¿Por qué una conciencia nacional de *ciberseguridad*?

«La implantación de una cultura de *ciberseguridad* sólida. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento.» Estrategia de Seguridad Nacional.

«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.» Estrategia de Seguridad Nacional.

Bajo la pregunta: «¿Por qué una conciencia nacional de *ciberseguridad*?» se desarrolla una monografía que lleva como título: «Necesidad de una conciencia nacional de *ciberseguridad*. La *ciberdefensa*: un reto prioritario», y donde hemos intentado responder a una pregunta que, cuando nos la formulábamos el primer día de nuestro trabajo, suscitaba interrogantes, pero, sobre todo, entusiasmo que solo rivalizaba con la amplitud y vigencia del proyecto que teníamos frente a nosotros.

Cuando comenzamos el estudio no se había publicado la Estrategia de Seguridad Nacional y esperábamos que antes de la finalización del presente trabajo pudiéramos contar con dicha estrategia y con la Estrategia Nacional de Ciberseguridad. La segunda aún no ha sido publicada pero la primera ya hace una especial mención a la *ciberseguridad*.

El tercer capítulo de la Estrategia de Seguridad Nacional, «Los riesgos y amenazas para la Seguridad Nacional», describe los riesgos y amenazas que afectan singularmente a la seguridad nacional: los conflictos armados, el terrorismo, las amenazas cibernéticas, el crimen organizado, la inestabilidad económica y financiera, la vulnerabilidad energética, la proliferación de armas de destrucción masiva, los flujos migratorios irregulares, el espionaje, las emergencias y catástrofes, la vulnerabilidad del espacio marítimo y la vulnerabilidad de las infraestructuras críticas y los servicios esenciales. También se contemplan factores potenciadores como el cambio climático, la pobreza, la desigualdad, los extremismos ideológicos, los desequilibrios demográficos o la generalización del uso nocivo de las nuevas tecnologías que, sin ser en sí mismos un riesgo o una amenaza, pueden desencadenarlos o agravarlos.

El cuarto capítulo, «Líneas de acción estratégicas», expone en el área de seguridad cibernética un objetivo: garantizar un uso seguro de las redes y sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y reacción frente a los ataques cibernéticos. Para ello, traza las siguientes líneas de acción estratégicas:

- Incremento de la capacidad de prevención, detección, investigación y respuesta ante las *ciberamenazas*, con apoyo en un marco jurídico operativo y eficaz. Se mejorarán los procedimientos y se impulsarán los recursos necesarios con especial énfasis en las Administraciones Públicas, las infraestructuras críticas, las capacidades militares y de defensa y todos aquellos sistemas de interés nacional.
- Garantía de la seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones Públicas. Se finalizará la implantación del Esquema Nacional de Seguridad, previsto en la Ley 11/2007, de 22 de junio, mediante el refuerzo de las capacidades de detección y la mejora de la defensa de los sistemas clasificados. Se fortalecerá la seguridad de los sistemas de información y las redes de comunicaciones que soportan las infraestructuras críticas. Se impulsará la normativa sobre protección de infraestructuras críticas con el desarrollo de las capacidades necesarias para la protección de los servicios esenciales.
- Mejora de la seguridad y resiliencia de las tecnologías de la información y la comunicación (TIC) en el sector privado a través del uso de las capacidades de los poderes públicos. Se impulsarán y liderarán actuaciones destinadas a reforzar la colaboración público-privada y la seguridad y robustez de las redes, productos y servicios de las TIC empleados por el sector industrial.
- 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. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento.

– Intensificación de la colaboración internacional. Se promoverán los esfuerzos tendentes a conseguir un ciberespacio internacional donde se alineen las iniciativas de todos los países que persiguen un entorno seguro y fiable. En todo momento se salvaguardarán los intereses nacionales.

Ha sido un trabajo de altísimo nivel profesional, acorde con los miembros del Comité que he tenido el placer y orgullo de presidir. Este equipo lo han constituido José Manuel Roldán Tudela, Luis Jiménez, Óscar Pastor Acosta, Emilio Sánchez de Rojas y José Tomás Hidalgo Tarrero. Los capítulos que han configurado esta monografía son los siguientes:

Capítulo 1: Principios de una conciencia nacional de *ciberseguridad*.
Capítulo 2: Concienciar a los particulares.
Capítulo 3: Concienciar a la Administración.
Capítulo 4: Concienciar a las empresas.
Capítulo 5: La cooperación internacional en *ciberseguridad*.

Entender la realidad social en nuestros días pasa ineludiblemente por analizar las circunstancias que rodean a los ciudadanos, tanto en su comportamiento individual como colectivo, y tanto en su concepto de personas físicas como en su forma de agrupamientos jurídicos, siendo empresas, fundaciones, asociaciones u organismos públicos. En este análisis, forma parte sustancial el ecosistema donde la vida se realiza. Dicho ecosistema se compone de elementos físicos y de otros elementos que, aun siendo físicos, no son tangibles como ciertos elementos naturales o algunos creados por el hombre. Dentro de estos últimos se encuentran las tecnologías de las comunicaciones que han evolucionado en estos últimos años de una forma vertiginosa, posibilitando el cambio social aun antes de que la sociedad haya tomado conciencia de su desarrollo. Siendo la tecnología, una vez más, un disparador de esta modificación sustancial de las reglas del juego social, modificando los modelos de relación desde un punto de vista antropológico.

La emergencia de Internet –después de haber sido durante años en sus fases incipientes un instrumento de comunicaciones militares– y su difusión y proliferación han servido de base para acelerar procesos de cambio social de una forma distinta a la que venía produciéndose tradicionalmente, pues ha roto dos dimensiones: el espacio y el tiempo.

Si algo define a Internet es la «democratización» de la información, favoreciendo movimientos a escala planetaria como la globalización y posibilitando también aquellas reacciones organizadas transnacionalmente

como son las corrientes antiglobalización. Elementos como la inmediatez de las acciones en el espacio virtual se trasladan a elementos visibles en cuestión de segundos, y la posibilidad de la acción social directa cambia la capacidad de obtener resultados que en otro tiempo se veían más lejanos.

A la hora de abordar este trabajo, mantuvimos la primera aproximación de estructurar las distintas ponencias basándonos en los actores de esta aproximación, a saber, las personas, las organizaciones privadas, los organismos públicos y la cooperación internacional. Ningún aspecto ha quedado sin considerar, desde los entornos jurídicos a las amenazas y los riesgos que afectan a cada uno de los colectivos sujetos del estudio.

La necesidad de una concienciación pasa por una definición del término «conciencia», que es, según la Real Academia Española: «(Del lat. *conscientĭa, y del gr. συνείδησις*) Propiedad del espíritu humano de reconocerse en sus atributos esenciales y en todas las modificaciones que en sí mismo experimenta. Acto psíquico por el que un sujeto se percibe a sí mismo en el mundo». Y concienciar: «Hacer que alguien sea consciente de algo. Adquirir conciencia de algo».

Para empezar podemos hablar de la aproximación a una nueva era organizativa donde los esquemas tradicionales tanto de comportamiento como de influencia se han visto modificados. Observando estas transformaciones podemos llegar a concluir que los paradigmas clásicos de comprensión de la estructura social han sido reemplazados por esquemas mucho más dinámicos en los que los acontecimientos se suceden a velocidades hasta ahora jamás experimentadas por las sociedades en las que tradicionalmente hemos vivido.

Pero los seres humanos intentamos entender las diferencias desde nuestros esquemas históricos de pensamiento. Según Lévi-Strauss, «estas uniformidades surgen de la estructura del cerebro humano y del proceso de pensamiento inconsciente. La característica estructural más importante de la mente humana es la tendencia a *dicotomizar,* o a pensar en términos de oposiciones binarias, y después intentar mediar esta oposición mediante un tercer concepto, que puede servir como base para otra oposición. Una oposición recurrente presente en muchos mitos, por ejemplo, es cultura/naturaleza. Desde el punto de vista estructural, cuanto más cambien las culturas más permanecerán siendo las mismas, puesto que simplemente constituyen variaciones del tema de las oposiciones recurrentes y sus resoluciones». Este esquema de pensamiento nos ha servido para la tradicional distinción bueno-malo, aliado-enemigo, pero el entendimiento de la realidad no es lineal; lo mismo sucede con Internet, un elemento donde la democratización aparente de la información es un continuo, donde la *anonimización* es prácticamente omnipresente, un espacio de comunicación interpersonal sin barreras de espacio donde

la velocidad, la inmediatez transforma nuestra percepción de nuestra vivencia como ser humano, como ser social.

Dentro de este esquema, las relaciones sociales cambian, los modelos productivos se ven modificados, aparecen nuevos negocios, desaparecen empresas, la relación entre los administrados y su administración varía sustancialmente, la cual se vuelve más participativa y para ello necesita nuevos canales de expresión. Por todo ello, Internet es un fenómeno de revolución social que posibilita cambios y fuerza la acomodación de estructuras tanto jurídicas como políticas, educativas, formativas, de negocios, delincuenciales, de protección y seguridad. Todo bajo el prisma de la comprensión y de la adecuación, incluida, como no podía ser de otra forma, la seguridad personal y estatal donde aparecen nuevos riesgos, amenazas, oportunidades... Internet y su medio «natural», el ciberespacio, se convierten en un nuevo ecosistema donde todos hemos empezado a convivir. La convivencia exige adaptación a unas nuevas reglas, a la comprensión de los modelos nuevos sobre formas de relación tradicionales, es por ello que la necesidad de una concienciación sobre este nuevo entorno es fundamental. No se excluyen de este modelo ningún fenómeno de relación social ni interindividual ni colectiva ni familiar ni empresarial ni las relaciones entre estados.

Estamos ante un nuevo modelo cultural, entre otras características, fascinante que permite al observador inquieto observar más allá de los fenómenos aparentes. Una oportunidad para el desarrollo de nuevos campos formativos, de desarrollo tecnológico, de nuevas formas de relación, de nuevas formas de modelos productivos, de nuevos pesos de los estados en el panorama internacional. Todos estamos desarrollando nuevas herramientas para acomodarnos a este nuevo ecosistema, la evolución del ser social está ante nosotros y en nosotros.

En el libro VII de *República* Platón presenta su mito más importante y conocido, el mito de la caverna, donde dice expresamente que el mito quiere ser una metáfora «de nuestra naturaleza respecto de su educación y de su falta de educación», es decir, sirve para ilustrar cuestiones relativas a la teoría del conocimiento. El mito describe nuestra situación respecto del conocimiento: al igual que los prisioneros de la caverna que solo ven las sombras de los objetos, nosotros vivimos en la ignorancia cuando nuestras preocupaciones se refieren al mundo que se ofrece a los sentidos. Solo la reflexión puede liberarnos y permitirnos salir de la caverna e incorporarnos al mundo verdadero o Mundo de las Ideas.

En este sentido, Internet se convierte en un escenario donde todo cobra un nuevo sentido. Un espacio donde la persona expresa y comunica espacios de su personalidad que, de otra forma, le serían difíciles de transmitir. Este espacio genera nuevas formas de comportamiento, nuevas relaciones; desde esta monografía hemos abordado una faceta de esta relación, la de profundizar en la necesidad de un desarrollo de una con-

ciencia de *ciberseguridad*. Faceta que se convierte en vertebral ya que la seguridad es una sensación que permite al ser humano y a las organizaciones desarrollar de una forma estable sus relaciones.

Las relaciones sociales se desarrollan en marcos conceptuales definidos, en los que la seguridad jurídica y el cumplimiento de la ley y de las normas establecidas permiten una ordenación definida. Pero cuando los espacios donde esas relaciones no están aún regulados porque la velocidad del cambio es sustancialmente superior al de su marco establecido, se generan tensiones que han de ser suavizadas por un esfuerzo en la formación de las personas para adecuar su acción ante estos nuevos retos. Los nativos en Internet no encuentran razonables determinadas limitaciones que son reclamadas por aquellos que hemos visto el nacimiento de este nuevo modelo de interacción social.

Las iniciativas sobre materias de *ciberseguridad* que están siendo desarrolladas en todos los países ante este entorno de cambio y en el ciberespacio configuran un reto de entendimiento de este «nuevo mundo». Un mundo que permite grandes oportunidades y presenta grandes retos, una experiencia fascinante para el investigador social donde, transformado en analista de inteligencia, debe interpretar los datos, ver más allá de lo evidente y concluir que, desde un punto de vista interpretativo y otro prospectivo, el papel que desarrollan los individuos, las empresas, las organizaciones públicas y los Estados está sometido a cambios y revisión.

En el presente estudio comenzaremos por la definición de los principios de una conciencia nacional de *ciberseguridad;* para ello, el coronel José Tomás Hidalgo Tarrero nos hablará sobre el concepto de *ciberguerra* comparándolo con otros paradigmas conocidos históricamente:

> *El paradigma de la «ciberguerra» es en todo similar a los paradigmas de la guerra asimétrica y de la guerra total; fundamento esta aseveración en lo siguiente:*

- *Los efectos pueden alcanzar a todos los ciudadanos, administraciones, instituciones y empresas del Estado aunque no estén conectados al ciberespacio (paradigma de la guerra total).*
- *Involucra, voluntaria o involuntariamente, a todos los ciudadanos, administraciones, instituciones y empresas del Estado (paradigma de la guerra total).*
- *La relación entre eficacia y coste es muy alta, posiblemente la más alta, ya que puede inutilizar sistemas básicos y críticos de un país con un coste para el atacante extraordinariamente bajo (paradigma de la guerra asimétrica).*
- *No necesita de una infraestructura grande y costosa como la industria de armamento clásico –terrestre, naval, aéreo y NBQR– (paradigma de la guerra asimétrica).*

– *Solo necesita personas con muy buena formación en ingeniería informática y en psicología.*

– *En la ciberdefensa pasiva deben participar todos los ciudadanos, administraciones, instituciones y empresas del Estado, cada uno a su nivel y con sus medios (paradigmas de la guerra total y de la guerra asimétrica).*

– *La ciberdefensa activa es, o debe ser, función exclusiva, a nivel dirección, del Gobierno de la nación.*

  Es muy difícil probar fehacientemente la autoría de un ataque a menos que el atacante quiera que se sepa, lo que proporciona un nivel de anonimato muy grande y convierte a la «ciberguerra» en una guerra pérfida (paradigma de la guerra asimétrica).

Una vez hecha esta apreciación, el coronel Hidalgo Tarrero profundizará sobre el concepto de conciencia de defensa cibernética, haciendo una mención especial al concepto de:

> *...la conciencia nacional de ciberseguridad y hay que utilizar ambos significados porque es necesario ser conscientes de las amenazas y es necesario conocer nuestros deberes como individuos, como miembros de diversas organizaciones y de la administración e instituciones y como directivos, en su caso, de ellas; debemos ser conscientes de nuestras responsabilidades tanto individuales como colectivas en el campo de la ciberseguridad; estas responsabilidades son, como en el texto transcrito, personales, ciudadanas, éticas y políticas.*
>
> *La conciencia nacional de ciberseguridad, para que sea nacional, debe incluir a todos los ciudadanos y todas las instituciones, empresas y organizaciones pues de lo contrario presentará carencias y flancos débiles que serán usados, sin ninguna duda, por los atacantes.*

La concienciación en la protección frente a las amenazas «debe cubrir todos los aspectos de los sistemas informáticos y de las comunicaciones, empezando por el eslabón débil en todos ellos: el ser humano que los construye, los mantiene y los usa».

En España, al igual que en otros países, es necesario desarrollar esta cultura de concienciación en *ciberseguridad*, pero, como todo proceso cultural, necesita tiempo, recursos y convicción para llevar a cabo una política y una estrategia en esta materia. El coronel Hidalgo Tarrero hace especial referencia en este aspecto al informe del Spanish Cyber Security Institute (SCSI) titulado *La ciberseguridad nacional, un compromiso de todos*, donde queda reflejado el bajo nivel de concienciación en *ciberseguridad* de la sociedad civil, resaltando las siguientes causas:

> *Escaso protagonismo de los actores privados en materia de «ciberseguridad». La ciberseguridad nacional, hoy en día, es un sistema cerrado*

y exclusivo de los actores gubernamentales. En la actualidad, más del 80% de las infraestructuras críticas de nuestro país son propiedad, están dirigidas y gestionadas por el sector privado (empresas nacionales e internacionales). Por tanto, la aportación del sector privado al proceso de construcción de la «ciberseguridad» nacional resulta esencial.

Ausencia de una política estatal en materia de «ciberconcienciación» y «cibereducación». Muchos países de nuestro entorno están desarrollando ambiciosas políticas en materia de «ciberconcienciación» y «ciberseguridad» como eje fundamental para la creación de una cultura de «ciberseguridad». Estas políticas han sido desarrolladas e impulsadas, en primera instancia, por el sector privado y, posteriormente, han recibido un fuerte apoyo gubernamental.

En este caso, cabe destacar una doble función, por un lado, concienciar y educar al conjunto de la ciudadanía de los riesgos del ciberespacio y, por otro, identificar futuros talentos en el campo de la «ciberseguridad» dentro de la comunidad escolar y universitaria.

En España, INTECO y el CCN disponen de programas de «ciberconcienciación» y «ciberseguridad». Desde el sector privado, organismos como el ISMS Forum Spain han lanzado su propia campaña de «ciberconcienciación» bajo la denominación protegetuinformacion.com. De momento, estas iniciativas tienen una repercusión insuficiente en la sociedad civil.

Ausencia de políticas específicas para el I+D+i nacional en materia de «ciberseguridad». No existen políticas, programas o iniciativas para el I+D+i de ámbito nacional que promuevan y faciliten actividades en materia de «ciberseguridad», lo que contrasta con el gran protagonismo que a nivel europeo el nuevo marco de trabajo del Horizonte 2020 (continuación del 7.º Programa Marco) otorga a la «ciberseguridad».

Con la nueva Estrategia de Seguridad Nacional y con la inminente Estrategia Nacional de Ciberseguridad se desarrollará una actividad de concienciación por parte de la organización del Estado pero es imprescindible tener en cuenta que ha de desarrollarse una acción conjunta por parte de todos los organismos implicados en la sociedad civil.

En el capítulo segundo, el general Roldán Tudela aborda el problema de la concienciación de los particulares. Empezará por reflejar las relaciones entre el ciberespacio y la persona. Para ello, estructurará su reflexión en tres partes: una definición del ciberespacio, la adopción de un modelo y una descripción del mismo, para posteriormente centrarse en la persona y su relación con el ciberespacio: sus datos personales, la identidad digital y la evolución hacia el nuevo «ciudadano digital».

Una vez sentadas las bases de la relación de las personas con el ciberespacio, se realizará un análisis basado en el riesgo para poner de mani-

fiesto qué es lo que deben temer las personas al actuar en el ciberespacio y cómo se pueden defender contra ello. Se analizarán los orígenes de los ataques en el ciberespacio, las víctimas de estos ataques, los activos o bienes que corren peligro, las amenazas y las medidas para disminuir el riesgo.

La tercera parte resulta la más significativa puesto que se refiere a la creación de la conciencia de seguridad cibernética, basada en los análisis de los apartados anteriores. Se hablará de los grados de conciencia de seguridad cibernética a alcanzar, de los sujetos a los que se les va a imbuir esta conciencia, de los actores que participan activamente en estas actividades, de las materias objeto de concienciación y de las vías y los medios a emplear.

> *Hay muchas definiciones de ciberespacio. El Cuaderno de Estrategia núm. 149 (1) del IEEE (pág. 51), recoge varias, de las que nos quedamos, como más conveniente, con la del Departamento de Defensa de los EE. UU. El ciberespacio es «un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores».*

Nos hablará el general sobre los distintos modelos para describir este nuevo dominio, el ciberespacio, para la acción humana, distinguiendo entre este e Internet, ya que Internet es una parte de aquel. Posteriormente, profundizará en la persona como objeto fundamental del estudio en este capítulo y sus principales activos que aportan información, datos, elementos que, en su crecimiento exponencial tanto en cantidad como en calidad, aportan un enorme valor para la economía global. Estos datos son objeto de «monetización». Las personas han comprendido el valor que los datos personales tienen para las administraciones y las corporaciones y quieren aprovecharlo en su beneficio.

> *Este valor está creciendo continuamente, ya que cuantos más datos hay, más valor posee, al contrario que otras mercancías, como el oro. La estabilidad depende de la disposición de las personas para comunicar sus datos, que se ve mermada si sienten amenazada su privacidad. Resulta necesario por tanto que las empresas y administraciones sean capaces de crear y mantener la confianza que hace fluir los datos. La protección de datos personales y la posibilidad de usarlos en un contexto económico deben alcanzar un equilibrio en el que la persona pueda decidir libremente si comunica o comparte sus datos y en qué grado.*

En definitiva, podemos decir que una regulación adecuada de la protección de datos personales, la creación de un clima de confianza, la educación de las personas en relación con el control de su privacidad y una

compensación equitativa pueden hacer sumamente provechosas las aplicaciones de los datos personales.

El control de la privacidad de los datos, objeto en estos momentos de especial controversia, puede ser ejercido, en general, a través del proceso de la anonimización que permite desconectar entre sí los datos que forman la identidad digital. Por otra parte, el proceso de garantizar la identidad de la persona depende del enlace existente entre la identidad digital y la identidad real, es decir, el proceso de «autenticación» puede ser más o menos fuerte. Frente a estas prevenciones veremos quiénes son los atacantes, desde dónde atacan y qué motivaciones les mueven a actuar, sean políticas, de lucro o satisfacciones personales (conductas desviadas), entre otras. Y veremos quiénes son las víctimas, haciendo el general una distinción fundamental por su riesgo y alarma social entre los menores y el resto de los ciudadanos, resaltando que «por motivos legales y morales, el Estado, la sociedad y todos sus integrantes tienen un imperativo que obliga a la protección de los menores».

El factor humano es el eslabón más débil de la cadena de seguridad y del que se pueden explotar tres rasgos presentes en el ser humano: el miedo, la confianza y la inconsciencia (o inadvertencia). Se utilizarán tres vías principalmente para crear una conciencia nacional de *ciberseguridad*: la educación, la enseñanza y la concienciación. La conciencia de *ciberseguridad* se alcanza paulatinamente, según ciertos grados; no todas las personas pueden llegar a alcanzar el mismo grado. La edad también influye: cada grado de madurez de la persona permite alcanzar un grado de conciencia de *ciberseguridad*. Podemos establecer cuatro grados, de los que los tres primeros podrían ser alcanzados por una parte significativa de la población. Desde el nivel más básico al más avanzado se pueden establecer los siguientes grados: *ciberhigiene, ciberconciencia, ciberciudadanía* y *ciberespecialistas cibernéticos*. Siendo los sujetos primarios los que deben crear conciencia de *ciberseguridad* en los sujetos últimos, es decir, en la población.

En el tercer capítulo, Luis Jiménez nos hablará sobre la necesidad de una concienciación en la Administración sobre los riesgos asociados al uso de las tecnologías de la información por parte del personal de las Administraciones Públicas, así como la importancia de su gestión en los marcos regulatorios del funcionamiento de la Administración.

> *Haciendo especial hincapié en la necesidad de comunicación y conocimiento (toma de conciencia), que es mayor en los niveles jerárquicos superiores del personal de las Administraciones Públicas, incluido el nivel político, pues la toma de decisiones en relación con la seguridad cibernética debe tener una buena ubicación para que las prioridades puedan ser adecuadas y el eterno equilibrio entre seguridad y eficacia pueda ser alcanzado.*

Para ello, la Administración en su conjunto no puede ser ajena al escenario de riesgos, amenazas y vulnerabilidades y, en función de sus responsabilidades, debe asumir que el desarrollo, la adquisición, conservación y utilización segura de las TIC debe ser considerado como algo imprescindible para garantizar el funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales. Una seguridad que debe estar orientada a garantizar o mantener tres cualidades propias de esta última: disponibilidad, integridad y confidencialidad. En algunos entornos, especialmente en los dedicados a la administración electrónica, interesan, además, otros aspectos muy importantes de las transacciones *on line* como son la autenticidad o la trazabilidad.

Todos los empleados públicos, de todos los niveles, tienen la obligación legal de conocer y cumplir las políticas de seguridad de la información y la normativa de seguridad. Normas de seguridad (*security standards*), guías de seguridad (*security guides*) y procedimientos de seguridad (*security procedures*). La concienciación de los empleados públicos en materia de seguridad es una tarea imprescindible para el cumplimiento de esta obligación.

A la hora de abordar el apartado de vulnerabilidades, Luis Jiménez desarrolla los distintos elementos que lo componen haciendo mención a los servicios en la nube, que en estos momentos se están desplegando de una forma masiva. Nos enfrentamos a fugas de información y dispositivos no controlados en las organizaciones –el fenómeno del *bring your own device* provoca grandes riesgos ante las vulnerabilidades que aportan unos dispositivos no normalizados dentro de las políticas de seguridad de las organizaciones–. Las políticas de seguridad han de ser seguidas con especial cuidado y su plan de acción ha de ser rigurosamente monitorizado y, para ello, es fundamental el proceso de concienciación y de formación en estos procedimientos, ya que muchas organizaciones no los tienen en cuenta.

Las normas de seguridad en la información, como la SGSI, la ISO 27001 o la protección de los servicios de la administración electrónica (Esquema Nacional de Seguridad, Real Decreto 3/2010), son obligadas si queremos cumplir escrupulosamente la normativa. Pero nos enfrentamos a un mundo dinámico donde los riesgos evolucionan, mutan a una velocidad impensable para muchos, y aquellos que tienen la responsabilidad de gestionar estos riesgos y ven diariamente los ataques por parte de los atacantes exigen un análisis de riesgos que incorpore una gestión preventiva. Los análisis de riesgos tradicionales confeccionados desde un despacho no se adecuan a la realidad actual. Por ello necesitamos un análisis dinámico y preventivo de las medidas de protección adecuadas y proporcionadas al valor de lo protegido frente a una caracterización del entorno hostil en que se encuentra, sea por incidentes externos, ataques deliberados o vulnerabilidades propias del sistema de información.

La necesidad de una capacidad de reacción ante un ataque, una respuesta adecuada a dicho ataque en tiempo real, nos obliga a aumentar nuestras capacidades y nuestro presupuesto. En estas situaciones se requiere revisar el análisis de riesgos del nuevo escenario y tomar rápidamente decisiones correctivas que mitiguen el impacto y permitan salir lo antes posible del escenario de crisis, recuperando el control de la situación.

Los aspectos de concienciación sobre los riesgos y de formación en seguridad pueden verse reflejados en los principios de conducta que establece la Ley 7/2007 relativos a la actuación diligente, eficaz, responsable, etc. Sin embargo, se echa de menos una expresión explícita a la observancia de las normas de seguridad informática tal como hace con las normas de seguridad y salud laboral. La necesidad de concienciación en materias de seguridad viene recogida expresamente en la ley y obliga al funcionario de la Administración a ser cumplidor estricto de las normativas que se aplican.

La responsabilidad del éxito de una organización recae, en última instancia, en su Dirección. La Dirección es responsable de organizar las funciones y responsabilidades y la política de seguridad del organismo, y de facilitar los recursos adecuados para alcanzar los objetivos propuestos. Los directivos son también responsables de dar buen ejemplo siguiendo las normas de seguridad establecidas. En una organización pueden coexistir diferentes informaciones y servicios, debiendo identificarse al responsable (o propietario) de cada uno de ellos, pues una misma persona puede aunar varias responsabilidades. Por ejemplo, en el ENS dos figuras son especialmente relevantes:

- El responsable de la información que establece las necesidades de seguridad de la información que se maneja.
- El responsable del servicio que establece las necesidades de seguridad del servicio que se presta.
- Una campaña de concienciación orientada a los empleados debe tener presente los diferentes aspectos del problema de la *ciberseguridad*. Aunque cualquier acción es positiva, es realmente necesario que se planifiquen y detallen los objetivos a conseguir.
- Los programas de «concienciación» no solo deben concienciar a las personas sino también formarlas y mostrar suficientes casos prácticos en los que se pueda apreciar la realidad.
- El fin último de dichos programas es que el empleado público sepa identificar las situaciones de riesgo en el uso de las TIC y que adquiera hábitos de uso seguro de las mismas. Para ello será imprescindible que alcance un cierto nivel de conocimiento sobre los motivos para llevar a cabo dichas conductas.

– Los mensajes de concienciación de seguridad necesitan ser adaptados al público objetivo. Para asegurar que los mensajes son relevantes y que se han recibido y entendido, se deben tener en cuenta las particularidades de cada organización y su entorno de trabajo. Aumentar la concienciación no es un ejercicio único, es un proceso continuo que provoca un cambio cultural que con el tiempo se irá integrando en el día a día del organismo.

La necesidad de formación en materias de seguridad en la Administración ha de ser continuada y se deben aumentar los esfuerzos en tiempo e intensidad.

Tras el tercer capítulo, Óscar Pastor nos hablará de la necesidad de una concienciación de *ciberseguridad* en las empresas, sometidas en estos momentos a todo tipo de ataques, incluidos los provenientes del *ciberespionaje.* El presente capítulo abordará los aspectos más importantes que las empresas deben considerar para alcanzar una adecuada concienciación de su seguridad cibernética. Para ello, se revisarán cada uno de los grupos conceptuales que todo buen análisis de riesgos debe abordar, esto es: los activos de las empresas, como elementos que aportan valor a las mismas; sus amenazas y vulnerabilidades, que pueden ocasionar impactos negativos en los anteriores, y las salvaguardas, que pueden reducir el riesgo de que dichos impactos negativos se materialicen finalmente.

Revisar con detenimiento aquellos elementos que son de especial significación para la *ciberseguridad* de las empresas es de capital importancia a la hora de abordar los principales activos que las empresas exponen en el ciberespacio, analizando sus activos intangibles, como son la propiedad intelectual, la reputación o la imagen de marca, y el creciente valor que estos elementos están tomando en el conjunto de activos de las empresas frente a los activos materiales tradicionales como son edificios, materiales, existencias de productos, etc. También se revisarán las infraestructuras críticas, como activos cuya propiedad recae mayoritariamente en empresas privadas pero cuya protección se ha convertido en una cuestión de Seguridad Nacional, dado que un impacto negativo sobre los mismos podría afectar no solo a la empresa que los operan sino a la sociedad en su conjunto.

A continuación, se abordarán las amenazas provenientes del ciberespacio a las que se enfrentan los activos de las empresas previamente analizados. Se revisarán los ataques reales o potenciales de los que son o pueden ser objeto los citados elementos, su finalidad y sus principales características, pues solo así las empresas pueden alcanzar una conciencia de su *cibersituación* que les permita mejorar su *ciberseguridad*.

También se examinarán las principales vulnerabilidades que las tecnologías más avanzadas del ciberespacio suponen para las empresas. Las organizaciones del siglo XXI, si quieren garantizar su eficiencia y perdu-

rar en el tiempo, no pueden prescindir de los servicios y funcionalidades que estas tecnologías proporcionan. Sin embargo, deben implementarlas con el conocimiento suficiente de los riesgos intrínsecos que conllevan para mejor gestionar su exposición a los mismos. En este capítulo, se abordará el análisis de nuevas funcionalidades y servicios como el *cloud computing* y el *big data,* la «consumerización» de los terminales de usuario y su movilidad en las redes empresariales, o lo que se ha denominado con el acrónimo anglosajón «BYOD»; así como las redes sociales, en las que la presencia empresarial como lugar donde hacer negocios es cada vez mayor.

Vistos los elementos que conjuntamente colaboran a conformar los riesgos a los que las empresas se enfrentan en el ciberespacio, posteriormente se analizarán las principales herramientas de que disponen las empresas para gestionar dichos riesgos hasta limitarlos a niveles aceptables. En este apartado se revisarán las buenas prácticas de ciberseguridad, entre las que se incluyen el uso de productos certificados y el establecimiento de sistemas de gestión de la seguridad de la información.

Por último, para concluir el presente capítulo, se analizará cómo se podría abordar en las empresas un adecuado programa de concienciación de *ciberseguridad* como herramienta mediante la que difundir a lo largo de la organización los conceptos de ciberseguridad analizados en el presente capítulo, asegurando que los diferentes miembros disponen del conocimiento adecuado, según su rol y responsabilidad, para asegurar una adecuada conciencia de la situación de la empresa en el ciberespacio y que permita a esta garantizar su éxito en este nuevo medio.

Las empresas están sometidas a continuos cambios, entre ellos, el peso en su valor de los activos intangibles frente a los tangibles. Las necesidades de protección frente a ataques deliberados vienen acompañadas de una concienciación por parte de la alta dirección de las empresas para que los medios necesarios para su protección se desarrollen y se implanten como una cultura empresarial; es un modelo de gestión estratégica. Los países occidentales, en especial Estados Unidos y los miembros de la Unión Europea, se enfrentan a un grave desafío para su seguridad y estabilidad económica debido al incremento progresivo de los *ciberataques* recibidos.

Los ataques son diversos desde las APT (las amenazas persistentes avanzadas), los ataques de denegación de servicio distribuido (DDoS), la ingeniería social, el *defacement* (modificación de las páginas web), uso de vulnerabilidades *zero-day,* etc. Los objetivos tradicionales habían sido los bancos pero en estos momentos los ataques van dirigidos a todos los sectores. La protección de las infraestructuras críticas se ha considerado una prioridad a nivel mundial, siendo traspuestas las obligaciones normativas europeas a nuestra legislación a través de la Ley de Infraestruc-

turas Críticas, donde se integran los aspectos de seguridad física y lógica en la preservación de la integridad de la seguridad de las infraestructuras estratégicas.

La seguridad es un proceso de mejora continua y es necesario adoptar una cultura estratégica que permita desarrollar dicho proceso, siendo su elemento clave el Ciclo de *Deming* o PDCA (*Plan Do Check Act*). Adoptando normas internacionales como las ISO 27000 y 27001 y las normas que afectan directamente a los denominados «20 controles críticos de seguridad para una ciberdefensa efectiva», que son el resultado de un consenso alcanzado por el consorcio auspiciado por el CSIS *(Center for Strategic and International Studies)* de Estados Unidos a través del organismo de control que es el *SANS Institute*; desde aquí se desarrolla un conjunto de medidas de seguridad cuyo objetivo es servir como elemento de apoyo a la decisión, proporcionando una guía que permita a las organizaciones priorizar sus inversiones en materia de seguridad y garantizando que las medidas que se implantan son aquellas cuya efectividad ha quedado acreditada por la experiencia real. De esta forma, se busca maximizar el retorno de la inversión realizada para la implantación de medidas de seguridad.

Óscar Pastor acaba su capítulo abundando en la necesidad de reforzar el eslabón más débil de la cadena de la seguridad, el individuo, y, para ello, hace especial hincapié en la necesidad de redoblar los esfuerzos en materias de formación, educación y concienciación en *ciberseguridad*.

El quinto capítulo, desarrollado por el coronel Emilio Sánchez de Rojas, aborda la cooperación internacional en *ciberseguridad*. Desde una perspectiva global provista de un profundo conocimiento del mundo internacional en materias de seguridad, defensa y ciberdefensa, el coronel Sánchez de Rojas traza un recorrido en el que aparecen los claroscuros de la voluntad de colaboración en estas materias y la realidad que, muchas veces, nos hace replantearnos si alguna vez se conseguirán los objetivos que se han diseñado como inspiradores de esta estrategia de colaboración, al estar presentes los intereses legítimos de los actores intervinientes es este teatro de operaciones.

Comienza la exposición con una cita al discurso del presidente Obama realizado a principios de 2013 y que, en estos días del mes de junio, toman una especial notoriedad:

> *EE. UU. también debe hacerle frente a la amenaza real y creciente de «ciberataques». Sabemos que los piratas informáticos roban las identidades de personas y se infiltran en correos electrónicos privados. Sabemos que empresas extranjeras sustraen nuestros secretos corporativos. Y nuestros enemigos buscan la capacidad de sabotear nuestra red de energía eléctrica, nuestras instituciones financieras, y nuestros sistemas de control del tráfico aéreo.*

> *No podemos mirar hacia atrás en años venideros y preguntarnos por qué no hicimos nada ante las serias amenazas a nuestra seguridad y nuestra economía (...). Es por eso que hoy, más temprano, firmé un nuevo decreto ejecutivo que fortalecerá nuestras defensas cibernéticas aumentando el intercambio de información y desarrollando normas que protejan nuestra seguridad nacional, nuestros empleos y nuestra privacidad. Ahora bien, el Congreso también debe actuar, aprobando las leyes que otorguen a nuestro Gobierno una mayor capacidad para proteger nuestras redes y disuadir los ataques. (2)*
>
> *Barack Obama*

La defensa de los intereses estratégicos marca una línea a seguir en la política de defensa de un Estado impulsado por su legítimo interés de defensa de su soberanía. Los escenarios cambian y el ciberespacio permite la conexión global de dominios donde se desarrollan los enfrentamientos entre actores estatales y no estatales. La *ciberamenaza* es transnacional y se acrecienta debido a la falta de normativas internacionales, la dificultad de asignar la atribución real de los ataques y una asimetría entre el atacante y el atacado.

La configuración de un ciberespacio seguro dependerá de la capacidad de colaboración entre las distintas agencias gubernamentales, los actores internacionales –tanto públicos como privados–, el desarrollo de nuevas tecnologías para prevenir y reaccionar ante dichas amenazas y la capacitación suficiente para afrontarlas. El establecimiento de medidas de persecución real y efectiva de los actores maliciosos es urgente y se ha convertido en un objetivo de todas las organizaciones nacionales e internacionales en la lucha contra este tipo de ataques. Pongamos como ejemplo el informe de la OCDE *Reducción del riesgo sistémico en «ciberseguridad»*, que afirma que la cooperación internacional es una de las claves para reducir los riesgos de *ciberseguridad*. El Convenio sobre la *ciberdelincuencia* firmado en Budapest en 2001 necesita ser ratificado por todos los estados para una adecuada persecución de los delitos.

Según el coronel Sánchez de Rojas,

> *...nos encontramos con que existen en estos momentos tres cosmovisiones básicas de la ciberseguridad: la ciberliberal defensiva representada por la UE y compartida por casi todos los países europeos, la ciberliberal-ofensiva representada por los EUA y la cibernacionalista-aislacionista representada por China y Rusia. A ellas hay que añadir las que, como Irán o Corea del Norte, sin disponer de la sofistificación de las grandes potencias disponen de unas capacidades ofensivas que están dispuestas a emplear directamente o indirectamente.*

Entre las prioridades de todos los estados en su Estrategia de Seguridad figuran:

> *Acciones de mitigación proactivas, preventivas y reactivas para alcanzar y neutralizar las fuentes de problemas y el apoyo a la creación de un ecosistema global de seguridad, incluidos los acuerdos de colaboración público-privada, el intercambio de información, bilaterales y acuerdos multilaterales con los CERT en el extranjero, los organismos de seguridad y los proveedores de seguridad...*

En el plano internacional, la inclusión de una serie de conceptos (la guerra de información, seguridad de la información, las armas de la información, el terrorismo en el ciberespacio) hace que se observe la preservación de la soberanía del Estado sobre su espacio de información, así como las disposiciones relativas a la acción en el ciberespacio a fin de socavar el sistema político, económico y social de otro Estado, el tratamiento psicológico de la población o la desestabilización de la sociedad. El derecho internacional ha de modificarse con el objetivo de desarrollar un marco legal en el que se circunscriban todas las materias a tratar. Con esta intención, la OSCE se centra en la confianza, mientras que el Grupo de las Naciones Unidas de Expertos Gubernamentales (GEG) 2012 se ha comprometido a la construcción de un consenso internacional. Desde esta perspectiva, se estudian los casos de las principales organizaciones internacionales, como la ONU, la OTAN, el Consejo de Europa y la OSCE.

Pero los distintos países muestran sus visiones sobre la configuración de estos escenarios que se reflejan en sus políticas de seguridad: países como China, Rusia, Estados Unidos o la Unión Europea plantean distintas aproximaciones. Para ejemplificar este punto de vista, el coronel Sánchez de Rojas se centra en dos casos de análisis: la Unión Europea y los Estados Unidos.

La UE propone esta estrategia una visión articulada en cinco prioridades estratégicas:

1. Lograr la *ciberresiliencia*.
2. Reducir drásticamente la *ciberdelincuencia*.
3. El desarrollo de la política de *ciberdefensa* y las capacidades relacionadas con la Política Común de Seguridad y Defensa (PCSD).
4. Desarrollar los recursos industriales y tecnológicos para la *ciberseguridad*.
5. Establecer una política internacional coherente para la Unión Europea en el ciberespacio y promover valores esenciales de la UE.

En febrero de 2013 la Unión Europea (UE) ha aprobado el documento *Estrategia de Ciberseguridad de la Unión Europea: un ciberespacio abierto, seguro y protegido.*

Como puede apreciarse deja bien sentada su prioridad: ciberespacio abierto y libre; pero para cualquiera que esté familiarizado con las negociaciones en el marco de la UE sabe que la sustancia viene después del «but»...:

«Pero la libertad en línea requiere también protección y seguridad. El ciberespacio debe ser protegido de los incidentes, las actividades maliciosas y mal uso; y los Gobiernos tienen un papel importante para garantizar un ciberespacio libre y seguro».

Y reserva las tareas más importantes para los Gobiernos:

«Los Gobiernos tienen varias tareas: para salvaguardar el acceso y apertura, de respeto y protección de los derechos fundamentales en línea y para mantener la fiabilidad y la interoperabilidad de Internet. Sin embargo, el sector privado posee y opera una parte significativa del ciberespacio, por lo que cualquier iniciativa que pretenda tener éxito en esta área tiene que reconocer su papel de liderazgo (3)».

Sin embargo, es en el punto 5 donde la UE puede ser más proactiva y eficaz: *preservar el ciberespacio abierto, libre y seguro es un desafío global, que la UE debe abordar junto con los interlocutores pertinentes y organizaciones internacionales, el sector privado y la sociedad civil.* La Comisión, el alto representante y los estados miembros deberían articular una política internacional coherente de la UE sobre el ciberespacio que se dirija a una mayor participación y fortalecimiento de las relaciones con los principales socios internacionales y las organizaciones, así como con la sociedad civil y el sector privado (3 pág. 15).

En el caso de Estados Unidos, La Estrategia Nacional para asegurar el Ciberespacio del presidente George W. Bush fue publicada en 2003. Posteriormente, publicó en 2006 el Plan Nacional de Protección de Infraestructuras, que designa 17 (ahora 18) sectores clave de infraestructura que requieren planes de protección individual. También publicó la Iniciativa Nacional Integral de *ciberseguridad* en 2008. La Administración Obama inició sus esfuerzos en *ciberseguridad* con el *Los 60 días de examen de las políticas sobre el ciberespacio,* publicado en mayo de 2009, que presenta una revisión sólida de dónde estaba el gobierno en relación con la *ciberseguridad*, pero ofrecía poco de su visión de la forma de llegar a su destino. La principal recomendación fue que el presidente debería nombrar a un solo coordinador central de los esfuerzos nacionales y del Gobierno para las políticas de *ciberseguridad*.

En cuanto a los posicionamientos de los dos partidos en Estados Unidos, tanto republicanos como demócratas convergen en el reconocimiento de que existe una importante amenaza de naturaleza *ciber* contra la seguridad nacional y en la necesidad de la cooperación público-privada y del intercambio de información.

El presidente Obama ha declarado que la «amenaza cibernética es una de los más graves desafíos de la seguridad económica y nacional al que nos enfrentamos como nación» y que «la prosperidad económica de EE. UU. en el siglo XXI dependerá de la seguridad cibernética». Y en su ánimo está ampliar la cooperación ciberespacial con aliados y socios para aumentar la seguridad colectiva e iniciar diálogos para intercambiar las mejores prácticas en áreas como la forense, el desarrollo de la capacidades, participación en ejercicios y alianzas público-privadas.

Termina el capítulo con una llamada de atención:

> *En cualquier caso, no debemos perder la esperanza de que las grandes ciberpotencias lleguen a un acuerdo que permita fomentar la confianza y aumentar la transparencia reduciendo los crecientes riesgos asociados con los cada vez más numerosos y cada vez más complejos ciberataques. En unos años podría alcanzarse un acuerdo... ¡O no!*

Como el lector ha podido comprobar, nuestros panelistas le despertarán la curiosidad y satisfarán no solo la curiosidad ante una situación de candente actualidad sino también el conocimiento en esta materia, por el trabajo cuidadoso y extraordinariamente bien conducido y documentado que han llevado a cabo.

Disfruten de su lectura tanto como yo he disfrutado en su dirección.

Bibliografía

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), *Information systems defence and security - France's strategy*. 2011

1. JOYANES AGUILAR, Luis, y otros. *Cuadernos de Estrategia 149: Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.* Madrid: Ministerio de Defensa, 2010. Instituto Español de Estudios Estratégicos. ISBN 978-84-9781-622-9.
2. OBAMA, Barak. *Discurso sobre el estado de la Unión de Barack Obama.* Washington: The White House, 2013.
3. UE. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Bruselas: European Commission & High Representative of the European Union for Foreign Affairs and Security Policy, 2013.
4. United States Army Training and Doctrine Command. *TRADOC Pamphlet 525-7-8, The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028.* Fort Monroe, VA: TRADOC Publications, 2010.
5. LIBICKI, Martin C. *Cyberdeterrence and cyberwar.* Santa Monica, CA: RAND Corporation, 2009. ISBN 978-0-8330-4734-2.

6. World Economic Forum y The Boston Consulting Group. *Rethinking personal data: Strengthening trust.* Ginebra (Suiza): World Economic Forum, 2012.
7. DUDMAN, Jane. «Data is the new raw material of the 21st century». *The Guardian.* Electrónica, 18 de abril de 2012 [consultada el 11 de abril de 2013]. <www.guardian.co.uk/public-leaders-network/2012/apr/18/francis-maude-data-raw-material>.
8. REDING, Viviane. Press conference: «Commission proposes a comprehensive reform of EU data protection rules». *European Commission Audiovisual Services.* s. l.: vídeo en web, 25 de enero de 2012. <http://ec.europa.eu/avservices/video/player.cfm?ref=82655&sitelang=en>.
9. ABELSON, Hal y LESSIG, Lawrence. «Digital Identity in Cyberspace», White Paper Submitted for 6.805/Law of Cyberspace: Social Protocols. *MIT's Computer Science and Artificial Intelligence Laboratory.* [En línea] 10 de diciembre de 1998 [citado el: 17 de febrero de 2013]. http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall98-papers/identity/linked-white-paper.html.
10. ROUNDS, M. y PENDGRAFT, N. *Diversity in Network Attacker Motivation: A Literature Review.* Computational Science and Engineering, agosto de 2009. CSE'09 International Conference, vol. 3, págs. 319-323.
11. Spanish Cyber Security Institute. *La ciberseguridad nacional, un compromiso de todos.* Junio de 2012.
12. FEDORENKO, Andrei. «The fight over the draft UN Convention on International Information Security». *Regulatory Cyber Security: The FISMA Focus IPD.* [En línea] 15 de julio de 2012 [citado el: 12 de mayo de 2013]. http://www.thecre.com/fisma/?p=2173.
13. NEWMEYER, Kevin P. *Who should lead U.S. Cyber Security efforts?* 2012, PRISM 3, n.º 2, págs. 115-126.
14. EGUILLOR, Marcos. *Social media.* n.º 185, 2011, Bit, págs. 68-71.
15. EFE. «Un nuevo caso de 'ciberacoso' se lleva por delante la vida de una chica de 15 años». *ABC.* 18 de octubre de 2012.
16. HEARN, Alison. *Structuring feeling: Web 2.0, online ranking and rating, and the digital «reputation» economy.* Ephemera, 2010, págs. 421-438.
17. SHELDON, John. «State of the Art: Attackers and Targets in Cyberspace». 2012, *Journal of Military and Strategic Studies,* vol. 14, n.º 2.
18. MUIR, Lawrence L. «The Case Against an International Cyber Warfare convention». *Wake Forest Law Review.* Winston-Salem, NC., EE. UU.: Wake Forest University School of Law, diciembre de 2011, vols. 2, n.º 5.
19. VAN HEERDEN, R. P., IRWIN, B. y BURKE, I. D. *Classifying network attack scenarios using an ontology.* Seattle: University of Washington, 2012. Proceedings of the 7th International Conference on Information Warfare and Security, 22-23 de mazo de 2012, págs. 311-324.

20. DESFORGUES, Alix. «Cyberterrorisme: quel périmètre?» *Fiche de l'Irsem n.° 11.* [En línea] diciembre de 2011 [citado el: 24 de febrero de 2013]. http://www.irsem.defense.gouv.fr.
21. GOLDSTEIN, Emmanuel. *The Best of 2600, Collector's Edition: A Hacker Odyssey.* Indianapolis, IN: Wiley Publishing Inc., 2009. ISBN 97-0-470-45853-2.
22. MIZRACH, Steven. «Is there a Hacker Ethic for 90s Hackers?» *Old and New Hacker Ethics.* [En línea] 1997 [citado el: 25 de febrero de 2013]. http://www2.fiu.edu/~mizrachs/hackethic.html.
23. MIRÓ LLINARES, Fernando. *El cibercrimen.* Madrid: Marcial Pons, 2012.
24. MITNICK, Kevin D. y SIMON, William L. *The art of Deception.* [Ed.] Carol Long. Indianapolis, IN: Wiley Publishing Inc., 2002. ISBN 0-471-23712-4.
25. Government Accountability Office. *Cyber Threats Facilitate Ability to Vommit Economic Espionage.* Government Accountability Office. Washington: s. n., 2012. Testimony before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives. GAO-12-876T.
26. POSTEL, J. RFC 801. *NCP/TCP Transition Plan.* [Electrónico] s.l.: Network Working Group, noviembre de 1981.
27. FALLIERE, Nicolas, MURCHU, Liam O. y CHIEN, Eric. *W32. Stuxnet Dossier. Version 1.4.* Symantec Coporation, 2011.
28. ZETTER, Kim. *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History.* [En línea], Wired.com, 11 de julio de 2011 [citado el 24 de marzo de 2013]. http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/.
29. ETSI. *TR 101 771V1.1.1. Service Independent Requirements Definition: Threat Analysis.* Sophia Antipolis, Francia: European Telecommunications Standards Institute, 2001-2004. Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).
30. Department of Defense (DoD). MIL-STD-882E. *Standard Practice. System Safety .* s.l., EE. UU.: Department of Defense (DoD), 11 de mayo de 2012.
31. Ponemon Institute. *The Human Factor in Data Protection.* Ponemon Institute LLC, 2012. Patrocinado por Trend Micro.
32. LYNN, William J. [*Defending a New Domain. The Pentagon's Cyberstrategy.* [En línea]: Council on Foreign Relations, Foreign Affairs, 1 de septiembre de 2010, [citado el 26 de marzo de 2013]. <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>.
33. CIALDINI, Robert B. *The Science of Persuasion.* Edición especial enero de 2004, Scientific American special edition, vol. 14, n.º 1, págs. 70-77.

34. CIALDINI, Robert B. *Influence.* [Ed.] Carolyn Merryll. Needham Heights, MA: Allynn & Bacon, 2001. ISBN 0-321-01147-3.
35. NIST. *Special Publication 800-30. Guide for conducting risk assessments.* Gaithersburg, MD: National Institute of Standards and Technology, 2012.
36. ISO. *ISO/IEC 27005: 2011 Information technology-Security techniques-Information security risk management.* ISO/IEC, 2011.
37. OIKARINEN, J. y REED, D. RFC 1459. *Internet Relay Chat Protocol.* [Electrónico] Network Working Group, mayo de 1993.
38. *Symantec Intelligence Report: February 2013.* Symantec Corporation, 2013. <http://www.symanteccloud.com/es/es/mlireport/SYMCINT_2013_02_February_ES.pdf>.
39. MARINO, Louis y SFAKIANAKIS, Andreas. *ENISA Threat Landscape. Responding to the Evolving Threat Environment.* European Network and Information Security Agency (ENISA). 2012.
40. KRAMER, Simon y BRADFIELD, Julian C. «A general definition of malware». Springer-Verlag, 2010, *Journal in Computer Virology,* vol. 6, n.º 2, págs. 105-114. Online ISSN 1772-9904.
41. KRYSIUK, Piotr y DOHERTY, Stephen. *The World of Financial Trojans.* Symantec Security Response. Mountain View, CA (EE.UU): Symantec Corporation, 2013 [citado el 7 de abril de 2013]. <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_world_of_financial_trojans.pdf>.
42. DANG, Hiep. «The origins of social Engineering». *McAfee Security Journal.* Otoño de 2008. Santa Clara, CA (EE. UU.): McAfee Inc., 2008.
43. SHAH, Jimmy. «Los riesgos contra los datos confidenciales de los dispositivos móviles en el origen de las amenazas futuras». *McAfee Security Journal,* n.º 7. Santa Clara, CA (EE. UU.): McAfee Inc., 2011.
44. ISTTF. *Enhancing child safety and online technologies: final report of the Internet Safety Technical Task Force to the Multi-state Working Group on Social Networking of State Attorneys General of the United States.* Berkman Center for Internet & Society at Harvard University, 2008.
45. Equipo de Estudios del ONTSI. *Perfil sociodemográfico de los internautas, análisis de datos INE 2012.* Observatorio Nacional de las Tecnologías y de la Sociedad de la Información, 2013. ISSN 2172-9212.
46. The Boston Consulting Group, Inc. *The value of our digital identity.* Liberty Global Inc., 2012 [documento electrónico]. <http://www.lgi.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf>.
47. RICHARDS, Reshan. «Digital Ctizenship and Web 2.0 tools». [En línea] Merlot, junio de 2010, *Journal of Online Learning and Teaching,* vol. 6, n.º 2. <http://jolt.merlot.org/vol6no2/richards_0610.htm>.

48. Blue Coat Systems. *2012 Web Security Report.* Blue Coat Systems Inc., 2013. <http://www.bluecoat.com/sites/default/files/documents/files/BC_2012_Security_Report-v1i-optimized.pdf>.
49. RIBBLE, Mike. *Digital Citizenship in Schools.* 2.ª ed. International Society for Technology in Education (ISTE), 2011. ISBN: 978-1564843012.
50. Kindsight. *Kindsight Security Labs Malware Report - Q4 2012.* [En línea]. Kindsight Inc., 2012. <http://www.kindsight.net/sites/default/files/Kindsight_Security_Labs-Q412_Malware_Report-final.pdf>.
51. Damballa. *Damballa Threat Report - First Half 2011.* [En línea]. Damballa Inc., 2011. <https://www.damballa.com/downloads/r_pubs/Damballa_Threat_Report-First_Half_2011.pdf>.
52. NAO. *The UK cyber security strategy: Landscape review.* Reino Unido: National Audit Office, 2013.
53. MAIALEN, Garmendia y otros. *Riesgos y seguridad en Internet: los menores españoles en el contexto europeo.* Universidad del País Vasco. Bilbao: EU Kids Online, 2011.
54. AGRE, P. E. y ROTENBERG, M. *Technology and privacy: The new landscape.* Cambridge (MA): MIT Press, 1998. ISBN: 9780262511018.
55. *MAGERIT versión 3.* Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012. NIPO: 630-12-171-8.
56. «New firewall to safeguard against medical-device hacking». *Purdue University.* [En línea] 12 de abril de 2012 [citado el 14 de abril de 2013]. http://www.purdue.edu/newsroom/research/2012/120412RaghunathanHacking.html.
57. BUZAI, Gustavo D. «El ciberespacio desde la geografía. Nuevos espacios de vigilancia y control global». *Meridiano. Revista de Geografía.* [En línea] 2012, n.º 1 [citado el 25 de febrero de 2013]. http://www.revistameridiano.org/.
58. EUA, Joint Chief of Staff. *Estrategia nacional militar de los Estados Unidos de América .* Washington: Joint Chief of Staff EUA, 2011.
59. OCDE. *Future Global Shocks. Improving Risk Governance.* París: OCDE, 2011.
60. SOMMER, Peter y BROWN, Ian. *Reducing Systemic Cybersecurity Risk.* Informe: OCDE, 2011.
61. OSCE_MC.DEC/7/06. *DECISION No. 7/06: Countering the Use of the Internet for Terrorist Purposes.* Brussels: OSCE, 2006.
62. KAGAN, Robert. *Paradise and Power: America and Europe in the New World Order.* Londres: Atlantic Books, 2004.
63. WEGENER, Henning. *Regulating Cyber Behavior: Some Initial Reflections on Codes of Conduct and Confidence Building Measures.* [En línea] 23 de agosto de 2012 [citado el 29 de marzo de 2013]. http://www.federationofscientists.org/PlanetaryEmergencies/Seminars/45th/Wegener publication.docx.

64. BAILEY, Eric. *«Nothing Can Justify Torture»: An interview with Noam Chomsky on Obama's human rights record.* [En línea] 12 de diciembre de 2012 [citado el 30 de marzo de 2013]. http://chomsky.info/interviews/20121212.htm.
65. The White House. *Cyberspace Policy Review.* Washington: The White House, 2011. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
66. The_White_House2. *International Strategy for Cyberspace.* Washington: The White House, 2011.
67. BIDEN, Joseph R. *VP's Remarks to London Cyberspace Conference.* Londres: The White House, 2011.
68. CLAPPER, James R. *Worldwide Threat Assessment of the US Intelligence Community 2013.* Washington DC: Office of the Director of National Intelligence, 12 de marzo de 2013.
69. ALEXANDER, Keith B. *Statement of general Keith B. Alexander Commander United States Cyber Command before the Senate Committee on armed services.* Washington: United States Cyber Command, 2013.
70. PELLERIN, Cheryl. *American Forces Press Service. Cybercom Builds Teams for Offense, Defense in Cyberspace.* [En línea] 12 de marzo de 2013 [citado el: 30 de marzo de 2013]. http://www.defense.gov/news/newsarticle.aspx?id=119506.
71. KEHLER, C. R. *Statement of general C. R. Kehler Commander United States Strategic Command before the Senate Committee on Armed Services.* Washington: United States Strategic Command, 12 de marzo de 2013.
72. LEWIS, James Andrew. *Critical Questions for 2013: Global Challenges. What's Next in Cybersecurity?* Center for Strategic and International Studies. [En línea] 25 de enero de 2013 [citado el: 30 de marzo de 2013]. http://csis.org/publication/critical-questions-2013-global-challenges.
73. BUMILLER, Elisabeth. «Pentagon to Beef Up Cybersecurity Force to Counter Attacks». *The new York Times*. [En línea] 29 de marzo de 2013 [citado el 31 de marzo de 2013]. www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html.
74. GEERS, Kenneth. *Cyberspace and the changing nature of warfare.* [En línea] 27 de agosto de 2008 [citado el 31 de marzo de 2013]. http://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/.
75. HEALEY, Jason y BOCHOVEN, Leendert van. *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow.* Washington: The Atlantic Council of the United States, 2011.
76. PRINCE, Matthew. «The DDoS that Almost Broke the Internet». *Cloud Flare.* [En línea] 27 de marzo de 2013 [citado el 28 de marzo de 2013]. http://blog.cloudflare.com/the-ddos-that-almost-broke-the-Internet.

77. TIKK, Eneken. *Comprehensive legal approach to cyber security 2011*. Tarfu, Estonia: Faculty of Law, University of Tartu, 2011.
78. Unión Europea. «Council Framework Decision 2005/222/JHA». *Official Journal of the European Union.* [En línea] 16 de marzo de 2005 [citado el 31 de marzo de 2013]. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf.
79. FROOMKIN, Michael. «Cybercrime Treaty Goes Live». *Discourse.net.* [En línea] 19 de marzo de 2004 [citado el 31 de marzo de 2013]. http://www.discourse.net/archives/2004/03/cybercrime_treaty_goes_live.html.
80. ARCHICK, Kristin. *CRS Report for Congress. Cybercrime: The Council of Europe Convention.* Washington: Congressional Research Service, 2004.
81. SCHJØLBERG, Stein y GHERNAOUTI-HÉLIE, Solange. *A Global Protocol on Cybersecurity and Cybercrime: An Initiative for peace and Security in Cyberspace,* segunda edición. Oslo: AiTOslo, 2011.
82. EUA_OSCE. [En línea] 16 de octubre de 2009 [citado el 31 de marzo de 2013]. https://dazzlepod.com/cable/09STATE107552/.
83. SCHNEIDER, Deborah. *United States Mission to the OSCE Cyber Security Keynote Address by Dr. Deborah Schneider, U.S. Department of State as delivered to the Joint FSC/PC.* Viena: OSCE, 2010.
84. SAFIRE, William. «The Farewell Dossier». *The New York Times.* [En línea] 2 de febrero de 2004 [citado el 2 de enero de 2013]. http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html?ref=williamsaire.
85. BROWN, Gary y POELLET, Keira. *The Customary International Law of Cyberspace.* IV, Strategic Studies Quarterly, otoño de 2012, vol. 6, págs. 126-145.
86. STEPHENS, Bret. «The limits of Stuxnet». *The Wall Street Journal.* [En línea] 18 de enero de 2011 [citado el 2 de enero de 2013]. http://online.wsj.com/article/SB10001424052748703396604576087632882247372.html.
87. PERTERMANN, Kerstin. *Conference Report: Challenges in Cybersecurity, Risks, Strategies, and Confidence Building International Conference.* Hamburgo: Institute for Peace Research and Security Policy at the University of Hamburg, 2011.
88. VENTRE, Daniel. *La politique de cyberdéfense peut-elle être a-politique?* Paris: Ministère de la défense Délégation aux Affaires Stratégiques, 2013.
89. EES. *Estrategia Española de Seguridad.* Madrid: Gobierno de España, 2011.
90. PÉREZ, Jesús. «Cómo Cyberbunker atacó a Spamhaus y casi se llevó a medio Internet por delante». *Security By Default.* [En línea] 28 de

marzo de 2013 [citado el 12 de mayo de 2013]. http://www.security-bydefault.com/2013/03/como-cyberbunker-ataco-spamhaus-y-casi.html.

91. VENTRE, Daniel. *Japon: stratégies de cyberdéfense, Multi-System and Internet Security Cookbook.* MISC, n.° 64, 2012, págs. 65-73.
92. BAGCHI, Sohini. «India needs more warriors in the cyber space». *Cxotoday.com.* [En línea] 3 de mayo de 2013 [citado el 12 de mayo de 2013]. http://www.cxotoday.com/story/india-needs-more-warriors-in-the-cyber-space/.
93. ZORZ, Zeljka. «India has a new National Cyber Security Policy». *Help net security organization.* [En línea] 10 de mayo de 2013 [citado el 12 de mayo de 2013]. http://www.net-security.org/secworld.php?id=14891.