberseguridad de los sistemas TIC de la ciberdefensa, ampliamente entendidos, no en base al secreto y al número restringido de proveedores, sino en base a la verificación efectiva y formal del nivel de seguridad que se precisa. Y facilitar dichos sistemas, servicios y productos, y no otros, a quienes los tengan que usar.

Este hecho afecta a tecnologías concretas, que deberían estar holgadamente atendidas en los esfuerzos de I+D+i de la ciberdefensa⁸⁹:

- Comunicaciones seguras, autenticadas y auditadas en las redes, más allá de las de combate.

⁸⁹ Los frentes tecnológicos aludidos han sido analizados por el profesor Jorge Dávila Muro a lo largo de los años en su sección fija de *SIC* (www.revistasic.com) denominada «En construcción».

- Equipos/*gadgets* personales y de entretenimiento certificados para su uso exclusivo en entornos militares. El BYOD por ahora no puede ser una opción.
- Sistemas inalterables, redundantes y a «toda prueba» para la auditoría de comunicaciones y de documentos digitales (toda la información debería estar clasificada en su justo nivel y poder ser «atribuida» a alguien y con el control de quién la ve y qué hace con ella). Los sistemas modernos IRM están tecnológicamente maduros.
- Sistemas de actualización y mantenimiento remotos de equipos a prueba de intrusos y de errores. No debería arrancar ningún artefacto TIC sin que todos los componentes del mismo estén activamente verificados (*secure boot*).
- Sistemas que aseguren la integridad de las redes IT.
- Sistemas de identidad digital y personal intransferibles.
- Técnicas IT de engaño que ayuden a eliminar «canales laterales» de ataque que pudiesen poner de manifiesto directa o indirectamente actividades de interés militar por su reflejo en las actividades de la red.
- Sistemas TIC de contrainteligencia militar (pasiva y activa).
- Sistemas de todo tipo redundantes a prueba de fallos, una resiliencia automática y puntual, así como todas las medidas que permitan siempre tener un plan B y otro plan C en tiempo.
- Sistemas para el entrenamiento ciber de usuarios de todos los niveles.
- Investigar los tipos de analistas, especialidades de ciberseguridad y de perfiles de especialistas que va a necesitar a largo plazo la ciberdefensa.

La viabilidad de llevar esto a efecto no puede conseguirse en un mercado clásico, sino en uno diversificado en el que realmente la ciberdefensa contribuya y participe en iniciativas CPP de I+D+i en cuyo contexto tengan un papel creativo esos expertos con habilidades especiales a los que llamamos *hackers* y que siguen evolucionando con los tiempos. En suma, estudiar fórmulas para suscitar en la sociedad civil el interés por compartir sus ideas/innovaciones en ciberseguridad con la ciberdefensa.

Hay cuatro campos, entre otros, que conviene tratar en iniciativas de CPP + I+D+i, uno es el de la atribución de acciones en el ciberespacio, se decida o no dar curso a la apertura de conflicto. Se requiere, por tanto, estudiar y poner a punto sistemas de reconocimiento de ataques (y su origen) en «tiempo real» que involucren a la ciberdefensa militar y a otras estructuras de la ciberseguridad nacional, o solo a la ciberdefensa militar.

El segundo, aunque esté en fases muy tempranas, es el de la computación cuántica y sus implicaciones en la ciberseguridad, muy concretamente en lo que atañe a la criptografía y el criptoanálisis.

El tercero presenta hoy un grado de complejidad notable: cómo hacer más eficiente el sistema de certificación funcional de la seguridad de productos TIC. En el estado actual, los tiempos requeridos y el esfuerzo inversor son,

en ocasiones, disuasorios en términos de mercado sin que exista certeza por parte de la empresa que pone en evaluación sus productos de que serán adquiridos.

El cuarto pasaría por estudiar con un enfoque interdisciplinar qué protocolos y sistemas de notificación serían los más adecuados para que las estructuras actuales de la ciberseguridad puedan funcionar del modo más eficiente posible como un sistema integrado de ciberseguridad nacional, y señalamos aquí la defensa militar, la inteligencia (Centro Nacional de Inteligencia-CNI), la protección de infraestructuras críticas (Centro Nacional para la Protección de Infraestructuras Críticas-CNPIIC) y la seguridad interior.

Y en último término habría espacio en la I+D+i para estudiar muy por lo menudo, y aunque el asunto exceda con mucho lo ventilado en este capítulo, las implicaciones (técnicas, tecnológicas, sociales y económicas) que tendrá la puesta en explotación de sistemas de ciberseguridad desatendidos, autónomos y el uso de robots y asistentes cibernéticos de ciberseguridad.

Como es sabido, la mecanización esclaviza y la automatización excluye. Lo que está sucediendo en esta fase del *Homoceno* es que en los sistemas productivos de la sociedad global se puede prescindir de fuerza de trabajo. Y esos millones de personas, jóvenes en base a las expectativas de vida actuales, y con conocimientos y experiencia, antes de llegar a edades muy avanzadas, pueden ser útiles. La I+D+i y la CPP pueden ser instrumentos para aprovechar la sabiduría y la destreza que atesoran y, ya que hablamos de ciberseguridad, ganarlos para la noble causa de la concienciación.

Interdependencia entre innovación y ciberseguridad

En las modernas economías basadas en el conocimiento, este es reconocido como el propulsor de la productividad y la creación de valor a través de la innovación, que se configura así como la piedra angular del crecimiento económico y por ende del bienestar material de la sociedad⁹⁰. Hoy día el ciberespacio es el soporte fundamental de los procesos de innovación tanto en bienes como en servicios. La existencia de redes de comunicaciones universales, abiertas e interoperables, hace posible una potencial creación de valor de gran magnitud⁹¹, solo condicionada a la existencia de suficiente confianza en esas redes. En otras palabras, un ciberespacio seguro significa una garantía para los agentes económicos y ello se ha de traducir en mayor inversión, mayor transparencia y dinamización de los mercados y, en

⁹⁰ —, «The Knowledge-based Economy», Organisation for Economic Co-Operation and Development, París, 1996. Disponible en: <https://www.oecd.org/sti/sci-tech/1913021.pdf>

⁹¹ La Ley de Metcalfe establece que el valor de una red de telecomunicaciones es proporcional al cuadrado del número de usuarios o nodos conectados a dicha red. Atribuida a Robert Metcalfe, esta ley explica muchos de los efectos económicos producidos por las redes de comunicación como Internet o sus derivados la *World Wide Web* y las redes sociales.

consecuencia, crecimiento económico y prosperidad. Recíprocamente, es la innovación en ciberseguridad una de las actividades que permiten conservar la estabilidad del ciberespacio en términos de seguridad, de manera que sea confiable para los usuarios del mismo. Se da, pues, una realimentación positiva entre los procesos de innovación y de ciberdefensa.

La idea de que un ciberespacio seguro significa una ventaja económica competitiva para España ya había sido apuntada por la antigua Estrategia Española de Seguridad de 2011⁹². La actual Estrategia de Seguridad Nacional va más allá al señalar al «espionaje económico», que aprovecha las posibilidades que ofrecen las tecnologías de la información y las comunicaciones, como una amenaza cuyo «impacto potencial es cada vez mayor por su capacidad de dañar el sistema económico y afectar al bienestar de los ciudadanos»⁹³.

Pero será en particular la Estrategia de Ciberseguridad Nacional la que recoja explícitamente y en mayor extensión estos planteamientos. En su prólogo, el presidente del Gobierno afirma que «para España, los avances en el ámbito de la ciberseguridad contribuyen además a incrementar nuestro potencial económico, ya que promueven un entorno más seguro para la inversión, la generación de empleo y la competitividad»⁹⁴ y que «únicamente si nos comprometemos de forma decidida con la seguridad del ciberespacio, la competitividad de nuestra economía y la prosperidad de España serán una realidad posible»⁹⁵. Más aún, la Estrategia considera la ciberseguridad como «una necesidad de nuestra sociedad y de nuestro modelo económico»⁹⁶ y llama a la unidad de acción entre los diferentes actores, tanto públicos como privados, con el fin de alcanzar ese estado de ciberseguridad que a todos ha de beneficiar. Así, sostiene que «el fortalecimiento de la ciberseguridad proporcionará a las Administraciones Públicas, al tejido industrial y empresarial, a la comunidad científica y a los ciudadanos en general una mayor confianza en el uso de las TIC» y que «para ello, los organismos públicos responsables trabajarán en coordinación con el sector privado y con los propios ciudadanos para garantizar la seguridad y la confiabilidad de los sistemas que sustentan la llamada Sociedad de la Información»⁹⁷.

Pioneros en este concepto han sido países como Reino Unido y Estados Unidos. El primero aprobó en noviembre de 2011 su Estrategia Nacional de Ciberseguridad, cuyo primer objetivo consistía precisamente en «luchar contra el cibercrimen y convertir al Reino Unido en el lugar más seguro del mundo para hacer

⁹² EES, pp. 65 y 68.

⁹³ ESN, p. 34.

⁹⁴ ECSN, p. iv.

⁹⁵ ECSN, p. v.

⁹⁶ ECSN, p. 10.

⁹⁷ ECSN, p. 21.

negocios en el ciberespacio⁹⁸». En Estados Unidos, la Casa Blanca hizo pública en 2011 su «Estrategia Internacional para el Ciberespacio», la cual defendía que «el ciberespacio sirve a las necesidades de la economía y de los innovadores», siendo la ciberseguridad un factor crítico no solo para la seguridad nacional en términos generales sino para la seguridad económica en particular⁹⁹. Por su parte, el Departamento de Comercio del Gobierno de los Estados Unidos reconocía que internet es una pieza central en la política norteamericana de promoción del crecimiento económico de la nación y de orientación del modelo económico al mantenimiento del liderazgo de Estados Unidos durante el siglo XXI. De ahí que ese departamento ministerial oriente su esfuerzo normativo, aunque limitándose a Internet sin abarcar la totalidad del ciberespacio, a encarar los grandes retos que puedan minar la confianza en la Red, retos entre los que se encuentra la mejora sustancial de la ciberseguridad¹⁰⁰.

Hasta aquí observamos una concepción utilitarista del ciberespacio: se protege porque es garantía de beneficio económico, de lo que se deriva su utilidad social. Sin embargo, *sensu contrario*, encontramos que la innovación constituye un factor necesario, aunque obviamente no suficiente, para hacer posible el estado de ciberseguridad deseado. A escala global se aprecia que alcanzar un determinado estado de ciberseguridad es imposible sin innovación, y se desprende que a escala nacional alcanzar el deseado estado de ciberseguridad es inviable sin una I+D+i propia. Dicho de otra manera, sin una industria nacional de ciberseguridad puntera no es posible la construcción de un sistema nacional de ciberseguridad¹⁰¹.

Consciente de ello, aunque sin particularizarlo en el caso de la ciberseguridad, el Ministerio de Defensa en su Estrategia de Tecnología e Innovación de la Defensa (ETID) defiende que la innovación «supone, asimismo, una pieza fundamental para promover el crecimiento, la competitividad y la internacionalización de la BTID¹⁰², favorece su capacidad de respuesta ante nuevas necesidades tecnológicas y ayuda a evitar posibles dependencias tecnológicas futuras que condicionen la capacidad de respuesta ante situaciones sobrevenidas o que impliquen un coste excesivo en las adquisiciones»¹⁰³.

En este sentido, se constata que los países que están desarrollando un mayor esfuerzo inversor en ciberseguridad están obteniendo un rápido retorno de inversión (ROI) y se están convirtiendo en la referencia en exportación de tecnología, procesos y recursos humanos. Sin embargo, es una realidad que

⁹⁸ —, «The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world», UK Government, Londres, 2011, p. 8.

⁹⁹ —, «International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World», The White House, Washington DC, 2011, p. 18.

¹⁰⁰ —, «Cybersecurity, Innovation and the Internet Economy», The Department of Commerce Internet Policy Task Force, Washington DC, June 2011.

¹⁰¹ Ciberelcano n.º 14, p. 5.

¹⁰² Base Tecnológica e Industrial de la Defensa.

¹⁰³ ETID, p. 15.

España presenta un déficit en este aspecto, derivado en gran medida del hecho de que los sistemas de transferencia de resultados de la investigación y, en general, las relaciones entre las universidades, los centros de investigación teórica y aplicada, Gobierno y empresa están más desarrolladas y son más fluidas en otros países de lo que lo son en España¹⁰⁴.

Concluimos, pues, que la relación entre ciberseguridad e innovación es de mutua interdependencia, ya que si bien el I+D+i conduce a un entorno ciberespacial más seguro, este, recíprocamente, contribuye favorablemente a la innovación y al crecimiento económico. Por ello, disponer de una industria nacional potente en materia de ciberseguridad no solo es beneficioso para el sistema de ciberseguridad nacional *per se*, sino que la confianza, factor clave en economía, que podría aportar al espacio nacional como lugar seguro, favorecería la inversión y el crecimiento económico, así como, por realimentación, la propia I+D+i en seguridad cibernética.

Conclusión

Tras nuestro análisis de la situación, concluimos que la relación entre I+D+i y ciberseguridad es de mutua interdependencia, en presencia o no de la colaboración público-privada. En este contexto ciberespacial, si bien por una parte el propósito de la innovación es el de fortalecer un estado de ciberseguridad, *sensu contrario*, la ciberseguridad será soporte, garantía de innovación en diferentes ámbitos, lo que constituye un factor de crecimiento económico y bienestar de nuestra sociedad.

Una ciberdefensa eficaz depende no solo de la capacidad de innovación en tecnología, sino además de la capacitación técnica del personal y de la idoneidad de las operaciones defensivas.

El I+D+i en ciberseguridad debe estar alineado con la Estrategia Española de Ciencia, Tecnología e Innovación y orientarse a la consecución de los objetivos fijados por la Estrategia de Ciberseguridad Nacional. En todo caso, se hace preciso definir métricas o indicadores de rendimiento del esfuerzo realizado en I+D+i en ciberseguridad, en base a los resultados obtenidos¹⁰⁵.

El problema de medir, de fijar un patrón de medida y de saber qué medir y cómo, se presenta habitualmente. El ejemplo más claro es la propia ciberseguridad a la hora de establecer controles e invertir en medidas en base al valor de los activos que hay que proteger. El escollo se agrava cuando aparecen en los cálculos los temidos intangibles, que se resisten al análisis «eurométrico» (o «dolarométrico», si lo prefiere el lector).

¹⁰⁴ Ciberelcano, n.º 13, p. 16.

¹⁰⁵ —, «Oslo Manual: The Measurement of Scientific and Technological Activities. Proposed guidelines for collecting and interpreting technological innovation data», OCDE, 1993.

Medir el rendimiento del esfuerzo en I+D+i en ciberseguridad en base a los resultados obtenidos en tiempos parece lo razonable, siempre y cuando pre-supongamos que los que hayan realizado el esfuerzo en I+D+i hayan justificado la pertinencia de ese esfuerzo, hecho que se encuentra con la misma problemática de medición antes aludida.

Dado que hoy en día el motor de los avances tecnológicos no es la cobertura de necesidades militares sino el rendimiento económico en la sociedad civil, los planes de desarrollo de nuevas capacidades ciberdefensivas deberían contemplar algún esquema de colaboración público-privada ágil y bien preparado para sintonizar con los negocios de la industria.

Ya hay, como hemos mencionado, alguna experiencia (OTAN, por ejemplo, para el aprovechamiento de la propia Alianza, de los aliados y de sus industrias y expertos). En España no se detectan iniciativas completas al respecto, ni parece que el nivel de inversión del comprador sea lo suficientemente elevado como para cerrar el círculo y unir de modo más estrecho a la industria y a los investigadores. Sí hay acuerdos entre compañías y universidades, pero no tenemos ecosistema. Las acciones de CPP emprendidas por la Unión Europea deberían dar un impulso a la creación de un ecosistema sostenible de CPP para la I+D+i en España en el que la ciberdefensa habría de participar de modo destacado, y no exclusivamente en el descubrimiento y/o la obtención de vulnerabilidades no documentadas, sea cual sea el fin.

El compromiso del Estado con la I+D+i en materia de ciberseguridad (línea de acción 6 de la ECSN) debería estar respaldado con una adecuada dotación presupuestaria, que tendría que ser gestionada de manera centralizada por el organismo competente dentro de la estructura de ciberseguridad del Estado.

La ciberdefensa debe escuchar con atención los ecos del futuro en lo que toca a la transformación a la que pueden verse sometidos algunos actores del sector privado; es el caso de los operadores de telecomunicaciones, en contraposición a las grandes compañías digitales (las denominadas informalmente como GAFA: Google, Apple —aunque sea una histórica de las TIC—, Facebook y Amazon), que más allá de las barreras regulatorias, pudieran ir asumiendo un papel dominante en las comunicaciones globales y en la transformación de sectores nucleares como el financiero, el de contenidos y, en general, en la distribución digital de bienes y servicios. Esta circunstancia también tendría consecuencias en el ciberespacio y en la ciberdefensa.

España goza de un tejido profesional de ciberseguridad muy competitivo en todos los estratos, que se ha ido cultivando y curtiendo desde finales de la década de los noventa; hay, por tanto, continuidad intergeneracional y expertos situados en estratos de dirección estratégica, dirección organizativa y en toda la cadena de valor de la gestión técnica y la operación en casi todos los sectores privados y en las Administraciones Públicas. Las generaciones

más jóvenes de expertos siguen valorando la labor del *hacker* y su filosofía primigenia, contexto en el que atesoran conocimientos vivos día a día en un ecosistema colaborativo al que se van incorporando los *millennials*. Merece la pena estudiar, en un enfoque de I+D+i, la forma en la que estas personas pueden contribuir de forma más activa, no ya solo a la ciberseguridad, sino también a la ciberdefensa militar. Todo un reto.

Un alto porcentaje del conocimiento de elevado nivel de ciberseguridad en España se localiza en los departamentos de ciberseguridad de grandes compañías estratégicas del sector público y el privado: sector de banca y seguros, eléctrico, telecomunicaciones, combustibles, transportes, farmacológico, aguas, logística, construcción, gestión de infraestructuras... Estos responsables de seguridad de la información y responsables de seguridad tecnológica pueden brindar a la defensa su experiencia y conocimiento de la gestión de riesgos de seguridad y ayudar y sugerir numerosas líneas de modernización y mejora dignas de incluirse en programas de I+D+i, entre otras razones porque los servicios que operan son objetivos en el marco de cualquier confrontación, y no solo pueden verse desde la óptica de la ciberseguridad interior.

La ciberseguridad puede permitir a España alcanzar en un tiempo razonable y con una inversión proporcionada y bien dosificada cotas de competitividad elevadas a escala internacional. Pero el paso previo es construir una plataforma de CPP estable entre los agentes involucrados —la defensa como uno de los más importantes—, saber potenciar nuestros mercados exteriores y ser capaces de ganarnos una imagen prestigiosa en consonancia con el alto nivel de nuestras habilidades y capacidades.

La relación de interdependencias que caracteriza hoy al mundo, y el proceso de globalización, todavía no ha provocado que los Estados-nación dejen de aspirar, en defensa de su soberanía (aunque algunos hayan cedido alguna parte de la misma para preservar su grueso), a la independencia tecnológica como apoyo a la autonomía en la decisión responsable.

Esa independencia tecnológica no ha de confundirse con autarquía, comportamiento extremo que llevaría al empobrecimiento tecnológico. Esto es algo muy estudiado. Las TIC fluyen para todos, y cada vez será más difícil tener una supremacía estrictamente tecnológica que dure algo más que días, semanas y, en ocasiones, horas.

Pero siendo posiblemente así, la circunstancia permite tener alguna esfera de independencia, y en lo tocante a la ciberseguridad este hecho toma especial relevancia, ya que no requiere un esfuerzo cuantitativo desproporcionado en I+D+i y en P (de producción), y sí planes de mucha calidad y con perspectiva no cortoplacista.

Como es sabido, la ciberdefensa militar, —especialmente en algunos países— y en algunas organizaciones internacionales, como es el caso de la

OTAN, está revolucionando el esfuerzo industrial y la atención que las empresas proveedoras y la estructuras de I+D+i han de prestar a este asunto.

Hay numerosos aspectos, tratados ya¹⁰⁶: la gestión del conocimiento, la *IoT* en la ciberdefensa, los agentes inteligentes, el *Big Data* y la computación cognitiva aplicada a la ciberinteligencia en apoyo del analista, la gestión de identidades, la ciberdefensa aplicada a las plataformas militares (este epígrafe, concretamente, es nuclear para las defensa y donde la innovación juega un papel determinante), la conciencia situacional, el intercambio de información, la gestión de configuración evolucionada para la seguridad TIC, la gobernanza en la ciberseguridad, la CPP en formación, la orientación a servicios de la ciberseguridad...

Sobre este último punto basta decir que la orientación de los procesos y actividades privados y públicos a la prestación de servicios gestionados por terceros y el pago por uso es un rasgo de la transformación digital. La ciberdefensa debe adaptarse a este modelo, adaptar el modelo a sus necesidades o dejarlo en tablas. Y para ello hay que investigar los cambios que se avecinan en la ciberdefensa y en los procesos TIC, porque el ciberespacio actual no siempre será así, y la requisitoria de ciberseguridad de la ciberdefensa podría cambiar.

La ciberseguridad es una disciplina y una práctica. Las personas que han de gestionarla y operarla deben ser expertas y sus conocimientos han de entrar en ciclos continuos de instrucción y actualización. Uno de los frentes en los que se ha de invertir es en la I+D en nuevas formas de instrucción, de actualización y reciclaje. Tradicionalmente, y a efectos presupuestarios, no se suele incluir este epígrafe en las inversiones en la I+D+i. En nuestra opinión, mal no vendría reflexionar sobre la pertinencia de modificar esta situación.

En prácticamente todas las zonas del mundo ha empezado a aparecer legislación relacionada directamente con la ciberseguridad y la privacidad. La ciberdefensa militar debe estudiar cómo le afectan dichas leyes y normas. Por decirlo de algún modo: los profesionales de letras también cuentan en el mundo de la I+D+i.

En el caso de Europa, la Directiva NIS y el Reglamento General de Protección de Datos –y antes la normativa de protección de infraestructuras críticas y la de telecomunicaciones–, aunque no sean específicas para la ciberdefensa militar, sí la afectan, por cuanto atañen al intercambio de información de amenazas y ataques y a su notificación. Las estructuras de ciberseguridad de un país deben discriminar si una amenaza o un ciberataque notificado son de interés para la ciberdefensa. Y la defensa ha de tener información para estudiar profesionalmente si dicha amenaza y dicho ciberataque pudie-

¹⁰⁶ Los expertos españoles en ciberseguridad militar José Ramón Coz y Vicente Pastor han escrito sobre la mayoría de estos puntos en diversas ediciones de *SIC* (www.revistasic.com).

ra tener implicaciones en su campo de actuación. Es un terreno más para la I+D+i. y para la cooperación.

La ciberseguridad está precipitando, quizá de un modo soterrado, un debate más profundo y que afecta a la organización de las muy asentadas estructuras de seguridad de los Estados, que todavía están intentando encajar en su seno las estructuras nacientes de ciberseguridad.

En el caso de la defensa, hay polémica en lo que toca a decidir, a la luz de la transformación, si procede en un futuro centralizar la función de ciberseguridad de los sistemas tecnológicos de la defensa, debate que sobrepasa la propia ciberseguridad por afectar a la raíz organizativa de la defensa. Lo mismo sucede con la pertinencia o no de crear un ciberejército. Obviamente, un ciberejército no debe confundirse con una organización dedicada a la gestión de riesgos de seguridad de los sistemas tecnológicos de la defensa.

Sea como fuere, nadie pondrá en duda que se sugiera incluir en la maquinaria de la I+D+i el estudio pormenorizado de las transformaciones organizativas que tendrá que ir adoptando la defensa para ir adaptándose a la transformación digital. A buen seguro que del estudio profundo y sin cargas del pasado del papel de la ciberseguridad (a todos los efectos) dependerá que España disponga de una defensa militar adaptativa y con las capacidades siempre adecuadas para operar en un ciberespacio cambiante.

Capítulo octavo

Capacitación profesional y formación especializada en ciberseguridad

Óscar Pastor Acosta
*Gerente de Seguridad
Isdefe*

José Javier Martínez Herráiz
*Director de la Cátedra Amaranto de Seguridad Digital
Universidad de Alcalá de Henares*

Resumen

En el presente capítulo se abordará uno de los aspectos donde mayor puede llegar a ser la colaboración público-privada en materia de ciberseguridad y ciberdefensa: la necesidad de capacitar de manera adecuada a los profesionales especialistas en esta materia. Veremos cómo esta necesidad es casi un imperativo, el de la colaboración, al continuar aumentando la brecha entre la necesidad de profesionales y la oferta de los mismos.

Empezaremos, precisamente, analizando esta escasez de profesionales en todo el mundo y las cotas de preocupación que está alcanzando, tanto a nivel de los Estados y sus políticas nacionales como en el sector privado.

Continuaremos estudiando las iniciativas procedentes de organismos públicos en lo que respecta a la formación, certificación y acreditación de conocimientos en ciberseguridad, terminando con las procedentes del sector privado, en este caso, más centradas en la importancia de las certificaciones como garantía y aseguramiento de calidad y nivel.

El presente análisis no pretende hacer una descripción y búsqueda exhaustiva ni una descripción pormenorizada de todas las iniciativas en esta temática, sino centrarse en aquellas que nos parecen más relevantes y significativas. Quedan, manifiestamente, también fuera del mismo las innumerables iniciativas académicas, tanto públicas como privadas.

Palabras clave

ciberseguridad, ciberdefensa, formación, capacitación, certificación, habilidades, conocimientos, competencias, talento, escasez, profesional, pública, privada.

Abstract

In this chapter, it will be addressed one aspect which can become the greatest public-private collaboration landscape on cyber security and cyber defence: the need to adequately train specialized professionals in this field. We will see how this need is almost an imperative, that of collaboration, because the gap between the need for professionals and the offer of them continues to increase.

We will begin precisely analyzing the shortage of professionals worldwide and the dimensions of concern which it is achieving, both at governmental and national policies level and to private sector.

We will continue studying the initiatives from public agencies with regard to training, certification and accreditation of knowledge on cybersecurity, ending with those from the private sector, in this case, more focused on the importance of certifications as security and quality assurance and level.

This analysis is not intended to provide a description and exhaustive search or a detailed description of all initiatives in this area but focus on those that seem more relevant and significant. The uncountable academic initiatives, both public and private, are, obviously, also outside of this analysis.

Keywords

Cyber security, cyber defence, education, training, certification, skills, abilities, knowledge, talent, shortage, professional, public, private.

Introducción

Parece claro y reconocido que las tecnologías de la información y las comunicaciones están llamadas a convertirse en la columna vertebral de la economía europea.

La Comisión Europea, en su Estrategia para el Mercado Único Digital de Europa de 2015, lo reconoce como un objetivo prioritario dentro de sus políticas¹:

«La economía mundial se está convirtiendo rápidamente en digital. Las tecnologías de la información y la comunicación (TIC) ya no son un sector específico, sino el fundamento de todos los sistemas económicos innovadores modernos. Internet y las tecnologías digitales están transformando la vida que llevamos y la forma en que trabajamos (como personas, en las empresas y en nuestras comunidades) cuanto más se integran en todos los sectores de nuestra economía y nuestra sociedad».

En numerosos párrafos de dicho documento se muestra la preocupación por la seguridad digital y se insiste en la necesidad de «Reforzar la confianza y la seguridad en los servicios digitales y en el tratamiento de los datos personales», citando iniciativas ya en marcha como la Estrategia de Ciberseguridad de la Unión Europea, la Agenda Europea de Seguridad o la adopción de la Directiva sobre Seguridad de las Redes y de la Información.

Pues bien, en este contexto, se destaca que «En el primer semestre de 2016 la Comisión iniciará la creación de una asociación entre los sectores público y privado en materia de ciberseguridad en el ámbito de las tecnologías y soluciones de seguridad de la red en línea», incluyéndolo como punto de la «Hoja de ruta para la realización del mercado único digital» y, por lo que respecta a cualificaciones digitales, se resalta que: «La demanda de empleados con cualificaciones digitales crece en torno a un 4 % anual. La escasez de profesionales de las TIC en la Unión Europea podría alcanzar los 825.000 puestos vacantes de aquí a 2020 si no se adoptan medidas firmes». Entre esas medidas de apoyo que se proponen se menciona a la iniciativa de la Unión Europea: la «Gran Coalición para el empleo digital».

Ya en 2006, en la Declaración de Salónica, adoptada en la Conferencia Europea sobre Cibercapacidades de 1 de octubre de ese año, se identificaron tres mensajes clave, el segundo de los cuales decía: «En segundo lugar, es necesario realizar grandes esfuerzos para mejorar la cooperación a largo plazo entre los sectores público y privado, a fin de garantizar un marco transpa-

¹ Comisión Europea, «Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones: una Estrategia para el Mercado Único Digital de Europa, COM(2015) 192 final», 2015, <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015DC0192&rid=1>

rente que vincule la formación básica en cibercapacidades, la formación profesional, la enseñanza superior y el desarrollo profesional»².

Surge así como algo reconocido, importante y crítico, la llamada brecha entre la necesidad y demanda de profesionales especializados en ciberseguridad y la escasez de los mismos.

A estudiar la evolución que esta brecha ha tenido en los últimos cinco o seis años dedicaremos el primer punto de este capítulo, analizando diferentes informes tanto públicos como privados y procedentes de diferentes países del mundo occidental (Estados Unidos, el Reino Unido y la Unión Europea). El principal objetivo del capítulo es mostrar la unánime opinión en la acuciante necesidad de profesionales tanto en el ámbito público como en el privado y algunas propuestas para intentar paliarla mediante la colaboración público-privada en materia de formación.

Volviendo a la Conferencia Europea sobre Cibercapacidades anteriormente citada, podemos encontrar la siguiente recomendación: «La experiencia de integrar certificaciones de cibercapacidades del sector de las TIC en el marco nacional de cualificaciones, como se ha hecho por primera vez en el Reino Unido y en algunos nuevos Estados miembros, proporciona casos interesantes que deberían analizarse y compartirse con los demás Estados miembros».

Más recientemente, en 2015, el grupo de trabajo *European Cybersecurity Industry Leaders (ECIL)* remitía un informe a M. Günther H. Oettinger —*European Commissioner for Digital Economy and Society*— titulado «Recommendations on Cybersecurity for Europe»³, en el que se puede encontrar como recomendación: «La certificación de profesionales de ciberseguridad trabajando en infraestructuras críticas con sistemas ICS/SCADA». Recomendación que puede ser perfectamente extrapolada a cualquier otro ámbito relacionado con la ciberseguridad y la ciberdefensa.

En esta línea de recomendaciones ampliamente aceptadas en materia de certificaciones profesionales podemos encontrar numerosa información sobre los beneficios de las acreditaciones y certificaciones, tanto para los profesionales de la ciberseguridad como para los empleadores de estos profesionales.

² Comisión de las Comunidades Europeas, «Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones: cibercapacidades para el siglo XXI: fomento de la competitividad, el crecimiento y el empleo, COM(2007) 496 final», 2007, http://www.cdiex.org/documentos/documento_121.pdf

³ *European Cybersecurity Industrial Leaders (ECIL)*, «Recommendations on Cybersecurity for Europe», 25 de enero de 2016, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=13326

Incluso en estudios de un marcado corte académico como puede ser el de ACM del año 2013 «Toward Curricular Guidelines for Cybersecurity»⁴, se concluye en la necesidad de certificar y acreditar a profesionales en ciberseguridad mediante la necesaria colaboración público-privada.

Al estudio y análisis de iniciativas para la formación y certificación profesional en ciberseguridad es a lo que dedicaremos los dos siguientes apartados de este capítulo. Primero trataremos las iniciativas de organismos públicos y por último, las privadas.

El objetivo en ambos epígrafes es el de presentar los diferentes trabajos que se están llevando a cabo para tratar de «acoplar» lo más ajustadamente posible distintos esquemas de certificación profesional con los esquemas de competencias en el ámbito de la ciberseguridad en los que se está trabajando desde hace tiempo. Las iniciativas públicas analizadas han sido estadounidenses, británicas y, por supuesto, españolas.

En la parte de iniciativas privadas, nos centramos en aquellas más ampliamente difundidas y con más prestigio a nivel internacional. El objetivo ha sido el de analizar las más recientes propuestas de estas organizaciones y, siempre, vinculadas directamente al profesional de la ciberseguridad. No se incluyen aquellas propuestas de certificaciones que, si bien pudieran estar relacionadas con aspectos de seguridad digital, no forman, estrictamente, parte central de lo que se entiende por ciberseguridad.

Escasez de profesionales en ciberseguridad

Desde hace años podemos encontrar en estudios, análisis y artículos de opinión la afirmación reiterada de que no hay suficiente personal con los conocimientos y habilidades en ciberseguridad necesarios para desempeñar con éxito las responsabilidades que empresas y departamentos gubernamentales necesitan y demandan. Es un consenso a nivel mundial que dicha escasez de profesionales de la ciberseguridad tendrá implicaciones negativas en la seguridad nacional, impactando gravemente tanto en entidades del sector público como del privado.

Ya en 2010, un informe⁵ de la Comisión sobre Ciberseguridad para la 44ª Presidencia (de los Estados Unidos) elaborado por el CSIS (*Center for Stra-*

⁴ Andrew McGettrick y Association for Computing Machinery (ACM). «Towards Curricular Guidelines for Cybersecurity - Report of a Workshop on Cybersecurity Education and Training», 30 de agosto de 2013, <https://www.acm.org/education/TowardCurricularGuidelines-Cybersec.pdf>

⁵ Karen Evans y Franklin Reeder. «A Human Capital Crisis in Cybersecurity», Technical Proficiency Matters (1800 K Street, NW, Washington, DC 20006: CSIS Center for Strategic and International Studies - Commission on Cybersecurity for the 44th Presidency, noviembre de 2010), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/101111_Evans_HumanCapital_Web.pdf

tegic and International Studies) abordaba el tema en profundidad, apuntando que un elemento crítico de una estrategia de ciberseguridad robusta es disponer de profesionales adecuados, a todos los niveles, para construir y dotar de personal a las defensas frente a las ciberamenazas, y precisamente esa era el área identificada como más débil. Se identificaba el problema tanto en cantidad como en calidad, sobre todo cuando se buscaban profesionales con muy altas competencias en *red teaming* (entendido como un proceso diseñado para detectar vulnerabilidades de la red y del sistema y examinar la seguridad mediante la adopción de una enfoque similar al de un atacante que quiera acceder a la red/sistema/datos, también se le conoce como «*hacking ético*»⁶). La escasez de personal técnico altamente cualificado no solo afectaba a la operación y soporte de sistemas ya desplegados, sino que la carencia era todavía más acuciante en personal que pudiera diseñar sistemas robustos, desarrollar código seguro y crear herramientas sofisticadas para prevenir, detectar, mitigar y reconstruir los impactos en los sistemas atacados.

En julio de ese mismo año 2010, en una entrevista⁷ a varios analistas de ciberseguridad conducida por Jim Gosler, científico de la NSA (*National Security Agency*) y fundador de la Oficina de Tecnología de la Información Clandestina de la CIA (*Central Intelligence Agency*), se afirmaba que en los Estados Unidos tan solo unas mil personas disponían de las habilidades necesarias para defender los sistemas informáticos complejos contra los ciberataques. Sin embargo, ese mismo grupo de analistas afirmaba que se precisaban entre veinte y treinta veces la cantidad disponible.

Según un informe⁸ de 2012, producido por el Grupo de Trabajo «CyberSkills» del DHS (*Department of Homeland Security*) estadounidense, el número de profesionales con conocimientos prácticos y habilidades suficientemente avanzadas en ciberseguridad era tan limitado que las empresas proveedoras del Gobierno y las agencias federales competían «fieramente» entre ellas, así como con el sector privado, por contratarlos. Entre las recomendaciones del Grupo de Trabajo se incluían:

- Desarrollar escenarios de entrenamiento que permitan evaluar los perfiles de ciberseguridad críticos.
- Diseñar un proceso de contratación preciso y eficaz, y hacer que las vacantes de ciberseguridad críticas sean atractivas para los empleados federales.

⁶ Chris Peake. «Red Teaming: The Art of Ethical Hacking» (SANS Institute - InfoSec Reading Room, 16 de julio de 2003), <https://www.sans.org/reading-room/whitepapers/auditing/red-teaming-art-ethical-hacking-1272>

⁷ Jim Gosler. Cyberwarrior Shortage Threatens US Security, NPR Morning Edition, 29 de julio de 2010, <http://www.npr.org/templates/story/story.php?storyId=128574055>

⁸ Homeland Security Advisory Council, «CyberSkills Task Force Report» (US Department of Homeland Security, otoño de 2012), [https://www.dhs.gov/sites/default/files/publications/HSAC %20CyberSkills %20Report %20- %20Final.pdf](https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf)

- Lanzar una iniciativa importante y sostenida para mejorar las oportunidades para que los veteranos estadounidenses puedan ser adiestrados y contratados en puestos de ciberseguridad críticos.
- Especificar las habilidades críticas y el nivel de competencia para toda la contratación relacionada con la ciberseguridad.
- Establecer un programa piloto de «CiberReservistas» para garantizar que expertos avanzados en ciberseguridad fuera del Gobierno sean conocidos y estén disponibles en caso de necesidad.

En febrero de 2013, el interventor general del Reino Unido, en su informe «The UK cyber security strategy: Landscape review»⁹, advierte de que la brecha existente entre la disponibilidad de personal con las habilidades y conocimientos en ciberseguridad y la necesidad de los mismos sigue creciendo: «las conversaciones con el Gobierno, la academia y los representantes de las empresas privadas confirman que el Reino Unido carece de las suficientes habilidades técnicas y que la provisión de graduados y profesionales no cubrirá la demanda necesaria», poniendo de manifiesto que el número de profesionales de ciberseguridad no ha seguido el ritmo creciente de la ciberamenazas a las que se enfrenta la nación. Añade que la falta de personal con competencias en ciberseguridad podría persistir durante muchos años: «podría llevar hasta veinte años el poder hacer frente a la falta de competencias en todos los niveles educativos», afirmando que grupos de criminales se están aprovechando de este déficit de cualificaciones, dando una cifra del coste de la ciberdelincuencia para el Reino Unido que estaría entre £18.000 millones y £27.000 millones al año.

Asimismo, en octubre de 2014, un comité parlamentario especial en la Cámara de los Lores del Reino Unido predijo una escasez mundial de «no menos de dos millones de profesionales de seguridad cibernética»¹⁰ para el año 2017.

Otra prueba de la escasez de talento en ciberseguridad aparece en el informe¹¹ de septiembre de 2013 de la Oficina de Responsabilidad Gubernamental de los Estados Unidos (GAO, *Government Accountability Office*), en el que se mostraba una tasa de vacantes del 22 % en puestos de trabajo dentro de la Oficina de Ciberseguridad y las Comunicaciones de la Dirección General de Programación y Protección del Departamento de Seguridad Nacional (DHS, *Department of Homeland Security*).

⁹ Comptroller and Auditor General, «The UK Cyber Security Strategy: Landscape Review» (London: National Audit Office, 5 de febrero de 2013), <http://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/>

¹⁰ Lewis Morgan. «Global Shortage of Two Million Cyber Security Professionals by 2017», *IT Governance Blog*, 30 de octubre de 2014, <http://www.itgovernance.co.uk/blog/global-shortage-of-two-million-cyber-security-professionals-by-2017/>

¹¹ GAO, «GAO-13-742 - DHS Recruiting and Hiring: DHS Is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Recruiting Efforts», Report to Congressional Requesters (United States Government Accountability Office, septiembre de 2013), <http://www.gao.gov/products/GAO-13-742>

En enero del año 2016, un informe¹² del Servicio de Investigación del Congreso de los Estados Unidos analiza la mano de obra de ciberseguridad en los Departamentos de Defensa y de Seguridad Nacional, reconociendo que desarrollar y mantener una fuerza de trabajo robusta en ciberseguridad dentro de las Agencias Federales se ha convertido en un desafío continuo. Así, según recoge el mencionado informe, aunque la Administración Obama había creado una prioridad para todas las agencias gubernamentales con el objeto de reducir a la mitad, a finales de 2013, el déficit en los puestos de ciberseguridad, que había detectado un grupo de trabajo del Consejo Federal de Directores de Capital Humano, según un informe¹³ de la GAO, de enero de 2015, los esfuerzos necesarios para cerrar las carencias de profesionales de ciberseguridad en las Agencias Federales se encontraban en un estado de madurez muy inicial.

El 12 de julio de 2016, la Oficina de Administración y Presupuesto (OMB, *Office of Management and Budget*) de los Estados Unidos publica la Estrategia Federal para la Fuerza Laboral de Ciberseguridad¹⁴, que incluye acciones para ayudar al Gobierno Federal en las siguientes áreas:

- Identificar las necesidades del personal de seguridad cibernética.
- Ampliar los recursos humanos de ciberseguridad a través de la educación y la formación.
- Reclutar y contratar talentos altamente cualificados.
- Retener y desarrollar talentos altamente cualificados.

Dentro de las instituciones del sector privado, la disponibilidad de profesionales de la ciberseguridad ha sido abordada en profundidad en las diferentes ediciones del Estudio Global sobre Personal de Seguridad de la Información, de los años 2011¹⁵, 2013¹⁶ y 2015¹⁷, de la organización (ISC)² (*International In-*

¹² Kathryn A. Francis y Wendy Ginsber, «The Federal Cybersecurity Workforce: Background and Congressional Oversight Issues for the Departments of Defense and Homeland Security», CRS Report (Congressional Research Service, 8 de enero de 2016), <https://www.fas.org/sgp/crs/natsec/R44338.pdf>

¹³ GAO, «GAO-15-223, Federal Workforce: OPM and Agencies Need to Strengthen Efforts to Identify and Close Mission-Critical Skills Gaps», Report to Congressional Requesters (United States Government Accountability Office, enero de 2015), <http://www.gao.gov/assets/670/668202.pdf>

¹⁴ OMB (Office of Management and Budget), *Federal Cybersecurity Workforce Strategy, M-16- 15*, 2016, <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf>

¹⁵ Robert Ayoub. «The 2011 (ISC)² Global Information Security Workforce Study», Frost & Sullivan Market Survey [(ISC)², 2011], https://www.isc2.org/uploadedFiles/Industry_Resources/FS_WP_ISC_%20Study_020811_MLW_Web.pdf

¹⁶ Michael SUBY. «The 2013 (ISC)² Global Information Security Workforce Study», Frost & Sullivan Market Study [(ISC)², 2013], <https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf>

¹⁷ Michael SUBY y Frank DICKSON. «The 2015 (ISC)² Global Information Security Workforce Study», A Frost & Sullivan White Paper [(ISC)², 16 de abril de 2015], [https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-\(ISC\)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf](https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf)

formation Systems Security Certification Consortium). Así, en la última edición del estudio se indica que el déficit de mano de obra de seguridad de la información es cada vez mayor. En la encuesta del año 2015, en la que participaron casi catorce mil profesionales de la seguridad de la información de todo el mundo, el 62 % de los encuestados declaró que sus organizaciones tienen muy pocos profesionales de la ciberseguridad, lo que supone un incremento del 6 % si se compara con los que respondieron lo mismo en la encuesta del año 2013. Los cinco roles de ciberseguridad más demandados son:

- Analista de seguridad.
- Auditor de seguridad.
- Arquitecto de seguridad (de productos y de soluciones).
- Analista forense.
- Gestor de incidentes (corporativo).

Otra de las diferencias significativas en la edición de 2015 del mencionado estudio de (ISC)² aparece en las razones del déficit, dado que ahora son menos los que indican la falta de presupuesto para contratar personal, apareciendo con mayor relevancia la insuficiente oferta del mercado laboral de candidatos con el perfil profesional adecuado. Estas observaciones, y otras generadas a partir de este amplio estudio, permiten a los autores del informe estimar el déficit global en la fuerza de trabajo de ciberseguridad, que se prevé llegará a 1,5 millones en cinco años. Este déficit es la diferencia entre la previsión de la fuerza de trabajo necesaria para dar respuesta plena a las crecientes necesidades de ciberseguridad y la proyección de las restricciones en la oferta de mano de obra en este sector. Esto no implica una disminución de la contratación, sino que se prevé un aumento global de 195.000 profesionales de la ciberseguridad de la información en el año 2016, lo que supone un incremento de casi un 6 % respecto a 2014.

Estas predicciones se alinean con las realizadas por otras empresas e instituciones privadas, así Cisco en julio de 2015¹⁸ situaba la cifra global de ofertas de trabajo de ciberseguridad no cubiertas en más de un millón. Forbes, en un artículo¹⁹ de enero de 2016, indicaba que se espera que el mercado de la seguridad cibernética crezca a más del doble de su tamaño actual, pasando de \$75.000 millones en 2015 a \$170.000 millones en 2020. Por otro lado, Michael Brown, CEO de Symantec, uno de los mayores proveedores de *software* de seguridad del mundo, espera que para el año 2019 la demanda aumente a 6 millones de ofertas de trabajo a nivel mundial, con un déficit previsto de 1,5 millones²⁰.

¹⁸ Cisco Security Advisory Services, «Mitigating the Cybersecurity Skills Shortage» (Cisco Systems, Inc, julio de 2015), <http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf>

¹⁹ Steve MORGAN. «One Million Cybersecurity Job Openings In 2016», *Forbes*, 2 de enero de 2016, <http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/print/>

²⁰ Rebecca Vogel. «Closing The Cybersecurity Skills Gap», *Salus Journal* 4, n.º 2 (2016): 32.

Una encuesta realizada por Raytheon²¹ en 2014 mostraba que la demanda de profesionales de la seguridad informática estaba creciendo 3,5 veces más rápido que el mercado de trabajo IT genérico, y doce veces más rápido que el mercado de trabajo total. Según ese mismo estudio, en 2013, hubo en Estados Unidos 209.749 anuncios de ofertas de trabajo de ciberseguridad y cubrir estas demandas exigió un 36 % más de tiempo de dedicación para las empresas de reclutamiento.

En 2015, ISACA y RSA²² encuestaron a seiscientos cuarenta y nueve profesionales de todo el mundo sobre la magnitud del problema de la falta de habilidades en ciberseguridad. Los resultados mostraron que el 35 % de las organizaciones encuestadas no podían cubrir las vacantes de ciberseguridad, a pesar de que un 82 % de esas mismas organizaciones esperaban ser atacadas cibernéticamente. Además, lo que podría considerarse más preocupante es que, el 52 % de dichas organizaciones manifestó que menos de una cuarta parte de todos los candidatos disponían de las habilidades de ciberseguridad realmente necesarias para el puesto.

Finalmente, según datos del Bureau of Labor Statistics²³ de Estados Unidos, en 2015 más de 209.000 puestos de trabajo de seguridad cibernética quedaron vacantes en Estados Unidos y la demanda aumentó un 74 % durante los cinco últimos años. Además, se espera que la demanda de profesionales de ciberseguridad crezca en un 53 % hasta el año 2018.

Iniciativas de organismos públicos para la formación y certificación profesional en ciberseguridad

Entre las propuestas que incluía el ya mencionado informe²⁴ de la Comisión sobre Ciberseguridad para la 44ª Presidencia (de los Estados Unidos) del CSIS, estaba la de construir un sistema de certificación de alto prestigio profesional, en dos o tres áreas de especialidad, creando un organismo gubernamental para desarrollar y administrar las mencionadas certificaciones donde no se identificaba la existencia de una oferta previa de certificación profesional suficientemente rigurosa. Asimismo, ese mismo organismo público debería también desarrollar criterios para la evaluación de otros programas de certificación de forma que, usando un modelo federado, otros programas de cer-

²¹ Raytheon y NCSA, «Preparing Millennials to Lead in Cyberspace» (National Cyber Security Alliance, octubre de 2014), <http://www.raytheoncyber.com/news/feature/blog-cyber60-helpwanted.html>

²² ISACA y RSA Conference, «State of Cybersecurity: Implications for 2015» (ISACA, 11 de abril de 2015), http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

²³ Ariha Setalvad. «Demand to fill cybersecurity jobs booming», *Península Press*, 31 de marzo de 2015, <http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/>

²⁴ Karen Evans y Franklin Reeder. «A Human Capital Crisis in Cybersecurity».

tificación, existentes o futuros, públicos o privados, que cumplieran con unas estrictas normas de calidad, pudieran también ser acreditados.

Asimismo, en diciembre de 2014, *ENISA* (*European Union Agency for Network and Information Security*) publicaba un informe²⁵ abordando la certificación de competencias de ciberseguridad para los entornos *ICS/SCADA*²⁶ (*Industrial Control Systems / Supervisory Control and Data Acquisition*). Entre sus recomendaciones se incluía la de crear un esquema europeo global de certificación profesional de ciberseguridad *ICS/SCADA*, así como crear un comité independiente para evaluar y aprobar las certificaciones actuales y futuras.

Según *ENISA*, las nuevas certificaciones de ciberseguridad deberían ser multinivel, para llegar a un mayor número de profesionales, así como diferentes campos de aplicación, reflejando adecuadamente el diferente conjunto de habilidades que son necesarias para los profesionales. *ENISA* proponía como ejemplo los siguientes niveles de certificación profesional:

- Nivel básico.
- Nivel avanzado.
- Nivel máster.
- Nivel gerencial.

En este contexto, son numerosas las iniciativas, muchas de ellas respaldadas por organismos y agencias gubernamentales, promoviendo esquemas de certificación de profesionales en ciberseguridad, que ayuden a salvar esta escasez de personal experto en la materia. Su principal objetivo es asegurar que los conocimientos y habilidades de los profesionales certificados garanticen de forma efectiva el cumplimiento de las misiones que dichos organismos tienen marcadas, permitiendo diferenciar en la oferta formativa de ciberseguridad aquellos programas de formación con rigor y profesionalidad de los que no la tengan, poniendo en evidencia la ineficacia de multitud de iniciativas formativas oportunistas, que surgen aprovechando la actual carencia de profesionales expertos en ciberseguridad, pero que carecen de la capacidad para conseguir que quienes las cursan realmente adquieran competencias avanzadas en ciberseguridad.

A continuación se analizarán algunas de las principales iniciativas de formación y certificación profesional en ciberseguridad, promovidos por organismos públicos de las naciones más avanzadas de nuestro entorno.

National Cybersecurity Workforce Framework

²⁵ Adriana Pauna. «Certification of Cyber Security Skills of ICS - Good Practices and Recommendations for Developing Harmonised Certification Schemes» (Heraklion: *ENISA*, 2014), <http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714040:EN:HTML>

²⁶ NIST, «NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security» (National Institute of Standards and Technology, junio de 2011).

En noviembre de 2011, la Iniciativa Nacional para la Educación sobre Ciberseguridad (*National Initiative for Cybersecurity Education, NICE*)²⁷, del estadounidense Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology, NIST*), dio a conocer para comentarios el Marco de Referencia para la Mano de Obra en Ciberseguridad (*National Cybersecurity Workforce Framework*)²⁸.

NICE es una iniciativa de colaboración público-privada, dirigida por el *NIST*, en la que participan el Gobierno, la academia y el sector privado, centrada en la educación, la formación y el desarrollo profesional de ciberseguridad. La misión de *NICE* es dinamizar y promover una red robusta y un ecosistema de educación, formación y desarrollo profesional en ciberseguridad. *NICE* cumple esta misión mediante la mencionada coordinación público-privada, partiendo de los programas de capacitación existentes que hayan demostrado su éxito, para facilitar el cambio y la innovación, promoviendo el liderazgo y la visión para aumentar el número de profesionales cualificados en ciberseguridad.

El mantenimiento y desarrollo del *National Cybersecurity Workforce Framework* actualmente es coordinado²⁹ por la Iniciativa Nacional para las Carreras y los Estudios de Ciberseguridad (*National Initiative for Cybersecurity Careers and Studies, NICCS*)³⁰, del Departamento de Seguridad Nacional (*Department of Homeland Security, DHS*), en colaboración con otros organismos públicos norteamericanos y representantes del sector privado.

La misión de *NICCS* es ser un recurso nacional para la concienciación, educación, capacitación y las carreras profesionales en ciberseguridad. *NICCS* garantiza la disponibilidad de la información de investigación y formación a través de un robusto catálogo que facilita las búsquedas, permitiendo a los usuarios encontrar programas de formación según su ubicación, método de impartición, área de especialidad o nivel de competencia. *NICCS* apoya el objetivo de *DHS* de hacer crecer la mano de obra disponible en ciberseguridad, proporcionando información acerca de ciencia, tecnología, ingeniería y matemáticas (*Science, Technology, Engineering & Mathematics, STEM*) y los programas universitarios de grado relacionados con la ciberseguridad, así como prácticas, becas, desafíos y eventos de ciberseguridad.

²⁷ NIST, «The National Initiative for Cybersecurity Education (NICE)», accedido 29 de agosto de 2016, <http://csrc.nist.gov/nice/about/index.html>

²⁸ NIST, «NICE Issues Cybersecurity Workforce Framework for Public Comment», accedido 29 de agosto de 2016, <http://www.nist.gov/itl/cyberwork-110811.cfm>

²⁹ DHS y NICCS, «National Cybersecurity Workforce Framework Slick Sheet» (National Initiative for Cybersecurity Careers and Studies (NICCS), noviembre de 2011), [https://niccs.us-cert.gov/sites/default/files/documents/files/Workforce %20Framework %20Slick %20Sheet_1.pdf?trackDocs=Workforce %20Framework %20Slick %20Sheet.pdf](https://niccs.us-cert.gov/sites/default/files/documents/files/Workforce%20Framework%20Slick%20Sheet_1.pdf?trackDocs=Workforce%20Framework%20Slick%20Sheet.pdf)

³⁰ NICCS, «National Initiative for Cybersecurity Careers and Studies», accedido 29 de agosto de 2016, <https://niccs.us-cert.gov/home/about-niccs>

El *National Cybersecurity Workforce Framework*³¹ proporciona una forma coherente para definir y describir el trabajo de ciberseguridad en cualquier organización, pública o privada, al permitir clasificar y categorizar el marco de trabajo de ciberseguridad en virtud de las áreas de especialidad, que se agrupan en siete categorías. Dentro de cada área de especialidad, el marco define funciones estándar, así como las competencias, destrezas y habilidades (*Knowledge, Skills & Abilities, KSA*) requeridas en los profesionales de la seguridad informática que las desempeñen y los títulos de trabajo por los que habitualmente se conoce a dichos grupos de actividades profesionales.

Como ya hemos mencionado, el Marco de Referencia para la Mano de Obra en Ciberseguridad se estructura inicialmente en siete categorías, cada una compuesta por varias áreas de especialidad, en base a un extenso análisis de las tareas que agrupan a los trabajadores y que comparten funciones comunes, independientemente de los títulos de trabajo u otras condiciones laborales.

Las categorías del *Workforce Framework* y sus respectivas áreas de especialidad son las siguientes:

- **Provisión de Forma Segura:** que agrupa las áreas de especialidad responsables de la conceptualización, diseño y construcción segura de sistemas de tecnologías de la información (IT), es decir, responsables de algún aspecto del desarrollo de sistemas.
 - Cumplimiento de seguridad de la información.
 - Ingeniería de seguridad y aseguramiento del software.
 - Desarrollo de sistemas.
 - Planificación de los requisitos de sistemas.
 - Arquitectura de seguridad de sistemas.
 - Investigación y desarrollo tecnológico.
 - Evaluación y prueba.
- **Proteger y Defender:** que incluye las áreas de especialidad responsables de la identificación, análisis y mitigación de las amenazas a los sistemas de TI o redes internas.
 - Análisis de la defensa de redes informáticas.
 - Apoyo a la infraestructura de la defensa de redes informáticas.
 - Respuesta a incidentes.
 - Evaluación y gestión de vulnerabilidades.
- **Supervisión y Desarrollo:** son las áreas que proporcionan liderazgo, gestión, dirección y/o desarrollo y promoción, de manera que la organiza-

³¹ NICE, «The National Cybersecurity Workforce Framework» (National Initiative for Cybersecurity Careers and Studies (NICCS), 15 de mayo de 2014), [https://niccs.us-cert.gov/sites/default/files/documents/files/National %20Cybersecurity %20Workforce %20Framework %20Version %201.0.pdf?trackDocs=National %20Cybersecurity %20Workforce %20Framework %20Version %201.0.pdf](https://niccs.us-cert.gov/sites/default/files/documents/files/National%20Cybersecurity%20Workforce%20Framework%20Version%201.0.pdf?trackDocs=National%20Cybersecurity%20Workforce%20Framework%20Version%201.0.pdf)

ción y todos los individuos puedan conducir eficazmente los trabajos de ciberseguridad.

- Formación y entrenamiento.
 - Operaciones de seguridad de sistemas de información (*Information Systems Security Officer, ISSO*).
 - Asesoramiento y defensa legal.
 - Gestión de programas de seguridad (*Chief Information Security Officer, CISO*).
 - Planificación estratégica y desarrollo de políticas.
- Recoger y Operar: con las áreas de especialidad encargadas de las operaciones especializadas de denegación y decepción, así como de la recopilación de información de ciberseguridad que pueda ser utilizada para la elaboración de inteligencia.
- Operaciones de recolección.
 - Ciberoperaciones.
 - Planificación de ciberoperaciones.
- Operar y Mantener: que agrupa las áreas de especialidad responsables de la prestación de soporte, administración y mantenimiento necesarios para garantizar de forma eficaz y eficiente el funcionamiento y la seguridad del sistema de información.
- Soporte técnico y servicio al cliente.
 - Administración de datos.
 - Gestión del conocimiento.
 - Servicios de red.
 - Administración de sistemas.
 - Análisis de seguridad de sistemas.
- Analizar: que incluye las áreas de especialidad responsables de la revisión y evaluación altamente especializadas de información entrante sobre ciberseguridad para determinar su utilidad para la elaboración de inteligencia.
- Inteligencia de todas las fuentes.
 - Análisis de la explotación.
 - Objetivos.
 - Análisis de amenazas.
- Investigar: con las áreas de especialidad encargadas de la investigación de eventos de ciberseguridad y/o delitos en sistemas y redes de información, así como de las evidencias digitales.
- Forense digital.
 - Investigación.

Como ya se ha indicado, dentro de cada área de especialidad, el *Workforce Framework* define las competencias, destrezas y habilidades requeridas, hasta completar un total de trescientas cincuenta y ocho, así como las tareas a desempeñar por los profesionales de esa área de la ciberseguridad, hasta un total de cuatrocientas cuarenta y cuatro tareas diferentes.

El *Workforce Framework* entiende conocimiento, destrezas y habilidades como los atributos necesarios para llevar a cabo un trabajo y, en general, se ponen de manifiesto a través de la experiencia cualificada, la educación o la formación. El conocimiento es un conjunto de información aplicada directamente a la realización de una función. La destreza es una competencia observable para llevar a cabo un acto psicomotor aprendido. La habilidad es una competencia para llevar a cabo un comportamiento observable o un comportamiento que se traduce en un producto observable. El *Workforce Framework* asocia conocimiento, destrezas y habilidades con cada área de especialidad para definir claramente las cualificaciones, educación o formación necesarias para realizar con éxito las tareas o funciones asociadas con esa especialidad.

Por tanto, el *Workforce Framework* constituye el modelo de clasificar, organizar y describir el trabajo de ciberseguridad, para proporcionar a los educadores, estudiantes, empresarios, empleados, proveedores de formación, así como a los responsables políticos, una herramienta sistemática y coherente para organizar la forma en que pensamos y hablamos sobre el trabajo de ciberseguridad y entendemos lo que se requiere para mejorar la mano de obra disponible en ciberseguridad.

Al alinear los grados universitarios, los puestos de trabajo, la formación y las certificaciones con el *Workforce Framework* se obtienen los siguientes beneficios para:

- Educadores: que pueden alinear mejor sus programas de formación con los empleos requeridos.
- Estudiantes: al graduarse con los conocimientos y competencias necesarios.
- Empleadores: al contratar sobre una oferta de candidatos mejor cualificados.
- Empleados: que pueden identificar mejor diferentes carreras profesionales y oportunidades de empleo.
- Responsables políticos: para desarrollar las políticas necesarias para promover la disponibilidad de mano de obra.

La capacitación es un componente fundamental para cualquier Marco de Referencia para la Mano de Obra, por lo que este se complementa con un Catálogo de Formación³², mantenido por el NICCS, en el que se incluyen los

³² NICCS, «Training Catalog | National Initiative for Cybersecurity Careers and Studies», accedido 30 de agosto de 2016, <https://niccs.us-cert.gov/training/tc/search>

cursos según las áreas de especialidad del Marco de Referencia. Esto permite, tanto a los profesionales con experiencia como a los que acaban de entrar en la profesión de la ciberseguridad, identificar rápidamente los cursos que necesitan para avanzar dentro de su área o adquirir habilidades para pasar a otra especialidad. En la actualidad, el Catálogo de Formación del *NICCS* incluye 2.885 cursos a lo largo de diferentes ubicaciones geográficas de Estados Unidos.

CESG Certified Professional Scheme

En el Reino Unido, el *CESG* (originalmente *Communications Electronics Security Group*), dependiente del *GCHQ* (*Government Communications Headquarters*), que es la autoridad nacional británica para la Seguridad de la Información, ha desarrollado un Esquema de Certificación Profesional de Ciberseguridad (*Certified Professional Scheme, CESG*)³³, para aquellos candidatos que cumplan con los requisitos de competencia y habilidad para las funciones definidas por dicho organismo.

Los objetivos del Esquema de Certificación son:

- Mejorar la concordancia entre los requisitos de experiencia avanzada en seguridad de la información del sector público y la competencia de los profesionales de ciberseguridad, ya sean empleados públicos o subcontratados.
- Alentar a los trabajadores de ciberseguridad a desarrollar las habilidades y conocimientos necesarios para ser plenamente operativos.
- Proporcionar la garantía de que los profesionales certificados cubren los requisitos de los roles de ciberseguridad definidos.
- Proporcionar definiciones más claras de los conocimientos y habilidades requeridos para los diferentes roles de seguridad de la información.

La estructura general³⁴ del Esquema de Certificación de Profesionales de Ciberseguridad del *CESG* consta de los siguientes elementos principales:

- Órganos asesores: procedentes de departamentos gubernamentales, la industria, la academia y el *CLAS* (*CESG Listed Advisor Scheme*).
- *CESG*: que actúa como organismo propietario y supervisor del Esquema de Certificación, seleccionando a los organismos de certificación reconocidos, definiendo los roles y competencias del esquema y desarrollando el portafolio de políticas de ciberseguridad.
- Organismos de certificación: que evalúan la competencia de los candidatos de diferentes formas, dependiendo de las habilidades necesarias

³³ CESG, «CESG Certified Professional Scheme», 19 de mayo de 2016, <https://www.cesg.gov.uk/articles/cesg-certified-professional-scheme>

³⁴ CESG, «Guidance to CESG Certification for IA Professionals v2-1» (GCHQ, enero de 2015), <https://www.cesg.gov.uk/file/701/download?token=QM1gwRoi>

para cada rol. El proceso de evaluación incluirá típicamente revisión de evidencias escritas, pruebas de conocimiento, referencias, una entrevista, la recomendación de los evaluadores y la decisión final de un panel de ratificación. Cuanto más nivel de competencia implique el rol evaluado, más extensa se espera que sea la evaluación.

- **Candidatos:** que serían todos aquellos profesionales que quieran certificar sus competencias en ciberseguridad, solicitando la evaluación a uno de los organismos de certificación acreditados y obteniendo el certificado una vez hayan superado positivamente la evaluación.
- **Empleadores de profesionales certificados:** entre los que se encontrarán tanto organismos del sector público como entidades e industrias del sector privado.

Los roles³⁵ de seguridad de la información definidos por el *CESG* para su Esquema de Certificación son:

- **Acreditador (*Accreditor*).**
 - Actuará como un asesor imparcial de los riesgos a los que un sistema de información puede estar expuesto, para cumplir con los requisitos de negocio, y autorizará formalmente el sistema en nombre del Consejo de Administración.
- **Asesor de Riesgos de Seguridad de la Información (*Security Information Risk Advisor, SIRA*).**
 - Asesorará al negocio sobre la gestión de la seguridad y el riesgo de la información de forma consistente con las políticas, normas y guías gubernamentales y/o con las buenas prácticas de ciberseguridad de la industria.
- **Auditor de Seguridad de la Información (*IA Auditor*).**
 - Evaluará el cumplimiento de los objetivos, políticas, normas y procesos de seguridad.
- **Arquitecto de Seguridad de la Información (*IA Architect*).**
 - Impulsará el cambio beneficioso de la seguridad en el negocio, mediante el desarrollo o revisión de arquitecturas que mitiguen los riesgos y cumplan con las políticas de seguridad pertinentes, balanceen los riesgos de seguridad de la información y el coste de las contramedidas para protegerla, y ajusten los requisitos de negocio para la seguridad.
- **Director de Seguridad TI (*IT Security Officer, ITS0*).**
 - Proporcionará gobernabilidad, gestión y control de la seguridad de los sistemas de información.
- **Director de Seguridad de las Comunicaciones (*Communications Security Officer, ComSO*).**
 - Gestionará los sistemas criptográficos según normativa gubernamental y los procedimientos de seguridad específicos para productos de

³⁵ CESG, «CESG Certification for IA Professionals 5.2» (GCHQ, octubre de 2015), <https://www.cesg.gov.uk/file/520/download?token=j8vebyeM>

referencia. Esta función abarca a aquellos que realizan funciones similares según normativa PCI/DSS³⁶.

- Evaluador de Vulnerabilidades (*Penetration Tester*).
- Evaluará de forma independiente los diferentes elementos que componen un sistema de información o producto, con el objetivo de encontrar y documentar las vulnerabilidades presentes.

Cada rol se define con tres niveles de competencia:

- Practicante (*Practitioner*): nivel de entrada al Esquema, adecuado para las personas que trabajan en las tareas rutinarias bajo supervisión y pueden no tener experiencia previa en ciberseguridad.
- Practicante Senior (*Senior Practitioner*): nivel adecuado para personas que trabajan de forma independiente en proyectos complejos y que normalmente lideran un equipo o supervisan el trabajo de otros profesionales de ciberseguridad. Suelen contribuir al éxito de un programa o varios proyectos. Tiene suficiente experiencia para manejar situaciones complejas y requiere de una supervisión mínima.
- Practicante Principal (*Lead Practitioner*): nivel apropiado para los profesionales altamente experimentados, que trabajan en los niveles superiores de una organización, prestando asesoramiento y liderazgo en temas estratégicos y complejos de ciberseguridad. Suelen participar en toda una área de un responsable senior de riesgos. Influyen en los presupuestos y en el marco de gobierno corporativo para optimizar el equilibrio entre seguridad y el resto de objetivos de la organización, asegurando que contribuye a sus objetivos estratégicos.

Los mencionados niveles, para cada uno de los roles profesionales de ciberseguridad, están alineados con los niveles de responsabilidad definidas por SFIA (*Skills Framework for the Information Age*)³⁷. El conjunto completo de los niveles de responsabilidad³⁸ SFIA es el siguiente:

1. Seguir (*Follow*).
2. Ayudar (*Assist*).
3. Aplicar (*Apply*).
4. Permitir (*Enable*).
5. Garantizar/Aconsejar (*Ensure/Advise*).
6. Poner en marcha/Influir (*Initiate/Influence*).
7. Establecer estrategia/Inspirar, movilizar (*Set Strategy/Inspire*).

³⁶ PCI Security Standards Council, «PCI (industria de tarjetas de pago) - Normas de seguridad de datos - Requisitos y procedimientos de evaluación de seguridad», noviembre de 2013, https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

³⁷ SFIA Foundation, «Versión 6 del Marco de Competencias para la Era de la Información - Español», accedido 29 de agosto de 2016, <https://www.sfia-online.org/es/reference-guide>

³⁸ SFIA Foundation, «Responsabilidades y habilidades - Español», accedido 31 de agosto de 2016, <https://www.sfia-online.org/es/how-sfia-works/responsibilities-and-skills>

SFIA define cada nivel de responsabilidad en términos de autonomía, influencia, complejidad y habilidades de negocio. La mayor parte de las responsabilidades del nivel Practicante, Practicante Senior y Practicante Principal se alinean con los niveles 2, 4 y 6 de *SFIA*, respectivamente.

La línea base de entrada para la certificación es bastante alta y se espera que el candidato aporte evidencias sobre la aplicación práctica de las habilidades requeridas en el rol solicitado, por lo que disponer de una titulación relacionada, pero sin experiencia práctica, no garantiza la obtención de la certificación.

Por otro lado, para la definición de las habilidades, el *CESG* se apoya en las definidas por el Marco de Referencia³⁹ del *IISP* (*Institute of Information Security Professional*), pero complementándolas, en consulta con los órganos asesores, procedentes de los departamentos gubernamentales, la academia, la industria y el *CLAS*, para ayudar a la evaluación con respecto a cada uno de los cuatro niveles de habilidad definidos por *IISP*.

Los niveles de habilidad del *IISP* son:

- Nivel 1: conocimiento (*awareness*). Comprende la habilidad y su aplicación. Ha adquirido y puede demostrar conocimientos básicos asociados con la habilidad. Entiende cómo la habilidad debe ser aplicada, pero puede no tener la experiencia práctica en su aplicación.
- Nivel 2: aplicación básica (*basic application*). Comprende la habilidad y la aplica a tareas básicas bajo alguna supervisión. Ha adquirido los conocimientos básicos asociados con la habilidad, por ejemplo, ha adquirido un título académico o profesional en la habilidad. Entiende cómo deben aplicarse las habilidades. Tiene experiencia en la aplicación de la habilidad para una variedad de tareas básicas. Determina cuándo los problemas se deben escalar a un nivel más alto. Contribuye con ideas en la aplicación de la habilidad. Demuestra conocimiento de la evolución reciente de la habilidad.
- Nivel 3: aplicación competente (*skilful application*). Comprende la habilidad y la aplica a tareas complejas sin supervisión. Ha adquirido una comprensión profunda de los conocimientos asociados a la habilidad. Entiende cómo la habilidad debe ser aplicada. Tiene experiencia de la aplicación de la habilidad para una variedad de tareas complejas. Demuestra una significativa responsabilidad personal o autonomía, con poca necesidad de escalar problemas. Contribuye con ideas en la aplicación de la habilidad. Demuestra conocimiento de la evolución reciente de la habilidad. Contribuye con ideas para el desarrollo técnico y nuevas áreas de aplicación de la habilidad.

³⁹ Institute of Information Security Professional, «IISP Skills Framework - Version 2.0», accedido 31 de agosto de 2016, https://www.iisp.org/imis15/iisp/About_Us/Our_Skills_Framework/iispv2/Accreditation/Our_Skills_Framework.aspx?hkey=e77a6f03-9498-423e-aa7b-585381290ec4

- Nivel 4: experto (*expert*). Es una autoridad que dirige el desarrollo de la habilidad. Es un experto reconocido por sus compañeros en la habilidad. Tiene experiencia en la aplicación de las habilidades en circunstancias sin precedentes. Propone, lleva a cabo y/o conduce un trabajo innovador para mejorar la habilidad.

El Esquema de Certificación de Profesionales de Ciberseguridad del *CESG* incluye veintitrés habilidades, agrupadas en nueve secciones, según el siguiente esquema:

- Sección A: Gestión de la Seguridad de la Información.
 - A1: Gobierno.
 - A2: Política y Estándares.
 - A3: Estrategia de Seguridad de la Información.
 - A4: Innovación y Mejora en el Negocio.
 - A5: Sensibilización y Capacitación en Seguridad de la Información.
 - A6: Entorno Legal y Regulatorio.
 - A7: Gestión de Terceras Partes.
- Sección B: Gestión de Riesgos de la Información.
 - B1: Análisis de Riesgos.
 - B2: Gestión de Riesgos.
- Sección C: Implementación de Sistemas Seguros.
 - C1: Arquitectura de Seguridad.
 - C2: Desarrollo Seguro.
- Sección D: Metodologías y Pruebas para la Seguridad de la Información.
 - D1: Metodologías de Seguridad de la Información.
 - D2: Pruebas de Seguridad.
- Sección E: Disciplina de Seguridad: Gestión de la Seguridad Operacional.
 - E1: Gestión de Operaciones Seguras.
 - E2: Operaciones Seguras y Provisión del Servicio.
 - E3: Evaluación de Vulnerabilidades.
- Sección F: Disciplina de Seguridad: Gestión de Incidentes.
 - F1: Gestión de Incidentes.
 - F2: Investigación.
 - F3: Forense.
- Sección G: Disciplina de Seguridad: Auditoría, Control y Revisión.
 - G1: Auditoría y Revisión.
- Sección H: Disciplina de Seguridad: Gestión de la Continuidad del Negocio.
 - H1: Planificación de la Continuidad del Negocio.

- H2: Gestión de la Continuidad del Negocio.
- Sección I: Disciplina de Seguridad: Investigación de Sistemas de Información.
- I3: Investigación Aplicada.

El *CESG* complementa cada grupo de habilidades *IISP* con una descripción de los conocimientos más relevantes para esa habilidad, así como con una declaración de lo que se espera en cada nivel de habilidad, seguido de ejemplos de comportamientos, competencias, experiencias, versatilidad, autonomía o influencia, consistentes con la declaración previa. Además, las definiciones de habilidad están destinadas a ser acumulativas, es decir, para cumplir con los requisitos en los niveles superiores se debe cumplir con los de los niveles más bajos. Sin embargo, hay que tener en cuenta que, en cambio, las definiciones de roles realizadas por el *CESG* no son acumulativas.

Como ya se ha mencionado anteriormente, la certificación es proporcionada por los organismos de certificación acreditados por el *CESG*, que actualmente son los siguientes:

- *APM Group.*
- *BCS, the Chartered Institute for IT.*
- *IISP, CREST and RHUL consortium.*

Los beneficios del Esquema de Certificación del *CESG* para los profesionales de ciberseguridad son:

- Se evaluarán y verificarán de forma independiente su experiencia y competencia profesional por los organismos de certificación aprobados por el *CESG*.
- Se avalará su capacidad de aplicar de forma eficaz los conocimientos y experiencia para ofrecer beneficios al negocio.
- La pericia en roles de ciberseguridad específicos les permitirá la diferenciación del resto de profesionales.
- Formar parte de una comunidad profesional reconocida y creciente, a partir de la cual los empleadores pueden contratar a los profesionales de ciberseguridad.
- Ser elegible para trabajar en las redes del Gobierno del Reino Unido y en los proyectos de Infraestructuras Críticas Nacionales (sujeto a las habilitaciones de seguridad).

Los beneficios del Esquema de Certificación del *CESG* para los empleadores de profesionales de ciberseguridad son:

- Tener la confianza de que los profesionales de la ciberseguridad certificados han sido evaluados de forma rigurosa e independiente.
- Saber que los profesionales certificados han demostrado su experiencia en ciberseguridad y su capacidad para aplicar las habilidades, el conocimiento y la experiencia de manera efectiva en un entorno operativo.

- Tener la confianza de que los profesionales certificados tienen los conocimientos específicos necesarios para satisfacer las necesidades de negocio.
- Poder utilizar el esquema en la propia organización, para asegurarse de que los profesionales están desarrollando su experiencia, permitiendo a los empleados propios beneficiarse de ser parte de una comunidad reconocida de profesionales de la ciberseguridad.
- Influir en sus proveedores para emplear profesionales certificados, lo que también puede ayudar a reducir los riesgos de la cadena de suministro, ofreciendo una mayor confianza en la capacidad de los proveedores para gestionar con eficacia los riesgos de la información, tanto propia como ajena.

DoD 8570.01-M

Aunque la Directiva 8570.01⁴⁰ del Departamento de Defensa de Estados Unidos (*DoD, Department of Defense*) quedó derogada por la Directiva *DoD* 8140.01⁴¹, publicada el 11 de agosto de 2015, el manual *DoD* 8570.01-M que acompañaba a la primera de ellas sigue estando vigente mientras la nueva Directiva no desarrolle uno propio.

Como su predecesora, la Directiva *DoD* 8140.01 establece las bases para una respuesta departamental a la capacitación, cualificación y gestión de la fuerza de trabajo en seguridad de la información del *DoD*, unificándola a nivel global y estableciendo elementos específicos de mano de obra de ciberseguridad, para alinear, gestionar y estandarizar los roles de trabajo de ciberseguridad, la línea base de cualificaciones y los requisitos de capacitación del *DoD*.

Como su propio nombre indica, el manual *DoD* 8570.01-M⁴² (*Information Assurance Workforce Improvement Program*) constituye un programa en el que se identifican los requisitos específicos y obligatorios establecidos por el *DoD* para la gestión de su personal de seguridad de la información. El objetivo final es mantener una fuerza de trabajo con los conocimientos y habilidades necesarias para prevenir y responder a los ciberataques contra el *DoD*, permitiendo poner a las personas más adecuadas, con las habilidades requeridas, en los puestos necesarios para proteger los sistemas de información del Departamento.

La clave es la definición e identificación de todos los puestos de trabajo de seguridad de la información, de forma que cualquier persona que cubra uno

⁴⁰ Department of Defense, «DoD Directive 8570.01. Information Assurance Training, Certification, and Workforce Management, 8570.01», 2007, <http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf>

⁴¹ Department of Defense, «DoD Directive 8140.01, Cyberspace Workforce Management, DoD», vol. 8140.01, 2015, https://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf

⁴² DoD, «DoD 8570.01-M - Information Assurance Workforce Improvement Program - Incorporating Change 4, November 10, 2015» 19 de diciembre de 2005, <https://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf>

de esos puestos pasa a formar parte de dicha fuerza de trabajo (independientemente de su especialidad). Para ello, el *DoD* establece las funciones de perfiles profesionales de seguridad de la información para todo el Departamento, estructurándolos en categorías, especialidades y niveles.

La fuerza de trabajo de ciberseguridad del *DoD* se divide en dos grandes categorías, una centrada en los aspectos técnicos y otra en las funciones de gestión, con las siguientes denominaciones:

- *Information Assurance Technical (IAT)*.
- *Information Assurance Manager (IAM)*.

Las especialidades son grupos de perfiles profesionales de ciberseguridad del *DoD* que realizan funciones avanzadas o especializadas, que pueden exigir el dominio de un nivel técnico o de gestión específicos. Las especialidades del *DoD* son:

- *Information Assurance System Architect and Engineer (IASAE)*.
- *Computer Network Defense Service Provider (CNDSP)*.

Como ya se ha mencionado previamente, tanto las categorías como las especialidades se pueden desempeñar según diferentes niveles:

- *Computing Environment (level I)*: servidores de redes de área local y su sistema operativo, periféricos y aplicaciones.
- *Networks Environment (level II)*: elementos responsables de la conexión entre elementos del nivel anterior, proporcionando capacidades de transferencia de datos de corto alcance, tales como redes locales o redes de campus, o la capacidad de transporte de datos de larga distancia, tales como redes de área metropolitana o extensa, redes en operaciones o redes troncales.
- *Enclave Environment (level III)*: colección de elementos de nivel 1, conectados por una o más redes internas, bajo el control de una autoridad y política de seguridad únicas, incluyendo al personal y a la seguridad física. Los enclaves proporcionan capacidades de seguridad estándar, como la defensa perimetral, la detección y la respuesta ante incidentes o la gestión de claves, ofreciendo aplicaciones comunes tales como las de ofimática o correo electrónico. Los enclaves pueden ser específicos para una organización o una misión y la organización de los entornos computacionales que albergan se pueden realizar por proximidad física o por función, en este caso independientemente de su ubicación. Ejemplos de enclaves son las redes de área local y las aplicaciones que alojan, así como redes troncales y centros de procesamiento de datos.

Por otro lado, para definir las funciones y requisitos de los puestos de trabajo de la especialidad *CNDSP*, en lugar de utilizar los tres niveles antes referidos, el manual *DoD 8570.01-M* usa los siguientes perfiles profesionales:

- *Analyst*.
- *Infrastructure support*.

- *Incident responder.*
- *Auditor.*
- *Manager.*

El *DoD* establece que todo el personal perteneciente a la fuerza de trabajo de seguridad de la información, tanto militares como civiles o contratistas externos, tanto a tiempo parcial como a tiempo completo, debe estar plenamente cualificado para llevar a cabo adecuadamente sus funciones de seguridad.

Cada categoría y especialidad tiene unos requisitos específicos de formación y certificación establecidos por niveles. Para el cumplimiento de dichos requisitos se requerirá una combinación de capacitación formal y actividades experimentales, como formación en el puesto de trabajo y formación continua.

En lo que se refiere a la capacitación formal, el *DoD* establece una tabla de certificaciones (no propias, sino de mercado, promovidas por empresas u organismos privados), aprobadas según las diferentes categorías, especialidades y niveles, para garantizar que el personal certificado dispone de un entendimiento suficiente de los principios fundamentales de ciberseguridad y de las prácticas relacionadas con las funciones propias de la posición asignada, garantizando así que todo el personal que desempeñe funciones de seguridad de la información en el *DoD* obtenga una de las certificaciones de base necesarias según su puesto de trabajo.

Las certificaciones actualmente aprobadas en el manual *DoD* 8570.01-M según diferentes categorías, especialidades y niveles son las siguientes:

- *Information Assurance Technical (IAT).*
 - *Level I: A+ CE⁴³, Network+ CE⁴⁴, SSCP⁴⁵ y CCNA-Security⁴⁶.*
 - *Level II: GSEC⁴⁷, Security+ CE⁴⁸, SSCP y CCNA-Security.*

⁴³ CompTIA, «A+ (Plus) Certification», accedido 1 de septiembre de 2016, <https://certification.comptia.org/certifications/a>

⁴⁴ CompTIA, «Network+ Certification», accedido 1 de septiembre de 2016, <https://certification.comptia.org/certifications/network>

⁴⁵ (ISC)², «SSCP - Systems Security Certified Practitioner», accedido 1 de septiembre de 2016, <https://www.isc2.org/sscp/default.aspx>

⁴⁶ Cisco, «CCNA (Cisco Certified Network Associate) Security», *Cisco*, accedido 1 de septiembre de 2016, <http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-security.html>

⁴⁷ GIAC, «GSEC - GIAC Security Essentials Certification», accedido 1 de septiembre de 2016, <http://www.giac.org/certification/security-essentials-gsec>

⁴⁸ CompTIA, «Security+ Certification», accedido 1 de septiembre de 2016, <https://certification.comptia.org/certifications/security>

- *Level III: CISA*⁴⁹, *GCIH*⁵⁰, *GCED*⁵¹, *CISSP*⁵² (or *Associate*⁵³) y *CASP CE*⁵⁴.

– *Information Assurance Manager (IAM)*.

- *Level I: CAP*⁵⁵, *GSLC*⁵⁶ y *Security+ CE*.
- *Level II: CAP, GSLC, CISM*⁵⁷, *CISSP* (or *Associate*) y *CASP CE*.
- *Level III: GSLC, CISM y CISSP* (or *Associate*).

– *Information Assurance System Architect and Engineer (IASAE)*.

- *Level I: CISSP* (or *Associate*), *CASP CE* y *CSSLP*⁵⁸.
- *Level II: CISSP* (or *Associate*), *CASP CE* y *CSSLP*.
- *Level III: CISSP-ISSEP*⁵⁹ y *CISSP-ISSAP*⁶⁰.

– *Computer Network Defense Service Provider (CNDSP)*.

- *Analyst: GCIA*⁶¹, *GCIH*, *CEH*⁶² y *SCYBER*⁶³.
- *Infrastructure Support: SSCP* y *CEH*.

⁴⁹ ISACA, «CISA - Certified Information Systems Auditor», accedido 1 de septiembre de 2016, <http://www.isaca.org/certification/cisa-certified-information-systems-auditor/pages/default.aspx>

⁵⁰ GIAC, «GCIH - GIAC Certified Incident Handler», accedido 1 de septiembre de 2016, <http://www.giac.org/certification/certified-incident-handler-gcih>

⁵¹ GIAC, «GCED - GIAC Certified Enterprise Defender», accedido 1 de septiembre de 2016, <http://www.giac.org/certification/certified-enterprise-defender-gced>

⁵² (ISC)², «CISSP - Certified Information Systems Security Professional», accedido 1 de septiembre de 2016, <https://www.isc2.org/cissp/default.aspx>

⁵³ (ISC)², «Become an Associate of (ISC)2 Prior to Obtaining Certification», accedido 1 de septiembre de 2016, <https://www.isc2.org/associate/default.aspx>

⁵⁴ CompTIA, «CASP - CompTIA Advanced Security Practitioner Certification», accedido 1 de septiembre de 2016, <https://certification.comptia.org/certifications/comptia-advanced-security-practitioner>

⁵⁵ (ISC)², «CAP - Certified Authorization Professional», accedido 1 de septiembre de 2016, <https://www.isc2.org/cap/default.aspx>

⁵⁶ GIAC, «GSLC - GIAC Cyber Security Leadership Certification», accedido 1 de septiembre de 2016, <http://www.giac.org/certification/security-leadership-gslc>

⁵⁷ ISACA, «CISM - Certified Information Security Manager», accedido 1 de septiembre de 2016, <http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx>

⁵⁸ (ISC)², «CSSLP - Certified Secure Software Lifecycle Professional», accedido 1 de septiembre de 2016, <https://www.isc2.org/csslp/default.aspx>

⁵⁹ (ISC)², «CISSP-ISSEP - Information Systems Security Engineering Professional», accedido 1 de septiembre de 2016, <https://www.isc2.org/issep.aspx>

⁶⁰ (ISC)², «CISSP-ISSAP - Information Systems Security Architecture Professional», accedido 1 de septiembre de 2016, <https://www.isc2.org/issap.aspx>

⁶¹ GIAC, «GCIA - GIAC Certified Intrusion Analyst», accedido 1 de septiembre de 2016, <http://www.giac.org/certification/certified-intrusion-analyst-gcia>

⁶² EC-Council, «CEH - Certified Ethical Hacker», *EC-Council*, 25 de febrero de 2016, <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>

⁶³ Cisco, «Cybersecurity Specialist», *Cisco*, accedido 1 de septiembre de 2016, <http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/specialist/security/cybersecurity.html>

- *Incident Responder*: GCIH, GCFA⁶⁴, CSIH⁶⁵, CEH y SCYBER.
- *Auditor*: CISA, GSNA⁶⁶ y CEH.
- *Manager*: CISSP-ISSMP⁶⁷ y CISM.

CCN/INAP - Esquema Nacional de Certificación de Profesionales en Ciberseguridad

El 31 de enero de 2014 se publica un comunicado⁶⁸ del Centro Criptológico Nacional (CCN)⁶⁹, adscrito al Centro Nacional de Inteligencia (CNI), informando sobre su propuesta, conjuntamente con el Instituto Nacional de Administración Pública (INAP)⁷⁰ para la creación de un Esquema Nacional de Certificación de Profesionales en Ciberseguridad. Ambos organismos comparten misiones y competencias en la formación del personal de las Administraciones públicas en materia de seguridad de las tecnologías de la información y las comunicaciones. Como indica el comunicado, la propuesta se fundamenta en la escasez de personal con los conocimientos y habilidades en ciberseguridad necesarios para cubrir las exigencias de empresas y Administraciones públicas ante el incremento de las ciberamenazas.

Esta iniciativa es similar a otras desarrolladas en países de nuestro entorno y permitirá diferenciar aquellos programas de formación con rigor y profesionalidad de los que no la tengan.

La propuesta, que viene a complementar algunos de los aspectos recogidos en la Estrategia de Ciberseguridad Nacional (objetivo 5)⁷¹ y del Esquema

⁶⁴ GIAC, «GCFA - GIAC Certified Forensic Analyst», accedido 1 de septiembre de 2016, <http://www.giac.org/certification/certified-forensic-analyst-gcfa>

⁶⁵ SEI (Software Engineering Institute), «CERT-Certified Computer Security Incident Handler», accedido 1 de septiembre de 2016, <https://www.sei.cmu.edu/certification/opportunities/csih/>

⁶⁶ GIAC, «GSNA - GIAC Systems and Network Auditor», accedido 1 de septiembre de 2016, <http://www.giac.org/certification/systems-network-auditor-gsna>

⁶⁷ (ISC)², «CISSP-ISSMP - Information Systems Security Management Professional», accedido 1 de septiembre de 2016, <https://www.isc2.org/issmp/default.aspx>

⁶⁸ CCN (Centro Criptológico Nacional), «El CCN y el INAP apuestan por un Esquema Nacional de Certificación de Profesionales en Ciberseguridad», *Comunicados CCN-CERT*, 31 de enero de 2014, <https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/1846-el-ccn-y-el-inap-apuestan-por-un-esquema-nacional-de-certificacion-de-profesionales-en-ciberseguridad.html>

⁶⁹ Ministerio de Defensa, Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, *BOE*, accedido 27 de mayo de 2013, <https://www.boe.es/boe/dias/2004/03/19/pdfs/A12203-12204.pdf>

⁷⁰ Ministerio de Política Territorial y Administración Pública, Real Decreto 464/2011, de 1 de abril, por el que se aprueba el Estatuto del Instituto Nacional de Administración Pública, vol. BOE-A-2011-6872, 2011, <http://www.boe.es/buscar/pdf/2011/BOE-A-2011-6872-consolidado.pdf>

⁷¹ Gobierno de España, *Estrategia de Ciberseguridad Nacional*, 2013, <http://www.lamoncloa.gob.es/NR/rdonlyres/680D00B8-45FA-4264-9779-1E69D4FEF99D/256935/20131332EstrategiadeCiberseguridadx.pdf>

Nacional de Seguridad (artículo 15)⁷², ofrecerá importantes ventajas tanto para las Administraciones públicas como para las empresas privadas y los profesionales en general. La orientación a las competencias adecuadas a las necesidades de cada organismo, el incremento de la eficiencia de las inversiones de formación y el aumento de la madurez profesional del sector son algunos de los beneficios que traería esta certificación.

El desarrollo detallado del manual de competencias, definiendo todos los conocimientos y habilidades que les serán requeridos a los diferentes perfiles/ categorías profesionales del esquema, el establecimiento de mecanismos de evaluación de candidatos, la elaboración de un código de conducta profesional, la determinación de los prerrequisitos de certificación y los procesos de renovación, así como la acreditación del esquema por la Entidad Nacional de Acreditación (ENAC), según la norma UNE-EN ISO/IEC 17024⁷³, serían los siguientes pasos a abordar dentro del Esquema.

La estructura general del posible Esquema de Certificación de Profesionales de Ciberseguridad para España constaría de cuatro elementos principales:

- ENAC: que acreditaría el esquema de certificación según la norma UNE-EN ISO/IEC 17024.
- CCN/INAP: que actuarían conjuntamente como Organismo de Certificación del Esquema, autorizando y supervisando a las entidades de evaluación reconocidas, y emitiendo los certificados profesionales que hayan superado las pruebas de evaluación.
- Entidades de evaluación: que, una vez autorizadas por el Organismo de Certificación, llevarían a cabo las evaluaciones de los candidatos.
- Candidatos: que serían todos aquellos profesionales que quieran certificar sus competencias en ciberseguridad.

La propuesta para un Esquema de Certificación incluiría dos roles profesionales⁷⁴:

- Ingeniero de Ciberseguridad.
- Auditor de Ciberseguridad.

Cada uno de los roles anteriores con tres categorías profesionales, según la experiencia y el nivel de competencias requeridos:

- Profesional.

⁷² Ministerio de la Presidencia, Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, 2010, <http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf>

⁷³ International Organization for Standardization, «ISO/IEC 17024:2012 - Evaluación de la conformidad. Requisitos generales para los organismos que realizan certificación de personas» (ISO/IEC, 2012), http://www.iso.org/iso/catalogue_detail?csnumber=52993

⁷⁴ INAP, CCN y Óscar PASTOR, «Esquema de Certificación de Personas», en *VII Jornadas STIC CCN - CERT* (Madrid, 2013), <https://www.ccn-cert.cni.es/privatedocs/viijornadas/742-12-opastor-ccn-isdefe-esquemadecertificaciondepersonas/file.html>

- Senior.
- Principal.

Inicialmente, el manual de conocimientos y habilidades de la propuesta de Esquema de Certificación de personas incluiría noventa competencias básicas, estructuradas en cuatro dominios y once subdominios:

- Gestión de la Seguridad de la Información.
 - Seguridad de la Información y Objetivos de la Organización.
 - Marco Normativo.
 - Cultura de Seguridad.
 - Cumplimiento.
 - Entidades Externas.
 - Gestión de Riesgos (Análisis y Tratamiento de Riesgos).
- Seguridad en el Ciclo de Vida del Sistema.
 - Obtención de Sistemas Seguros (Arquitectura de Seguridad, Diseño/Desarrollo de Sistemas y Pruebas).
 - Seguridad en las Operaciones (Aplicación de Procedimientos, Configuraciones de Seguridad y Prevención de Incidentes).
- Gestión de Excepciones de Seguridad.
 - Incidentes de Seguridad (Gestión y Respuesta a Incidentes de Seguridad e Investigación/Forense).
 - Continuidad del Servicio (Planificación y Pruebas/Ejercicios).
- Auditoría de Seguridad.
 - Auditoría de Seguridad (Planificación, Ejecución e Informe).

Los posibles beneficios de la implantación de un Esquema Nacional de Certificación de Profesionales en Ciberseguridad serían⁷⁵:

- Para las Administraciones públicas:
 - Incrementar la eficiencia de las acciones de formación en seguridad de su personal, orientándolas a competencias adecuadas para el desempeño de sus funciones.
 - Aumentar el conocimiento sobre sus capacidades/necesidades de profesionales de la ciberseguridad.
 - Mejorar los criterios de asignación de destinos.
 - Disponer de criterios objetivos de competencia profesional en ciberseguridad para la licitación y selección de servicios con proveedores externos.
 - Asegurarse, mediante la gestión y el control del esquema de certificación, que las competencias, conocimientos y habilidades de los profesio-

⁷⁵ Óscar Pastor y Javier Candau, «Propuesta para un Esquema Nacional de Certificación de Profesionales en Ciberseguridad para España», *Revista SIC*, febrero de 2014.

nales de la ciberseguridad están siempre alineadas con el cumplimiento de su misión y las correspondientes estrategias nacionales.

- Para la empresas del sector privado:
 - Disponer de criterios objetivos sobre los requisitos profesionales para la licitación de servicios.
 - Incrementar la eficiencia de las inversiones de formación de su personal.
 - Disponer de un esquema de garantía profesional independiente y de calidad.
- Para los profesionales en general:
 - Incrementar la madurez profesional del sector de la ciberseguridad.
 - Mejora de las expectativas y plan de carrera profesional.

SEPE - Certificado de Profesionalidad en Seguridad Informática

El Servicio Público de Empleo Estatal (SEPE)⁷⁶ es un organismo autónomo dependiente del Ministerio de Empleo y Seguridad Social. Entre sus competencias se encuentra la de elaborar, y elevar al Ministerio para su aprobación, propuestas normativas de ámbito estatal en materia de formación para el empleo, así como gestionar los correspondientes programas de formación profesional para el empleo.

En el mes de junio del año 2011 se publica el Real Decreto 686/2011⁷⁷, por el que se establecen seis certificados de profesionalidad, siendo uno de ellos el denominado Seguridad Informática. En el anexo III⁷⁸ de dicho Real Decreto se incluyen los detalles correspondientes a la Certificación Profesional en Seguridad Informática, que se creaba a partir de dicha norma, con el código IFCT0109.

El objeto de este Certificado de Profesionalidad es acreditar personal capaz de garantizar la seguridad de los accesos y usos de la información contenida en equipos informáticos, así como del propio sistema, protegiéndose de los posibles ataques, identificando vulnerabilidades y aplicando sistemas de cifrado a las comunicaciones que se realicen hacia el exterior y en el interior de la organización.

⁷⁶ Ministerio de Empleo y Seguridad Social, «Servicio Público de Empleo Estatal», accedido 2 de septiembre de 2016, <http://www.empleo.gob.es/es/organizacion/empleo/contenido/OM29.htm>

⁷⁷ BOE, Real Decreto 686/2011, de 13 de mayo, por el que se establecen seis certificados de profesionalidad de la familia profesional Informática y comunicaciones que se incluyen en el Repertorio Nacional de Certificados de Profesionalidad, 2011, https://sede.sepe.gob.es/es/portaltrabaja/resources/pdf/normativaCertificados/RD686_2011.pdf

⁷⁸ BOE, anexo III al Real Decreto 686/2011, Certificado de Profesionalidad en Seguridad Informática, 2011, <https://sede.sepe.gob.es/es/portaltrabaja/resources/pdf/especialidades/IFCT0109.pdf>

Se prevé que estos profesionales desarrollen su actividad en el área de sistemas del departamento de informática de empresas públicas o privadas que utilizan equipamiento informático, desempeñando tareas de auditoría, configuración y temas relacionados con la seguridad informática, tanto por cuenta ajena como por cuenta propia. Además, se supone que aunque estarán presentes en múltiples sectores productivos, trabajarán sobre todo en el sector servicios, aunque se percibe una marcada característica de transectorialidad. Los tipos de empresas a las que prestarán sus servicios serán:

- Empresas de cualquier sector y tamaño que utilizan equipamiento informático en sus procesos de gestión.
- Empresas que prestan servicios de asistencia técnica informática.
- Empresas de externalización (*outsourcing*) de servicios.
- El Certificado está desglosado en unidades de competencia, para detallar mejor los conocimientos y habilidades que deben poseer los profesionales certificados:
- Asegurar equipos informáticos (UC0486_3).
- Auditar redes de comunicación y sistemas informáticos (UC0487_3).
- Detectar y responder ante incidentes de seguridad (UC0488_3).
- Diseñar e implementar sistemas seguros de acceso y transmisión de datos (UC0489_3).
- Gestionar servicios en el sistema informático (UC0490_3).

Se establece que una formación asociada para estos profesionales de 500 horas, desglosada en los siguientes módulos formativos:

- Seguridad en Equipos Informáticos (MF0486_3): 90 horas.
- Auditoría de Seguridad Informática (MF0487_3): 90 horas.
- Gestión de Incidentes de Seguridad Informática (MF0488_3): 90 horas.
- Sistemas Seguros de Acceso y Transmisión de datos (MF0489_3): 60 horas.
- Gestión de Servicios en el Sistema Informático (MF0490_3): 90 horas.
- Prácticas Profesionales no Laborales de Seguridad informática (MP0175): 80 horas.

Además, al tratarse de un Certificado Profesional de nivel 3, se establecen una serie de requisitos previos:

- Estar en posesión del título de Bachiller.
- Estar en posesión de un certificado de profesionalidad del mismo nivel del módulo o módulos formativos y/o del certificado de profesionalidad al que se desea acceder.
- Estar en posesión de un certificado de profesionalidad de nivel 2 de la misma familia y área profesional para el nivel 3.
- Cumplir el requisito académico de acceso a los ciclos formativos de grado superior, o bien haber superado las correspondientes pruebas de acceso reguladas por las Administraciones educativas.

- Tener superada la prueba de acceso a la universidad para mayores de 25 años y/o de 45 años.
- Tener los conocimientos formativos o profesionales suficientes que permitan cursar con aprovechamiento la formación.
- Además, las personas que no tengan experiencia laboral en el sector, deben realizar obligatoriamente el módulo de prácticas, siendo este un requisito indispensable para obtener el título oficial.

Finalmente, una vez se haya obtenido la Certificación Profesional en Seguridad Informática, el SEPE establece que los profesionales acreditados puedan ocupar la siguiente relación de puestos de trabajo:

- Programador de Aplicaciones Informáticas (Código Nacional de Ocupación 3820.1017).
- Técnico en Informática de Gestión (Código Nacional de Ocupación 3812.1014).
- Técnico en Seguridad Informática.
- Técnico en Auditoría Informática.

Iniciativas privadas de formación y certificación en ciberseguridad

Analicemos a continuación los programas de formación y certificación profesional de ciberseguridad promovidos por empresas y organizaciones privadas, líderes a nivel internacional.

ISACA-CSX (Cybersecurity Nexus)

*ISACA (Information Systems Audit and Control Association)*⁷⁹ es una de las organizaciones señeras en los ámbitos del control, la auditoría y la seguridad de los sistemas y tecnologías de la información, que desde hace casi cincuenta años ayuda a los profesionales a liderar, adaptar y asegurar la confianza en un mundo digital en evolución, ofreciendo conocimiento, estándares, relaciones, acreditación y desarrollo de carreras profesionales innovadoras y de primera clase. Establecida en 1969, *ISACA* es una asociación internacional sin ánimo de lucro que cuenta con unos ciento cuarenta mil profesionales en ciento ochenta y siete países. La asociación dispone de más de doscientos diez capítulos en todo el mundo.

ISACA es la creadora de COBIT⁸⁰, un marco de negocio para gobernar la tecnología de la empresa, y promueve desde hace años el avance y la certificación de habilidades y conocimientos críticos para el negocio, a través de las

⁷⁹ ISACA, «ISACA Fact Sheet», accedido 29 de agosto de 2016, http://www.isaca.org/About-ISACA/Press-room/Documents/2016-ISACA-Fact-Sheet_pre_eng_0716.pdf

⁸⁰ Information Systems Audit and Control Association, *Cobit 5: A Business Framework for the Governance and Management of Enterprise IT* (Rolling Meadows. IL: ISACA, 2012).

certificaciones, de reconocido prestigio a nivel internacional, entre las que se encuentran:

- *CISA (Certified Information Systems Auditor)*⁸¹.
- *CISM (Certified Information Security Manager)*⁸².
- *CGEIT (Certified in the Governance of Enterprise IT)*⁸³.
- *CRISC (Certified in Risk and Information Systems Control)*⁸⁴.

En 2014, *ISACA* crea el programa *Cybersecurity Nexus (CSX)*⁸⁵ con el objetivo de ayudar a cubrir la brecha de habilidades de seguridad cibernética, surgida entre la demanda y la oferta de profesionales de este ámbito (ya analizados previamente), y así proporcionar un desarrollo para los profesionales de este sector, en cada etapa de su carrera, ayudando a las empresas a desarrollar su fuerza de trabajo cibernético. *CSX* representa el compromiso de *ISACA* para ayudar a abordar la necesidad mundial de profesionales cualificados en ciberseguridad.

El programa *CSX* se diseña para ayudar a las empresas a fortalecer sus capacidades de ciberseguridad, mediante educación, formación y certificación de su personal, haciéndoles capaces de proteger la información de sus organizaciones. Para ello, *CSX* ayuda a obtener los conocimientos y habilidades que se necesitan para llevar a cabo completamente las tareas de ciberseguridad con una orientación de formación por competencias y de certificación basada en el desempeño. *CSX* está alineado con marcos de referencia internacionales como los ya mencionados *National Cybersecurity Workforce Framework*, del *NICE/NICCS*, o *SFIA*.

El programa de acreditación *CSX*⁸⁶ ofrece varios niveles de certificación, desde el más inicial hasta el experto, según la experiencia y formación de los candidatos a obtener estas credenciales.

⁸¹ *ISACA*, «Certified Information Systems Auditor™ (CISA®) Fact Sheet», accedido 29 de agosto de 2016, http://www.isaca.org/About-ISACA/Press-room/Documents/2015-CISA-Fact-Sheet_pre_eng_1015.pdf

⁸² *ISACA*, «Certified Information Security Manager® (CISM®) Fact Sheet», accedido 29 de agosto de 2016, http://www.isaca.org/About-ISACA/Press-room/Documents/2015-CISM-Fact-Sheet_pre_eng_1015.pdf

⁸³ *ISACA*, «Certified in the Governance of Enterprise IT (CGEIT) Fact Sheet», accedido 29 de agosto de 2016, http://www.isaca.org/About-ISACA/Press-room/Documents/2015-CGEIT-Fact-Sheet_pre_eng_1015.pdf

⁸⁴ *ISACA*, «Certified in Risk and Information Systems Control (CRISC)», accedido 29 de agosto de 2016, http://www.isaca.org/About-ISACA/Press-room/Documents/2015-CRISC-Fact-Sheet_pre_eng_1015.pdf

⁸⁵ *ISACA*, «Cybersecurity Nexus (CSX) Fact Sheet», accedido 29 de agosto de 2016, http://www.isaca.org/cyber/Documents/Cybersecurity-Nexus-Fact-Sheet_pre_Eng_0115.pdf

⁸⁶ *ISACA*, «Cybersecurity Nexus™ (CSX) General Awareness Brochure», 2016, http://www.isaca.org/cyber/Documents/CSX-General-Awareness-Brochure_Bro_Eng_0816.pdf

Cybersecurity Fundamentals Certificate

Es el nivel de entrada en el programa y se trata de un certificado basado en el conocimiento. Está diseñado para universitarios recién graduados o aquellas personas que buscan un cambio en su carrera profesional hacia el ámbito de la ciberseguridad, ya que les permite demostrar su comprensión de los conceptos básicos de la seguridad cibernética.

Los exámenes revisan los conocimientos básicos en ciberseguridad a través de cinco áreas clave:

- Conceptos de ciberseguridad.
- Principios de arquitectura de ciberseguridad.
- Ciberseguridad de las redes, sistemas, aplicaciones y datos.
- Implicaciones de seguridad en la adopción de tecnologías emergentes.
- Respuesta a incidentes.

CSX Practitioner (CSXP)

Se trata de la primera certificación basada en el desempeño, dentro del esquema de certificaciones *CSX*, que permite a los que la poseen demostrar su capacidad para trabajar como primera línea de respuesta ante incidentes de ciberseguridad, siguiendo procedimientos establecidos, utilizando procesos definidos y trabajando con problemas conocidos en un único sistema.

La certificación *CSXP* indica que se dispone de experiencia en la configuración de cortafuegos, la gestión de parches de seguridad y los antivirus, así como capacidad de implementar controles de seguridad comunes y realizar exploraciones y análisis de vulnerabilidades. Para cumplir con requisitos de educación profesional continua, los poseedores de la certificación *CSXP* deben demostrar anualmente habilidades prácticas en un laboratorio y volver a examinarse cada tres años (al nivel de certificación *CSX* más alto que hubieran obtenido).

CSX Specialist

El siguiente nivel en la serie de certificaciones *CSX* es *Specialist*, y permite demostrar un profundo conocimiento y habilidad en ciberseguridad. En realidad, se trata de una serie de tres certificaciones independientes que cubren los cinco dominios del Marco de Referencia de Ciberseguridad del *NIST*⁸⁷: identificar, proteger, detectar, responder y recuperarse.

- *CSX | Specialist: Identify and Protect*. Los especialistas dentro de este dominio son capaces de analizar y estimar las ciberamenazas a diferentes niveles de la infraestructura, desde un equipo individual hasta el nivel del sistema en su globalidad, utilizando buenas prácticas y herramientas

⁸⁷ NIST, «Framework for Improving Critical Infrastructure Cybersecurity», Cybersecurity Framework (National Institute of Standards and Technology, 12 de febrero de 2014), <http://www.cslawreport.com/files/2015/04/07/nist-combined-file.pdf>

comúnmente aceptadas. Estos profesionales son capaces de implementar controles de ciberseguridad con el fin de proteger tanto los sistemas como las redes.

- *CSX | Specialist: Detect*. Estos especialistas son capaces de distinguir incidentes y eventos mediante la identificación de indicadores de compromiso de red y de sistema, estimando posibles daños y proporcionando datos necesarios a los equipos de primera respuesta.
- *CSX | Specialist: Respond and Recover*. Los especialistas dentro de este dominio son capaces de desarrollar, implementar y mantener planes de respuesta a incidentes individuales, están familiarizados con técnicas de respuesta y están capacitados para comunicar correctamente eventos e incidentes. Pueden desarrollar, implementar y mantener planes de recuperación, así como utilizar herramientas especializadas para la evaluación de la integridad y de copias de seguridad distribuidas, proporcionan la restauración del servicio y sus tareas de apoyo.

Estas certificaciones se basan en las habilidades desarrolladas en la certificación *CSXP* (puesto que es un requisito previo disponer de la certificación *CSXP* antes de obtener una de las *CSX Specialist*) y en conceptos avanzados en cada uno de los dominios. *ISACA* ofrece un curso de formación de cinco días, para cada una de las certificaciones *CSX Specialist*, diseñado para enseñar las habilidades necesarias para practicar en un nivel que combina clases teóricas con al menos el 50 % de ejercicios prácticos en un entorno de laboratorio virtual.

CSX Expert

Aunque todavía no está abierta a candidatos, la certificación *CSX Expert* constituirá el vértice más alto del programa de certificación *CSX* de *ISACA*, permitiendo demostrar una maestría profesional y técnica en ciberseguridad, que garantiza el ser capaz de identificar, analizar, responder y mitigar los incidentes de ciberseguridad más complicados, generalmente en entornos empresariales complejos, en ambientes de alto nivel de exposición a los ciberataques.

Los expertos con esta certificación están destinados a servir como fuente autorizada para todos los asuntos de ciberseguridad, dentro de la organización, y a ser los responsables en la aprobación de los controles de seguridad, de los análisis de causa raíz y de correlación, para la evaluación de impacto en el negocio. Trabajan con la alta dirección para maximizar los éxitos de ciberseguridad en la organización y para comunicar los impactos comerciales relacionados con problemas cibernéticos, sirviendo como jefes de los equipos de respuesta a incidentes y de recuperación de desastres.

Certified Information Security Manager (CISM).

Aunque se trata de una certificación creada con anterioridad al programa *CSX*, *ISACA* incluye *CISM* dentro de la serie de certificaciones *CSX*, al mismo

nivel que *CSX Expert*, como certificación para demostrar el máximo nivel de pericia en la gestión de la seguridad de la información. Constituye, por tanto, una ruta de certificación alternativa o complementaria a la *CSX Expert*, centrada en los aspectos más técnicos, mientras que *CISM* se centra en los de gestión, que completa la serie *CSX* para ofrecer una trayectoria curricular completa, desde el nivel inicial al experto, desde los aspectos más técnicos a los gerenciales.

La certificación *CISM* identifica a personas que entienden el negocio para gestionar, diseñar, supervisar y evaluar la seguridad de la información en la empresa. Demuestra el entendimiento de quien la ostenta sobre las relaciones entre un programa de seguridad de la información y los objetivos de negocio de la organización. Garantiza no solo la máxima pericia en la seguridad de la información, sino también un profundo conocimiento y experiencia en el desarrollo y gestión de un programa de seguridad de la información.

ISACA establece los requisitos para obtener la certificación *CISM* agrupándolos en cuatro dominios, con diferentes pesos relativos, que después son definidos y detallados en conocimientos y tareas profesionales, que representan un análisis de las prácticas profesionales que llevan a cabo en todo el mundo los gestores de seguridad de la información.

Los cuatro dominios de la certificación *CISM* son:

- Dominio 1: Gobernanza de la Seguridad de la Información (24 %).
- Dominio 2: Gestión de Riesgos de la Información y Cumplimiento (33 %).
- Dominio 3: Desarrollo y Gestión de Programas de Seguridad de la Información (25 %).
- Dominio 4: Gestión de Incidencias de Seguridad de la Información (18 %).

(ISC)²-CISSP (Certified Information Systems Security Professional)

El Consorcio Internacional de Certificación de Seguridad de Sistemas de Información (*ISC*)², siguiendo su denominación original en inglés (*International Information System Security Certification Consortium*)⁸⁸, es otra de las asociaciones más veteranas y con mayor prestigio en el campo de la seguridad de la información.

(*ISC*)² es una asociación internacional, sin ánimo de lucro, centrada en inspirar un mundo cibernético seguro y protegido. (*ISC*)² ofrece un conjunto de certificaciones profesionales con un enfoque integral y estructurado a la ciberseguridad. Dispone de más de 115.000 miembros, constituyendo una robusta comunidad de profesionales certificados en ciberseguridad que están contribuyendo al avance de la industria de este sector.

⁸⁸ (*ISC*)², «(*ISC*)² Overview», accedido 5 de septiembre de 2016, [https://www.isc2.org/uploadedfiles/\(isc\)2_public_content/\(isc\)2-company-overview.pdf](https://www.isc2.org/uploadedfiles/(isc)2_public_content/(isc)2-company-overview.pdf)

La certificación más conocida y demandada de (ISC)² es *CISSP (Certified Information Systems Security Professional)*⁸⁹. Se trata de una certificación, independiente de los fabricantes de tecnología, destinada a aquellos profesionales con avanzadas y probadas competencias técnicas y de gestión, con habilidades, experiencia y credibilidad para crear, diseñar e implementar programas globales de seguridad de la información, con el objetivo de proteger a las organizaciones ante la creciente sofisticación de los ataques cibernéticos.

Entre los perfiles profesionales a los que va destinada esta certificación se encontrarían los de consultor de seguridad, gerente de seguridad, director/gerente TI, auditor de seguridad, arquitecto de seguridad, analista de seguridad, ingeniero de sistemas de seguridad, *CISO (Chief Information Security Officer)*, director de seguridad y arquitecto de redes.

CISSP es una de las credenciales más veteranas en el campo de la seguridad de la información y cumple con los estrictos requisitos de las Norma ISO/IEC 17024, convirtiéndose en una certificación de reconocido prestigio internacional asociada a la excelencia profesional. Para ello, la certificación *CISSP* se fundamenta en un Cuerpo de Conocimiento Común (*CBK, Common Body of Knowledge*) continuamente revisado y puesto al día por (ISC)², para asegurar que los profesionales certificados tienen un profundo conocimiento y comprensión de las nuevas amenazas, las tecnologías, la legislación, la normativa y las buenas prácticas en ciberseguridad.

El *CISSP CBK* se desglosa en ocho dominios, cada uno de los cuales cubre diferentes tópicos o aspectos de la seguridad de la información:

- Seguridad y gestión de riesgos:
 - Conceptos de confidencialidad, integridad y disponibilidad.
 - Principios de gobierno de la seguridad.
 - Cumplimiento.
 - Aspectos legales y reglamentarios.
 - Ética profesional.
 - Políticas, normas, procedimientos y directrices de seguridad.
- Seguridad de activos:
 - Clasificación de la información y de los activos.
 - La propiedad (propietarios de datos, propietarios del sistema).
 - Proteger la privacidad.
 - Retención adecuada.
 - Controles de seguridad de los datos.
 - Requisitos de manipulación (marcas, etiquetas y almacenamiento).

⁸⁹ (ISC)², «*CISSP (Certified Information Systems Security Professional) Brochure*», 16 de diciembre de 2015, https://www.isc2.org/uploadedfiles/credentials_and_certification/cis-sp/cissp-information.pdf

- Ingeniería de seguridad:
 - Procesos de ingeniería por medio de principios de diseño seguro.
 - Conceptos fundamentales de los modelos de seguridad.
 - Modelos de evaluación de la seguridad.
 - Capacidades de seguridad de los sistemas de información.
 - Arquitecturas de seguridad, diseños y vulnerabilidades de elementos de las soluciones.
 - Vulnerabilidades de sistemas basados en la web.
 - Vulnerabilidades de sistemas móviles.
 - Dispositivos empotrados y vulnerabilidades de los sistemas ciberfísicos.
 - Criptografía.
 - Principios de diseño seguro de ubicaciones y edificios.
 - Seguridad física.
- Seguridad de comunicaciones y red:
 - Diseño de arquitecturas de red seguras (protocolos IP y no IP, segmentación).
 - Componentes de redes seguras.
 - Canales de comunicación seguros.
 - Ataques de red.
- Gestión de identidades y acceso:
 - Control de activos físicos y lógicos.
 - Identificación y autenticación de personas y dispositivos.
 - Identidad como servicio (identidad en la nube).
 - Servicios de identidad de terceros (en las instalaciones).
 - Ataques de control de acceso.
 - Ciclo de vida del aprovisionamiento de identidades y accesos (revisión de aprovisionamiento).
- Evaluación y pruebas de seguridad:
 - Estrategias de evaluación y prueba.
 - Datos del proceso de seguridad (la gestión y los controles operacionales).
 - Pruebas de control de la seguridad.
 - Salidas de prueba (automatizado, manual).
 - Vulnerabilidades de las arquitecturas de seguridad.
- Operaciones de seguridad:
 - Apoyo a las investigaciones y sus requisitos.
 - Actividades de gestión de registros y monitorización.
 - Aprovisionamiento de los recursos.
 - Conceptos fundamentales de operaciones de seguridad.
 - Técnicas de protección de recursos.
 - Gestión de incidentes.
 - Medidas preventivas.

- Gestión de parches y vulnerabilidades.
 - Procesos de gestión del cambio.
 - Estrategias de recuperación.
 - Procesos y planes de recuperación ante desastres.
 - Planificación y ejercicios de la continuidad de negocio.
 - Seguridad física.
 - Consideraciones sobre la protección del personal.
- Seguridad en el desarrollo *software*:
- Seguridad en el ciclo de vida de desarrollo *software*.
 - Controles de seguridad del entorno de desarrollo.
 - Efectividad de la seguridad del *software*.
 - Impacto en la seguridad del *software* adquirido.

Los candidatos a *CISSP* deben acreditar al menos cinco años de experiencia a tiempo completo en dos o más de los dominios anteriores. Además, deberán superar un examen de seis horas de duración, compuesto de doscientas cincuenta preguntas, de elección múltiple, debiendo obtener una calificación de 700 o más sobre un total de 1.000 puntos.

Además, para mantener la credencial, se requiere la recertificación cada tres años, para lo que se deben obtener y presentar un mínimo de 40 créditos *CPE* (*Continuing Professional Education*) cada año del ciclo de certificación de tres años y un total de 120 créditos *CPE* al final del ciclo de certificación de tres años.

Debido a la constante evolución de los diferentes aspectos que afectan a la ciberseguridad, (*ISC*)² ha evolucionado la concepción original de la certificación *CISSP*, desarrollando nuevas credenciales específicas que la complementan, que ha denominado *CISSP-Concentrations*⁹⁰, para abordar las necesidades concretas de las diferentes comunidades de profesionales de la ciberseguridad, centradas en las áreas funcionales de:

- Arquitectura.
- Ingeniería.
- Gestión.

Superar el examen de una de las *CISSP-Concentrations* demuestra una mayor capacidad y experiencia, en ese aspecto concreto, que la requerida para las credenciales *CISSP* estándar.

CISSP-ISSAP - Information Systems Security Architecture Professional

Esta credencial está destinada a profesionales certificados *CISSP* que desarrollen su trabajo en posiciones tales como arquitecto de sistemas, director

⁹⁰ (*ISC*)², «*CISSP Concentrations*», accedido 5 de septiembre de 2016, [https://www.isc2.org/uploadedfiles/\(isc\)2_public_content/certification_programs/cissp_concentrations/concentrations-web.pdf](https://www.isc2.org/uploadedfiles/(isc)2_public_content/certification_programs/cissp_concentrations/concentrations-web.pdf)

de informática (*CTO, Chief Technology Officer*), ingeniero de redes y sistemas, analista de negocio o jefe de ciberseguridad.

Para (*ISC*)², los arquitectos de ciberseguridad juegan un papel fundamental dentro del departamento de seguridad de la información de las organizaciones, con responsabilidad para ajustar funcionalmente las expectativas de la alta dirección y la implementación de los programas de ciberseguridad. Normalmente, estos profesionales deben desarrollar, diseñar o analizar el plan de ciberseguridad global de la organización. Aunque, por lo general, el rol que desempeñan estos profesionales puede estar estrechamente vinculado a la tecnología, su desempeño fundamental debe estar más próximo al proceso de consultoría y análisis de ciberseguridad de la información, por lo que (*ISC*)² entiende que *ISSAP* es una credencial muy apropiada para profesionales *CISSP* que trabajan como consultores independientes.

El Cuerpo de Conocimiento del *CISSP-ISSAP* se desglosa en seis dominios:

- Sistemas y Metodologías de Control de Acceso.
- Seguridad de Comunicaciones y Red.
- Criptografía.
- Análisis de la Arquitectura de Seguridad.
- Tecnologías Relacionadas con el Plan de Continuidad de Negocio y el Plan de Recuperación ante Desastres.
- Consideraciones de Seguridad Física.

Para obtener la certificación *CISSP-ISSAP*, un candidato debe demostrar dos años de experiencia profesional, a tiempo completo, en el ámbito de la arquitectura de ciberseguridad y, además, superar un examen de tres horas de duración, compuesto de ciento veinticinco preguntas, de elección múltiple, debiendo obtener una calificación de 700 o más sobre un total de 1.000 puntos.

CISSP-ISSEP - Information Systems Security Engineering Professional

(*ISC*)² desarrolló la certificación *CISSP-ISSEP* conjuntamente con la Agencia Nacional de Seguridad de Estados Unidos (*NSA, National Security Agency*)⁹¹, con el objetivo de proporcionar una valiosa herramienta para cualquier profesional de la ingeniería de sistemas de seguridad. *ISSEP* se constituye así como una guía para la incorporación de la ciberseguridad en proyectos, aplicaciones, procesos de negocio y cualquier sistema de información. Esto responde a la urgente demanda de los profesionales de la ciberseguridad por disponer de metodologías viables y mejores prácticas, que se puedan utilizar de forma real, para integrar la seguridad en todas las facetas de las operaciones de negocio.

⁹¹ NSA, «Mission & Strategy», accedido 5 de septiembre de 2016, <https://www.nsa.gov/about/mission-strategy/>

Esta credencial está destinada a profesionales certificados *CISSP* que desarrollen su trabajo en posiciones tales como ingeniero senior de sistemas, ingeniero de sistemas de seguridad de la información, director de seguridad de la información, analista de seguridad de la información o analista senior de seguridad.

El Cuerpo de Conocimiento del *CISSP-ISSEP* se desglosa en cuatro dominios:

- Ingeniería de Seguridad de Sistemas.
- Certificación y Acreditación/Marco de Referencia para la Gestión de Riesgos.
- Gestión Técnica.
- Políticas y Publicaciones del Gobierno de Estados Unidos Relacionadas con la Seguridad de la Información.

Para obtener la certificación *CISSP-ISSEP*, un candidato debe demostrar dos años de experiencia profesional, a tiempo completo, en este ámbito de la ciberseguridad y, además, superar un examen de tres horas de duración, compuesto de ciento cincuenta preguntas, de elección múltiple, debiendo obtener una calificación de 700 o más sobre un total de 1.000 puntos.

CISSP-ISSMP - Information Systems Security Management Professional

Esta credencial está destinada a profesionales certificados *CISSP* que desarrollen su trabajo en posiciones tales como director de informática, director de seguridad de la información, director de tecnología o ejecutivo senior de seguridad.

Esta certificación contiene elementos que implican profundos conocimientos de gestión, tales como gestión de proyectos, gestión de riesgos, desarrollo y puesta en práctica de un programa de concienciación sobre seguridad o la gestión de un programa de planificación de la continuidad del negocio. Para (ISC)², un profesional *CISSP-ISSMP* establece, presenta y gestiona los programas de seguridad de la información, demostrando profundas habilidades de gestión y liderazgo. Normalmente, los profesionales que ostenten la certificación *ISSMP* serán los encargados de diseñar la estructura del departamento de ciberseguridad de una empresa u organización, así como de definir los medios para apoyar a este grupo internamente. Estos profesionales disponen de una comprensión completa, avanzada y definida de la gestión de la seguridad de la información.

El Cuerpo de Conocimiento del *CISSP-ISSMP* se desglosa en cinco Dominios:

- Liderazgo y Gestión de la Seguridad.
- Gestión del Ciclo de Vida de Seguridad.
- Gestión del Cumplimiento de Seguridad.
- Gestión de Contingencias.
- Legislación, Ética y Gestión de Incidentes.

Para obtener la certificación *CISSP-ISSMP* un candidato debe demostrar dos años de experiencia profesional, a tiempo completo, en la gestión de un gran

modelo de seguridad de toda una empresa u organización y, además, superar un examen de tres horas de duración, compuesto de ciento veinticinco preguntas, de elección múltiple, debiendo obtener una calificación de 700 o más sobre un total de 1.000 puntos.

SANS/GIAC

El Instituto SANS (originalmente, *SysAdmin, Networking and Security Institute*)⁹² es una institución privada, fundada en 1989, con sede en los Estados Unidos, cuyos programas de formación son seguidos por más de 165.000 profesionales de la seguridad informática de todo el mundo, desde auditores y administradores de sistemas hasta directores de seguridad informática.

Sus principales objetivos son:

- La investigación y recopilación de información sobre todo lo referente a seguridad informática (sistemas operativos, *routers*, *firewalls*, aplicaciones, *IDS*, etcétera). En este campo, muchos de los valiosos recursos del SANS son de libre acceso, entre los que cabe mencionar:
 - *Internet Storm Center* (Sistema de Alerta Temprana de la Internet).
 - *NewsBites* (boletín semanal de noticias).
 - *@RISK* (boletín semanal de vulnerabilidades).
 - *CIS Critical Security Controls* (clasificación de consenso de los controles de seguridad que son más eficaces en la reducción del riesgo a los ciberataques del mundo real).
- Ofrecer programas de capacitación y certificación en el ámbito de la seguridad informática.
 - Más de cuatrocientos cursos, en noventa ciudades de todo el mundo, diseñados para dominar las medidas prácticas necesarias para la defensa de redes y sistemas contra las ciberamenazas más virulentas, que están siendo explotados de forma activa.
 - Los cursos tienen una orientación eminentemente técnica, para que los conocimientos adquiridos puedan ser puestos en práctica de forma inmediata en los respectivos puestos de trabajo.

Por otro lado, *GIAC (Global Information Assurance Certification)*⁹³ es una entidad de certificación de seguridad de la información, especializada en la certificación técnica y práctica, que fue fundada en 1999 por el *SANS Institute*. Los primeros profesionales *GIAC* fueron certificados en el año 2000 y en la actualidad se han emitido más de 84.000 certificaciones *GIAC*.

⁹² SANS, «SANS Institute: About», accedido 6 de septiembre de 2016, <https://www.sans.org/about/>

⁹³ GIAC, «About GIAC», accedido 6 de septiembre de 2016, <http://www.giac.org/about>

GIAC proporciona un conjunto de certificaciones de ciberseguridad, independientes de los proveedores de tecnología, vinculados a los cursos de formación impartidos por el *Instituto SANS*. Aunque están alineados, los programas de formación del *SANS* y los de certificación de *GIAC* son independientes, no siendo necesario seguir un curso de formación del *SANS* para obtener una certificación *GIAC*, ni obligatorio certificarse por *GIAC* tras haber realizado alguna capacitación con *SANS*. Esto último es solo una opción.

Así, mientras que la formación de *SANS* tiene como objetivo proporcionar a los estudiantes la mejor formación disponible, en las diferentes áreas clave de la ciberseguridad, la certificación *GIAC* está diseñada para proporcionar un punto de referencia objetivo, que permita demostrar que un individuo se encuentra con un nivel mínimo de habilidades prácticas y conocimientos para las personas que desean demostrar esta capacidad a un empleador actual o potencial.

Para obtener una de las certificaciones *GIAC* se debe superar un examen controlado por un supervisor, permitiendo además alcanzar dos niveles o *status*⁹⁴:

- *GIAC Gold Status*: que permite demostrar un conocimiento más profundo de la materia. Requiere que los candidatos desarrollen un trabajo de investigación y escriban un informe técnico o documento detallado al respecto, bajo la supervisión de un asesor.
- *GIAC Expert Status*: que acredita como profesional del máximo nivel de conocimiento en la materia. Entre los prerrequisitos se incluyen la consecución de varias certificaciones y disponer de varios *gold status*. Los exámenes para obtener el nivel «Experto» se convocan anualmente e incluyen varias actividades prácticas, abarcando varios días de duración. Las pruebas incluyen ejercicios de ciberseguridad, individual y en grupo, presentaciones, trabajos de investigación y ensayo, así como secciones de test prácticos basados en escenarios, con el objetivo de garantizar que el candidato está listo para hacer frente a diversas amenazas de ciberseguridad, en diferentes niveles de gravedad.

GIAC ofrece más de veinte certificaciones independientes, cada una de ellas con un dominio de conocimientos y habilidades, en diferentes ámbitos de la ciberseguridad, como la administración y gestión, los aspectos legales, las auditorías, el análisis forense o la seguridad del *software*. De esta forma, *GIAC* promueve que cada profesional pueda crearse su propia hoja de ruta de certificación profesional, determinando qué certificaciones son las más adecuadas para las necesidades específicas de su entorno de trabajo o las metas de su carrera profesional.

⁹⁴ *GIAC*, «*GIAC Certification Program Candidate's Handbook*» (Global Information Assurance Certification, 2012), <http://www.giac.org/pdfs/certification-candidate-handbook.pdf>

Revisemos brevemente algunas de las certificaciones *GIAC* más prestigiosas.

GSEC-GIAC Security Essentials Certification

Certificación destinada para aquellos profesionales de la ciberseguridad que desean demostrar que están cualificados para llevar a cabo tareas prácticas de seguridad en sistemas de información y comunicaciones. Los candidatos deben demostrar una sólida comprensión de los diferentes aspectos que implica la seguridad de la información, más allá del dominio de la terminología y los conceptos más simples.

Para obtener la certificación, los candidatos deben superar un examen supervisado de ciento ochenta preguntas, a responder en un tiempo máximo de cinco horas, obteniendo como mínimo un 74 % de respuestas acertadas.

Las áreas de conocimiento que aborda esta certificación incluyen:

- Conceptos de redes.
- Defensa en profundidad.
- Tecnologías de seguridad de internet.
- Comunicaciones seguras.
- Seguridad en Windows.
- Seguridad en Unix/Linux.

GSLC-GIAC Cyber Security Leadership Certification

Esta certificación va destinada al personal de gestión de las organizaciones y empresas, con responsabilidades de dirección y/o supervisión de otro personal de ciberseguridad a su cargo.

Para obtener la certificación, los candidatos deben superar un examen supervisado de ciento quince preguntas, a responder en un tiempo máximo de tres horas, obteniendo como mínimo un 68 % de respuestas acertadas.

Las áreas de conocimiento que aborda esta certificación incluyen:

- Gestión de la empresa, planificación, red e instalaciones físicas.
- Conceptos IP, ataques contra la empresa y defensa en profundidad.
- Comunicaciones seguras.
- El valor de la información.
- Gestión práctica.

GCIH-GIAC Certified Incident Handler

Los gestores de incidentes de seguridad son capaces de manejarlos por medio de una profunda comprensión de las técnicas más comunes de ataque, sus vectores y sus herramientas asociadas, así como del conocimiento de los fundamentos de la defensa para prevenir y/o responder a estos ataques cuando se produzcan.

La certificación *GCIH* se centra en detectar, responder y resolver incidentes de ciberseguridad y abarca las siguientes áreas de conocimiento de la ciberseguridad:

- Pasos del proceso de gestión de incidentes.
- Detección de aplicaciones maliciosas y actividad de la red.
- Técnicas comunes de ataque para comprometer servidores.
- Detección y análisis de vulnerabilidades en redes y sistemas.
- Proceso de mejora continua mediante el descubrimiento de las causas raíz de los incidentes.

Para obtener la certificación, los candidatos deben superar un examen supervisado de ciento cincuenta preguntas, a responder en un tiempo máximo de cuatro horas, obteniendo como mínimo un 73 % de respuestas acertadas.

GCED-GIAC Certified Enterprise Defender

La certificación *GCED* está pensada para completar y profundizar, sin solapamiento, los conocimientos y habilidades de ciberseguridad acreditados por medio de la certificación *GSEC*, ya vista anteriormente. En la certificación *GCED* se evalúan habilidades y conocimientos técnicos avanzados necesarios para defender el entorno de la empresa y proteger una organización en su conjunto.

Los conocimientos, competencias y habilidades que se evalúan en esta certificación abarcan las siguientes áreas:

- Infraestructura de red defensiva.
- Análisis de paquetes.
- Test de penetración.
- Gestión de incidentes.
- Eliminación de *malware*.

Para obtener la certificación, los candidatos deben superar un examen supervisado de ciento quince preguntas, a responder en un tiempo máximo de tres horas, obteniendo como mínimo un 70 % de respuestas acertadas.

GCIA-GIAC Certified Intrusion Analyst

Los profesionales con la certificación *GCIA* disponen de los conocimientos, competencias y habilidades para configurar y supervisar los sistemas de detección de intrusos, así como para leer, interpretar y analizar el tráfico de red y los archivos de registro de eventos relacionados.

Para obtener la certificación, los candidatos deben superar un examen supervisado de ciento cincuenta preguntas, a responder en un tiempo máximo de cuatro horas, obteniendo como mínimo un 67 % de respuestas acertadas.

Las áreas de conocimiento que aborda la certificación *GCIA* incluyen:

- Fundamentos del análisis del tráfico.
- Protocolos de aplicación y análisis de tráfico.
- Sistemas de detección de intrusiones *open-source*.
- Monitorización y análisis forense del tráfico de red.

- Desafío a los sistemas de detección de intrusiones.

GCFA-GIAC Certified Forensic Analyst

Certificación destinada a los profesionales que trabajan en la seguridad de la información, informática forense, así como en la gestión y respuesta a incidentes. La certificación se centra en las habilidades y conocimientos básicos para recoger y analizar los datos de sistemas informáticos en entornos Windows y Linux.

La certificación *GCFA* acredita que los candidatos tienen los conocimientos, competencias y habilidades para llevar a cabo investigaciones formales de incidentes y gestionar el manejo de incidentes en escenarios avanzados, incluyendo intrusiones externas y/o violaciones internas del control de acceso a los datos, amenazas persistentes avanzadas (*APT, Advanced Persistent Threat*), técnicas antiforenses utilizadas por los atacantes, así como casos forenses digitales complejos.

Para obtener la certificación, los candidatos deben superar un examen supervisado de ciento quince preguntas, a responder en un tiempo máximo de tres horas, obteniendo como mínimo un 71 % de respuestas acertadas.

Las áreas de conocimiento que aborda esta certificación incluyen:

- Técnicas avanzadas de respuesta a incidentes y caza de amenazas.
- Técnicas forenses en memorias volátiles en la respuesta a incidentes.
- Técnicas forenses de detección de intrusiones.
- Análisis de la línea de tiempo.
- Detección y respuesta a incidentes a nivel de toda la empresa.
- Adversarios avanzados y detección de técnicas antiforenses.
- El desafío de la respuesta a incidentes de *APT*.

GSNA-GIAC Systems and Network Auditor

Los profesionales con la certificación *GSNA* acreditan los conocimientos, competencias y habilidades para aplicar las técnicas de análisis de riesgos más básicos y para llevar a cabo una auditoría técnica de los servicios esenciales de los sistemas de información. Esta certificación va dirigida al personal técnico responsable de la seguridad y la auditoría de los sistemas de información.

Para obtener la certificación, los candidatos deben superar un examen supervisado de ciento quince preguntas, a responder en un tiempo máximo de tres horas, obteniendo como mínimo un 73 % de respuestas acertadas.

Las áreas de conocimiento que aborda la certificación *GCIA* incluyen:

- Auditoría, evaluación de riesgos y generación de informes de forma eficaz.
- Auditoría y monitorización eficaz de la red y el perímetro.
- Auditoría de aplicaciones web.

- Auditoría y monitorización avanzada de entornos Windows.
- Auditoría y monitorización avanzada de entornos Unix.
- Ciberejercicios.

EC-Council - CEH (Certified Ethical Hacker)

International Council of E-Commerce Consultants, también conocido como *EC-Council*⁹⁵, es uno de los mayores organismos del mundo para la certificación técnica de profesionales de la seguridad cibernética. Con implantación en ciento cuarenta países, el *EC-Council* ha formado y certificado a más de 140.000 profesionales de la seguridad de la información de todo el mundo, que han influido en la visión de la ciberseguridad de un gran número de organizaciones internacionales.

La misión del *EC-Council* es validar que los profesionales de la ciberseguridad disponen de las habilidades y conocimientos necesarios, en un entorno profesional muy exigente, que les permitirá ayudar a evitar que surjan ciberconflictos. *EC-Council* se compromete a mantener el más alto nivel de imparcialidad y objetividad en sus prácticas, toma de decisiones y autoridad en todos los asuntos relacionados con la certificación.

El *EC-Council* dispone de varios programas de certificación de seguridad, con gran prestigio y reconocimiento a nivel internacional, siendo el *CEH (Certified Ethical Hacker)*⁹⁶, creado en 2003, el más demandado.

El propósito de la credencial *CEH* es:

- Establecer y regular las normas mínimas para la acreditación del conocimiento y dominio de las medidas de *hacking* ético por parte los profesionales especialistas en ciberseguridad.
- Acreditar al público en general que los individuos certificados cumplen o exceden los estándares profesionales mínimos.
- Reforzar el ejercicio profesional del *hacking* ético como una profesión única y autorregulada.

Una persona con la certificación *CEH* es un profesional experto, que entiende y sabe cómo buscar debilidades y vulnerabilidades en los sistemas objetivo, y utiliza los mismos conocimientos y herramientas que un *hacker* malicioso, pero de una manera legal y legítima para evaluar la postura de seguridad de un sistema de objetivo. La credencial *CEH* certifica individuos en la disciplina específica del *hacking* ético desde una perspectiva neutral de los proveedores de tecnologías de seguridad de redes.

⁹⁵ EC-Council, «About - International Council of E-Commerce Consultants», 25 de febrero de 2016, <https://www.eccouncil.org/about/>

⁹⁶ EC-Council, «CEH Handbook v2.0», enero de 2015, <https://www.eccouncil.org/wp-content/uploads/2016/06/CEH-Handbook-v2.0.pdf>

El examen *CEH* incluye los siguientes dominios de conocimiento:

- Fundamentos:
 - Tecnologías de red.
 - Tecnologías web.
 - Tecnologías de sistemas de información.
 - Protocolos de comunicaciones.
 - Operaciones *malware*.
 - Tecnologías móviles.
 - Tecnologías de redes de telecomunicaciones.
 - Copias de seguridad y archivado.
- Análisis/Evaluación:
 - Análisis de datos.
 - Análisis de sistemas.
 - Evaluación de riesgos.
 - Métodos de evaluación técnica.
- Seguridad:
 - Controles de seguridad en sistemas.
 - Servidores de archivos/aplicaciones.
 - Cortafuegos.
 - Criptografía.
 - Seguridad de red.
 - Seguridad física.
 - Modelado de amenazas.
 - Procedimientos de verificación (falsos positivos).
 - Ingeniería social.
 - Escaneo de vulnerabilidades.
 - Implicaciones de la política de seguridad.
 - Privacidad/confidencialidad.
 - Biometría.
 - Tecnología de acceso *wireless*.
 - Redes confiables.
 - Vulnerabilidades.
- Herramientas/Sistemas/Programas:
 - Intrusiones basadas en red/servidor.
 - Sniffers de red/*wireless* (*WireShark*, *Airsnort*).
 - Mecanismos de control de acceso.
 - Técnicas criptográficas.
 - Lenguajes de programación.
 - Lenguajes de programación de *scripts*.
 - Dispositivos de protección del perímetro.
 - Topologías de red.

- *Subnetting*.
- Escaneo de puerto.
- Sistema de nombres de dominio.
- *Routers/modems/switches*.
- Escáneres de vulnerabilidades.
- Gestión de vulnerabilidades y protección de sistemas.
- Sistemas operativos.
- Sistemas y programas antivirus.
- Herramientas de análisis de registros.
- Modelos de seguridad.
- Herramientas de explotación.
- Estructuras de bases de datos.
- Procedimientos/Metodología:
 - Criptografía.
 - Infraestructura de clave pública (PKI).
 - Arquitectura de seguridad.
 - Arquitectura orientada a servicios.
 - Incidente de seguridad de la información.
 - Diseño de aplicaciones en N-capas.
 - Comunicaciones TCP/IP.
 - Metodología de evaluaciones de seguridad.
- Regulación/Política:
 - Políticas de seguridad.
 - Cumplimiento de regulaciones.
- Código ético:
 - Código de conducta profesional.
 - Adecuación del *hacking*.

Para obtener la certificación *CEH*, un candidato deberá superar un examen de ciento veinticinco preguntas, en formato de respuestas múltiples, en un tiempo máximo de cuatro horas.

Conclusiones

Conviene precisar que las necesarias conclusiones que a continuación exponemos y desarrollamos no solamente se desprenden de la lectura del presente capítulo, que también, sino que son conclusiones y puntos para la reflexión recogidos por los autores durante su realización.

Por lo que respecta a la más que palmaria escasez de profesionales en materia de Ciberseguridad, nos hemos retrotraído a seis años atrás en el análisis de estudios e informes para evidenciar que no se trata de un problema nuevo, sino que se veía venir desde hace tiempo y, como reflejan las reseñas

más actuales, existe incluso un aumento de la brecha entre oferta y demanda de profesionales en este ámbito a pesar de los esfuerzos realizados en estos últimos cinco años.

Quisiéramos en estas conclusiones subrayar que este déficit está enmarcado en un problema más general como es la falta de ingenieros y técnicos especialistas en las tecnologías de la información y las comunicaciones (TIC), si bien agravado en el caso de la ciberseguridad y ciberdefensa.

En Europa existen actualmente dos grandes iniciativas que están ya influyendo en la configuración de las ocupaciones relacionadas con las TIC.

La primera de ellas es la publicación del estándar EN 16234-1:2016⁹⁷ que define un marco de trabajo (*eCompetence Framework: eCF*) para la definición de perfiles profesionales en TIC basado en cuarenta competencias con cinco niveles de capacidad y con un total de doscientas nueve habilidades y conocimientos asociados.

El modelo ya está siendo la referencia para los grandes actores del mundo de las certificaciones como demuestran los mapas competenciales de varias decenas de sus certificaciones⁹⁸. La previsión es que los proveedores de formación y los entes de cualificación y certificación acaben mapeando sus productos hacia *eCF* para permitir un lenguaje común y homogéneo que conecte a formadores, empleadores y candidatos a un empleo.

Actualmente en cuanto al ámbito de la ciberseguridad se han modelado dos perfiles en *eCF* (disponibles junto a otras veintiuna ocupaciones en el documento CWA 16458-2012⁹⁹ CWA, *European ICT Professional Profiles*):

- Gerente de seguridad TIC (*ICT Security Manager*), que gestiona la política de seguridad de los sistemas de información.
- Especialista en seguridad de los sistemas de información, que asegura la implementación de dicha política de seguridad en sus distintos aspectos.

Además, la seguridad digital es un elemento competencial transversal presente en hasta otros siete perfiles como *CIO* (*Chief Information Officer*), gerente de operaciones TIC, etcétera.

⁹⁷ European Committee for Standardization (CEN), «e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework - EN 16234-1:2016», 6 de abril de 2016, https://standards.cen.eu/dyn/www/f?p=204:110:0:::FSP_PROJECT,FSP_ORG_ID:41798,1218399&cs=17B0E0F8CABCDDBDD-B8066A46FA937510B

⁹⁸ e-Competence Quality Label, «e-Competence Certificates», accedido 2 de noviembre de 2016, <http://www.e-competence-quality.com/certification-profiles/>

⁹⁹ European Committee for Standardization (CEN), «CWA 16458 - European ICT Professional Profiles», mayo de 2012, http://www.kutsekoda.ee/fwk/fb/10456179/CEN-WSICT_N0393_Final_Draft_CWA_for_formal_approval_EU_ICT_P.pdf

La otra iniciativa europea que va a requerir la alineación de todos los esquemas de cualificaciones nacionales y locales es la nueva clasificación oficial laboral europea para todos los sectores, *ESCO (European Skills, Competences, Qualifications and Occupations)*¹⁰⁰, aún pendiente de publicarse en 2017.

Esta nueva clasificación laboral va a ser de uso obligatorio para todos los servicios públicos de empleo y para los recursos europeos como el portal EURES, además de promoverse como estándar para los portales privados, y estará traducida a todos los idiomas oficiales de la Unión Europea.

En el ámbito sectorial de las TIC se ha generado un nuevo catálogo de ocupaciones con ciento diez puestos y su correspondiente descripción y lista de habilidades y conocimientos, tanto esenciales como opcionales. En el ámbito de la seguridad se distinguen los puestos de *CISO (Chief Information Security Officer)*, administrador de seguridad TIC, consultor de seguridad TIC, gerente (*manager*) de seguridad TIC, técnico de seguridad TIC y *hacker* ético. Al igual que en *eCF*, existe una buena cantidad de otras ocupaciones con habilidades y conocimientos relacionados con la seguridad.

Actualmente estos modelos están generando importantes expectativas, pero también la necesidad de buscar su consistencia para permitir que los servicios para candidatos a empleos, reclutadores y formadores sean completos y sólidos. En ese sentido, los resultados de proyectos europeos como *eSkills Match*¹⁰¹, con un sistema de ayuda en el manejo de los modelos, y *eCF Council*¹⁰² permitirán mejorar este aspecto de forma práctica, incluyendo la conexión con el cuerpo europeo de conocimientos en TIC¹⁰³.

En todo caso, parece existir un consenso a nivel mundial de que dicha escasez de profesionales de las TIC y, en particular, de la ciberseguridad tendrá implicaciones negativas en la seguridad nacional, impactando gravemente tanto en entidades del sector público como del privado.

En este sentido, y en un ámbito nacional, es pertinente resaltar el documento y proyecto del Instituto Nacional de Ciberseguridad (INCIBE) de 2016 denominado «Punto de partida al modelo de gestión y seguimiento del talento

¹⁰⁰ Comisión Europea, «ESCO (European Skills, Competences, Qualifications and Occupations)», accedido 2 de noviembre de 2016, <https://ec.europa.eu/esco/portal/home>

¹⁰¹ European Commission Directorate General for Communications Networks, Content & Technology (DG CONNECT), «Proyecto e-Skills Match», accedido 2 de noviembre de 2016, <http://www.eskillsmatch.eu/>

¹⁰² eCF Council, «eCF ALLIANCE , qualifications and skills for the ICT industry», accedido 2 de noviembre de 2016, http://media.wix.com/ugd/71d4ca_273ca002273242c28d-1557836c68cbcc.pdf

¹⁰³ European Commission - DG Internal Market, Industry, Entrepreneurship and SMEs, Capgemini Consulting, y Ernst & Young, «The European Foundational ICT Body of Knowledge - Version 1.0», 22 de febrero de 2015, http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=925&PortalId=0&TabId=353

en ciberseguridad en España»¹⁰⁴ en el que, en el apartado de «Diagnóstico inicial», se realiza una muy buena valoración de la situación en nuestro país sobre los puestos de ciberseguridad sin cubrir y la falta de competencias del profesional en este ámbito.

En dicho documento, desde su mismo subtítulo: «Visión conjunta de la industria, sector académico e investigador y profesionales del sector», se puede ver claramente otro punto de concordancia con todos los informes analizados: hay un acuerdo, tanto implícito como explícito, de la importancia de la colaboración público-privada en materia de ciberseguridad y ciberdefensa para afrontar este problema.

En cuanto a las iniciativas de organismos públicos para la formación y certificación profesional en ciberseguridad, nos hemos centrado primera y principalmente en iniciativas del mundo anglosajón (Estados Unidos y Reino Unido), por ser las más prontamente iniciadas y más completamente desarrolladas, sin olvidarnos de las últimas iniciativas europeas y españolas.

Parece claro y hay conformidad en todos los ámbitos analizados sobre los beneficios de las certificaciones y acreditaciones, tanto para los profesionales de ciberseguridad como para los empleadores de los mismos. Dichas certificaciones y acreditaciones tienen necesariamente que coincidir todo lo más posible con las necesidades y los perfiles competenciales evidenciados en los diferentes estudios existentes.

En este aspecto, y en un ámbito estrictamente nacional, es importante señalar el inicio de trabajos emanados de los Planes Derivados del Plan Nacional de Ciberseguridad de 2014, que en algunas de sus diferentes vertientes: «Plan de seguridad de los sistemas de información y telecomunicaciones que soportan las administraciones públicas», «Seguridad de los sistemas de información y telecomunicaciones que soportan las infraestructuras», «Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia», «Ciberseguridad del sector privado y la industria» o «Cultura de ciberseguridad», acometen aspectos como la «Definición, aprobación e implantación de acciones para la evaluación, homologación y certificación de profesionales de ciberseguridad, dentro del marco de las AAPP» o el «Desarrollo de un marco de conocimientos de ciberseguridad en los ámbitos técnico, operativo y jurídico» mediante la elaboración del mapa de competencias en los distintos ámbitos (técnico, operativo y jurídico) y la definición de un marco de referencia de profesionales y competencias en materia de ciberseguridad.

Queda, por tanto, evidenciado que parece conveniente la creación y lanzamiento de un Esquema Nacional de Certificación de Profesionales en Ciberseguridad, contando para su desarrollo con la mayor parte posible de los

¹⁰⁴ INCIBE, «Punto de partida al Modelo de gestión y seguimiento del TALENTO en ciberseguridad en España», 18 de agosto de 2016, https://www.incibe.es/sites/default/files/contenidos/notaspress/doc/modelo_gestion_talento_incibe.pdf

actores implicados, tanto en ámbito público como privado. Todo ello con la debida seriedad y profesionalidad pero con carácter de inmediatez.

En la esfera privada, tal y como sostiene el anteriormente citado informe de INCIBE, «la creciente demanda de certificaciones es un hecho. Las titulaciones académicas pueden acreditar una formación básica pero, en un ambiente de evolución muy rápida, es difícil que puedan acreditar la actualización de conocimientos o competencias muy específicas. Este es el terreno en el que se desenvuelven las certificaciones, posicionándose como un elemento fundamental a la hora de modelar las competencias de los profesionales».

Por otra parte, se percibe una clara evolución en los diferentes modelos de acreditaciones y certificaciones hacia propuestas que incluyen aspectos de concienciación y formación más allá de la mera evaluación de conocimientos y experiencia en materia de ciberseguridad.

Tanto su realización como su evaluación se suelen ejecutar de manera práctica. Por un lado, la formación se realiza mediante talleres en los que se prueban los conceptos que son necesarios conocer y, por otro, los exámenes consisten en la contrastación práctica de unas habilidades y unos conocimientos sobre un caso simulado.

Bibliografía

- Adriana Pauna. Certification of Cyber Security Skills of ICS - Good Practices and Recommendations for Developing Harmonised Certification Schemes. Heraklion: ENISA, 2014. <http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714040:EN:HTML>
- Andrew McGettrick y Association for Computing Machinery (ACM). «Towards Curricular Guidelines for Cybersecurity - Report of a Workshop on Cybersecurity Education and Training», 30 de agosto de 2013. <https://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf>
- Ariha Setalvad. «Demand to fill cybersecurity jobs booming». Peninsula Press, 31 de marzo de 2015. <http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/>
- BOE. Anexo III al Real Decreto 686/2011, Certificado de Profesionalidad en Seguridad Informática, 2011. <https://sede.sepe.gob.es/es/portaltrabajo/resources/pdf/especialidades/IFCT0109.pdf>.
- . Real Decreto 686/2011, de 13 de mayo, por el que se establecen seis certificados de profesionalidad de la familia profesional informática y comunicaciones que se incluyen en el repertorio nacional de certificados de profesionalidad, 2011. https://sede.sepe.gob.es/es/portaltrabajo/resources/pdf/normativaCertificados/RD686_2011.pdf
- CCN (Centro Criptológico Nacional). «El CCN y el INAP apuestan por un Esquema Nacional de Certificación de Profesionales en Ciberseguridad».

- Comunicados CCN-CERT, 31 de enero de 2014. <https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/1846-el-ccn-y-el-in-ap-apuestan-por-un-esquema-nacional-de-certificacion-de-profesionales-en-ciberseguridad.html>
- CESG. «CESG Certification for IA Professionals 5.2». GCHQ, octubre de 2015. <https://www.cesg.gov.uk/file/520/download?token=j8vebyeM>
- . «CESG Certified Professional Scheme», 19 de mayo de 2016. <https://www.cesg.gov.uk/articles/cesg-certified-professional-scheme>
- . «Guidance to CESG Certification for IA Professionals v2-1». GCHQ, enero de 2015. <https://www.cesg.gov.uk/file/701/download?token=QM1gwRoi>
- Chris Peake. «Red Teaming: The Art of Ethical Hacking». SANS Institute - InfoSec Reading Room, 16 de julio de 2003. <https://www.sans.org/reading-room/whitepapers/auditing/red-teaming-art-ethical-hacking-1272>
- CISCO. «CCNA (Cisco Certified Network Associate) Security». Cisco. Accedido 1 de septiembre de 2016. <http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-security.html>
- . «Cybersecurity Specialist». Cisco. Accedido 1 de septiembre de 2016. <http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/specialist/security/cybersecurity.html>
- Cisco Security Advisory Services. «Mitigating the Cybersecurity Skills Shortage». Cisco Systems, Inc, julio de 2015. <http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf>
- Comisión de las Comunidades Europeas. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones: Cibercapacidades para el siglo XXI: fomento de la competitividad, el crecimiento y el empleo. COM(2007) 496 final, 2007. http://www.cdiex.org/documentos/documento_121.pdf
- Comisión Europea. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones: una Estrategia para el Mercado Único Digital de Europa. COM(2015) 192 final, 2015. <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015DC0192&rid=1>
- . «ESCO (European Skills, Competences, Qualifications and Occupations)». Accedido 2 de noviembre de 2016. <https://ec.europa.eu/esco/portal/home>.
- CompTIA. «A+ (Plus) Certification». Accedido 1 de septiembre de 2016. <https://certification.comptia.org/certifications/a>
- . «CASP - CompTIA Advanced Security Practitioner Certification». Accedido 1 de septiembre de 2016. <https://certification.comptia.org/certifications/comptia-advanced-security-practitioner>

- . «Network+ Certification». Accedido 1 de septiembre de 2016. <https://certification.comptia.org/certifications/network>
- . «Security+ Certification». Accedido 1 de septiembre de 2016. <https://certification.comptia.org/certifications/security>
- Comptroller and Auditor General. «The UK Cyber Security Strategy: Landscape Review». London: National Audit Office, 5 de febrero de 2013. <http://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/>
- Department of Defense. DoD Directive 8140.01, Cyberspace Workforce Management. DoD. Vol. 8140.01, 2015. https://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf
- . DoD Directive 8570.01. Information Assurance Training, Certification, and Workforce Management. 8570.01, 2007. <http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf>
- DHS y NICCS. «National Cybersecurity Workforce Framework Slick Sheet». National Initiative for Cybersecurity Careers and Studies (NICCS), noviembre de 2011. https://niccs.us-cert.gov/sites/default/files/documents/files/Workforce%20Framework%20Slick%20Sheet_1.pdf?track-Docs=Workforce%20Framework%20Slick%20Sheet.pdf
- DoD. «DoD 8570.01-M - Information Assurance Workforce Improvement Program - Incorporating Change 4, November 10, 2015», 19 de diciembre de 2005. <https://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf>
- EC-Council. «About - International Council of E-Commerce Consultants», 25 de febrero de 2016. <https://www.eccouncil.org/about/>
- . «CEH - Certified Ethical Hacker». EC-Council, 25 de febrero de 2016. <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>
- . «CEH Handbook v2.0», enero de 2015. <https://www.eccouncil.org/wp-content/uploads/2016/06/CEH-Handbook-v2.0.pdf>
- eCF Council. «eCF ALLIANCE , qualifications and skills for the ICT industry». Accedido 2 de noviembre de 2016. http://media.wix.com/ugd/71d4ca_273ca002273242c28d1557836c68cbcc.pdf
- e-Competence Quality Label. «e-Competence Certificates». Accedido 2 de noviembre de 2016. <http://www.e-competence-quality.com/certification-profiles/>
- European Commission - DG Internal Market, Industry, Entrepreneurship and SMEs, Capgemini Consulting, y Ernst & Young. «The European Foundational ICT Body of Knowledge - Version 1.0», 22 de febrero de 2015. http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=925&PortalId=0&TabId=353
- European Commission Directorate General for Communications Networks, Content & Technology (DG CONNECT). «Proyecto e-Skills Match». Accedido 2 de noviembre de 2016. <http://www.eskillsmatch.eu/>

European Committee for Standardization (CEN). «CWA 16458 - European ICT Professional Profiles», mayo de 2012. http://www.kutsekoda.ee/fw/fb/10456179/CEN-WSICT_N0393_Final_Draft_CWA_for_formal_approval_EU_ICT_P.pdf

———. «e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework - EN 16234-1:2016», 6 de abril de 2016. https://standards.cen.eu/dyn/www/f?p=204:110:0:::FSP_PROJECT,FSP_ORG_ID:41798,1218399&cs=17B0E0F8CABCDDB8066A46FA937510B

European Cybersecurity Industrial Leaders (ECIL). «Recommendations on Cybersecurity for Europe», 25 de enero de 2016. http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=13326

GAO. «GAO-13-742 - DHS Recruiting and Hiring: DHS Is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Recruiting Efforts». Report to Congressional Requesters. United States Government Accountability Office, septiembre de 2013. <http://www.gao.gov/products/GAO-13-742>

———. «GAO-15-223, Federal Workforce: OPM and Agencies Need to Strengthen Efforts to Identify and Close Mission-Critical Skills Gaps». Report to Congressional Requesters. United States Government Accountability Office, enero de 2015. <http://www.gao.gov/assets/670/668202.pdf>

GIAC. «About GIAC». Accedido 6 de septiembre de 2016. <http://www.giac.org/about>

———. «GCED - GIAC Certified Enterprise Defender». Accedido 1 de septiembre de 2016. <http://www.giac.org/certification/certified-enterprise-defender-gced>

———. «GCFA - GIAC Certified Forensic Analyst». Accedido 1 de septiembre de 2016. <http://www.giac.org/certification/certified-forensic-analyst-gcfa>

———. «GCIA - GIAC Certified Intrusion Analyst». Accedido 1 de septiembre de 2016. <http://www.giac.org/certification/certified-intrusion-analyst-gcia>

———. «GCIH - GIAC Certified Incident Handler». Accedido 1 de septiembre de 2016. <http://www.giac.org/certification/certified-incident-handler-gcih>

———. «GIAC Certification Program Candidate's Handbook». Global Information Assurance Certification, 2012. <http://www.giac.org/pdfs/certification-candidate-handbook.pdf>

———. «GSEC - GIAC Security Essentials Certification». Accedido 1 de septiembre de 2016. <http://www.giac.org/certification/security-essentials-gsec>

———. «GSLC - GIAC Cyber Security Leadership Certification». Accedido 1 de septiembre de 2016. <http://www.giac.org/certification/security-leadership-gslc>

———. «GSNA - GIAC Systems and Network Auditor». Accedido 1 de septiembre de 2016. <http://www.giac.org/certification/systems-network-auditor-gsna>

- Gobierno de España. Estrategia de Ciberseguridad Nacional, 2013. <http://www.lamoncloa.gob.es/NR/rdonlyres/680D00B8-45FA-4264-9779-1E69D-4FEF99D/256935/20131332EstrategiadeCiberseguridadx.pdf>
- Homeland Security Advisory Council. «CyberSkills Task Force Report». US Department of Homeland Security, Otoño de 2012. <https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf>
- INAP, CCN y Óscar Pastor. «Esquema de Certificación de Personas». En VII Jornadas STIC CCN - CERT. Madrid, 2013. <https://www.ccn-cert.cni.es/privatedocs/viiijornadas/742-12-opastor-ccn-isdefe-esquemadecertificaciondepersonas/file.html>
- INCIBE. «Punto de partida al Modelo de gestión y seguimiento del TALENTO en ciberseguridad en España», 18 de agosto de 2016. https://www.incibe.es/sites/default/files/contenidos/notasprensa/doc/modelo_gestion_talento_incibe.pdf
- Information Systems Audit and Control Association. Cobit 5: A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows. IL: ISACA, 2012.
- Institute of Information Security Professional. «IISP Skills Framework - Version 2.0». Accedido 31 de agosto de 2016. https://www.iisp.org/imis15/iisp/About_Us/Our_Skills_Framework/iispv2/Accreditation/Our_Skills_Framework.aspx?hkey=e77a6f03-9498-423e-aa7b-585381290ec4
- International Organization for Standardization. «ISO/IEC 17024:2012 - Evaluación de la conformidad. Requisitos generales para los organismos que realizan certificación de personas». ISO/IEC, 2012. http://www.iso.org/iso/catalogue_detail?csnumber=52993
- ISACA. «Certified in Risk and Information Systems Control (CRISC)». Accedido 29 de agosto de 2016. http://www.isaca.org/About-ISACA/Press-room/Documents/2015-CRISC-Fact-Sheet_pre_eng_1015.pdf
- . «Certified in the Governance of Enterprise IT (CGEIT) Fact Sheet». Accedido 29 de agosto de 2016. http://www.isaca.org/About-ISACA/Press-room/Documents/2015-CGEIT-Fact-Sheet_pre_eng_1015.pdf
- . «Certified Information Security Manager® (CISM®) Fact Sheet». Accedido 29 de agosto de 2016. http://www.isaca.org/About-ISACA/Press-room/Documents/2015-CISM-Fact-Sheet_pre_eng_1015.pdf
- . «Certified Information Systems Auditor™ (CISA®) Fact Sheet». Accedido 29 de agosto de 2016. http://www.isaca.org/About-ISACA/Press-room/Documents/2015-CISA-Fact-Sheet_pre_eng_1015.pdf
- . «CISA - Certified Information Systems Auditor». Accedido 1 de septiembre de 2016. <http://www.isaca.org/certification/cisa-certified-information-systems-auditor/pages/default.aspx>
- . «CISM - Certified Information Security Manager». Accedido 1 de septiembre de 2016. <http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx>

- . «Cybersecurity Nexus (CSX) Fact Sheet». Accedido 29 de agosto de 2016. http://www.isaca.org/cyber/Documents/Cybersecurity-Nexus-Fact-Sheet_pre_Eng_0115.pdf
- . «Cybersecurity Nexus™ (CSX) General Awareness Brochure», 2016. http://www.isaca.org/cyber/Documents/CSX-General-Awareness-Brochure_Bro_Eng_0816.pdf
- . «ISACA Fact Sheet». Accedido 29 de agosto de 2016. http://www.isaca.org/About-ISACA/Press-room/Documents/2016-ISACA-Fact-Sheet_pre_eng_0716.pdf
- ISACA, y RSA Conference. «State of Cybersecurity: Implications for 2015». ISACA, 11 de abril de 2015. http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf
- (ISC)². «Become an Associate of (ISC)² Prior to Obtaining Certification». Accedido 1 de septiembre de 2016. <https://www.isc2.org/associate/default.aspx>
- . «CAP - Certified Authorization Professional». Accedido 1 de septiembre de 2016. <https://www.isc2.org/cap/default.aspx>
- . «CISSP - Certified Information Systems Security Professional». Accedido 1 de septiembre de 2016. <https://www.isc2.org/cissp/default.aspx>
- . «CISSP (Certified Information Systems Security Professional) Brochure», 16 de diciembre de 2015. https://www.isc2.org/uploadedfiles/credentials_and_certification/cissp/cissp-information.pdf
- . «CISSP Concentrations». Accedido 5 de septiembre de 2016. [https://www.isc2.org/uploadedfiles/\(isc\)2_public_content/certification_programs/cissp_concentrations/concentrations-web.pdf](https://www.isc2.org/uploadedfiles/(isc)2_public_content/certification_programs/cissp_concentrations/concentrations-web.pdf)
- . «CISSP-ISSAP - Information Systems Security Architecture Professional». Accedido 1 de septiembre de 2016. <https://www.isc2.org/issap.aspx>
- . «CISSP-ISSEP - Information Systems Security Engineering Professional». Accedido 1 de septiembre de 2016. <https://www.isc2.org/issep.aspx>
- . «CISSP-ISSMP - Information Systems Security Management Professional». Accedido 1 de septiembre de 2016. <https://www.isc2.org/issmp/default.aspx>
- . «CSSLP - Certified Secure Software Lifecycle Professional». Accedido 1 de septiembre de 2016. <https://www.isc2.org/csslp/default.aspx>
- . «(ISC)² Overview». Accedido 5 de septiembre de 2016. [https://www.isc2.org/uploadedfiles/\(isc\)2_public_content/\(isc\)2-company-overview.pdf](https://www.isc2.org/uploadedfiles/(isc)2_public_content/(isc)2-company-overview.pdf)
- . «SSCP - Systems Security Certified Practitioner». Accedido 1 de septiembre de 2016. <https://www.isc2.org/sscp/default.aspx>
- Jim Gosler. Cyberwarrior Shortage Threatens U.S. Security. NPR Morning Edition, 29 de julio de 2010. <http://www.npr.org/templates/story/story.php?storyId=128574055>.

- Karen Evans y Franklin Reeder. «A Human Capital Crisis in Cybersecurity». Technical Proficiency Matters. 1800 K Street, NW, Washington, DC 20006: CSIS Center for Strategic and International Studies - Commission on Cybersecurity for the 44th Presidency, noviembre de 2010. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/101111_Evans_HumanCapital_Web.pdf
- Kathryn A. Francis y Wendy Ginsber. «The Federal Cybersecurity Workforce: Background and Congressional Oversight Issues for the Departments of Defense and Homeland Security». CRS Report. Congressional Research Service, 8 de enero de 2016. <https://www.fas.org/sgp/crs/natsec/R44338.pdf>
- Lewis Morgan. «Global Shortage of Two Million Cyber Security Professionals by 2017». IT Governance Blog, 30 de octubre de 2014. <http://www.itgovernance.co.uk/blog/global-shortage-of-two-million-cyber-security-professionals-by-2017/>
- Michael Suby. «The 2013 (ISC)² Global Information Security Workforce Study». Frost & Sullivan Market Study. (ISC)², 2013. <https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf>
- Michael Suby y Frank Dickson. «The 2015 (ISC)² Global Information Security Workforce Study». A Frost & Sullivan White Paper. (ISC)², 16 de abril de 2015. [https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-\(ISC\)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf](https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf)
- Ministerio de Defensa. Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional. BOE. Accedido 27 de mayo de 2013. <https://www.boe.es/boe/dias/2004/03/19/pdfs/A12203-12204.pdf>
- Ministerio de Empleo y Seguridad Social. «Servicio Público de Empleo Estatal». Accedido 2 de septiembre de 2016. <http://www.empleo.gob.es/es/organizacion/empleo/contenido/OM29.htm>
- Ministerio de la Presidencia. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, 2010. <http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf>
- Ministerio de Política Territorial y Administración Pública. Real Decreto 464/2011, de 1 de abril, por el que se aprueba el Estatuto del Instituto Nacional de Administración Pública. Vol. BOE-A-2011-6872, 2011. <http://www.boe.es/buscar/pdf/2011/BOE-A-2011-6872-consolidado.pdf>
- NICCS. «National Initiative for Cybersecurity Careers and Studies». Accedido 29 de agosto de 2016. <https://niccs.us-cert.gov/home/about-niccs>
- . «Training Catalog | National Initiative for Cybersecurity Careers and Studies». Accedido 30 de agosto de 2016. <https://niccs.us-cert.gov/training/tc/search>

- NICE. «The National Cybersecurity Workforce Framework». National Initiative for Cybersecurity Careers and Studies (NICCS), 15 de mayo de 2014. <https://niccs.us-cert.gov/sites/default/files/documents/files/National%20Cybersecurity%20Workforce%20Framework%20Version%201.0.pdf?trackDocs=National%20Cybersecurity%20Workforce%20Framework%20Version%201.0.pdf>
- NIST. «Framework for Improving Critical Infrastructure Cybersecurity». Cybersecurity Framework. National Institute of Standards and Technology, 12 de febrero de 2014. <http://www.cslawreport.com/files/2015/04/07/nist-combined-file.pdf>
- . «NICE Issues Cybersecurity Workforce Framework for Public Comment». Accedido 29 de agosto de 2016. <http://www.nist.gov/itl/cyber-work-110811.cfm>
- . «NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security». National Institute of Standards and Technology, junio de 2011
- . «The National Initiative for Cybersecurity Education (NICE)». Accedido 29 de agosto de 2016. <http://csrc.nist.gov/nice/about/index.html>
- NSA. «Mission & Strategy». Accedido 5 de septiembre de 2016. <https://www.nsa.gov/about/mission-strategy/>
- OMB (Office of Management and Budget). Federal Cybersecurity Workforce Strategy. M-16- 15, 2016. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf>
- Óscar Pastor y Javier Candau. «Propuesta para un Esquema Nacional de Certificación de Profesionales en Ciberseguridad para España». *Revista SIC*, febrero de 2014
- PCI Security Standards Council. «PCI (industria de tarjetas de pago) - Normas de seguridad de datos - Requisitos y procedimientos de evaluación de seguridad», noviembre de 2013. https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf
- Raytheon y NCSA. «Preparing Millennials to Lead in Cyberspace». National Cyber Security Alliance, octubre de 2014. <http://www.raytheoncyber.com/news/feature/blog-cyber60-helprawanted.html>
- Rebecca Vogel. «Closing The Cybersecurity Skills Gap». *Salus Journal* 4, n.º 2 (2016): 32.
- Robert Ayoub. «The 2011 (ISC)² Global Information Security Workforce Study». Frost & Sullivan Market Survey. (ISC)², 2011. https://www.isc2.org/uploadedFiles/Industry_Resources/FS_WP_ISC%20Study_020811_MLW_Web.pdf
- SANS. «SANS Institute: About». Accedido 6 de septiembre de 2016. <https://www.sans.org/about/>
- SEI (Software Engineering Institute). «CERT-Certified Computer Security Incident Handler». Accedido 1 de septiembre de 2016. <https://www.sei.cmu.edu/certification/opportunities/csih/>

SFIA Foundation. «Responsabilidades y habilidades - Español». Página. Accedido 31 de agosto de 2016. <https://www.sfia-online.org/es/how-sfia-works/responsibilities-and-skills>

———. «Versión 6 del Marco de Competencias para la Era de la Información - Español». Accedido 29 de agosto de 2016. <https://www.sfia-online.org/es/reference-guide>

Steve Morgan. «One Million Cybersecurity Job Openings In 2016». Forbes, 2 de enero de 2016. <http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/print/>

EPÍLOGO

Presente y futuro de la ciberseguridad: el impacto y la necesidad de la colaboración público-privada

Luis Joyanes Aguilar

Presidente de la Fundación I+D del Software Libre (Fidesol)

La ciberseguridad en la transformación digital

La transformación digital de las organizaciones y empresas es hoy día, y camino del futuro, una necesidad imprescindible para no quedarse desconectadas de su propio sector. Como se ha constatado en los diferentes capítulos de esta obra, y también en los numerosos informes y estudios consultados y publicados en estos últimos años y, en particular, en 2016, consideramos como pronostica la consultora Gartner en un informe especial sobre seguridad¹ que «la transformación digital de las empresas debe estar dirigida por la ciberseguridad». La consultora predice que para 2020 el 60 % de los negocios digitales sufrirán grandes fallos en sus servicios por culpa de la incapacidad de sus equipos de TI de gestionar el «riesgo digital». La seguridad es un pilar fundamental de la transformación digital y, en una economía basada en datos, la ciberseguridad se ha convertido en una prioridad para las organizaciones que deben anticiparse a los riesgos digitales para evitar posibles ataques y pérdidas de información.

La Comisión Europea puso en marcha una iniciativa de colaboración público-privada a primeros de julio de 2016 (véase capítulo 1) firmando un acuerdo de asociación público-privada con los actores e industrias del ámbito de

¹ <http://cso.computerworld.es/seguridad-en-cifras/el-60-de-las-empresas-sufrira-grandes-fallos-en-sus-servicios-en-2020>

la ciberseguridad para mejorar la capacidad de la Unión Europea de enfrentarse a los ciberataques. La Unión Europea se comprometió a invertir 450 millones de euros bajo el programa Horizonte 2020 para contribuir al desarrollo del sector. Se ha creado expresamente para la puesta en marcha de la iniciativa, la Organización Europea de Ciberseguridad (ECSSO) constituida por grandes empresas europeas del sector de la seguridad de la información que aportará tres veces la cifra de la Comisión, de modo que se alcanzarán los 1.800 millones euros en 2020, fecha prevista de despliegue.

La concienciación en ciberseguridad

La empresa y la Administración pública deben implementar estrategias para hacer frente a las amenazas cibernéticas. La ciberseguridad se ha convertido en una prioridad tanto para compañías privadas como instituciones públicas. La concienciación dentro de la propia empresa de la importancia de políticas de seguridad es vital para su definición, despliegue y cumplimiento.

Se requiere una concienciación proactiva dentro de las organizaciones para estar preparadas para el presente y, sobre todo, el futuro. Iniciativas de colaboración público-privada como la ya citada de la Unión Europea e iniciativas más intelectuales y sencillas, como esta obra, pueden constituir un punto de partida para esa preparación de las estrategias de ciberseguridad de empresas y organismos de la Administración.

La colaboración público-privada sintetizada en las conclusiones de los diferentes autores de este Cuaderno de Estrategia del Instituto Español de Estudios Estratégicos consideramos es una herramienta indispensable para hacer frente a las ciberamenazas del presente y el futuro, y soporte clave para la realización e implementación de estrategias de ciberseguridad.

Durante la inauguración de la décima edición de ENISE (Encuentro Internacional de Seguridad de la Información, celebrado en León los días 18 y 19 de octubre de 2016), cuyo lema central fue «Trabajando para el desarrollo de la industria nacional de Ciberseguridad», el alcalde de León (España), Antonio Silván², señalaba en su presentación una frase que entronca con los objetivos principales de esta obra: «La apuesta por la interconexión con los emprendedores y el sector privado, claves en la lucha contra los ciberdelitos».

El futuro de la ciberseguridad

Las tendencias del sector de seguridad de la información y ciberseguridad se centran en servicios en la nube, *Big Data & Analytics*, Internet de las Cosas

² EFE. *Diario de León*. «Enise reúne a 1.100 expertos con el reto de crear industria nacional de ciberseguridad». http://www.diariodeleon.es/noticias/leon/enise-reune-1-100-expertos-reto-crear-industria-nacional-ciberseguridad_1107556.html [consultado 18 de octubre, 2016].

(con todos sus pilares fundamentales: sensores, redes inteligentes —contadores y medidores inteligentes—, drones —especialmente inteligentes y programables—,...) y todas las tecnologías asociadas a Industria 4.0. Se requieren herramientas y soluciones que se centren en elementos como la «vulnerabilidad de la empresa, la auditoría de TI y el *hacking* ético» (especialistas en seguridad informática y ciberseguridad que permitan conocer y comprobar el grado de vulnerabilidad tecnológica de las organizaciones y empresas y que dispongan no solo de los conocimientos informáticos adecuados sino que estén dotados de herramientas que les ayuden a prevenir potenciales ataques).

INCIBE, presentó —el 29 de septiembre de 2016— un diagnóstico de déficit de perfiles especialistas en ciberseguridad en la Unión Europea que tendrá la necesidad de incorporar en la próxima década en torno a 825.000 empleos cualificados en este sector³. Por estas razones, INCIBE ha lanzado diferentes iniciativas para propiciar el desarrollo de emprendedores y empresas en ciberseguridad, así como la publicación reciente del estudio⁴ «Punto de partida al modelo de gestión y seguimiento del talento en ciberseguridad en España». El estudio ha sido una buena prueba práctica de colaboración público-privada, ya que han intervenido en su elaboración los principales actores del mercado de ciberseguridad: la industria, el sector académico e investigador y profesionales de la ciberseguridad.

Para cerrar este epílogo citaremos dos propuestas de decálogo de ciberseguridad realizadas a lo largo de 2016 por dos instituciones con una gran experiencia en el campo de la ciberseguridad: FTF & Fundación Bankinter e INCIBE, y que consideramos de un alto nivel de calidad teórica y práctica para la estrategia de ciberseguridad de organizaciones y empresas.

El decálogo de ciberseguridad FTF & Fundación Bankinter

El estudio «Ciberseguridad, un desafío mundial»⁵ de la Fundación Innovación Bankinter, que recoge trabajos e intervenciones de expertos en seguridad,

³ INCIBE[en línea]<https://www.incibe.es/sala-prensa/notas-prensa/el-futuro-ciberseguridad-demandara-825000-profesionales-del-sector-2025>

⁴ INCIBE [en línea] https://www.incibe.es/sites/default/files/contenidos/notasprensa/doc/modelo_gestion_talento_incibe.pdf.

⁵ El estudio completo fue presentado el 5 de mayo de 2016 [en línea]: <https://www.fundacionbankinter.org/documents/20183/42758/Ciberseguridad/f22bf829-7bb5-447c-9c88-9f7bac51f482> El estudio es también una publicación del *Future Trends Forum* donde se analizan los desafíos de la ciberseguridad en el entorno global y se plantea una hoja de ruta de diez propuestas para regular y mejorar nuestras ciberseguridad.

El resumen ejecutivo también se puede descargar *online* en: <https://www.fundacionbankinter.org/documents/20183/42758/Ciberseguridad+-+Resumen+ejecutivo/63992dfa-c3e1-476f-9e3f-eeb7db6f6d86>

nacionales e internacionales⁶ en el foro *FutureTrends Forum* celebrado en diciembre de 2015, termina sus conclusiones con una hoja de ruta a modo de «Decálogo de propuestas» —en el informe se pueden ver ampliamente las actuaciones recomendadas para cada propuesta— para la ciberseguridad del futuro y que hacemos nuestras dado que la décima y última propuesta coincide, precisamente, con uno de los temas centrales de nuestra obra, la colaboración público-privada:

1. Reducir los costes globales de los ciberataques y cibercrimen. Se insta a trabajar conjuntamente a los países a nivel internacional bajo el liderazgo de Enisa (Agencia Europea de Seguridad de las Redes y de la Información: <https://www.enisa.europa.eu/>).
2. Garantizar la integridad de las infraestructuras y soluciones tecnológicas.
3. Extender el uso de la tecnología de autenticación de doble factor que verifica dos veces la identidad digital.
4. Educar a los ciudadanos en ciberseguridad.
5. Concienciar al consumidor digital en seguridad.
6. Proteger los datos nacionales en internet más allá de las fronteras territoriales.
7. Responsabilidad penal por el *software* inseguro.
8. Software de calidad.
9. Impulsar una estrategia de ciberseguridad global.
10. Colaboración público-privada.

El decálogo de ciberseguridad de INCIBE

INCIBE ha publicado un «Decálogo de Ciberseguridad»⁷ —ya comentado en el capítulo 1— dirigido a dar recomendaciones para garantizar la ciberseguridad a las empresas. Los diez pasos recomendados por INCIBE son:

1. Analizar los riesgos.
2. Los responsables de seguridad.
3. Seguridad en el proyecto de trabajo.
4. La protección de la información.
5. Movilidad con seguridad.
6. Protección anti-*malware*.
7. Actualización y parcheo.
8. La seguridad de la red.

⁶ Entre los expertos mundiales convocados por el foro FTF se destacan tres grandes expertos españoles en ciberseguridad: Carlos Jiménez, presidente y fundador de Secuware; Isaac Gutiérrez, jefe internacional de Ciberseguridad en Prosegur, y Miguel Rego, director general de INCIBE.

⁷ INCIBE. «Decálogo de ciberseguridad. El camino hacia la ciberseguridad de su empresa» [en línea]: https://www.incibe.es/extfrontinteco/img/File/empresas/blog/2014Octubre/decalogo_ciberseguridad_empresas.pdf. 2015

9. Monitorización.

10. Seguridad gestionada.

En el prólogo de su decálogo dirigido a la empresa, INCIBE plantea una serie de interrogantes a los que trata de dar respuesta a lo largo del documento, tales como: «¿Cuáles son los servicios más críticos de su empresa? ¿Ha analizado los riesgos tecnológicos de sus servicios más críticos? ¿Tiene un plan B si falla algo? ¿Sus clientes lo saben? ¿Cumple la LOPD⁸? ¿Ofrece servicio *online* a través de su página web? ¿Sabe qué medidas de seguridad deberá tener implantadas?...».

Ciberseguridad 4.0

Dado que nos encontramos al comienzo de la cuarta revolución industrial como consecuencia del advenimiento de la tendencia Industria 4.0 —comentada en el capítulo 1— y consideramos nos encontramos en una nueva era tecnológica y social que obligará a todas las organizaciones y empresas afrontar su transformación digital, queremos proponer —a modo exclusivamente personal del autor de este epílogo— una Ciberseguridad 4.0, como la nueva era de la ciberseguridad que consideramos traerá grandes retos y oportunidades para afrontar con éxito las ciberamenazas, ciberataques, ciberdelitos y ciberriesgos del futuro.

⁸ [¿Y cumplirá en el futuro la ya aprobada Ley de Privacidad y Protección de Datos de la Unión Europea?, véase capítulo 1].

Composición del grupo de trabajo

Coordinador:	D. Luis Joyanes Aguilar <i>Presidente de la Fundación I+D del Software Libre (Fidesol)</i>
Secretario:	D. David Ramírez Morán <i>Analista Principal del Instituto Español de Estudios Estratégicos</i>
Vocales:	D. Joaquín Castellón Moreno <i>Director Operativo</i> <i>Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno</i> D.ª María Mar López Gil <i>Jefa de la Oficina de Tecnología y Seguridad. Responsable de Ciberseguridad</i> <i>Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno</i> D. Aníbal Villalba Fernández <i>Doctor en Ciencias Políticas y Sociología, UNED</i> <i>Asesor del Presidente del Consejo Nacional de Ciberseguridad</i>

D. Juan Manuel Corchado Rodríguez

*Doctor en Informática, Universidad de Salamanca
Doctor en Inteligencia Artificial, University of the West
of Scotland*

D. Miguel Rego Fernández

*Director General del Instituto Nacional de Ciberseguri-
dad (INCIBE)*

D. Pedro Pablo Pérez García

Global Security VP en Telefónica & CEO 11paths

D. Fernando Sánchez Gómez

*Director del Centro Nacional para la Protección de las
Infraestructuras Críticas*

D. Justo López Parra

*Responsable de Prevención y Respuesta a la Cibera-
menaza en Endesa*

D. Gregorio Miguel Pulido Alonso

*Teniente coronel del Ejército de Tierra DIM
Jefe de la Sección de Preparación del MCCD*

D. Rafael Rosell Tejada

Director Comercial de S2Grupo

D. Aurelio Hinarejos Rojo

*Capitán del Cuerpo de Ingenieros Politécnicos del
Ejército DGAM/SDGPLATIN*

D. José de la Peña Muñoz

Director de la Revista SIC

D. Óscar Pastor Acosta

*Gerente de Seguridad
Isdefe*

D. José Javier Martínez Herráiz

*Director de la Cátedra Amaranto de Seguridad Digital
Universidad de Alcalá de Henares*

Cuadernos de Estrategia

- 01 La industria alimentaria civil como administradora de las FAS y su capacidad de defensa estratégica
- 02 La ingeniería militar de España ante el reto de la investigación y el desarrollo en la defensa nacional
- 03 La industria española de interés para la defensa ante la entrada en vigor del Acta Única
- 04 Túnez: su realidad y su influencia en el entorno internacional
- 05 La Unión Europea Occidental (UEO) (1955-1988)
- 06 Estrategia regional en el Mediterráneo Occidental
- 07 Los transportes en la raya de Portugal
- 08 Estado actual y evaluación económica del triángulo España-Portugal-Marruecos
- 09 Perestroika y nacionalismos periféricos en la Unión Soviética
- 10 El escenario espacial en la batalla del año 2000 (I)
- 11 La gestión de los programas de tecnologías avanzadas
- 12 El escenario espacial en la batalla del año 2000 (II)
- 13 Cobertura de la demanda tecnológica derivada de las necesidades de la defensa nacional

- 14 Ideas y tendencias en la economía internacional y española
- 15 Identidad y solidaridad nacional
- 16 Implicaciones económicas del Acta Única 1992
- 17 Investigación de fenómenos belígenos: método analítico factorial
- 18 Las telecomunicaciones en Europa, en la década de los años 90
- 19 La profesión militar desde la perspectiva social y ética
- 20 El equilibrio de fuerzas en el espacio sur europeo y mediterráneo
- 21 Efectos económicos de la unificación alemana y sus implicaciones estratégicas
- 22 La política española de armamento ante la nueva situación internacional
- 23 Estrategia finisecular española: México y Centroamérica
- 24 La Ley Reguladora del Régimen del Personal Militar Profesional (cuatro cuestiones concretas)
- 25 Consecuencias de la reducción de los arsenales militares negociados en Viena, 1989. Amenaza no compartida
- 26 Estrategia en el área iberoamericana del Atlántico Sur
- 27 El Espacio Económico Europeo. Fin de la Guerra Fría
- 28 Sistemas ofensivos y defensivos del espacio (I)
- 29 Sugerencias a la Ley de Ordenación de las Telecomunicaciones (LOT)
- 30 La configuración de Europa en el umbral del siglo XXI
- 31 Estudio de «inteligencia operacional»
- 32 Cambios y evolución de los hábitos alimenticios de la población española
- 33 Repercusiones en la estrategia naval española de aceptarse las propuestas del Este en la CSBM, dentro del proceso de la CSCE
- 34 La energía y el medio ambiente
- 35 Influencia de las economías de los países mediterráneos del norte de África en sus respectivas políticas defensa
- 36 La evolución de la seguridad europea en la década de los 90
- 37 Análisis crítico de una bibliografía básica de sociología militar en España. 1980-1990
- 38 Recensiones de diversos libros de autores españoles, editados entre 1980-1990, relacionados con temas de las Fuerzas Armadas
- 39 Las fronteras del mundo hispánico
- 40 Los transportes y la barrera pirenaica

- 41 Estructura tecnológica e industrial de defensa, ante la evolución estratégica del fin del siglo XX
- 42 Las expectativas de la I+D de defensa en el nuevo marco estratégico
- 43 Costes de un ejército profesional de reclutamiento voluntario. Estudio sobre el Ejército profesional del Reino Unido y (III)
- 44 Sistemas ofensivos y defensivos del espacio (II)
- 45 Desequilibrios militares en el Mediterráneo Occidental
- 46 Seguimiento comparativo del presupuesto de gastos en la década 1982-1991 y su relación con el de Defensa
- 47 Factores de riesgo en el área mediterránea
- 48 Las Fuerzas Armadas en los procesos iberoamericanos de cambio democrático (1980-1990)
- 49 Factores de la estructura de seguridad europea
- 50 Algunos aspectos del régimen jurídico-económico de las FAS
- 51 Los transportes combinados
- 52 Presente y futuro de la conciencia nacional
- 53 Las corrientes fundamentalistas en el Magreb y su influencia en la política de defensa
- 54 Evolución y cambio del este europeo
- 55 Iberoamérica desde su propio sur. (La extensión del Acuerdo de Libre Comercio a Sudamérica)
- 56 La función de las Fuerzas Armadas ante el panorama internacional de conflictos
- 57 Simulación en las Fuerzas Armadas españolas, presente y futuro
- 58 La sociedad y la defensa civil
- 59 Aportación de España en las cumbres iberoamericanas: Guadalajara 1991-Madrid 1992
- 60 Presente y futuro de la política de armamentos y la I+D en España
- 61 El Consejo de Seguridad y la crisis de los países del Este
- 62 La economía de la defensa ante las vicisitudes actuales de las economías autonómicas
- 63 Los grandes maestros de la estrategia nuclear y espacial
- 64 Gasto militar y crecimiento económico. Aproximación al caso español
- 65 El futuro de la Comunidad Iberoamericana después del V Centenario
- 66 Los estudios estratégicos en España
- 67 Tecnologías de doble uso en la industria de la defensa

- 68 Aportación sociológica de la sociedad española a la defensa nacional
- 69 Análisis factorial de las causas que originan conflictos bélicos
- 70 Las conversaciones internacionales Norte-Sur sobre los problemas del Mediterráneo Occidental
- 71 Integración de la red ferroviaria de la península ibérica en el resto de la red europea
- 72 El equilibrio aeronaval en el área mediterránea. Zonas de irradiación de poder
- 73 Evolución del conflicto de Bosnia (1992-1993)
- 74 El entorno internacional de la Comunidad Iberoamericana
- 75 Gasto militar e industrialización
- 76 Obtención de los medios de defensa ante el entorno cambiante
- 77 La Política Exterior y de Seguridad Común (PESC) de la Unión Europea (UE)
- 78 La red de carreteras en la península ibérica, conexión con el resto de Europa mediante un sistema integrado de transportes
- 79 El derecho de intervención en los conflictos
- 80 Dependencias y vulnerabilidades de la economía española: su relación con la defensa nacional
- 81 La cooperación europea en las empresas de interés de la defensa
- 82 Los cascos azules en el conflicto de la ex-Yugoslavia
- 83 El sistema nacional de transportes en el escenario europeo al inicio del siglo XXI
- 84 El embargo y el bloqueo como formas de actuación de la comunidad internacional en los conflictos
- 85 La Política Exterior y de Seguridad Común (PESC) para Europa en el marco del Tratado de no Proliferación de Armas Nucleares (TNP)
- 86 Estrategia y futuro: la paz y seguridad en la Comunidad Iberoamericana
- 87 Sistema de información para la gestión de los transportes
- 88 El mar en la defensa económica de España
- 89 Fuerzas Armadas y sociedad civil. Conflicto de valores
- 90 Participación española en las fuerzas multinacionales
- 91 Ceuta y Melilla en las relaciones de España y Marruecos
- 92 Balance de las primeras cumbres iberoamericanas
- 93 La cooperación hispano-franco-italiana en el marco de la PESC

- 94 Consideraciones sobre los estatutos de las Fuerzas Armadas en actividades internacionales
- 95 La unión económica y monetaria: sus implicaciones
- 96 Panorama estratégico 1997/98
- 97 Las nuevas Españas del 98
- 98 Profesionalización de las Fuerzas Armadas: los problemas sociales
- 99 Las ideas estratégicas para el inicio del tercer milenio
- 100 Panorama estratégico 1998/99
- 100-B 1998/99 Strategic Panorama
- 101 La seguridad europea y Rusia
- 102 La recuperación de la memoria histórica: el nuevo modelo de democracia en Iberoamérica y España al cabo del siglo XX
- 103 La economía de los países del norte de África: potencialidades y debilidades en el momento actual
- 104 La profesionalización de las Fuerzas Armadas
- 105 Claves del pensamiento para la construcción de Europa
- 106 Magreb: percepción española de la estabilidad en el Mediterráneo, perspectiva hacia el 2010
- 106-B Maghreb: perception espagnole de la stabilité en Méditerranée, prospective en vue de L'année 2010
- 107 Panorama estratégico 1999/2000
- 107-B 1999/2000 Strategic Panorama
- 108 Hacia un nuevo orden de seguridad en Europa
- 109 Iberoamérica, análisis prospectivo de las políticas de defensa en curso
- 110 El concepto estratégico de la OTAN: un punto de vista español
- 111 Ideas sobre prevención de conflictos
- 112 Panorama Estratégico 2000/2001
- 112-B Strategic Panorama 2000/2001
- 113 Diálogo mediterráneo. Percepción española
- 113-B Le dialogue Méditerranéen. Une perception espagnole
- 114 Aportaciones a la relación sociedad - Fuerzas Armadas en Iberoamérica
- 115 La paz, un orden de seguridad, de libertad y de justicia
- 116 El marco jurídico de las misiones de las Fuerzas Armadas en tiempo de paz
- 117 Panorama Estratégico 2001/2002

- 117-B 2001/2002 Strategic Panorama
- 118 Análisis, estrategia y prospectiva de la Comunidad Iberoamericana
- 119 Seguridad y defensa en los medios de comunicación social
- 120 Nuevos riesgos para la sociedad del futuro
- 121 La industria europea de defensa: presente y futuro
- 122 La energía en el espacio euromediterráneo
- 122-B L'énergie sur la scène euroméditerranéenne
- 123 Presente y futuro de las relaciones cívico-militares en Hispanoamérica
- 124 Nihilismo y terrorismo
- 125 El Mediterráneo en el nuevo entorno estratégico
- 125-B The Mediterranean in the New Strategic Environment
- 126 Valores, principios y seguridad en la comunidad iberoamericana de naciones
- 127 Estudios sobre inteligencia: fundamentos para la seguridad internacional
- 128 Comentarios de estrategia y política militar
- 129 La seguridad y la defensa de la Unión Europea: retos y oportunidades
- 130 El papel de la inteligencia ante los retos de la seguridad y defensa internacional
- 131 Crisis locales y seguridad internacional: El caso haitiano
- 132 Turquía a las puertas de Europa
- 133 Lucha contra el terrorismo y derecho internacional
- 134 Seguridad y defensa en Europa. Implicaciones estratégicas
- 135 La seguridad de la Unión Europea: nuevos factores de crisis
- 136 Iberoamérica: nuevas coordenadas, nuevas oportunidades, grandes desafíos
- 137 Irán, potencia emergente en Oriente Medio. Implicaciones en la estabilidad del Mediterráneo
- 138 La reforma del sector de seguridad: el nexo entre la seguridad, el desarrollo y el buen gobierno
- 139 Security Sector Reform: the Connection between Security, Development and Good Governance
- 140 Impacto de los riesgos emergentes en la seguridad marítima
- 141 La inteligencia, factor clave frente al terrorismo internacional
- 142 Del desencuentro entre culturas a la Alianza de Civilizaciones. Nuevas aportaciones para la seguridad en el Mediterráneo

- 143 El auge de Asia: implicaciones estratégicas
- 144 La cooperación multilateral en el Mediterráneo: un enfoque integral de la seguridad
- 145 La Política Europea de Seguridad y Defensa (PESD) tras la entrada en vigor del Tratado de Lisboa
- 145-B The European Security and Defense Policy (ESDP) after the entry into Force of the Lisbon Treaty
- 146 Respuesta europea y africana a los problemas de seguridad en África
- 146-B European and African Response to Security Problems in Africa
- 147 Los actores no estatales y la seguridad internacional: su papel en la resolución de conflictos y crisis
- 148 Conflictos, opinión pública y medios de comunicación. Análisis de una compleja interacción
- 149 Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio
- 150 Seguridad, modelo energético y cambio climático
- 151 Las potencias emergentes hoy: hacia un nuevo orden mundial
- 152 Actores armados no estables: retos a la seguridad
- 153 Proliferación de ADM y de tecnología avanzada
- 154 La defensa del futuro: innovación, tecnología e industria
- 154-B The Defence of the Future: Innovation, Technology and Industry
- 155 La Cultura de Seguridad y Defensa. Un proyecto en marcha
- 156 El gran Cáucaso
- 157 El papel de la mujer y el género en los conflictos
- 157-B The role of woman and gender in conflicts
- 158 Los desafíos de la seguridad en Iberoamérica
- 159 Los potenciadores del riesgo
- 160 La respuesta del derecho internacional a los problemas actuales de la seguridad global
- 161 Seguridad alimentaria y seguridad global
- 161-B Food security and global security
- 162 La inteligencia económica en un mundo globalizado
- 162-B Economic intelligence in global world
- 163 Islamismo en (r)evolución: movilización social y cambio político
- 164 Afganistán después de la ISAF
- 165 España ante las emergencias y catástrofes. Las Fuerzas Armadas en colaboración con las autoridades civiles

- 166 Energía y Geoestrategia 2014
- 166-B Energy and Geostrategy 2014
- 167 Perspectivas de evolución futura de la política de seguridad y defensa de la UE. Escenarios de crisis
- 167-B Prospects for the future evolution of the EU's security and defence policy. Crisis scenarios
- 168 Evolución del mundo árabe: tendencias
- 169 Desarme y control de armamento en el siglo xxi: limitaciones al comercio y a las transferencias de tecnología
- 170 El sector espacial en España. Evolución y perspectivas
- 171 Cooperación con Iberoamérica en materia de defensa
- 172 Cuadernos de Estrategia 172 Cultura de Seguridad y Defensa: fundamentos y perspectivas de mejora
- 173 La internacional yihadista
- 174 Economía y geopolítica en un mundo globalizado
- 175 Industria Española de Defensa. Riqueza, tecnología y seguridad
- 176 Shael 2015, origen de desafíos y oportunidades
- 177 UE-EE.UU.: Una relación indispensable para la paz y la estabilidad mundiales
- 178 Rusia bajo el liderazgo de Putin. La nueva estrategia rusa a la búsqueda de su liderazgo regional y el reforzamiento como actor global.
- 179 Análisis comparativo de las capacidades militares españolas con las de los países de su entorno
- 180 Estrategias para derrotar al Dáesh y la reestabilización regional
- 181 América Latina: nuevos retos en seguridad y defensa
- 182 La colaboración tecnológica entre la universidad y las Fuerzas Armadas
- 183 Política y violencia: comprensión teórica y dearrollo en la acción colectiva
- 184 Una estrategia global de la Unión Europea para tiempos difíciles

