Concienciación[1] en las administraciones públicas

Por Luis Jiménez Muñoz

Capítulo tercero

Toma de conciencia y percepción del riesgo

El capítulo que se presenta analiza la problemática de la toma de conciencia[2] 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.

El concepto de riesgo asociado al uso de las tecnologías de la información no difiere mucho del tradicional concepto de riesgo manejado por diversas disciplinas (1). En este sentido, el riesgo es un constructo social, dinámico y cambiante que requiere para su prevención y mitigación de dos herramientas básicas, el conocimiento y la comunicación (información y formación).

En el ámbito de las tecnologías de la información hace tiempo que se ha asumido la necesidad de convivir con un nivel de riesgo ya que la seguridad total o absoluta no existe. El grado de complejidad de las tecnologías de la información y las comunicaciones ha aumentado considerablemente y cada vez es más difícil de administrar el riesgo adecuadamente, y por tanto, de controlarlo.

[1] Concienciación: Acción y efecto de concienciar o concienciarse (Real Academia Española).

[2] Concienciar: Hacer que alguien sea consciente de algo. Adquirir conciencia de algo.

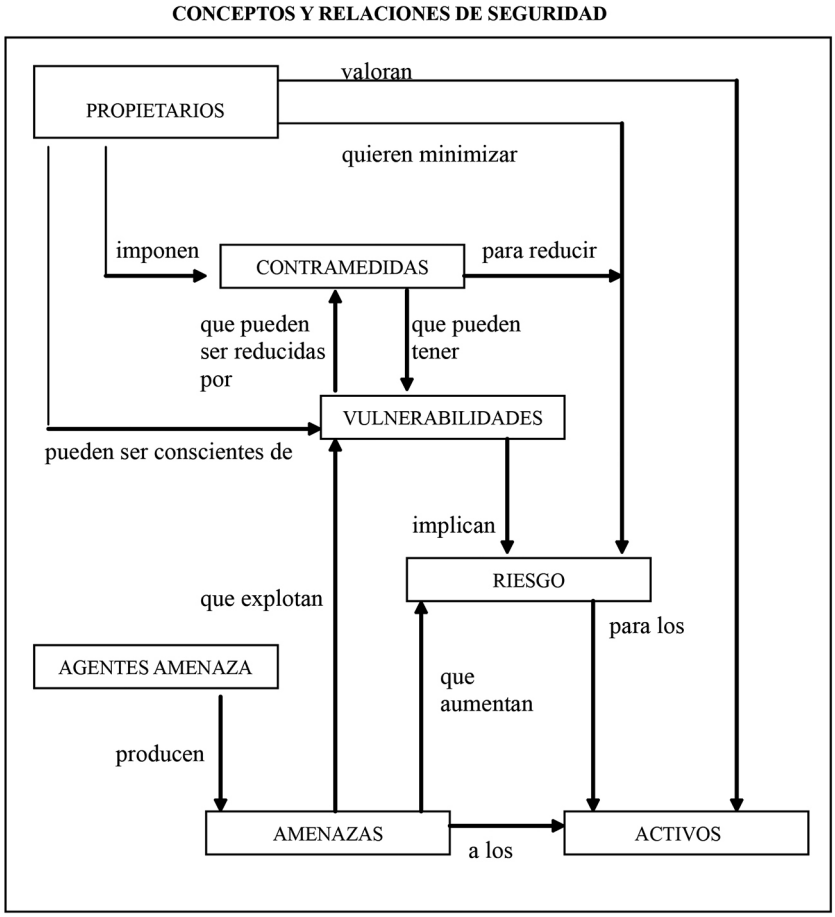

Figura 3.1: Conceptos y relaciones de seguridad en Common criteria ISO15408.

En las Administraciones Públicas, la gran mayoría de autores señalan que el nivel adecuado donde deben prevenirse los incidentes de seguridad es el nivel de usuario final del sistema de información, porque es allí donde se presupone que el eslabón más débil de la cadena existe y porque la experiencia ha demostrado que es donde ocurren la mayoría de violaciones, intencionadas o no, de la seguridad.

Sin embargo, aun siendo cierto lo anterior, la necesidad de comunicación y conocimiento (toma de conciencia) 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 *ciberseguridad* debe tener una buena ubicación para que las prioridades puedan ser adecuadas y el eterno equilibrio entre seguridad y eficacia pueda ser alcanzado.

La gestión del riesgo es para el experto en riesgos Lavell (2):

> *... no solo la reducción del riesgo, sino la comprensión que en términos sociales se requiere de la participación de los diversos estratos, sectores de interés y grupos representativos de conductas y modos de vida (incluso de ideologías y de perspectivas del mundo, la vida, la religión) para comprender cómo se construye un riesgo social, colectivo, con la concurrencia de los diversos sectores de una región, sociedad, comunidad o localidad concreta...*

Resulta interesante la idea expresada por el autor en cuanto al hecho de que la gestión del riesgo no consiste simplemente en disminuir la vulnerabilidad, sino en la búsqueda de acuerdos sociales para soportar o utilizar productivamente los impactos. Este acuerdo social al que hace referencia Lavell se manifiesta en el *principio de proporcionalidad* (3) que debe inspirar la toma de decisiones a la hora de implementar las medidas de seguridad en un sistema de información.

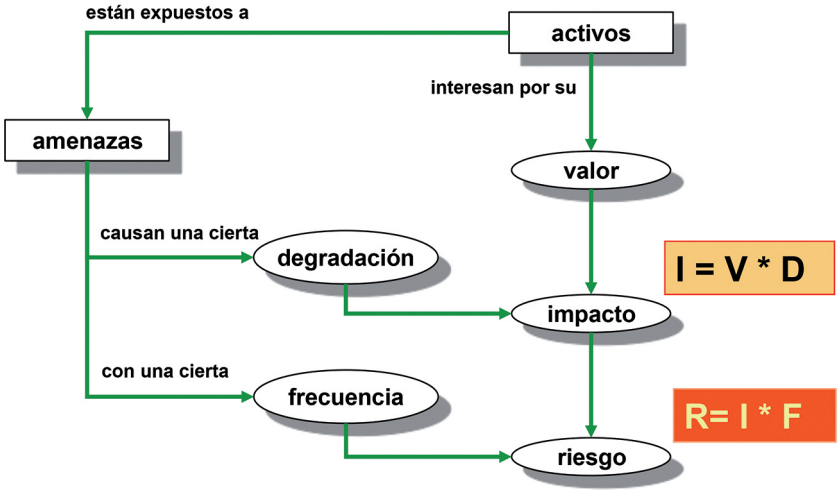

Figura 3.2. MAGERIT: Modelo conceptual de análisis de riesgos.

En tal sentido, resulta importante considerar que la gestión del riesgo no puede ser reducida a meras intervenciones tecnológicas, sino que debe estar referida al proceso a través del cual la sociedad, en sus diferentes niveles de estructuración:

> *...toma conciencia del riesgo, lo analiza y lo entiende, considera las opciones y prioridades en términos de su reducción, considera los recursos disponibles para asumirlo, diseña las estrategias e instrumentos necesarios para ello, negocia su aplicación y toma la decisión de hacerlo para finalmente implementar la solución más apropiada en términos del contexto concreto en que se produce o se puede producir el riesgo.*

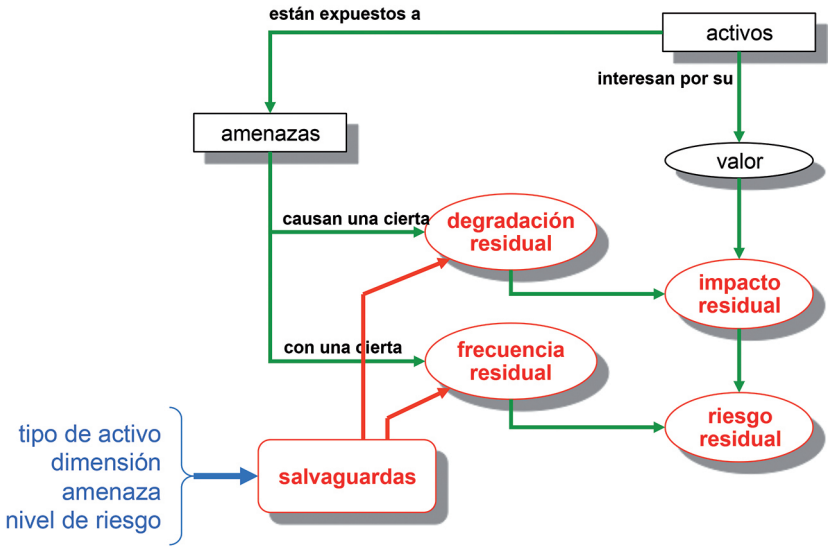

Figura 3.3. MAGERIT: Modelo conceptual de gestión de riesgos.

La gestión del riesgo es definida por Keipi, Bastidas y Mora (4) «... como el proceso que permite identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se desprenden de las amenazas, así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse...». Los autores señalan la importancia de desarrollar la capacidad preventiva y de respuesta, la que en numerosas ocasiones se ha visto inhibida por el conocimiento técnico insuficiente, el pobre desarrollo institucional y la aplicación incompleta de instrumentos preventivos, lo que ha condicionado una orientación mayormente dirigida hacia planes de contingencia con inspiración reactiva, los cuales se aplican a los efectos y no a las causas.

También podemos ver en otros especialistas de la gestión de riesgos el mismo planteamiento de la necesidad del conocimiento técnico suficiente y la información adecuada como factores imprescindibles para generar la capacidad preventiva de una organización ante los *ciberataques* (5).

Ante la «invisibilidad» de las amenazas que existe en el ámbito de las tecnologías de la información y las comunicaciones, es el saber lo que permite «reconocerlos» y «darles existencia». Sin embargo, el saber también puede negarlos o transformarlos, ya sea minimizándolos o dramatizándolos. Ideas similares se tienen en cuenta a la hora de diseñar el papel de la información y el conocimiento adecuado en la gestión de centros de operaciones de seguridad.

Las amenazas y vulnerabilidades que afectan a los sistemas de información han venido aumentando constantemente en los últimos años, llegan-

do incluso a incrementarse un 55% en los dos últimos años, según datos recogidos por el CCN-CERT (6). Respecto a los tipos de riesgos que estas vulnerabilidades implican para nuestros sistemas de información, según publica el CERT gubernamental, la mayoría de las amenazas recibidas constituyen casos de *cibercrimen* o *ciberdelincuencia.* Sin embargo, las más críticas han sido los casos de *ciberespionaje*, de tal forma que esta amenaza se ha convertido en una debilidad crítica en las naciones occidentales, máxime si tenemos en cuenta que estas amenazas evolucionan continuamente y a una velocidad cada vez mayor.

Dado que las amenazas cada vez son más complejas y, a veces, difíciles de detectar, se hace necesaria una formación del personal responsable de las TIC en todos los organismos de las Administraciones Públicas para luchar contra la ingenuidad, la ignorancia de buenas prácticas y la falta de concienciación existente sobre la necesidad de preservar la seguridad de la información. 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.

La Administración en su conjunto no puede ser ajena a este escenario y debe considerar el desarrollo, la adquisición, conservación y utilización segura de las TIC como algo imprescindible que garantice el funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

La Administración depende de los sistemas TIC para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los organismos deben aplicar un conjunto coherente y proporcionado de medidas de seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes organismos de la Administración deben «concienciarse» y cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad (7) (8) y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas y en pliegos de licitación para proyectos de TIC.

La Administración debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes. Los organismos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se deben implementar las medidas mínimas de seguridad determinadas por las políticas de seguridad que sean de aplicación, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados (9).

Todos los empleados públicos, de todos los niveles, tienen la obligación legal, como se verá más adelante, de conocer y cumplir las políticas de seguridad de la información y la normativa de seguridad. La concienciación de los empleados públicos en materia de seguridad es una tarea imprescindible para el cumplimiento de esta obligación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC deben recibir formación para el manejo seguro de los

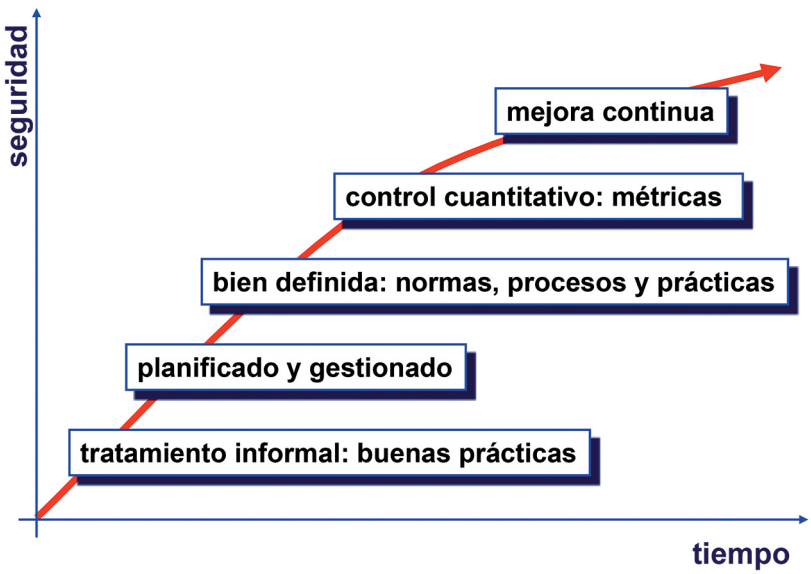

Figura 3.4. Niveles de madurez en la implantación de seguridad en una organización (International Systems Security Engineering Association).

sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo (10).

Las vulnerabilidades

Una vulnerabilidad (11) es una debilidad que puede ser aprovechada por una amenaza[3]. Solucionar las vulnerabilidades es la mejor forma de reducir el riesgo y, en consecuencia, disminuir la probabilidad de incidentes. Las vulnerabilidades aparecen por diversos factores: técnicos, humanos y de organización.

En general, una vulnerabilidad en un sistema se puede agrupar bajo uno de los siguientes apartados en función de su naturaleza:

- Vulnerabilidad debido al uso incorrecto del sistema por parte de usuarios autorizados.
- Vulnerabilidad debido a que no se controla el acceso al sistema.
- Vulnerabilidad generada por medidas de seguridad de procedimiento ineficaces.
- Vulnerabilidad generada por averías o por fallos en el hardware y software.
- Vulnerabilidad intrínseca de los sistemas debido a su complejidad y desconocimiento de sus posibilidades o limitaciones.

La última década ha sido testigo de un crecimiento muy importante en el descubrimiento y publicación de nuevas vulnerabilidades, alcanzándose su punto máximo en 2006 y 2007, para disminuir en los siguientes años e iniciar una nueva escalada, en la que nos encontramos.

El sistema CVSS *(Common Vulnerability Scoring System)* es un estándar, independiente de la plataforma, para la calificación de vulnerabilidades IT. El CVSS asigna un valor (entre 0 y 10) a las vulnerabilidades, atendiendo a su gravedad.

Las vulnerabilidades que conducen a incidentes provocados por factores humanos y organizativos son, en parte, el resultado de errores de los usuarios. Sin embargo, también pueden surgir debido a deficiencias en la organización y en la política y normativa de seguridad de instituciones y organismos.

Determinados estudios han señalado que las vulnerabilidades de aplicaciones web en el periodo considerado de 2012 no habían disminuido respecto de las de 2011.

[3] Definición dada por el 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.*

1	Aplicaciones con insuficientes medidas de seguridad derivadas de una mala gestión de los usuarios o de los administradores. Este tipo de vulnerabilidades incluyen la conexión de sistemas a Internet con mecanismos de usuario-contraseña fáciles de adivinar.
2	Aplicaciones estándar tales como sistemas de gestión de contenidos, sin que se hayan instalado algunas de las actualizaciones de seguridad.
3	Errores de programación en desarrollos a medida para aplicaciones y páginas web.
4	Inyección SQL y Cross Site Scripting (XSS).

Figura 3.5. Vulnerabilidades más importantes detectadas en 2012.

Si bien las prácticas seguras de desarrollo han disminuido la presencia de vulnerabilidades en la producción de *software*, no parecen, sin embargo, estar ayudando significativamente en la reducción de las tasas de vulnerabilidades de aplicaciones *web*. De hecho, la enorme demanda de desarrolladores con experiencia en aplicaciones web, superior a la oferta, el modelo de amenazas en permanente evolución y la complejidad del *software* basado en web propician la aparición de nuevas vulnerabilidades, lo que provoca que las antedichas tasas no disminuyan.

Las vulnerabilidades que más se han reportado son las relativas a inyección SQL y *cross site scripting* (XSS). En segundo lugar, se encuentran las relativas a incidentes por denegación de servicio (DoS), *cross site request forgery* (CSRF) y *remote file include* (RFI).

En muchos casos, el acceso a aplicaciones web todavía se realiza mediante el par usuario-contraseña. Se ha evidenciado que este mecanismo puede burlarse con cierta facilidad, especialmente cuando se usan contraseñas débiles, fáciles de adivinar a través de mecanismos de *phishing* y *hacking*.

Otra de las vulnerabilidades importantes que se encuentra en los organismos e instituciones es la existencia de *software* sin actualizar. Un *software* es vulnerable antes de que el proveedor publique una actualización, y continuará siendo vulnerable hasta que esta actualización (o parche) ha sido adecuadamente implantada. Diferentes análisis han demostrado que, con frecuencia, las actualizaciones no se instalan con la suficiente rapidez o, incluso, no se instalan nunca.

Durante 2012, los atacantes siguieron explotando vulnerabilidades todavía no identificadas a través de los llamados *zero-days exploits.*

También los hábitos de navegación de los usuarios siguen siendo objetivo prioritario de los agentes maliciosos. Durante 2012, el organismo holandés National Cyber Security Centre (NCSC) realizó un estudio sobre 1.000 *websites,* detectando la presencia de 70 diferentes mecanismos de seguimiento ofrecidos por terceros[4]. La investigación también incluyó el uso de *cookies*. Estos trabajos de campo evidenciaron que el seguimiento también se utilizaba en las páginas web de ciertos hospitales, lo que hace especialmente delicado el ataque al afectar a datos de naturaleza personal.

Por otra parte, es preciso mencionar en este apartado de vulnerabilidades las asociadas al uso de los servicios en la nube. El pasado año 2012 los beneficios del uso de servicios en la nube atrajeron la atención de muchas organizaciones. Además de utilizar nubes públicas para los servicios menos comprometidos, las organizaciones han comenzado a invertir de manera más decidida en nubes privadas, construidas con tecnología de virtualización.

Los problemas de seguridad asociados a los servicios *cloud* pusieron de manifiesto, con el reconocimiento por parte de Dropbox, el hecho de que nombres de usuario y contraseñas robadas de otras webs habían sido utilizados para iniciar sesión en un cierto número de sus cuentas. Se adoptaron medidas de seguridad adicionales como la opción de autenticación de dos factores. En mayo de 2012, el Fraunhofer Institute for Securite Information Technology informó sobre las vulnerabilidades relacionadas con el registro, inicio de sesión, cifrado y compartición de datos de acceso en siete servicios de almacenamiento en la nube[5].

El incidente de Dropbox ha hecho aflorar cuestiones tales como: ¿cómo deben las organizaciones abordar la seguridad y la conformidad legal? ¿Autenticación de uno o dos factores? ¿Cómo se pueden manejar las fugas de información? ¿Cómo saber si los usuarios están transfiriendo información a terceros? ¿Cómo preservar el acceso del personal que ya no está en la organización? ¿Cómo seleccionar los proveedores adecuados? ¿Se están aplicando las mismas estrictas normas y requisitos contractuales que se exigen a otros socios críticos del negocio que tienen acceso a datos confidenciales o estratégicos? Y muchas otras.

Por último, hay que resaltar el nuevo escenario de vulnerabilidad que se abre con la implantación en las organizaciones del concepto denominado BYOD[6].

---

[4] http://www.alexa.com.

[5] *Fraunhofer Institute Finds Security Vulnerabilites in Cloud Storage Services. The H Security,* http://www.h-online.com/security/news/item/Fraunhofer-Institute-finds-security-vulnerabilites-in-cloud-storage-services-1575935.html.

[6] *Bring Your Own Device.*

BYOD es una modalidad de trabajo por la que las organizaciones permiten el uso de dispositivos personales (*smartphones* y *tablets,* habitualmente) para el tratamiento de los datos de la propia organización. En esta modalidad, cada usuario es responsable de sus propios dispositivos, que utiliza tanto para propósitos personales como corporativos. La llamada «consumerización» es una tendencia que está estrechamente ligada a BYOD. La consumerización significa que las TIC, cada vez más, se están desarrollando sobre la base de los requisitos de los propios consumidores y de sus dispositivos.

Recientes investigaciones muestran que casi el 75% de las organizaciones estudiadas permiten el acceso a activos de información a través de dispositivos que no están sujetos a la administración de seguridad corporativa[7].

Esta situación está impactando en la seguridad IT de las organizaciones, haciendo que sea necesario adoptar un nuevo enfoque que contemple cómo se accede a datos de negocio desde los puntos finales y cómo se custodiarán tales datos en los dispositivos de los usuarios. Estudios de 2012 muestran que, con frecuencia, la política de seguridad que se redacta y publica para tratar esta problemática es ignorada sistemáticamente por los empleados, cuya concienciación sobre los riesgos que se derivan de las fugas de datos es, todavía, baja[8].

Estas mismas fuentes señalaron que casi la mitad de las organizaciones ven una correlación entre el incremento de dispositivos móviles dentro del entorno corporativo y el incremento del número de incidentes de seguridad[9].

El nuevo enfoque en la gestión de riesgos

El análisis de riesgos es una actividad clásica que se requiere como base en múltiples ámbitos de la seguridad, desde certificaciones de sistemas de gestión de la seguridad (SGSI, ISO 27001) hasta la protección de los servicios de la administración electrónica (Esquema Nacional de Seguridad, Real Decreto 3/2010).

Clásicamente, el análisis de riesgos se ha venido realizando como una actividad de despacho para un análisis 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.

---

7 iPass (noviembre de 2011) *The iPass Mobile Enterprise Report:* http://info.ipass.com/forms/mobileenterprise-report.

8 PricewaterhouseCoopers (marzo de 2012): *Information Risk Maturity Index.*

9 Trend Micro (febrero de 2012) *Mobile Consumerization Trends&Perceptions:* http://www.trendmicro.com/cloud-content/us/pdfs/rpt_decisive- analytics_mobile_consumerization_trends_perceptions.pdf.

El análisis estático solo permite una gestión preventiva. Durante la ocurrencia de incidentes o ataques, es mero observador que aprende de lo ocurrido para el siguiente ciclo de despacho: revisión periódica. Pero no permite un análisis en tiempo real:

- Cuando descubrimos una vulnerabilidad en nuestro sistema (por ejemplo, un defecto de *software* o una deficiencia de fabricación o de ensamblaje o de gestión).
- Cuando un incidente o un ataque inutiliza parte de nuestras capas de defensa (por ejemplo, desastres naturales o *ciberataques*); en estos casos, el perímetro de seguridad cambia y el riesgo aumenta notablemente.
- Cuando un proveedor tiene problemas en su prestación de servicio con consecuencias sobre nuestra capacidad de operar.

En todos estos casos, lo que se requiere es 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 en que nos hemos visto envueltos.

Todo análisis necesita un modelo que defina los parámetros de entrada, el procesamiento y el significado de los resultados. En un análisis de riesgos, a veces es tanto o más importante el por qué del resultado porque si el riesgo es elevado la pregunta relevante es qué debemos hacer para reducirlo y, teniendo en cuenta que el entorno es el que es, normalmente lo que hay que mejorar es el sistema de protección propio para que de las mismas premisas se deriven situaciones de mejor riesgo. Eso implica entender cómo se traducen las amenazas en riesgos y cómo frenar las amenazas para que no lleguen a desgracias.

En el nuevo enfoque, los incidentes rara vez son atómicos (en el sentido académico del término: indivisibles) sino que usualmente siguen una ruta de avance desde donde se originan hasta donde hacen daño al sistema. Esto es muy gráfico en sistemas que disfrutan de capas de defensa, físicas y lógicas, de forma que un atacante tiene que ir progresando a través de varias etapas, a veces ayudado de forma inconsciente por problemas técnicos que debilitan alguna capa o por catástrofes naturales que destruyen o debilitan el esquema de capas.

Un modelo que dé respuestas debe incluir este concepto de progreso para poder entender:

- Qué capas debemos proteger preventivamente para impedir, dificultar o retrasar el progreso del incidente.
- Qué debemos hacer cuando una capa ha sido perforada y el atacante está más cerca de alcanzar su objetivo: esta es la parte más dinámica, pues supone conectar los detectores de intrusión al sistema

de análisis de riesgos para conocer el riesgo sobrevenido tras una intrusión.

En definitiva, el nuevo enfoque supone, por una parte, realizar los análisis de riesgos entendiendo los ataques posibles (tiempo, capacidad del atacante, progreso del ataque), y por otra parte, disponer de una capacidad de gestión que pueda informar adecuadamente a los que tienen que tomar decisiones preventivas y reactivas de forma que protejamos no los componentes, sino los servicios finales, sean relativos a la administración electrónica o a los servicios públicos esenciales que, a fin de cuentas, están fuertemente interrelacionados.

Toma de conciencia de lo que hay que proteger

Las políticas de seguridad de la información

La *Política de seguridad de la información* es un documento de alto nivel que define lo que significa «seguridad de la información» en una organización (12). El documento debe ser accesible por todos los miembros de la organización y redactado de forma sencilla, precisa y comprensible. Conviene que sea breve, dejando los detalles técnicos para otros documentos normativos.

El Esquema Nacional de Seguridad (ENS) (13) se refiere en varios puntos a la existencia de una política de seguridad en los organismos públicos:

ENS. Artículo 11. Requisitos mínimos de seguridad:

> *Todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente.*
>
> *ENS. Artículo 12. Organización e implantación del proceso de seguridad.*
>
> *La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad según se detalla en el Anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.*
>
> *ENS. Disposición transitoria. Adecuación de sistemas.*
>
> *Mientras no se haya aprobado una política de seguridad por el órgano superior competente serán de aplicación las políticas de seguridad que puedan existir a nivel de órgano directivo.*
>
> *ENS. Anexo II: Medidas de seguridad.*
>
> *Marco organizativo [org].*

Política de seguridad [org.1].

La política de seguridad será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el Artículo 11, y se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:

Los objetivos o misión de la organización.

- *El marco legal y regulatorio en el que se desarrollarán las actividades.*
- *Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.*
- *La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.*
- *Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.*

La política de seguridad debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Real Decreto 1720/2007, en lo que corresponda (14).

La *Política de seguridad de la información* debe hacer referencia además a aquellas otras políticas de seguridad nacionales o internacionales que afecten al organismo público.

Principios de seguridad

En la toma de decisiones en materia de política de seguridad, se deben tener en cuenta una serie de principios básicos ampliamente aceptados en el ámbito de la seguridad y que están reflejados en los documentos de política de seguridad de la OTAN y de la Unión Europea (15) así como en los de otros países de nuestro entorno:

- Clasificación de la información.
- Habilitación/autorización de seguridad.
- Necesidad de conocer.
- Compartimentación de la información.
- Imputabilidad.
- Equilibrio entre seguridad y eficacia o garantía razonable.
- Segregación de las funciones de administración, administración de seguridad y supervisión de la seguridad.

Los anteriores principios son válidos para cualquier entorno de la seguridad, ya sea seguridad física, seguridad de personal, seguridad documental o seguridad TIC. Existen además otros principios de seguridad generalmente aceptados y directamente relacionados con los sistemas de información:

- Análisis y gestión del riesgo. Se realizarán aquellos procesos necesarios de análisis y gestión de riesgos que permitan monitorizar, reducir, eliminar, evitar o asumir los riesgos asociados al sistema.
- Mínima funcionalidad. Solo estarán disponibles las funciones, protocolos y servicios necesarios para cumplir el requisito operacional o funcional del sistema.
- Mínimo privilegio. Los usuarios de los sistemas que manejen información clasificada solo dispondrán de los privilegios y autorizaciones que se requieren para la realización de las obligaciones de su puesto de trabajo.
- Nodo autoprotegido. Cada sistema interconectado deberá, inicialmente, tratar al otro sistema como un entorno no confiable y deberá implementar medidas que controlen el intercambio de información con el otro sistema.
- Defensa en profundidad. Las medidas de protección deberán implementarse en la medida de lo posible en varios componentes, niveles o capas, y en la máxima extensión, de manera que no haya una única línea (o componente) de defensa.
- Control de configuración. Se debe mantener una configuración básica del equipamiento *hardware* y *software* en los sistemas clasificados. Establecer con carácter obligatorio la aplicación de configuraciones de seguridad en las diferentes tecnologías utilizadas en el sistema.
- Verificación de la seguridad. La aplicación de estos principios y su consecuente implementación en medidas de protección deberá ser inicial y periódicamente verificada.
- Respuesta ante incidentes. Se debe disponer de una capacidad de respuesta que permita una rápida reacción ante un incidente de seguridad.

Los principios de seguridad antes mencionados se materializan en los sistemas de información y comunicaciones identificando un conjunto de objetivos de seguridad:

- Identificar a las personas que acceden a la información manejada por un sistema o a los recursos del mismo.
- Autenticar a las personas que acceden a la información manejada por un sistema o a los recursos del mismo.

- Controlar el acceso a la información manejada por un sistema o a los recursos del mismo.
- Proporcionar confidencialidad a la información manejada por un sistema.
- Proporcionar integridad a la información manejada por un sistema o a los recursos del mismo.
- Mantener la disponibilidad de la información manejada por un sistema o de los recursos del mismo.
- No repudio. Proporcionar la prueba de que una determinada transmisión o recepción ha sido realizada, no pudiendo su receptor/transmisor negar que se haya producido.
- Trazabilidad. Proporcionar los controles que determinen en que en todo momento se podrá determinar quién hizo qué y en qué momento.

El ENS, por su parte, establece otros principios básicos:

- Seguridad Integral: la seguridad de la información en la Administración se plantea como un proceso integral que excluye tratamientos coyunturales. Se prestará especial atención a las personas, la organización y los procedimientos de seguridad.
- Gestión basada en riesgos: se analizarán los riesgos donde se deberán identificar y evaluar riesgos inherentes en todos los activos de información, incluyendo las personas y la infraestructura que invierten en su gestión. Este conocimiento de los riesgos servirá para gestionarlos mediante el despliegue de medidas de seguridad para mitigar su impacto.
- Prevención, reacción y recuperación: los sistemas de seguridad deben tener una orientación preventiva para evitar las amenazas. Los sistemas dispondrán de medidas de recuperación que permitan restaurar la información y los servicios, sin que se ponga en peligro la continuidad de los mismos.
- Establecimiento de barreras de defensa: deberá existir una estrategia de protección con diversas capas de seguridad y control.
- Evaluación periódica: a través de auditorías y sistemas de verificación de cumplimientos.
- Función diferenciada: Las diversas responsabilidades inherentes a la gestión de la seguridad deberán diferenciarse de las relativas a las de gestión de los sistemas de información.

Los principios de seguridad mencionados deben estar recogidos en la *Política de seguridad de la información,* la cual se desarrolla por medio de normativa de seguridad que afronta aspectos específicos. La normativa

de seguridad debe estar a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Dado que la *Política de seguridad de la información* está escrita a un nivel muy amplio, se requiere complementarla con documentos más precisos que ayuden a llevar a cabo lo propuesto. Para ello, se utilizan otros instrumentos que reciben diferentes nombres, siendo comunes los siguientes:

- Normas de seguridad *(security standards)*.
- Guías de seguridad *(security guides)*.
- Procedimientos de seguridad *(security procedures)*.

Las normas uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios y suelen ser de carácter obligatorio.

Las guías tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.

Los procedimientos (operativos) de seguridad afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

Las organizaciones no siempre separan nítidamente estos diferentes tipos de herramientas, sino que a veces se generan manuales y reglamentos de seguridad que tienen un poco de todos los elementos anteriormente mencionados, buscando siempre una mayor efectividad en la concienciación y formación de los usuarios del sistema.

Si bien los manuales y reglamentos de carácter mixto pueden servir como herramientas importantes, a menudo es útil distinguir claramente entre lo que es política (abstracta) y su aplicación concreta. De esta forma, se es más flexible y se consigue una cierta uniformidad de resultados incluso cuando cambia la tecnología o los mecanismos empleados.

El Esquema Nacional de Seguridad

El Real Decreto 3/2010, de 8 de enero (BOE de 29 de enero), *por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración electrónica,* regula el citado esquema previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

Su objeto es establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Su finalidad es crear la confianza necesaria en el uso de la administración electrónica por parte de los ciudadanos y permitir el cumplimiento por parte de las administraciones de la obligación de prestar acceso electrónico y trámites públicos.

El ENS introduce los elementos comunes que han de guiar la actuación de las Administraciones Públicas en materia de seguridad de las tecnologías de la información.

En particular:

- Los principios básicos a ser tenidos en cuenta en las decisiones en materia de seguridad.
- Los requisitos mínimos que permitan una protección adecuada de la información.
- El mecanismo para lograr el cumplimiento de los principios básicos y requisitos mínimos mediante la adopción de medidas de seguridad proporcionadas a la naturaleza de la información, el sistema y los servicios a proteger (16).

Se desarrolla teniendo en cuenta, entre otras, las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes, y la utilización de estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos (17).

En su elaboración se han manejado, entre otros, referentes en materia de seguridad tales como directrices y guías de la OCDE (18), recomendaciones de la Unión Europea, normalización nacional e internacional (19) (20), normativa sobre administración electrónica, protección de datos de carácter personal (21), firma electrónica y Documento Nacional de Identidad Electrónico (22) (23), así como a referentes de otros países.

Sus objetivos principales son los siguientes:

- Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- Establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 11/2007, que estará constituida por

los principios básicos y los requisitos mínimos para una protección adecuada de la información.

- Introducir los elementos comunes que han de guiar la actuación de las Administraciones Públicas en materia de seguridad de las tecnologías de la información.
- Aportar un lenguaje común para facilitar la interacción de las Administraciones Públicas, así como la comunicación de los requisitos de seguridad de la información a la industria.

En el ENS se concibe la seguridad como una actividad integral en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

El ENS es de obligado cumplimiento para:

- Administración general del Estado (AGE): el conjunto de departamentos, entes, sociedades públicas, organismos y agencias estatales.
- La Administración de las comunidades autónomas (autonómica): los departamentos y consejerías, fundaciones públicas, institutos, agencias, sociedades públicas, universidades y otros entes de la Administración.
- La Administración local: ayuntamientos, diputaciones, mancomunidades y otras formas de organización de la Administración, fundaciones y patronatos, sociedades públicas y entes autónomos.
- Entidades de derecho público vinculadas o dependientes del conjunto de la Administración española.
- No obstante, no es obligatorio a aquellas administraciones que realicen sus actividades en régimen de derecho privado.

Para cumplir con el ENS, las administraciones deben cumplir al menos los siguientes puntos (24):

- Definir y aprobar formalmente la Política de seguridad por parte del titular responsable de la acción de gobierno, documento recopilatorio del marco de seguridad objetivo.
- Definir los tipos y niveles de información administrativa a efectos de seguridad y aprobar su estructura por el órgano de dirección.
- Crear y definir comités de seguridad, responsables de velar por la política de seguridad de la entidad.
- Designar la figura del responsable de seguridad por sistemas y/o departamentos.

- Definir la normativa de seguridad, indicando cómo y quién hace las distintas tareas y cómo se identifican y resuelven las incidencias que pudieran darse.
- Definir y escribir los procesos de autorización, formalizando autorizaciones que cubran todos los elementos de los sistemas de información: instalaciones, equipos, aplicaciones, medios de comunicación, accesos, soportes, etc.
- Establecer el cumplimiento técnico, con la revisión periódica de la normativa y los procedimientos por el personal técnico.
- Realizar auditorías bienales de seguridad en las que se revise la política de seguridad y su cumplimiento, así como el conjunto de riesgos, normativas, procedimientos y controles establecidos.
- Formar continuamente a todo el personal sobre la política, normativa y procedimientos de seguridad.

Están integrados en el ámbito del ENS todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información. De forma específica, se implementarán, gestionarán e integrarán para el cumplimiento del ENS los siguientes conceptos:

- Servicios, trámites y demás relaciones que se presten a ciudadanos electrónicamente.
- Las comunidades electrónicas relativas a la transmisión, almacenamiento y recepción de datos.
- Las sedes y registros electrónicos.
- Las notificaciones y publicaciones electrónicas.
- Los mecanismos de firma electrónica y certificados digitales.
- Las aplicaciones informáticas.
- Los ficheros con datos de terceros.
- La gestión de las copias de seguridad.
- Las herramientas de *hardware* y *software*, ya sean propias o provistas por terceros.
- La adquisición de nuevos componentes de los sistemas de información.
- La transmisión de datos entre distintas administraciones.
- El acceso y manejo de la información por el personal de las administraciones.
- Las redes, dispositivos periféricos, dispositivos móviles, etc.

– Procedimientos que aseguren la conservación y accesibilidad a largo plazo de los documentos electrónicos elaborados por las administraciones públicas.

El cumplimento del ENS engloba toda información que, estando en soporte físico, haya sido causa o consecuencia de la información electrónica, debiendo aplicarse las mismas medidas de seguridad conforme al soporte en el que se encuentre.

Para su implementación, se tiene que disponer de los siguientes elementos (25):

– Inventario de activos, recursos técnicos, organizativos, humanos y procedimentales sujetos al ENS.
– Catalogación de los tipos de información según su criticidad.
– Análisis de riesgos.
– Selección de medidas de protección en función de los tipos y niveles de la información.
– Elaboración de un marco organizativo de seguridad:
  • Documento de política de seguridad.
  • Documentos de normativa de seguridad.
  • Documentos de procedimientos de seguridad.
  • Documentos de autorización.
  • Documentos de cumplimiento técnico.
– Arquitectura de seguridad.
– Sistemas de registro, control y resolución de incidencias.
– Plan de continuidad de servicio.
– Plan de pruebas y monitorización del sistema.
– Medidas de protección.
– Plan de formación y sensibilización del personal.
– Actualización del sistema.
– Plan de auditoría bienal.

Respecto a su implantación, es de aplicación lo siguiente:

– Medidas de protección:
  • Protección de instalaciones e infraestructuras.
  • Gestión del personal.
  • Protección de equipos.
  • Protección de las comunicaciones.
  • Protección de soportes de información.

- Protección de aplicaciones.
- Protección de la información.
- Protección de los servicios.

– Categorización de los sistemas de información:

- Dimensiones de la seguridad: disponibilidad, autenticidad, integridad, confidencialidad, trazabilidad.
- Determinación de los niveles de seguridad por sistema: bajo, medio, alto.
- Relación entre tipos de información y dimensión de la confidencialidad.
- Determinación de categoría de cada sistema: básica, media, alta.

– Marco organizativo:

- Política de seguridad.
- Normativa de seguridad.
- Procedimientos de seguridad.
- Procesos de autorización.
- Órganos de gestión.
- Auditorías de seguridad: cumplimiento legal y cumplimiento técnico.

– Marco operacional:

- Planificación: análisis de riesgos, arquitecturas de seguridad, componentes, etc.
- Control de accesos.
- Explotación: inventario de activos, gestión de procesos, registros, sistemas de protección.

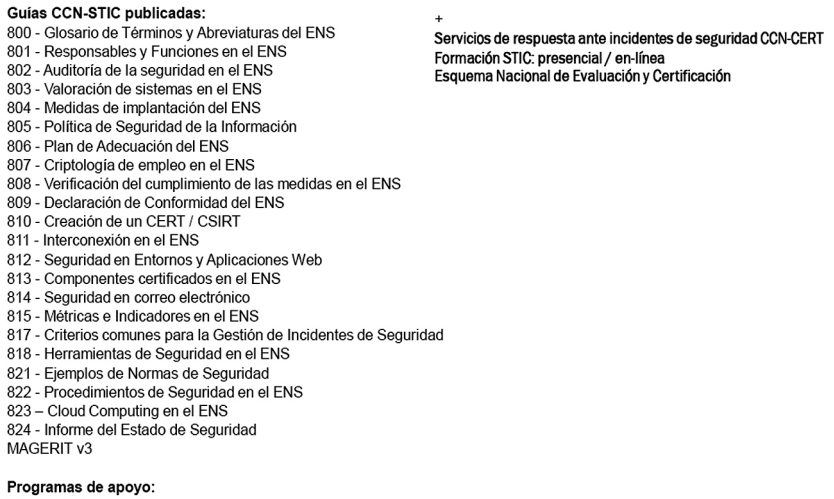

Figura 3.6. Instrumentos de apoyo a la implantación del ENS puestos a disposición de los organismos de las AA. PP. hasta 2012.

- Servicios externos.
- Continuidad del servicio.
- Monitorización del sistema.
- Acreditación de conocimientos de la vida laboral.

Las responsabilidades básicas del personal de la Administración

Las administraciones y entidades públicas de todo tipo deben contar con los factores organizativos que les permitan satisfacer el derecho de los ciudadanos a una buena Administración y contribuir al desarrollo económico y social. Entre esos factores el más importante es, sin duda, el personal al servicio de la Administración.

En general, la legislación básica de la función pública hace posible que existan los profesionales que la Administración necesita, estimula a los empleados para el cumplimiento eficiente de sus funciones y responsabilidades, les proporciona la formación adecuada y les brinda suficientes oportunidades de promoción profesional, al tiempo que facilita una gestión racional y objetiva, ágil y flexible del personal, atendiendo al continuo desarrollo de las nuevas tecnologías.

La Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público (26) recoge los principios generales exigibles a quienes son empleados públicos así como los derechos básicos y comunes, distinguiendo entre los de carácter individual y los derechos colectivos. El Estatuto establece en nuestra legislación una regulación general de los deberes básicos de los empleados públicos fundada en principios éticos y reglas de comportamiento, que constituye un auténtico código de conducta.

En definitiva, la condición de empleado público no solo comporta derechos, sino también una especial responsabilidad y obligaciones específicas para con los ciudadanos, la propia Administración y las necesidades del servicio. Este, el servicio público, se asienta sobre un conjunto de valores propios, sobre una específica «cultura» de lo público que, lejos de ser incompatible con las demandas de mayor eficiencia y productividad, es preciso mantener y tutelar.

El Estatuto Básico también define las clases de empleados públicos –funcionarios de carrera e interinos, personal laboral, personal eventual– y la figura del personal directivo, factor decisivo de modernización administrativa, puesto que su gestión profesional se somete a criterios de eficacia y eficiencia, responsabilidad y control de resultados en función de los objetivos.

El capítulo VI del Estatuto recoge el «Código de conducta» de los empleados públicos. En él se establece (art. 52) que:

Los empleados públicos deberán desempeñar con diligencia las tareas que tengan asignadas y velar por los intereses generales con sujeción y observancia de la Constitución y del resto del ordenamiento jurídico, y deberán actuar con arreglo a los siguientes principios: objetividad, integridad, neutralidad, responsabilidad, imparcialidad, confidencialidad, dedicación al servicio público, transparencia, ejemplaridad, austeridad, accesibilidad, eficacia, honradez, promoción del entorno cultural y medioambiental y respeto a la igualdad entre mujeres y hombres, que inspiran el Código de Conducta de los empleados públicos configurado por los principios éticos y de conducta regulados en los artículos siguientes.

Los principios éticos (art. 53) recogen entre otros la necesidad de que los empleados públicos «respeten la Constitución y el resto de normas que integran el ordenamiento jurídico», y de que su actuación persiga «la satisfacción de los intereses generales de los ciudadanos y se fundamentará en consideraciones objetivas orientadas hacia la imparcialidad y el interés común, al margen de cualquier otro factor que exprese posiciones personales, familiares, corporativas, clientelares o cualesquiera otras que puedan colisionar con este principio». Ajustarán su actuación a los principios de lealtad y buena fe con la Administración en la que presten sus servicios, y con sus superiores, compañeros, subordinados y con los ciudadanos. Su conducta se basará en el respeto de los derechos fundamentales y libertades públicas y fundamentalmente actuarán de acuerdo con los principios de eficacia, economía y eficiencia, y vigilarán la consecución del interés general y el cumplimiento de los objetivos de la organización.

Además, y en relación con la necesidad de concienciación que aquí nos ocupa, los empleados públicos «cumplirán con diligencia las tareas que les correspondan o se les encomienden», «guardarán secreto de las materias clasificadas u otras cuya difusión esté prohibida legalmente», «garantizarán la constancia y permanencia de los documentos para su transmisión y entrega a sus posteriores responsables», «mantendrán actualizada su formación y cualificación» y «observarán las normas sobre seguridad y salud laboral».

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 organización de seguridad

Los organismos de la Administración son entidades de distinta naturaleza, dimensión y sensibilidad y, sin entrar en casuísticas particulares,

está claro que el mantenimiento y gestión de la seguridad de las TIC va íntimamente ligada al establecimiento de una organización o estructura de seguridad dentro de los organismos (27).

Dicha «organización de seguridad» se establece mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas y la implantación de una estructura que las soporte. En general, la *Política de seguridad* debe establecer las funciones y responsabilidades, en materia STIC, del personal que constituye las diferentes estructuras de la organización. Por ejemplo, el artículo 10 del Esquema Nacional de Seguridad diferencia la responsabilidad de seguridad (responsable de seguridad) de la responsabilidad sobre la operación del servicio (responsable del sistema, ayudado por el administrador de seguridad), de forma que el responsable de seguridad supervisa la actividad operacional (28).

Como norma general, en la organización de seguridad de un organismo público se encontrarán definidas las figuras que se citan a continuación. Hay que tener en cuenta que estas figuras son un modelo de referencia que sirve de orientación en el desarrollo de la estructura de seguridad de cualquier organización, donde las necesidades de personal y recursos disponibles son determinantes.

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. 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.

El ENS habla del «responsable de la información» como la persona que tiene la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la persona que determina los niveles de seguridad de la información. Aunque la aprobación formal de los niveles corresponda al responsable de la información, se puede recabar una propuesta al responsable de seguridad y conviene que se escuche la opinión del responsable del sistema.

El ENS habla del «responsable del servicio» como la persona que tiene la potestad de establecer los requisitos del servicio en materia de seguri-

dad. O, en terminología del ENS, la persona que determina los niveles de seguridad de los servicios.

En todos los organismos públicos debería existir también un «responsable de seguridad» o persona específicamente designada por el organismo, según procedimiento descrito en su política de seguridad, con un conjunto más o menos concreto de las siguientes responsabilidades:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en su ámbito de responsabilidad.
- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Promover la formación y concienciación STIC dentro de su ámbito de responsabilidad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema (ver sección 9).
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para el propietario del sistema, incluyendo los incidentes más relevantes del periodo.

Esta figura de «responsable de seguridad» aparece con otras denominaciones en diferentes documentos de política de seguridad, como por ejemplo:

- NIST: Computer Security Program Manager [SP 800-12] (29).
- Unión Europea: Autoridad INFOSEC (ASTIC) [2001/264/CE].
- CCN: Autoridad de Seguridad de las Tecnologías de la Información y Comunicación (ASTIC) [CCN-STIC 201].
- Ministerio de Defensa: Autoridad INFOSEC (AI) [OM 76/2002] (30).

Otros roles especialmente importantes desde el punto de vista de la seguridad son aquellos directamente relacionados con la operación o explotación de los sistemas TIC. En este sentido, en los organismos públicos debería también existir un «responsable del sistema», persona designada por el propietario del sistema en la correspondiente documentación de seguridad con un conjunto de responsabilidades como las siguientes:

- Desarrollar, operar y mantener el sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del sistema y cerciorarse de que estas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el sistema.
- Elaborar y aprobar la documentación de seguridad del sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del sistema.
- Velar por el cumplimiento de las obligaciones del administrador de seguridad del sistema.
- Investigar los incidentes de seguridad que afecten al sistema y, en su caso, comunicación al responsable de seguridad o a quien este determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Además, el responsable del sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

La figura de responsable del sistema recibe también otras denominaciones tales como:

- NIST: Program and functional managers / application owners [SP 800-12].

- Unión Europea: Autoridad Operativa del Sistema de Tecnología de la Información (AOSTI) [2001/264/CE] (15).
- CCN: Autoridad Operacional del Sistema de las Tecnologías de la Información y Comunicación (AOSTIC) [CCN-STIC 201].
- Ministerio de Defensa: Autoridad Operacional del Sistema (AOS) [OM 76/2002].

En estrecha colaboración con el responsable del sistema, debería existir la figura de administrador de la seguridad del sistema. Esta persona debe ser designada por el propietario del sistema con las responsabilidades de gestión, configuración y actualización, en su caso, del *hardware* y *software* en los que se basan los mecanismos y servicios de seguridad, la implementación, gestión y mantenimiento de las medidas de seguridad y la supervisión de las instalaciones de *hardware* y *software*, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.

El administrador de seguridad del sistema es figura clave en la prevención, detección y respuesta ante los *ciberataques*. Como resultado de su trabajo y buen hacer, la organización garantiza que los controles de seguridad establecidos son cumplidos estrictamente, que se aplican los procedimientos aprobados para manejo del sistema y que se realiza la trazabilidad, la auditoría y el registro y análisis de eventos de seguridad.

El administrador de seguridad es el responsable, además, de iniciar el proceso de respuesta ante incidentes que se produzcan en el sistema bajo su responsabilidad, informando y colaborando con el responsable de seguridad en la investigación de los mismos.

Otras denominaciones de esta figura son:

- NIST: Security officer [SP 800-12].
- Unión Europea: Agente de Seguridad INFOSEC [2001/264/CE].
- CCN: Administrador de Seguridad del Sistema (ASS) [CCN-STIC-201].
- Ministerio de Defensa: Administrador de Seguridad del Sistema (ASS) [OM 76/2002].

En cada sistema, además, tienen cabida otras figuras tales como el administrador del sistema, el administrador de red, operadores, etc., y, finalmente, los usuarios del sistema, que es el conjunto de personas autorizado para acceder al sistema utilizando las posibilidades que les ofrece el mismo.

Como ya se ha mencionado, los usuarios juegan un papel fundamental en el mantenimiento de la seguridad del sistema, por tanto, es fundamental su concienciación en la seguridad de las TIC ya que en la mayoría de los casos constituyen voluntariamente o involuntariamente la principal amenaza para el propio sistema.

Deberes y obligaciones (mp.per.2):

1. Se informará a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.

a) Se especificarán las medidas disciplinarias a que haya lugar.

b) Se cubrirá tanto el periodo durante el cual se desempeña el puesto como las obligaciones en caso de término de la asignación o traslado a otro puesto de trabajo.

c) Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo como posteriormente a su terminación.

2. En caso de personal contratado a través de un tercero:

a) Se establecerán los deberes y obligaciones del personal.

b) Se establecerán los deberes y obligaciones de cada parte.

c) Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

Figura 3.7. Medidas de seguridad (mp.per.2) del ENS en relación con las responsabilidades.

Administradores y operadores deben estar debidamente informados de sus obligaciones y responsabilidades, así como haber sido instruidos para la labor que desempeñan. Administradores y operadores del sistema son responsables, entre otras cosas, de leer, comprender y seguir los procedimientos operativos de seguridad (POS) relativos a su sistema y de asegurarse de que están preparados adecuadamente para llevar a cabo operaciones en el sistema, en particular las correspondientes a la gestión de mecanismos de identificación y al procedimiento de gestión de incidentes.

«La seguridad como función diferenciada» exige que el responsable del sistema no sea la misma persona que el responsable de seguridad. Además, de acuerdo con el *principio de jerarquía* que rige en las administraciones públicas españolas, en caso de conflicto este deberá ser resuelto por el superior jerárquico. Esto debería concretarse para el caso de cada organización, acorde con la normativa que sea de aplicación. El mecanismo concreto debe figurar en la *Política de seguridad.*

Las responsabilidades y los riesgos

La gestión de los riesgos es una tarea que debe realizarse de manera continua sobre el sistema, y se deben orientar todas las demás actividades de acuerdo a los principios de «gestión de riesgos» y «reevaluación periódica»[10].

[10] Ver artículo 6, «Gestión de la seguridad basada en los riesgos», y artículo 9, «Reevaluación periódica», del ENS.

En el análisis de riesgos se debe tener en cuenta el principio de proporcionalidad entre el nivel de detalle del análisis y la importancia (categoría) del sistema. Es responsabilidad del responsable del sistema que se realice el preceptivo análisis de riesgos y se proponga el tratamiento adecuado, calculando los riesgos residuales.

Por su parte, el responsable de la seguridad es responsable de que el análisis de riesgos se ejecute en tiempo y forma, así como de identificar carencias y debilidades y ponerlas en conocimiento de los responsables de la información, del servicio y del sistema.

En todo organismo público debería quedar claro que el responsable de la información es el dueño de los riesgos sobre la información, del mismo modo que el responsable del servicio es el dueño de los riesgos sobre los servicios.

En este sentido, el dueño de un riesgo debe ser informado (¡y tener conciencia!) de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente dueño.

Una buena praxis en los organismos públicos sería establecer indicadores del estado de los riesgos críticos (KRI, *Key Risk Indicators*). Estos indicadores son propuestos por el responsable de seguridad; su definición debería ser acordada por el responsable de seguridad y el dueño del riesgo.

La definición de los indicadores contendrá expresamente en qué medidas se basan, cuál es el algoritmo de cálculo, la periodicidad de evaluación y los umbrales de aviso y alarma (atención urgente), y los umbrales de riesgo en los que es preciso informar al responsable correspondiente. Todo ello, además, debería estar a disposición de los auditores.

En definitiva, la responsabilidad de monitorizar un riesgo recae en su dueño, sin perjuicio de que la función puede ser delegada en el día a día, retomando el control de la situación cuando hay que tomar medidas para atajar un riesgo que se ha salido de los márgenes tolerables.

Existen numerosos puntos de concurrencia entre los roles y responsabilidades aquí mencionados, el Esquema Nacional de Seguridad y el Reglamento de Protección de Datos de Carácter Personal. En algunos puntos hay coincidencia, y en otros diferencias.

El RD 1720/2007 de Protección de Datos de Carácter Personal identifica varios responsables y encargados, pormenorizando las funciones y tareas que cada uno debe realizar. Los siguientes párrafos muestran cómo conviven con las tareas y funciones marcadas por el Esquema Nacional de Seguridad.

Todos los roles determinados en uno y otro ordenamiento deberán ser identificados y estar formalmente asignados, sin perjuicio de que algunas figuras puedan concurrir en la misma persona, según se desarrolla a continuación.

El artículo 5 del RD 1720/1997 establece que el responsable del fichero o del tratamiento es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Asimismo establece que el responsable de seguridad es la persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

En cierta medida, pueden coincidir las figuras de «responsable de la información» con el «responsable del fichero». Hay que tener en cuenta que la determinación del carácter personal de los datos viene regulada por la normativa y matizada por una amplia jurisprudencia, acotando el margen de discrecionalidad del responsable de la información. En general, si las funciones no coinciden en la misma persona, el responsable de la información que se maneja estará supeditado al responsable del fichero.

El responsable del sistema debe aunar los requisitos sobre los datos de carácter personal que se manejen en el sistema de su competencia, tanto si son propios del organismo propietario del sistema como si son datos cedidos por un tercero.

No cabe esperar que se produzcan conflictos entre los responsables de la información y de los servicios por una parte y los responsables del fichero y del tratamiento por otra. En caso de discrepancia, los datos de carácter personal constituyen un objeto protegido de mayor rango y marcarán la pauta a seguir.

La figura del «responsable de seguridad» aparece en ambas normativas con un papel muy similar como persona que vela porque los sistemas efectivamente respondan a los requisitos establecidos. Los organismos públicos harán bien en hacer coincidir estas responsabilidades en una única figura, recopilando todas las funciones en la *Política de seguridad.*

Por último, no cabe esperar que se produzcan conflictos entre las obligaciones del responsable de seguridad derivadas de una u otra normativa, pues siempre deberá cumplirse la mayor de las exigencias derivadas de uno u otro.

Las normas y los procedimientos

La Administración Pública, en el desarrollo de sus funciones de servicio, policía o fomento, está sometida a diferentes normativas, de carácter estatal, autonómico o local. La particularidad de la actuación administrativa realiza-

da por medios electrónicos viene requiriendo, en los mismos tres niveles, la existencia de normas asimismo específicas, al objeto de acomodar aquellas funciones originarias a los condicionantes y medios electrónicos.

En este sentido, la LAECSP ha supuesto el punto de partida de un extenso compendio de regulaciones que vienen completando nuestro moderno ordenamiento jurídico administrativo-electrónico, entre las que cabe destacar: el Real Decreto 1671/2009, de 6 de septiembre, de desarrollo parcial de la LAECSP; el 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*, y el Real Decreto 4/2010, de de enero, *por el que se regula el Esquema Nacional de Interoperabilidad,* entre otras.

Con el objetivo de profundizar en las medidas de seguridad requeridas por los sistemas de información del ámbito de la LAECSP, el ENS insta a los organismos de las AA. PP. a desarrollar, publicar y hacer valer normas de carácter interno a los propios organismos, tendentes a mejorar el nivel de seguridad de las informaciones que manejan y los servicios que prestan.

La necesidad de completar el marco normativo aparece explícitamente en muchos de los preceptos del ENS. Por ejemplo, en los artículos 14 («Gestión del personal»), 18 («Adquisición de productos de seguridad»), 21 («Protección de información almacenada y en tránsito»), 23 («Registro de actividad»), 34 («Auditoría de la seguridad»), 37 («Prestación de servicios de respuesta a incidentes de seguridad en las Administraciones Públicas»), Disposición adicional tercera («Comité de Seguridad de la Información de las Administraciones Públicas»), etc.

En concreto, en el anexo II del ENS («Medidas de seguridad») se encuentra la medida [org.2], que señala:

> *Normativa de seguridad [org.2].*
>
> *Se dispondrá de una serie de documentos que describan:*
>
> *a) El uso correcto de equipos, servicios e instalaciones.*
>
> *b) Lo que se considerará uso indebido.*
>
> *c) La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.*

Y en relación con los procedimientos de seguridad, nos encontramos también en el anexo II del ENS («Medidas de seguridad») la medida [org.3], que señala:

> *Procedimientos de seguridad [org.3].*
>
> *Se dispondrá de una serie de documentos que detallen de forma clara y precisa:*

a) *Cómo llevar a cabo las tareas habituales.*

b) *Quién debe hacer cada tarea.*

c) *Cómo identificar y reportar comportamientos anómalos.*

Esta habilitación a los organismos de las AA. PP. para que promuevan su propia normativa interna y de relación con terceros se alienta en varias medidas de seguridad del ENS: requisitos de acceso [op.acc.2], deberes y obligaciones [mp.per.2], concienciación [mp.per.3], formación [mp.per.4], protección del correo electrónico *(e-mail)* [mp.s.1], etc.

De acuerdo con lo previsto en el artículo 37 del ENS, el CCN-CERT investigará y divulgará las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones Públicas. Con esta finalidad, las series de documentos CCN-STIC, elaboradas por el Centro Criptológico Nacional, ofrecen normas, instrucciones, guías y recomendaciones para aplicar el Esquema Nacional de Seguridad y para garantizar la seguridad de los sistemas de información en la Administración.

Se suele decir que lo que no se mide no puede gobernarse adecuadamente (31). Este aserto es igualmente predicable de la presencia y grado de cumplimiento de las normas de seguridad en los organismos públicos, razón por la cual conviene determinar qué métricas (32) habrán de proporcionar los indicadores adecuados que permitan a la dirección del organismo gestionar debidamente la influencia de las antedichas normas en la seguridad de la información y de los servicios prestados[11].

En relación con la normativa de seguridad, pueden utilizarse los siguientes indicadores clásicos:

- Proporción de normas implantadas sobre normas previstas.
- Número de violaciones graves de la normativa de seguridad reportadas.
- Encuesta de legibilidad percibida por los usuarios.
- Encuesta de utilidad percibida por los usuarios.

Como acabamos de mencionar, la normativa de seguridad podrá ser evaluada atendiendo a dos cualidades:

Legibilidad de la normativa: regularmente se puede preguntar a los usuarios a los que va dirigida la normativa de seguridad por la facilidad con la que se entienden los textos proporcionados. Las respuestas podrán valorarse en una escala de 1 a 5, de la siguiente forma: se interpreta perfectamente, se interpreta con cierta dificultad, puede generar inseguridad, no se entiende nada o genera confusión.

[11] Véase *Guía CCN-STIC 815: Métricas e indicadores en el ENS.*

Para calcular la legibilidad de un documento a partir de un conjunto de encuestas, pueden usarse los estadísticos mediana y desviación estándar de las puntuaciones obtenidas. Si la media o la mediana están por debajo de 3, debería revisarse la documentación, reescribiéndola de forma más clara para los lectores previstos. Por otra parte, si la desviación estándar es elevada, debería revisarse el colectivo al que va destinada pues puede que sea en sí heterogéneo y la documentación deba fraccionarse en partes o incluso redactarse de varias formas para que llegue a cada colectivo específico.

Utilidad de la normativa: regularmente se puede preguntar a los usuarios a los que va dirigida la normativa de seguridad por la utilidad que obtiene de los textos proporcionados. Las respuestas podrán valorarse en una escala de 1 a 5, de la siguiente forma: se encuentra rápidamente respuesta a lo que se necesita, aunque cuesta trabajo; leyéndolo con cuidado y detenimiento, se consigue; no está claro a qué caso se aplica cada cosa; da muchas cosas por sobreentendidas, o no sirve.

También en este caso, para calcular la utilidad de un documento a partir de un conjunto de encuestas, se usarán los estadísticos mediana y desviación estándar de las puntuaciones obtenidas. Si la media o la mediana están por debajo de 3, debería revisarse la documentación para ajustarla a los casos de uso previstos; si la desviación estándar es elevada, deberían revisarse los escenarios a los que se pretende aplicar pues puede que sean en sí heterogéneos y la documentación deba fraccionarse en partes o incluso redactarse de varias formas para que se adapte a cada caso de aplicación y los lectores sepan cuándo aplica cada cosa que se dice.

Ejemplo del contenido de una norma general de utilización de los recursos y sistemas de información de un organismo de la Administración

1. Introducción. Ámbito de aplicación.
2. Vigencia, Revisión y evaluación.
3. Referencias.
4. Utilización del equipamiento informático y de comunicaciones.
   - 4.1. Normas generales.
   - 4.2. Usos específicamente prohibidos.
   - 4.3. Normas específicas para el almacenamiento de información.
   - 4.4. Normas específicas para equipos portátiles y móviles.
   - 4.5. Uso de memorias/lápices USB (*pendrives*).

4.6. Grabación de CD y DVD.

4.7. Copias de seguridad.

4.8. Borrado y eliminación de soportes informáticos.

4.9. Impresoras en red, fotocopiadoras y faxes.

4.10. Digitalización de documentos.

4.11. Cuidado y protección de la documentación impresa.

4.12. Pizarras y *flipcharts.*

4.13. Protección de la propiedad intelectual.

4.14. Protección de la dignidad de las personas.

5. Uso eficiente de equipos y recursos informáticos.
6. Instalación de *software.*
7. Acceso a los sistemas de información y a los datos tratados.
8. Identificación y autenticación.
9. Acceso y permanencia de terceros en los edificios, instalaciones y dependencias del organismo.

   9.1. Normas.

   9.2. Modelo de protocolo de firma.

   9.3. Modelo de autorizaciones y habilitaciones personales.
10. Confidencialidad de la información.
11. Protección de datos de carácter personal y deber de secreto.
12. Tratamiento de la información.
13. Salidas de información.
14. Copias de seguridad.
15. Conexión de dispositivos a las redes de comunicaciones.
16. Uso del correo electrónico corporativo (33).

    16.1. Normas generales.

    16.2. Usos especialmente prohibidos.

    16.3. Recomendaciones adicionales.
17. Acceso a Internet y otras herramientas de colaboración.

    17.1. Normas generales.

    17.2. Usos específicamente prohibidos.

18. Incidencias de seguridad.
19. Compromisos de los usuarios.
20. Control de actuaciones sobre las bases de datos del organismo.
21. Uso abusivo de los sistemas de información.
    21.1. Uso abusivo del acceso a Internet.
    21.2. Uso abusivo del correo electrónico.
    21.3. Uso abusivo de otros servicios y sistemas del organismo.
22. Monitorización y aplicación de esta normativa.
23. Incumplimiento de la normativa.
24. Modelo de aceptación y compromiso de cumplimiento.
25. Compendio de normas.

Información y concienciación

Tradicionalmente, se ha visto la seguridad como una materia del entorno corporativo de las TIC, y no del entorno de la función o el «negocio» de la organización, y ha sido responsabilidad del departamento TIC. Todavía se puede apreciar en muchos organismos de la Administración que los procesos relacionados con la función del organismo son independientes de los procedimientos de seguridad y en la mayoría de los casos el criterio de la seguridad no se ha tenido en cuenta a la hora de diseñar los procesos relacionados con la función. Sin embargo, la seguridad de los sistemas de los organismos puede ser mejorada aumentando la concienciación, mejorando las habilidades y desarrollando una estrecha relación entre funcionalidad y seguridad.

La necesidad de concienciación ha sido reconocida en la Estrategia de Seguridad Nacional recientemente aprobada, la cual tiene entre sus líneas estratégicas relacionadas con la *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» (34).

La concienciación y la formación ayudan a desarrollar una estrecha relación de trabajo entre las áreas y unidades de los organismos y los departamentos TIC, proporcionando un lenguaje y procesos comunes que se pueden utilizar para desarrollar una protección efectiva de los activos de la organización. Aumentar la concienciación es potencialmente la acción más valiosa en la tarea continua de la seguridad. Aumentar la concienciación consigue que todo el personal pertinente tenga suficiente

conocimiento de los riesgos y del impacto potencial en el negocio o función de los fallos de seguridad. El personal necesita saber qué hacer para prevenir los ataques y qué hacer en caso de un incidente.

Numerosos sitios web y recursos de información sirven de ayuda a usuarios finales y al personal de la Administración para proteger los sistemas de información, aunque muy pocos abordan o explican de manera específica la naturaleza y el alcance de los diferentes tipos de *ciberataques*. En ocasiones, además, el número de recursos disponibles y la información que contienen puede resultar aplastante para el usuario, ya que la información y orientación pueden variar entre las diferentes entidades. Del mismo modo, algunos consejos son inconsistentes e incluso inadecuados para hacer frente a la naturaleza rápidamente cambiante de esta amenaza, como, por ejemplo, los consejos que afirman que la única contramedida necesaria es mantener actualizados los sistemas operativos y los programas antivirus.

Los esfuerzos de concienciación deberían seguir haciendo hincapié en la disponibilidad de información clara que pueda ser entendida por todos los participantes y, en especial, por aquellos que carecen o poseen mínimos conocimientos técnicos. Dada la constante naturaleza cambiante del *malware*, las actividades de concienciación deberían ser revisadas o actualizadas regularmente para que sigan siendo efectivas, lo que ayudaría a mejorar la conducta y prácticas *online* de usuarios así como su capacidad para protegerse de los *ciberataques*.

Una campaña de concienciación orientada a los empleados debe tener presente los diferentes aspectos del problema de la seguridad informática. 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, que se han recibido y entendido, se debe 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.

El enfoque puede diferir de una organización a otra, pues la forma más eficaz de aumentar la concienciación en una organización dependerá de la cultura de la organización. En cualquier caso, para que un programa de concienciación en seguridad tenga éxito, hay dos elementos clave que son necesarios: la participación de la dirección y el establecimiento de objetivos claros y medibles.

La seguridad TIC puede llegar a ser complicada, abarca tecnologías y conceptos en general desconocidos y, en consecuencia, los mensajes claros deben formar parte de un programa de concienciación. Al determinar los mensajes de concienciación, es importante darse cuenta de que aumentar la concienciación e integrarla en el organismo es un proceso a largo plazo, no un esfuerzo de una vez (35) (36).

Es esencial que cualquier programa de concienciación de seguridad en un organismo esté correctamente planificado, ya que una sucesión de intentos mal planificados y mal ejecutados pueden obstaculizar los programas de seguridad. Para garantizar que un programa de concienciación está bien dirigido y ejecutado hay una serie de aspectos que deben considerarse y dar respuesta a las siguientes preguntas:

- ¿Cuál es el objetivo de concienciación de seguridad?
- ¿Cuál es el público objetivo?
- ¿Cómo funcionan las comunicaciones dentro de la organización?
- ¿Qué conocimientos existen en la organización con anterioridad?
- ¿Qué temas de concienciación necesitan tratarse?
- ¿Qué métodos de concienciación pueden usarse para transmitir el mensaje?
- ¿Cómo puede integrarse la concienciación de seguridad en la organización?
- ¿Cómo de bien es comprendido el mensaje?

Tener un objetivo específico de concienciación centrará los esfuerzos de difusión del mensaje clave en el público apropiado y permitirá medir el éxito del programa. Integrar la seguridad en cualquier organización lleva tiempo y el mejor enfoque es centrarse en los mensajes clave y construir lentamente y en profundidad la concienciación.

La formación del personal de la Administración

El nivel de formación necesario varía en función de los individuos y, en general, en los organismos públicos existen programas específicos de formación que combinan una serie de temas que pueden ser considerados para distintos públicos:

- Políticas y normas: se centra en las normas y la legislación.
- Procedimientos: detalla los procedimientos y cómo se relacionan con las políticas y las normas.
- Respuesta a incidentes: cubre lo que se debe hacer en caso de incidente.
- Arquitectura: cubre cómo los distintos sistemas están conectados entre sí y configurados, y será un tema con una fuerte componente técnica pero también procedimental, ya que esta actividad de formación deberá exponer claramente los flujos de información autorizados del organismo.
- Formación técnica detallada: cubre normalmente la seguridad TIC general.

En la Administración Pública española hay comparativamente pocos recursos diseñados específicamente para la formación en seguridad. De los cursos de seguridad TIC disponibles, encontrar cuál proporcionará un nivel adecuado de comprensión puede ser proceso difícil y largo. El análisis de las necesidades de formación es de gran ayuda en este ámbito y seleccionar cursos organizados por empresas y organizaciones profesionales reconocidas puede garantizar que se cumplan las necesidades de formación. Sin embargo, es poco probable que se oferte todo lo que se necesita y es probable que sea necesaria una mezcla de distintas actividades formativas. Los métodos típicos que se suelen utilizar son:

- Formación interna: las sesiones organizadas internamente a menudo proporcionan la formación más relevante, ya que se ocupan de temas específicos del organismo y pueden poner en contexto los conocimientos adquiridos externamente. Sin embargo, pueden consumir una gran cantidad de tiempo y valiosos recursos en su planificación y ejecución.
- Cursos de formación externos y formación aprobada de colaboradores: ya sea proporcionada por proveedores o por profesionales de la seguridad, son de carácter técnico y a veces difícil de relacionar con cuestiones específicas del puesto de trabajo. Hay una variedad de empresas y organismos profesionales que prestan certificaciones de seguridad tales como «Certificado CISA de Auditor de Sistemas de Información», «Certificación CISM de Director de Seguridad de la Información», «Certificado CISSP de Profesional de Seguridad de los Sistemas de Información (CISSP)», «Certificado GIAC de Garantía Global de la Información[12]», etc.

[12] Certified Information Systems Auditor (CISA), www.isaca.org; Certified Information Systems Security Professional (CISSP), www.isc2.org, y Global Information Assurance Certification (GIAC), www.giac.org.

- Formación *online* y seminarios web: se puede utilizar para formación de individuos y equipos con un coste relativamente bajo.
- Conferencias y talleres: asistir a conferencias es una buena manera de aprender acerca de la seguridad y muchos organismos que organizan conferencias suelen tener talleres de formación como parte del evento.
- Cursos de actualización: la formación no es algo puntual, se deben buscar cursos para garantizar que el personal se mantiene actualizado en los cambios, en las amenazas y en la tecnología y para mantener su nivel de destreza.
- Sesiones personales: se trata de una valiosa herramienta para los principales interesados, permitiendo que esas personas aprendan rápidamente y que el mensaje se entienda.
- Cursos de formación estructurados: pueden ser tanto externos como internos, y se centran en un tema u objetivo específico (p. ej., instalación y configuración de cortafuegos).
- Autoevaluación: la autoevaluación es una valiosa herramienta que permite a una organización obtener resultados de la formación en seguridad y medir el éxito de los planes de mitigación.
- Talleres multidisciplinares: reunir a diferentes partes interesadas de la organización para debatir las mejoras de la seguridad permite que se apliquen una amplia gama de experiencias y conocimientos a un problema, y puede poner de relieve las deficiencias que requieran ayuda externa.

Con independencia de las actividades de formación interna de los diferentes organismos, apoyadas o no por empresas especializadas, la Administración tiene instituciones propias para la formación de sus empleados públicos en el campo de la seguridad.

Instituto Nacional de Administración Pública

El Instituto Nacional de Administración Pública (INAP) tiene encomendadas las tareas de selección de los funcionarios de los cuerpos generales de la Administración General del Estado, la formación de directivos públicos y del resto de las personas que componen las organizaciones administrativas, así como la reflexión sobre las principales líneas de actuación de la Administración española.

El INAP es un organismo autónomo adscrito al Ministerio de Hacienda y Administraciones Públicas a través de la Dirección General de la Función Pública. Sus orígenes se remontan al Instituto de Estudios de Administración Local (IEAL), creado en 1940.

La misión del INAP es:

> *...crear conocimiento transformador en el sector público en beneficio de la sociedad, con el fin de propiciar la cohesión social y una democracia de alta calidad. Para alcanzar sus objetivos, el INAP cuenta con equipos transversales capaces de atraer ideas, personas y proyectos innovadores a los procesos de investigación, selección y formación, y actúa de acuerdo con los principios y valores de eficacia, aprendizaje en equipo, orientación al ciudadano, transparencia, ejemplaridad, autonomía y responsabilidad.*

El presupuesto total del INAP en 2011 fue de 146.071.100 €, de los cuales 18.375.400 € correspondieron a los gastos derivados de actividades propias del organismo y el resto, 127.695.700 €, correspondieron a créditos destinados a Formación para el Empleo de las Administraciones Públicas.

Las funciones principales que desarrolla el INAP se distribuyen en cuatro áreas de actividad: selección de funcionarios; formación y perfeccionamiento de empleados públicos; estudios y publicaciones, y relaciones internacionales. Además, organiza una amplia variedad de actividades docentes y académicas, de cooperación interadministrativa y de difusión en materia de Administración y políticas públicas, a través de jornadas, conferencias, encuentros y seminarios.

Actualmente, las cuatro grandes áreas de actividad del INAP son:

– Formación. La actividad formativa desarrollada por el INAP se ordena en torno a seis grandes programas formativos:

  - Directivos públicos: el INAP ha diseñado un programa para directivos que pretende ofrecer una formación de calidad para la mejora de la dirección pública. Las actividades formativas de este programa están dirigidas a los funcionarios de cuerpos y escalas del subgrupo A1, y al personal laboral fijo asimilado de las Administraciones Públicas.
  - Empleados públicos en funciones de gestión, de administración y auxiliares: el INAP ofrece actividades formativas que versan, dentro de estas funciones, sobre la organización, la actividad y el procedimiento administrativo, la gestión de los recursos humanos, la administración económica, la administración electrónica, las políticas públicas y las habilidades profesionales.
  - Administración local: una formación dirigida a los empleados públicos locales con el objetivo de adquirir los conocimientos y habilidades necesarias para una gestión de calidad de los servicios públicos locales.
  - Administración electrónica: el INAP incluye una amplia oferta de actividades formativas para todos los empleados públicos, como respuesta a la demanda y las necesidades de formación existente en administración electrónica.

- Idiomas y lenguas cooficiales: el INAP incorpora, en su oferta formativa, cursos de inglés, francés y alemán. Asimismo incluye, entre sus actividades formativas, la enseñanza de la lengua cooficial correspondiente a los funcionarios de la Administración General del Estado destinados en las comunidades autónomas bilingües.
- Cursos selectivos para funcionarios en prácticas: tienen como finalidad primordial la adquisición de conocimientos en orden a la preparación específica, para el ejercicio de sus funciones, de los aspirantes que han superado las pruebas selectivas.

– Selección:

- El INAP, a través de la Comisión Permanente de Selección, es responsable de la gestión de los procesos selectivos de los funcionarios de los cuerpos y escalas adscritos al Ministerio de Hacienda y Administraciones Públicas.
- También presta apoyo administrativo y técnico a los tribunales de los cuerpos y escalas del subgrupo A1.

– Estudios, publicaciones e investigación:

- El INAP dispone de una biblioteca especializada en Ciencia de la Administración y Derecho Público. Cuenta con más de 230.000 volúmenes y publicaciones periódicas. Posee, además, un fondo antiguo que integra más de 9.000 obras de los últimos cinco siglos.
- El INAP, desde su creación, mantiene una importante actividad editorial en sus materias de referencia y ha publicado más de 700 obras. Todas ellas se encuentran digitalizadas y disponibles para el público.
- Actualmente, el INAP publica las siguientes revistas: *Revista de Estudios de la Administración Local y Autonómica* (REALA), *Gestión y Análisis de Políticas Públicas* (GAPP), *Documentación Administrativa* (DA) y *Cuadernos de Derecho Público* (CDP)
- La actividad investigadora del INAP se realiza a través de la constitución de grupos de investigación, la convocatoria de premios y becas de formación y la realización de jornadas y seminarios de debate.

– Relaciones internacionales:

- El INAP desarrolla una amplia actividad de relaciones internacionales a través de la formación de empleados públicos extranjeros –principalmente iberoamericanos– en colaboración con otras instituciones, la participación en organizaciones y organismos internacionales especializados en el campo de la Administración Pública y las relaciones bilaterales con escuelas e institutos de formación extranjeros.

La formación ofrecida por el INAP en materia de seguridad de las tecnologías de la información y comunicaciones cuenta con la colaboración del Centro Criptológico Nacional (CCN-CNI). Tal colaboración fue formalizada

por convenio, suscrito el 5 de julio de 2011, entre la Secretaría de Estado para la Función Pública, el Centro Criptológico Nacional y el INAP.

Federación Española de Municipios y Provincias

La Federación Española de Municipios y Provincias (FEMP) es la asociación de entidades locales de ámbito estatal con mayor implantación, que agrupa ayuntamientos, diputaciones, consejos y cabildos insulares, en total 7.324, que representan más del 90% de los Gobiernos locales españoles.

Constituida al amparo de lo dispuesto en la disposición adicional quinta de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local, fue declarada como asociación de utilidad pública mediante acuerdo de Consejo de Ministros de 26 de junio de 1985.

La Subdirección de Formación de la Dirección General de Estudios y Formación es la encargada de la elaboración del Plan de Formación Continua.

El Plan de Formación Continua que la FEMP elabora cada año está dirigido fundamentalmente al personal de las corporaciones locales, con una clara intención de formar en cuestiones muy especializadas y que tengan impacto directo en el futuro del municipalismo. Las necesidades formativas se detectan como una actividad más de las comisiones sectoriales que trabajan en la FEMP y a partir de las novedades normativas y legislativas que se van produciendo. Asimismo están alineadas con el plan estratégico de la organización.

El objetivo del Plan es «la modernización y el desarrollo en la Administración local y por lo tanto la mejora en los servicios proporcionados a los ciudadanos, mediante el aumento de la cualificación y la mejora de las competencias de los empleados públicos locales».

Todos los empleados públicos locales pueden tener acceso a los cursos del Plan FEMP, con independencia de su relación laboral o el nivel de su puesto. Los cursos de formación continua son completamente gratuitos y el criterio de selección principal de los asistentes es la relación entre sus funciones y el perfil definido para el curso.

La FEMP cuenta además con una plataforma *online* para su actividad formativa en la página http://www.goblonet.es/formacion.

Centro Criptológico Nacional

El Centro Criptológico Nacional (CCN) es un organismo, adscrito al Centro Nacional de Inteligencia (CNI), creado en el año 2004 con el fin de garantizar la seguridad TIC en las diferentes entidades de la Administración Pública, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada.

Su ámbito de competencia está definido por el siguiente marco normativo:

- Ley 11/2002, 6 de mayo, Reguladora del Centro Nacional de Inteligencia (CNI), que incluye al Centro Criptológico Nacional (CCN) y que tiene entre otras misiones actuar contra el *ciberespionaje*, neutralizando las actividades de contrainteligencia y la seguridad de los sistemas de información del país, y protegiendo el patrimonio tecnológico de España.
- Real Decreto 421/2004, 12 de marzo, que regula y define el ámbito y funciones del Centro Criptológico Nacional (CCN).
- Orden del Ministerio de la Presidencia PRE/2740/2007, de 19 de septiembre, que regula el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, y que confiere al CCN la capacidad de actuar como organismo de certificación (OC) de dicho Esquema.
- Real Decreto 03/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad, en el que se establecen los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte del CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos. Así mismo, en sus artículos 36 y 37 articula en torno al CCN-CERT la capacidad de respuesta ante incidentes en las Administraciones Públicas.
- Comisión Delegada del Gobierno para Asuntos de Inteligencia, que define anualmente los objetivos del CNI mediante la Directiva de Inteligencia, que marca la actividad del Centro.

Desde su creación en el año 2004, el Centro Criptológico Nacional ha ido adecuándose y, en la medida de lo posible, adelantándose a una realidad cambiante en donde las *ciberamenazas* se incrementan día a día, varían (en función de la motivación de los atacantes o sus objetivos), se modifican los métodos de ataque, aparecen nuevas vulnerabilidades o se renuevan los dispositivos de los usuarios, los servicios ofrecidos a través de Internet o la tecnología empleada.

En esta evolución constante, y a medida que las amenazas y los riesgos cobran mayor importancia y alcanzan una mayor repercusión en todas las capas de la sociedad, la creación de la Capacidad de Respuesta a Incidentes, CCN-CERT, (y sus múltiples servicios orientados a una defensa preventiva frente a los *ciberataques* a las Administraciones Públicas y empresas estratégicas) y del Organismo de Certificación (OC) son la respuesta más importante en los últimos años al desafío planteado.

Dentro de esta actualización constante, y en virtud de las funciones asignadas al CCN, en los últimos diez años se han ido elaborando normas,

instrucciones, guías y recomendaciones para mejorar el grado de *ciberseguridad* en España. De este modo, a finales del año 2012 existían 223 documentos enmarcados en la serie CCN-STIC, con normas, procedimientos y directrices técnicas para optimizar la seguridad de las tecnologías de la información en nuestro país. De ellas, 73 se han elaborado o actualizado en los dos últimos años y abarcan todo tipo de aspectos de la seguridad, siendo algunas de difusión limitada para el personal de la Administración Pública y empresas estratégicas, y otras de difusión abierta para todos los usuarios que accedan al portal del CCN-CERT (www.ccn-cert.cni.es). Entre estas, se encuentran toda la serie CCN-STIC 800, elaboradas en colaboración con el Ministerio de Hacienda y Administraciones Públicas, de desarrollo del Real Decreto 3/2010, de 8 de enero, *por el que se regula el Esquema Nacional de Seguridad.* También son públicas las guías de la herramienta PILAR (versión 5.2 de 2012) y las destinadas a la seguridad de los dispositivos móviles (iPhone, Android o iPad).

Todos los documentos de la serie CCN-STIC son actualizados periódicamente y enviados a más de 300 organismos diferentes de la Administración (aparte de contar todos ellos con acceso a la parte privada del portal del CCN-CERT donde se encuentran).

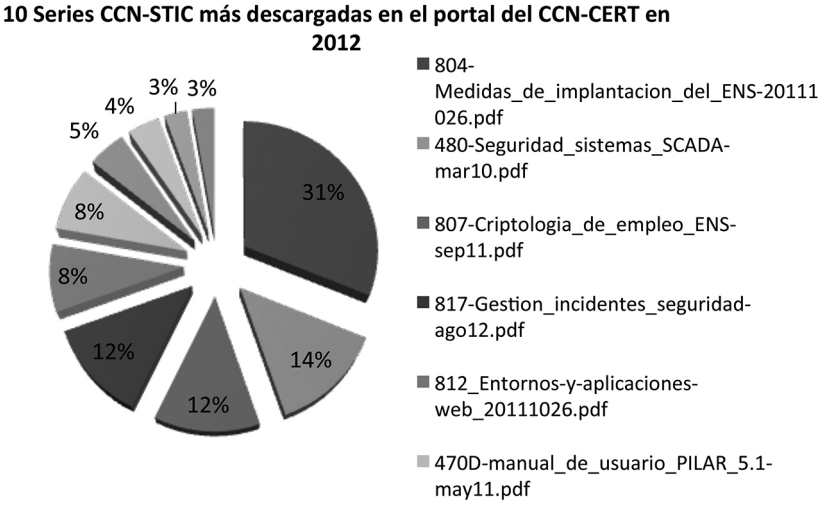

Figura 3.8. Los diez documentos de la serie CCN-STIC más descargados en el portal del CCN en 2012.

Disponer de personal cualificado en todos los niveles de la Administración (dirección, gestión e implantación) es considerado por el CCN un aspecto fundamental para proteger los sistemas de las *ciberamenazas*. De ahí que una de las funciones principales a lo largo de sus casi diez años de historia haya sido formar al personal de la Administración a través de

un amplio programa, en el que se incluyen los cursos STIC (presenciales, a distancia y *online*), jornadas de sensibilización, participación en ponencias y mesas redondas, etc.

Evolución de la oferta formativa del CCN

	2008	2009	2010	2011	2012	TOTAL
Alumnos	380	450	510	500	500	2.340
Cursos presenciales	17	18	17	14	14	80
Horas lectivas	1.200	1.400	1.200	900	900	5.600
Cursos *online*	-	1	3	5	6	15
Jornadas de sensibilización	2	4	3	6	7	22
Participación en mesas redondas/jornadas	8	10	15	15	40	88

Contenido de la oferta formativa del CCN en 2011-2012

- Cursos informativos y de concienciación en seguridad.
  - IX Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) (con fase *online*).
- Cursos básicos de seguridad.
  - VII Curso Básico STIC - Infraestructura de Red.
  - VII Curso Básico STIC - Base de Datos.
- Cursos específicos de gestión de seguridad.
  - IV Curso *Common Criteria*.
  - IX Curso de Gestión STIC - Implantación del ENS (fase *online*).
  - XXIII Curso de Especialidades Criptológicas (fase por correspondencia).
- Cursos de especialización en seguridad.
  - VII Curso STIC - Seguridad en Redes Inalámbricas.
  - I Curso STIC - Seguridad en Dispositivos Móviles (nuevo en 2012).
  - IV Curso STIC - Seguridad en Aplicaciones Web.
  - VIII Curso STIC - Cortafuegos.
  - VIII Curso STIC - Detección de Intrusos.
  - IX Curso Acreditación STIC - Entornos Windows.
  - V Curso STIC - Búsqueda de Evidencias.
  - VII Curso STIC - Inspecciones de Seguridad.
  - III Curso STIC - Herramienta PILAR (fase *online*).

Todos estos cursos están accesibles en la parte privada del portal del CCN-CERT (www.ccn-cert.cni.es).

Además, en estos dos últimos años, el Centro Criptológico Nacional ha ido ampliando su oferta formativa, adaptándose a las necesidades de muchos usuarios y facilitando, a través de un método de *e-learning*, algunos de sus cursos más demandados. De esta forma, a finales de 2012, estaban disponibles en el portal del CCN-CERT los siguientes cursos:

- Curso de Seguridad de las Tecnologías de la Información y las Comunicaciones STIC.
- Curso PILAR (Manejo de herramienta / Funciones más usadas).
- Curso Básico de Seguridad. Entorno Windows.
- Curso Básico de Seguridad. Entorno Linux.
- Curso del Esquema Nacional de Seguridad (acceso público).
- Curso de Análisis y Gestión de Riesgos de los Sistemas de Información (acceso público).

En apenas tres años desde la puesta en funcionamiento del primero de los cursos, se ha conseguido un total de 1.887 alumnos y más de 30.000 accesos al apartado del portal web.

Evolución de los cursos on-line (www.ccn-cert.cni.es)

Mes	2010	2011	2012	TOTAL
Número de accesos a los cursos *online*	5.430	13.876	11.735	30.681
Número de alumnos inscritos	891	1.511	1.887	4.289

Bibliografía

1. ISO Guide 73. *Risk management: Vocabulary.* 2009.
2. LAVELL, Allan. *Sobre la gestión del riesgo: apuntes hacía una Definición.* [En línea] http://www.bvsde.paho.org/bvsacd/cd29/riesgo-apuntes.pdf.
3. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. MAGERIT, versión 3.0. *Metodología de análisis y gestión de riesgos de los sistemas de información.* Secretaría General Técnica, Ministerio de Hacienda y Administraciones Públicas, 2012. NIPO: 630-12-171-8.
4. KEIPI, Juhani, MORA CASTRO, Sergio y BASTIDAS, Pedro. *Gestión de riesgo derivado de amenazas naturales en proyectos de desarrollo.* Banco Interamericano de Desarrollo, 2005.
5. NIST SP 800-30. *Risk Management Guide for Information Technology Systems.*
6. Centro Criptológico Nacional. *CCN-CERT. Informe. Ciberamenazas 2012 y tendencias 2013.* Mayo de 2013. www.ccn-cert.cni.es. CCN-CERT IA 09/13.

7. Guía CCN-STIC 301. *Requisitos de seguridad de las TIC.*
8. FIPS 200. *Minimum Security Requirements for Federal Information and Information Systems.* Marzo de 2006.
9. Guía CCN-STIC 400. *Manual de seguridad de las tecnologías de la información y comunicaciones.*
10. Guía CCN-STIC 402. *Organización y gestión para la seguridad de los sistemas TIC.*
11. 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.*
12. Guía CCN-STIC 805. *ENS. Política de seguridad.*
13. Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
14. Real Decreto 1720/2007, de 21 de diciembre, *por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*
15. Decisión del Consejo 2001/264/CE, de 19 de marzo de 2001, *por la que se adoptan las normas de seguridad del Consejo.*
16. Guía CCN-STIC 803. *ENS. Valoración de los Sistemas.*
17. Real Decreto 1671/2009, de 6 de septiembre, *de desarrollo parcial de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.*
18. OECD. *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.* París: s. n., 2002.
19. UNE - ISO/IEC 27002:2005. *Código de buenas prácticas para la gestión de la seguridad de la información.*
20. UNE - ISO/IEC 27001:2007. *Especificaciones para los sistemas de gestión de la seguridad de la información.*
21. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
22. Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
23. Real Decreto 1553/2005, de 23 de diciembre, *por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.*
24. Guía CCN-STIC 804. *ENS. Guía de implantación.*
25. Guía CCN-STIC 806. *ENS. Plan de adecuación.*
26. Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público.
27. Guía CCN-STIC 201. *Estructura de seguridad.*
28. Guía CCN-STIC 801. *ENS. Responsables y funciones.*
29. NIST SP 800-12. *An Introduction to Computer Security: The NIST Handbook.*
30. Orden Ministerial 76/2002, de 18 de abril, *por la que se establece la política de seguridad para la protección de la información del Ministerio*

de Defensa almacenada, procesada o transmitida por sistemas de información y telecomunicaciones. BOE de 29 de abril de 2002.

31. Guía CCN-STIC 807. *ENS. Inspección de las medidas de seguridad.*
32. Guía CCN-STIC 815. *Métricas e indicadores en el ENS.*
33. Guía CCN-STIC 814. *Seguridad en correo electrónico.*
34. ESN. *Estrategia de Seguridad Nacional 2013. Un proyecto compartido.* Mayo de 2013.
35. NIST SP 800-100. *Information Security Handbook: A Guide for Managers.*
36. NIST SP 800-53. *Recommended Security Controls for Federal Information Systems and Organizations.*