CAPÍTULO SEXTO

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD. CIBERTERRORISMO

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD. CIBERTERRORISMO

POR JAVIER CANDAU ROMERO

RESUMEN

Los ciberataques son muy rentables en términos de esfuerzo necesario para su ejecución, riesgos que se asumen y beneficios económicos o políticos que se pueden obtener y afecta transversalmente tanto al sector público, al sector privado como a los ciudadanos. Todas las naciones de nuestro entorno están desarrollando iniciativas para intentar controlar las amenazas que vienen del ciberespacio. La mayoría de ellas está apostando por concentrar y fortalecer las capacidades técnicas y de coordinación actuando especialmente sobre la respuesta a incidentes de seguridad. Se analizan las estrategias nacionales más relevantes.

En España las responsabilidades en el ciberespacio están muy fragmentadas en diferentes organismos que abordan el problema de forma parcial. Es necesario por tanto impulsar actuaciones en este sentido fortaleciendo las capacidades de respuesta ante incidentes y de inteligencia ante este tipo de amenazas. La dotación presupuestaria se considera crítica si se quieren llevar a cabo las líneas de acción que se plantean como posibles soluciones para reducir la amenaza. La aproximación debe ser a todos los niveles; el sector público, la industria, los ciudadanos y los aliados internacionales.

Palabras clave: Seguridad, ciberespacio, tecnologías, información, comunicaciones, amenaza, estrategia nacional, ataques, redes, internet, ciberseguridad, ciberataque, ciberdefensa, ciberterrorismo, ciberespionaje incidente, infraestructura crítica, SCADA.

NATIONAL CYBERSECURITY STRATEGIES. CYBERTERRORISM

ABSTRACT

Cyberattacks are very profitable in terms of the efforts needed for their performance, the risks assumed and the political or economic profits that might be achieved, and they affect transversely both the public and private sectors, as well as the citizens. All neighbouring nations are developing initiatives to try to monitor the threats coming from the cyberspace. Most of them are placing particular emphasis on focussing on and strengthening the coordination and technical capabilities, acting particularly on the response to security incidents. The most outstanding national strategies are analysed.

In Spain, cyberspace liabilities are highly compartmentalized among different bodies that tackle the problem partially. Thus, it is necessary to foster actions in this sense by strengthening the response capabilities in case of incident and the intelligence capabilities vis-à-vis this kind of threats. The budget allocation is considered critical to follow the lines of action presented as possible solutions to reduce the threat. Involvement should be made at all levels: public sector, industry, citizens and international allies.

Key words: Security, cyberspace, technology, information, communications, threats, national strategy, attacks, networks, Internet, cyber security, cyber attack, cyber defense, cyber terrorism, cyber espionage, incident, critical infrastructure, SCADA.

INTRODUCCIÓN

En los últimos años se ha detectado un incremento constante de vulnerabilidades y amenazas sobre los sistemas y tecnologías de la información y comunicaciones. Estas amenazas, que no tienen por qué ser deliberadas (los errores y omisiones del personal autorizado y bienintencionado pero desconocedor de buenas prácticas de seguridad también lo son), evolucionan continuamente y representan un verdadero desafío para los responsables de proporcionar servicios electrónicos.

En el caso de las amenazas voluntarias, el reto es aún mayor si tenemos en cuenta que aquellos que intentan infiltrarse o explotar nuestros

sistemas emplean recursos mejores y más sofisticados. Además, en la actualidad los ataques se pueden llevar a cabo desde cualquier parte del mundo y, en muchos casos, las posibilidades de descubrir su origen, e incluso su presencia, son muy remotas por lo que es necesario un esfuerzo de todos para intentar abordar este problema.

Con el desarrollo de las tecnologías de comunicaciones, se ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios han eliminado las barreras de distancia y tiempo. En el nuevo espacio relacional –el ciberespacio–, se han diluido las fronteras nacionales y, a la vez, se ha producido un considerable aumento de las posibilidades pero también de las amenazas, acrecentadas éstas por el constante crecimiento de la dependencia cibernética de las sociedades avanzadas.

Este hecho se agrava con la excesiva uniformidad de los medios empleados (tcp/ip, Windows, Web...) que facilitan la rentabilidad de la formación de los atacantes y el impacto global de la explotación de las vulnerabilidades y los fallos detectados. En definitiva la superficie de ataque es inmensa.

Por ello, ningún sistema, incluidos todos los de la Administración, está a salvo de sufrir un ataque de graves consecuencias como el robo, pérdida, destrucción o extracción de dispositivos de almacenamiento; destrucción o modificación de datos almacenados; redirección de Información para usos fraudulentos; interceptación de datos mientras se procesan, correo no deseado, etc.

Los ciberataques normalmente comparten las siguientes características comunes:

– **Bajo coste**. Muchas herramientas de ataque se pueden descargar de forma gratuita o con un coste muy bajo para el daño que pueden causar.
– **Fácil empleo**. Para muchos ataques no son necesarios grandes conocimientos técnicos. Existen herramientas con unos interfaces de usuario muy amigables y sencillas de usar.
– **Efectividad.** Existe una probabilidad muy alta de alcanzar los objetivos buscados con estos ataques por la ausencia de políticas de empleo o la limitación de recursos existentes en la parte defensiva debido a la falta de concienciación de las organizaciones gubernamentales, empresas y ciudadanos.
– **Bajo Riesgo para el atacante**. Es muy difícil atribuir un ataque con las herramientas de ocultación del origen existentes actualmente

en INTERNET y por la diferencia de legislaciones de los diferentes países.

Además, algunos de los siguientes factores tecnológicos incrementan la posibilidad de estos ataques:

– La complejidad creciente de la tecnología hace más difícil determinar el grado de seguridad de un determinado producto o sistema.
– La rapidez de la evolución tecnológica y las exigencias y competitividad del mercado ocasionan que, con frecuencia, se desplieguen productos con vulnerabilidades y fallos de seguridad que son aprovechados por los agresores.
– Existe un mayor riesgo en el caso de productos fabricados en países fuera de la órbita occidental, ya que es más difícil controlar la introducción de elementos inseguros.
– Hay una relativa falta de madurez de la industria de las tecnologías de la información y las comunicaciones, al no considerar la seguridad como un factor de diseño de los productos o sistemas.
– Se constata un constante incremento de la interconexión de todo tipo de sistemas utilizando Internet.

Existen evidencias de que determinados países tienen programas de capacitación técnica para lograr realizar ciberataques. En algunos casos, dicha capacitación técnica es considerada y abordada como una capacidad militar más con la que se plantean lograr la superioridad.

En un primer análisis sobre la situación global de la cibercriminalidad, puede afirmarse que las técnicas utilizadas son cada vez más depuradas y que existe una mayor interrelación entre los ciberdelincuentes de diversos países.

Muchos países han desarrollado o están desarrollando estrategias nacionales de Ciberdefensa con las que persiguen conseguir un ciberespacio más seguro mediante el intercambio de información de alertas, vulnerabilidades, amenazas y eventos; la mejora de las capacidades de contrainteligencia, la seguridad de sus productos y tecnologías, y la concienciación y formación de sus ciudadanos y servidores públicos en seguridad de sistemas de las Tecnologías de la Información y Comunicaciones (TIC).

Para ello, identifican los actores y responsabilidades presentes en un escenario de ciberseguridad, establecen unos principios comunes de actuación, proponen las líneas de acción para alcanzar como nación las

capacidades necesarias de ciberdefensa y crean las estructuras de decisión y coordinación y los flujos de información necesarios para coordinar la prevención y respuesta ante los ciberataques.

Finalmente, en la mayoría de ellas impulsan el desarrollo de los sistemas de alerta y prevención adecuados que les permitan disponer de una visión de conjunto sobre este problema.

En España, durante los últimos 10 años se han desarrollado iniciativas parciales (criterios de seguridad, conservación y normalización, Centro Criptológico Nacional, infraestructuras críticas, Instituto Nacional de Tecnologías de Comunicación o esquema nacional de seguridad) que se pasarán a describir con las que se intenta mitigar el riesgo de recibir cualquier tipo de ataque procedente de este nuevo tipo de amenaza.

AGENTES DE LA AMENAZA

Los posibles agentes que podrían realizar alguna acción dañina en el ciberespacio son:

– los Estados,
– los grupos extremistas, tanto ideológicos como políticos,
– el crimen organizado y
– las actuaciones delictivas individuales (se tratarán en otro capítulo de este cuaderno).

Estos agentes pueden tener múltiples motivaciones y finalidades: inteligencia, espionaje industrial, propiedad intelectual, motivos políticos, extremismos, motivaciones económicas, etc. Especialmente, los Estados pueden actuar a través de sus servicios de inteligencia, sus unidades cibernéticas de fuerzas armadas, manipulando grupos extremistas afines o contratando mercenarios. Los grupos extremistas ideológicos y políticos se manifiestan normalmente en lo que conocemos por ciberterrorismo.

Destacamos las siguientes manifestaciones, por su impacto en el ciberespacio actual:

– **Crimen Organizado.** Estas organizaciones realizan actividades relacionadas con el robo de información de tarjetas de crédito o de los certificados digitales asociados, con el fraude telemático asociado a operaciones bancarias o a cualquier transacción desde Internet, con el blanqueo de dinero y con el robo de identidades asociado a inmigración ilegal.

- **Espionaje industrial.** Son compañías o gobiernos que tienen interés en disponer de información crítica de desarrollos tecnológicos e industriales de industrias de la competencia.
- **Hacking Político / Patriótico.** Este tipo de actividad recogida abundantemente en prensa es el reflejo de un conflicto regional, étnico, religioso o cultural en el ciberespacio. Así son frecuentes los ataques de denegación de servicio entre China y Japón; Azerbaiyán y Turquía; India y Pakistán, chiitas y sunitas o el conflicto entre árabes e israelíes. Normalmente no tiene un gran impacto en los sistemas de información del País o área que recibe el ataque pues la actividad normalmente se limita a ataques realizados contra servicios Web y no alcanza los sistemas internos.
- **Servicios de Inteligencia.** Se considera el principal vector de amenaza contra la información sensible o clasificada manejada por los sistemas de información gubernamentales y de empresas nacionales de sectores estratégicos (y especialmente aquellas relacionadas con Defensa). Disponen de medios y recursos técnicos y una gran capacidad de acción. Sus actividades son muy prolongadas en el tiempo y el tipo de herramientas que utilizan normalmente muestran unos niveles muy bajos de detección en los sistemas de seguridad de los sistemas objetivos.
- **Unidades cibernéticas de Fuerzas Armadas.** Pueden ser un vector de amenaza crítico sobre todo en tiempo de crisis o conflicto. Muchas naciones disponen de esta capacidad sólo en los servicios de inteligencia aunque en otras, las FFAA,s disponen de unidades que tienen asignadas misiones de ataque a los sistemas de información de los adversarios. Estas unidades son la evolución de las capacidades de inteligencia de señales (SIGINT) disponibles en las FFAA,s de muchos países.
- **Terrorismo.** Los grupos terroristas emplean el ciberespacio como una herramienta más para realizar sus actividades delictivas. Normalmente lo emplean para establecer comunicaciones entre sus células y grupos de apoyo, para obtener información de posibles objetivos, para realizar acciones de propaganda o para obtener financiación a sus actividades.

Algunos de estos agentes suelen contratar capacidades técnicas de ataque disponibles en el mercado negro ofertadas por hackers y organizaciones criminales si no disponen de la capacidad tecnológica necesaria y podrían, en su caso, manipular usuarios internos para disponer de

la información o las credenciales necesarias con las que acceder a los sistemas de información objetivos desde dentro.

En muchas publicaciones se han clasificado estos agentes de la amenaza en 3 grandes grupos, el ciberespionaje, el ciberterrorismo y el cibercrimen. Se trataran brevemente en este capítulo los dos primeros.

Ciberterrorismo

Para que una actividad sea calificada de terrorismo se requiere que sus autores pertenezcan, actúen o colaboren con bandas armadas, organizaciones o grupos cuya finalidad sea la de subvertir el orden constitucional o alterar gravemente la paz pública, mediante la comisión de delitos de estragos, incendios, atenten contra las personas, o recolecten fondos.

Existe mucho debate doctrinal sobre si un terrorista puede realizar acciones violentas que produzcan efectos catastróficos y pánico empleando únicamente ciberataques. No obstante el ciberterrorismo se puede definir como el realizado por medios cibernéticos. Aunque esta definición no solo se extiende al objetivo último de estos grupos sino al empleo de Internet para conseguir los mismos.

Por ello, actualmente las actividades del terrorismo nacional e internacional en el ciberespacio se ciñen principalmente a lo especificado en el apartado anterior y su capacidad de realizar ciberataques a sistemas conectados a Internet es considerada limitada por lo que no parece probable que realice ataques a gran escala sobre los mismos. El impacto de estos ataques sería muy limitado en alcance tanto si el objetivo es la propia red de Internet como si lo son los sistemas conectados a esta red.

Sobre sistemas conectados a Internet y como se tratará posteriormente se destaca que los sistemas de control industrial (SCADA) podrían ser vulnerables a ataques de alcance limitado pero que podrían a llegar a ser críticos puntualmente. El impacto podría ser grave si alcanzan a interrumpir la funcionalidad principal de estos sistemas. En algunos casos el nivel real de interconexión entre el sistema de control industrial (que deberían estar aceptablemente aislado) es muy elevado y podrían ser alcanzados por un atacante (ya se ciberterrorista como otro agente de la amenaza). Además, el impacto en la confianza en los sistemas que produciría un ataque de este tipo, aunque fuera de muy pequeña escala sería muy alto si tiene el eco de los medios de comunicación.

De todas formas, dado el nivel tecnológico que se atribuyen a estos grupos, el ataque con medios tradicionales (explosivos improvisados, ataques suicidas…) se considera mucho más probable que el empleo de herramientas complejas de ciberataques.

Por otro lado, con la rápida evolución de la amenaza, el riesgo de un ciberataque terrorista tiene una tendencia leve a incrementarse y además, podrían actuar otros actores (que se describirán posteriormente) utilizando la cobertura del terrorismo tanto nacional como internacional para ejecutar estas actividades.

Además la actividad terrorista internacional emplea INTERNET como una herramienta más que le ayuda a cumplir sus objetivos. Existen importantes foros como el GIMF (1) que desde hace algunos años realizan actividades de propaganda para el terrorismo internacional. Desde estos y otras páginas Web se lanza el mensaje yihadista. Además, se está utilizando cada vez más asiduamente las redes sociales como Facebook (2) o Twitter (3), u otras redes de distribución de contenidos (Youtube (4)) para mandar sus mensajes de propaganda.

Las capacidades antiterroristas de los gobiernos tratan de limitar las posibilidades de estos grupos de realizar propaganda por Internet intentando clausurar las páginas Web que albergan contenidos que atentan contra la seguridad de las naciones. Ante estas acciones las páginas Web relacionadas directamente con este tipo de actividad migran a alojamientos muchos más robustos a acciones de cierre legal de su actividad. Por las diferencias en el tratamiento de estos delitos en las regulaciones nacionales y por la ausencia de una legislación internacional unificada en esta materia es posible la supervivencia de páginas Web vinculadas directa o indirectamente a organizaciones terroristas.

Otra actividad relevante del terrorismo internacional es la utilización de Internet para realizar acciones de propaganda (publicación de ficheros de audio, video y texto). En esta actividad, además de los mensajes

(1) Global Islamic Media Front (GIMF). Foro de propaganda de radicalismo islámico. www.globaljihad.net/

(2) Facebook. Se creó en 2004, en la actualidad esta red social cuenta con más de 500 millones de usuarios activos. www.facebook.com

(3) Twiter. Se creó en 2006, en la actualidad esta red social cuenta con más de 100 millones de usuarios activos. Se basa en mensajes de texto de 140 caracteres tipo SMS. www.twiter.com

(4) Youtube. Red de descarga de contenidos. www.youtube.com

tradicionales, los ciberterroristas están alerta ante cualquier difamación del Islam y sus símbolos para montar campañas de propaganda incitando a luchar por el orgullo y las creencias maltratadas. Esta actividad se ha reflejado en prensa en los movimientos ante la quema de ejemplares del Corán o la publicación de artículos que difamaban al profeta (5). En esta actividad se pueden encuadrar las numerosas acciones de suplantación de páginas Web y ataques de denegación de servicio en países donde se han realizado afrentas graves a las creencias islámicas.

El objetivo final de esta actividad es conseguir la radicalización del numeroso grupo de jóvenes musulmanes que ya utilizan Internet como medio de relación fundamental.

Se detectan numerosos sitios en Internet que tienen como objetivo apoyar el proceso de radicalización de algunos jóvenes. En estas páginas se encuentra la información necesaria para la formación ideológica y el refuerzo de la misma. Así, en las redes sociales esta actividad se incrementa notablemente. Por tanto, ahora miso es muy difícil diferenciar las actividades de propaganda de las de reclutamiento y radicalización que si se encontrarían fuera de la ley.

En determinadas circunstancias, estas actividades de propaganda o reclutamiento podrían incitar a la realización de actividades de desestabilización promoviendo manifestaciones violentas y actividades ilícitas por lo que su seguimiento por los organismos encargados se hace crucial en los diversos gobiernos.

Otro aspecto a considerar es la obtención de información a través de Internet de posibles objetivos y sus localizaciones especialmente centrada en organizaciones y personas susceptibles de ser atacadas por estos grupos. Con la cantidad de información que las organizaciones y los particulares publican en sus páginas Web, Blogs o redes sociales la obtención de información previa para realizar cualquier tipo de actividad terrorista se facilita enormemente. En el proceso de planeamiento los reconocimientos sobre el terreno se agilizan también por la información que publican aplicaciones como Google Maps (6) y sus nuevos servicios de fotografía satélite y fotografía de itinerario desde el punto de vista de un transeúnte en las diferentes localidades que disponen de este servicio.

---

(5) Caso de quema del Corán. Septiembre 2010. Ha sido recogida en muchos medios. Fecha de consulta 27 de octubre de 2010. www.abc.es/20100909/internacional/islam-clama-contra-quema-20100909.html

(6) www.google.es/map/

Por otro lado la obtención de financiación, aunque posible, es, hasta el momento, muy limitada en alcance aunque se sigue esperando que el ciberterrorismo realice actividades similares a las del crimen organizado (cibercrimen) para obtener una financiación adicional que soporte su actividad fundamental.

Otra actividad para la que se puede utilizar Internet por grupos terroristas es la de formación de sus integrantes y grupos de apoyo, aunque, hasta ahora la red se emplea más en tareas de archivo y almacenamiento de información que en tareas de instrucción on line pues, la necesidad de realizar prácticas e interactuar con los alumnos no está cubierta en esta modalidad de formación.

También destaca el empleo de Internet para establecer comunicaciones de una manera cifrada (mediante el empleo de aplicaciones del tipo PGP (7) o Truecrypt (8)) o enmascarada (empleo de herramientas de esteganografía que ocultan información en otros ficheros soporte) en otras comunicaciones legítimas. Todos los países han establecido regulaciones de interceptación legal de las comunicaciones que cubren tanto los medios tradicionales (telefonía móvil o fija) como el envío de datos a través de Internet. Los terroristas son conscientes de la vulnerabilidad de sus medios de comunicación y realizan acciones para intentar proteger estos.

De todas formas la agilidad y versatilidad que les permite Internet hace que para gran cantidad de sus comunicaciones sea empleado como medio principal, evitándose su uso solo para las que consideran de una criticidad muy elevada por ser acciones que están próximas a ejecutarse.

> *En conclusión, la posibilidad de combinar ataques físicos a infraestructuras de Internet con ataques cibernéticos complejos es poco probable por el nivel tecnológico del ciberterrorismo pero el empleo de Internet para actividades de propaganda, reclutamiento y comunicaciones se ha incrementado por los nuevos servicios que están a disposición como las redes sociales. También es de destacar la obtención de información a través de esta red.*

(7) Pretty Good Privacy (PGP o GnPG en su versión en Linux). Programa popular de cifrado. www.pgp.com

(8) TrueCrypt. Programa de cifrado. www.truecrypt.org

Ciberespionaje

Los ciberataques más sofisticados se esperan de los servicios de inteligencia y las agencias de operaciones de información militares extranjeras. En la mayoría de los casos, estos atacantes disponen de muchos recursos, tienen la paciencia necesaria para encontrar la debilidad del sistema y durante la explotación del ataque intentan lograr la mayor persistencia en el mismo instalando puertas traseras en previsión de una posible detección del mismo.

El objetivo de estos ataques es el mismo que la actividad de inteligencia que lo soporta, adquirir ventaja política, económica, comercial o militar con la información adquirida en los sistemas atacados.

Todos los estados del primer mundo que soportan sus actividades en sistemas de información y que necesitan la interconexión con Internet para alcanzar mayores cotas de eficiencia son susceptibles de recibir este tipo de ataques que intentan alcanzar la información clasificada o sensible, información privada de alto valor o secretos industriales.

Muchos Estados han declarado públicamente que el ciberataque puede ser empleado como una herramienta más de sus estrategias de inteligencia o militares. En este sentido su objetivo final es tanto la exfiltración de información del enemigo como la inutilización o destrucción de los sistemas enemigos tanto para evitar el mando y control de sus fuerzas como para causar daños en sus servicios esenciales y en su población.

La constatación clara de esta realidad es que en los últimos años se han detectado numerosos intentos de agresión, muchos de ellos exitosos, sobre sistemas sensibles de diferentes naciones en el ámbito de la UE y la OTAN. Como ejemplo algunas naciones como Estados Unidos, Reino Unido, Alemania o Francia han declarado públicamente haber recibido ataques muy graves con impactos serios sobre la información sensible manejada en los sistemas de sus respectivos gobiernos. Seguramente muchos otros gobiernos y empresas han recibido ataques similares que no se han hecho públicos.

Por ello se cree imprescindible la protección de estos sistemas contra ciberataques interesados en la información manejada por los mismos. Esta protección debe preservar tanto la confidencialidad de esta información como la disponibilidad e integridad de ésta. Una de las ac-

tividades críticas a realizar por las diferentes administraciones es incrementar las actividades de monitorización, detección y eliminación de estas agresiones que normalmente requiere un incremento notable en los presupuestos asignados a seguridad.

Asimismo se deben regular las salvaguardas a implementar según el nivel de la información manejada por los sistemas para que el perímetro de protección de todos los sistemas de la administración sea homogéneo y la dificultad a la que se enfrente el atacante sea similar independientemente del organismo al que ataque.

Se deben realizar las mismas actividades en los sistemas de empresas que se consideren estratégicas pues el nivel de amenaza es similar.

En conclusión, el ciberespacio ha reducido la dificultad de entrar en el juego del espionaje y el crecimiento de Internet incrementa la superficie de actuación, por ello, la posibilidad de recibir ataques procedente de otros estados intentando adquirir información sensible o clasificada de su gobierno, información de sus empresas estratégicas es quizás el riesgo más elevado al que se enfrentan las naciones.

INFRAESTRUCTURAS CRÍTICAS

Desde hace una década la seguridad de las infraestructuras críticas vienen ocupando la agenda de los responsables políticos en todo el mundo como un aspecto estratégico para garantizar la propia seguridad de nuestros países y nuestros ciudadanos.

Las Infraestructuras críticas, según se definen en el borrador de legislación pendiente de publicación (9) es el conjunto de recursos, servicios, tecnologías de la información y redes, que en el caso de sufrir un ataque, causarían gran impacto en la seguridad, tanto física como económica, de los ciudadanos o en el buen funcionamiento del Gobierno de la Nación.

Este impacto se mide según unos criterios horizontales que determinan la criticidad de una infraestructura. Se han establecido tres:

1. el **número potencial de víctimas** mortales o de lesiones graves que pueda producir;

(9) Borrador de legislación por el que se establecen medidas para la protección de las infraestructuras críticas. www.cnpic.es. Fecha de consulta 15 de junio de 2010 (estuvo disponible durante 1 mes).

2. el **impacto económico** en función de la magnitud de las pérdidas económicas y/o el deterioro de productos o servicios, incluido el posible impacto medioambiental;
3. el **impacto público**, por la incidencia en la confianza de la población, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

Las infraestructuras críticas se agrupan en 12 sectores entre los que se incluyen la Administración, el sector aeroespacial, el sector energético, el de la industria, el nuclear, el de la industria química, las instalaciones de investigación, el de agua, el de la salud, el de transporte, el de alimentación, el financiero y tributario y el de las tecnologías de la información y comunicaciones (10).

Centro Nacional de Protección de Infraestructuras Críticas

La Secretaría de Estado de Seguridad (SES), es el órgano responsable de la dirección, coordinación y supervisión de la protección de infraestructuras críticas (PIC) nacionales, de la creación del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC (11)), como órgano director y coordinador de dichas actividades, y de la determinación, clasificación y actualización del Catálogo de Infraestructuras críticas, de acuerdo con lo dispuesto en el acuerdo de Consejo de Ministros de 2 de noviembre de 2007.

El CNPIC desde su creación ha centrado sus esfuerzos en la elaboración de este catálogo y en el desarrollo de una ley (y normativa asociada) que defina de forma más clara su funcionamiento y con el que se pretende impulsar un importante conjunto de medidas, tanto organizativas como de protección, que reforzarán la eficacia de la coordinación y la cooperación entre todas las Administraciones y las diferentes entidades, organismos gestores o propietarios de infraestructuras que prestan servicios públicos esenciales para la sociedad.

Las funciones principales del CNPIC son las de coordinar la información y la normativa; convertirse en el punto de contacto permanente con los gestores, tanto públicos como privados, de las infraestructuras críti-

(10) Anexo borrador de legislación Protección de infraestructuras críticas: sectores estratégicos y ministerios / organismos del sistema competentes en su protección.
(11) Centro Nacional de Protección de Infraestructuras Críticas (CNPIC). http://www.cnpic-es.es/

cas; dirigir y coordinar los análisis de riesgos; establecer los contenidos mínimos de los planes de seguridad de operador (PSO) y de los planes de protección específicos (PPE) de las infraestructuras críticas; establecer un sistema de mando y control y actuar como punto de contacto con centros similares en todo el mundo.

La normativa que se está desarrollando tiene como objetivos principales dirigir y coordinar las actuaciones en materia de protección de Infraestructuras Críticas, previa identificación y designación de las mismas, impulsando, además, la colaboración e implicación de los organismos propietarios de dichas infraestructuras a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo.

Catálogo de Infraestructuras Críticas

Este catálogo está clasificado de SECRETO, registra las infraestructuras consideradas como críticas y que, en su caso, requieren de especiales medidas de protección. Actualmente existen unas 3.700 infraestructuras críticas, de las que el 80% de ellas pertenecen al sector privado. Asociado a cada infraestructura, esta base de datos especifica las medidas de protección, los planes de reacción y la criticidad de la misma.

Es la herramienta fundamental de trabajo pues además de almacenar toda la información sobre la infraestructura establece el punto de enlace con los operadores, fuerzas y cuerpos de seguridad del Estado (FCSE) y cualquier otro representante del sistema de protección de infraestructuras críticas. Permite la actualización continua y facilita el proceso de la evaluación de la criticidad y del nivel de seguridad de las infraestructuras evaluadas por el CNPIC.

Plan de Protección de Infraestructuras Críticas

Cualquier estrategia de seguridad en estas infraestructuras debe tener como uno de sus elementos centrales prevenir posibles ataques, disminuir la vulnerabilidad y, en el caso de que se produjeran situaciones de crisis que afectaran a las infraestructuras esenciales, minimizar los daños y el periodo de recuperación.

Según el borrador de legislación esta estrategia es el Plan Nacional de Protección de Infraestructuras Críticas en el que se establecen los criterios y las directrices precisas para movilizar las capacidades operativas de las Administraciones Públicas y para articular las medidas preventivas

necesarias, con el fin de asegurar la protección permanente, actualizada y homogénea del sistema de infraestructuras estratégicas frente a las amenazas provenientes de ataques deliberados contra ellas.

Además establece que se articulen unos planes estratégicos sectoriales basados en un análisis general de riesgos que contemple las vulnerabilidades y amenazas potenciales, tanto de carácter físico como lógico, que afecten a cada sector.

A partir de estos planes, cada operador debe articular los planes de Seguridad del Operador (PSO) y los planes de protección específicos (PPE) de sus infraestructuras críticas que asociado al análisis de riesgos de la instalación o sistema, establecerán la adopción de medidas permanentes de protección y de medidas temporales y graduadas, en razón a la amenaza específica que se detecte en cada momento (tanto físicas como de carácter lógico).

La elaboración de esta documentación se encuentra actualmente en su fase inicial y será necesaria una mayor publicación de esta normativa de desarrollo para poder definir de una forma clara los requisitos mínimos de seguridad que deben cumplir las mismas.

Ciberataques en las Infraestructuras Críticas

El borrador de legislación se centra especialmente en contemplar, evitar o minimizar los ataques físicos a las infraestructuras críticas; la única referencia disponible en el borrador a ciberataques es la plasmada en la realización del análisis de riesgos y en la redacción de los planes de protección específicos de las infraestructuras críticas donde se contemplan las amenazas lógicas.

Será necesario un desarrollo del mismo donde se contemplen con mayor detalle las amenazas y vulnerabilidades de estas infraestructuras relacionadas con el ciberespacio pues en la actualidad todas las consideraciones de detalle están centradas en ataques físicos (en su mayoría de carácter terrorista) sobre las mismas.

En otros países se contempla con mucha mayor profundidad la posibilidad de estos ataques identificándolos como un asunto crítico a tratar.

Los ciberataques se plantean con especial criticidad en el sector de Tecnologías de Información y Comunicaciones y en los sistemas de in-

formación y comunicaciones que soportan otros sectores estratégicos como los de la Administración y los sistemas SCADA (Supervisory Control And Data Acquisition, Sistemas de Control de Procesos. Ver glosario).

Sistemas SCADA

En muchos de los sectores estratégicos nombrados, para supervisar y mantener el control de las infraestructuras se utilizan sistemas de control, llamados comúnmente SCADA.

Así, con los sistemas SCADA se controlan los procesos de fábricas químicas, redes eléctricas, centrales de generación eléctrica, industrias de petróleo y gas, tratamiento de agua y residuos e industrias farmacéuticas entre otros.

Hasta hace poco, el relativo desconocimiento de este tipo de sistemas reducía al mínimo sus riesgos de seguridad. No obstante, ya en 2005 se anunció la primera vulnerabilidad de un sistema de control, generando un gran debate acerca de la divulgación de dicha información. Desde entonces, el interés en los sistemas de control industrial ha crecido exponencialmente, en parte como consecuencia de la conexión de éstos con redes de comunicaciones públicas (Internet) y por la incorporación de tecnologías comerciales (equipos de comunicaciones o sistemas operativos entre otros) para maximizar la rentabilidad de las inversiones.

En 2008 aparecieron los primeros programas diseñados para explotar las vulnerabilidades de los sistemas de control industrial. En 2009 y 2010 se han detectado ataques a estos sistemas.

El riesgo principal de estos sistemas es el desconocimiento por parte del propietario de las interconexiones reales de los sistemas SCADA, la ausencia de buenas prácticas de seguridad como la realización de actualizaciones periódicas o una adecuada gestión de las contraseñas y las deficiencias en la configuración de los diferentes dispositivos que proporcionan muchas posibilidades de realizar acciones remotas que permiten el control de los mismos.

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD EN OTROS PAÍSES

En este apartado se van a analizar algunas estrategias de seguridad publicadas oficialmente siempre desde el punto de vista defensivo. Es-

tos documentos, en sus versiones públicas, no tratan el aspecto ofensivo del ciberespacio y no se analizarán en este apartado.

Se presentan las aproximaciones de las naciones que han presentado públicamente las soluciones para abordar este problema.

Estados Unidos

Las dimensiones y estructuras creadas en Estados Unidos no son comparables a las del resto de los países.

Tras los ataques del 11 de septiembre de 2001 se impulsaron las estrategias de una defensa territorial más activa y coordinada que finaliza en la creación de un Departamento de Seguridad del Territorio Nacional (12) (noviembre de 2002). Asimismo se desarrolla una amplia legislación relacionada con la ciberseguridad y la protección de infraestructuras críticas.

La estrategia de Seguridad Nacional en el Ciberespacio (13) de febrero 2003 asigna la responsabilidad de la protección al DHS y reconoce que debe ser un esfuerzo coordinado de los gobiernos federal, estatal y local, del sector privado y de los ciudadanos. Establece 5 líneas estratégicas prioritarias a las que asigna responsables y acciones de detalle a realizar para alcanzarlas:

1. **Sistema de respuesta nacional de seguridad en el ciberespacio**. Para ello propone diversas acciones, entre las que destacan, la mejora de la gestión de incidentes, ampliar el sistema de alerta ante ciberataques, realizar ejercicios de coordinación o mejorar el intercambio de información público-privado.
2. **Programa de reducción de amenazas y vulnerabilidades**. Para ello propone diversas acciones, entre las que destacan, la mejora de las capacidades de las fuerzas de seguridad (FBI (14) y otras agencias policiales, la mejora del control de los sistemas SCADA o profundizar en el conocimiento sobre amenazas y vulnerabilidades.
3. **Formación y concienciación en el ciberespacio**. Este programa estaba preparado para cinco tipos de audiencias; ciudadanos y pequeñas empresas, empresas consideradas estratégicas (especialmente las que gestionan infraestructuras críticas), universida-

(12) Department of Homeland Security (DHS) www.dhs.gov
(13) The National Strategy to Secure Cyberspace. White House. www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf
(14) Federal Bureau of Investigation. (FBI). www.fbi.gov

des y centros de investigación (especialmente los que dispongan de gran capacidad de cálculo), sector privado (especialmente el que disponga de sistemas SCADA) y gobiernos locales y estatales.

4. **Asegurar el ciberespacio gubernamental**. Las acciones a realizar en el gobierno federal fueron el seguimiento de la evolución de las amenazas y vulnerabilidades y la implementación de las mejoras de seguridad adaptadas a estas, el impulso de la alianza nacional para asegurar la información (NIAP) (15), la mejora de la seguridad de las redes sin cables, la mejora de los requisitos de seguridad en la subcontratación y en las adquisiciones y la mejora en la realización de los procesos de auditoría o inspección. Además se debe impulsar la seguridad en los gobiernos locales y estatales.
5. **Cooperación nacional e internacional.** Como líneas de actuación destacan el refuerzo de las actividades de contrainteligencia, la mejora de las capacidades de prevención y atribución de un ataque y la coordinación entre las diferentes agencias. Internacionalmente se intentará mejorar los canales de comunicación y que se adopten en las legislaciones nacionales los acuerdos sobre cibercrimen.

La estrategia de Seguridad Nacional en el Ciberespacio de 2003 asigna responsabilidades que descansan en su mayoría en el DHS y dispone de un completo anexo con las acciones recomendadas para cada línea estratégica.

Para el desarrollo de esta estrategia, dentro del DHS, se impulsa el US-CERT (16) que proporciona apoyo en la respuesta ante ciberataques contra la parte civil del gobierno federal (.gov) y tendrá la responsabilidad de relacionarse con los gobiernos locales, estatales y la industria.

Destaca que el DHS tiene además, la misión de protección de infraestructuras críticas nacionales definida en el acta de 2002 (17).

En el ámbito del Ministerio de Defensa (DoD) (18) existen muchas iniciativas tanto de los tres ejércitos como de las agencias de inteligencia que tienen misiones en la protección de las redes sensibles y clasificadas

(15) National Information Assurance Partnership (NIAP). Iniciativa para evaluar las tecnologías de información entre el Nacional Institute of Standards and Technology (NIST) y la National Security Agency (NSA).

(16) US-CERT. http://www.us-cert.gov/

(17) Critical Infrastructure Information Act of 2002. http://www.dhs.gov/xlibrary/assets/CCI_Act.pdf

(18) Department of Defense (DoD) www.dod.gov

como la Agencia de Seguridad Nacional (NSA) (19). Esta agencia tiene un departamento encargado del aseguramiento de la información (NSA-IAD (20)) que se focaliza en el análisis permanente de nuevas amenazas y vulnerabilidades, en el desarrollo de guías, productos y soluciones de seguridad, en el desarrollo de productos de cifra y gestión de claves de los mismos y en la formación y concienciación de seguridad.

El DoD financia el CERT-CC (21) que tiene como una de sus misiones principales establecer un foro de coordinación entre CERT,s nacionales. Esta operado por la Universidad Carnegie Mellon) y su misión principal es la relación con otros CERT,s (especialmente gubernamentales) para intercambiar información y colaborar ante incidentes de seguridad.

Con el presidente Obama se han reforzado las iniciativas en ciberseguridad. Con su llegada y tras un periodo de revisión de 60 días, la Casa Blanca (22) en mayo de 2009 publicó la revisión de la política en el ciberespacio (23) en la que demanda una visión de conjunto y reconoce que debido a la disparidad de misiones de las diferentes agencias, el gobierno federal no se encuentra preparado para este desafío. Por ello la estrategia nacional se debe orientar a mejorar la resistencia ante ciberataques y a reducir la ciberamenaza. En el documento se establecen 10 acciones urgentes a ejecutar inmediatamente.

1. Nombramiento de un responsable de ciberseguridad nacional que coordine todas las políticas y actividades de las diferentes agencias. Se crea una oficina dependiente del consejo de seguridad Nacional (NSC) que le apoyará en estas tareas.
2. Actualizar y aprobar una nueva estrategia que asegure las infraestructuras de comunicaciones nacionales.
3. Designar la ciberseguridad como una de las prioridades del Presidente.
4. Designar un responsable de privacidad y libertades públicas en el NSC.
5. Desarrollar los mecanismos de coordinación entre las diferentes agencias y establecer claramente las responsabilidades de éstas.

(19) National Security Agency (NSA) www.nsa.gov
(20) National Security Agency. Information Assurance Directorate (IAD).
(21) CERT-CC. Centro de coordinación de CERT. Establecido en la Universidad Carnegie Mellon en 1988. www.cert.org
(22) White House. www.whitehouse.gov/administration/eop/nsc/cybersecurity
(23) Cyberspace Policy Review. www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

6. Realizar campañas nacionales de concienciación y formación.
7. Mayor implicación del gobierno de los Estados Unidos en la regulación internacional de la ciberseguridad que permita una mayor colaboración internacional.
8. Preparar un plan de respuesta ante incidentes de seguridad.
9. Potenciar las capacidades de investigación y desarrollo en este campo.
10. Asegurar la privacidad y las libertades civiles.

El objetivo último de estas acciones a corto plazo es conseguir una visión de conjunto y coordinar las acciones de los diferentes actores. Además, propone otras 14 acciones para el medio plazo entre las que destacan las de mejora de los recursos humanos y técnicos disponibles en el gobierno federal, la coordinación entre agencias y los controles en el presupuesto para alcanzar los objetivos marcados.

Para conseguir la plena consecución de los objetivos marcados, se refuerza la Iniciativa global sobre ciberseguridad nacional (CNCI) (24) elaborada por el Presidente Bush en enero de 2008 (clasificada en su momento) que establece los siguientes 3 objetivos estratégicos para conseguir un ciberespacio más seguro:

– **Establecer una línea de defensa contra todas las amenazas actuales.** Para ello se debe mejorar el intercambio de información de alertas, vulnerabilidades amenazas y eventos que se detecten en el gobierno federal, en el resto de gobiernos estatales y locales y en el sector privado que permitan actuar rápidamente para reducir estas y prevenir las intrusiones.
– **Defenderse contra todo el espectro de amenazas.** Por ello se deben mejorar las capacidades de contrainteligencia e incrementar la seguridad en las cadenas logísticas y en los productos y tecnologías desde su fase de diseño.
– **Fortalecer el entorno futuro de ciberseguridad.** Para ello se deben extender la formación y concienciación en seguridad, coordinar y dirigir los esfuerzos de investigación y desarrollar estrategias que disuadan la actividad hostil en el ciberespacio.

(24) Comprehensive National Cybersecurity Initiative (CNCI) lanzada por el Presidente George W. Bush en la «National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23)» en enero de 2008. http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

Esta aproximación está dotada de los fondos necesarios para que las fuerzas de seguridad y las comunidades de inteligencia y defensa mejoren funciones críticas como la recolección, proceso y análisis de información. El responsable de ciberseguridad nacional debe supervisar que se ejecuten las siguientes iniciativas:

1. **Gestión de las redes del gobierno federal como una red única** con conexiones seguras a Internet. Asigna esta responsabilidad al DHS y al GAO (25).
2. **Finalizar el despliegue de un sistema de sensores de detección de intrusos en toda la red del gobierno federal (EINSTEIN 2)**. Son sensores pasivos que utilizan tecnologías de detección basadas en firmas. Es operado por el US-CERT (DHS). Este sistema permite detectar cualquier actividad dañina y mejora el conocimiento de las vulnerabilidades de la red corporativa. Se ha realizado un estudio sobre el impacto en la privacidad de los datos del sistema (26).
3. **Iniciar el despliegue de un sistema Prevención de intrusos (EINSTEIN 3).** Es una mejora del sistema anterior con la capacidad de actuación en tiempo real sobre el tráfico dañino. Se colaborará con la NSA (según lo previsto en la ley) para realizar la monitorización de contenidos si es necesario y además ésta proporcionará nuevos patrones de ataque desarrollados dentro de sus misiones de recolección de información y de aseguramiento de la información. Ya existe un piloto basado en tecnología aportada por esta agencia.
4. **Coordinar y redirigir los esfuerzos de investigación y desarrollo**. Se desean eliminar redundancias y se crearán estructuras que coordinen y prioricen las inversiones tanto para sistemas clasificados como no clasificados.
5. **Interconexión de centros de operaciones de seguridad** para mejorar el intercambio de información y la visión de conjunto de las amenazas que se produzcan. Se asigna esta misión al Centro de Operaciones de Ciberseguridad (NCSC) (27) del DHS que integrará la información de los 6 centros que proporcionan actualmente este servicio.

---

(25) Government Accountability Office (GAO). www.gao.gov

(26) Privacy Impact Assessment for EINSTEIN 2. US-CERT. 19 de mayo 2008. www.dhs.gov/

(27) National Cybersecurity Center (NCSC).

6. **Desarrollar en todo el gobierno federal un plan de contrainteligencia cibernética.** Con esta acción se pretende detectar, disuadir y mitigar cualquier ataque realizado por los servicios de inteligencia extranjeros contra la información, los sistemas gubernamentales y los del sector privado.
7. **Aumento de seguridad de las redes clasificadas.** Estas redes manejan la información más sensible de la Administración para dirigir las operaciones de paz, las actividades diplomáticas, las actividades contraterroristas, las actividades de las FCSE o de inteligencia así como las actividades de seguridad interior.
8. **Extender la cibereducación**. Se detecta una falta de personal con las capacidades técnicas adecuadas en este campo. Los programas actuales se consideran limitados y faltos de visión global. Se considera que se deben impulsar estos perfiles al igual que en los años 50 se impulsaron los perfiles de ciencias y matemáticas.
9. **Definir y desarrollar nuevos programas, estrategias y tecnologías que refuercen la seguridad**.
10. **Definir y desarrollar nuevos programas y estrategias que refuercen la disuasión** desarrollando respuestas adecuadas ante amenazas estatales y no estatales.
11. **Desarrollar una aproximación global a la gestión de riesgos en la cadena logística de las tecnologías de información y comunicaciones**. Se requiere mayor concienciación de este problema y el desarrollo de una nueva política de adquisiciones que se adapte al nuevo mercado global de estas tecnologías intentando que se adapten a los estándares y buenas prácticas de referencia.
12. **Definir el papel del gobierno para mejorar la ciberseguridad en los sectores que manejan infraestructuras críticas**. Esta misión la tiene asignada el DHS pero se fuerza a realizar un programa con unos hitos tangibles a corto y medio plazo.

De la estrategia de ciberseguridad de 2003, la CNCI de 2008 y de la revisión de la política del ciberespacio de 2009 destaca el sentido práctico, al elevar el nivel tratamiento del problema desde el DHS a la Casa Blanca con el responsable designado al efecto y la decisión de coordinación de todos los esfuerzos nacionales.

En las 7 primeras propuestas de la CNCI se apuesta por alcanzar objetivos tangibles. Las dotaciones presupuestarias asignadas a la

misma reflejan la importancia de esta estrategia para el gobierno americano.

Además, en la revisión de 2009 se asigna una función más activa y operativa a las agencias de inteligencia, en especial a la NSA, por su conocimiento profundo de la ciberamenaza y las nuevas tendencias de ataque.

Reino Unido

La Estrategia de Ciberseguridad en el Reino Unido (28) fue publicada en junio de 2009 y tiene como objetivo asegurar las ventajas de este país en el ciberespacio mediante tres líneas estratégicas:

– Reducción del riesgo del uso del Ciberespacio por el Reino Unido actuando sobre la amenaza (disminuyendo su motivación y capacidad), sobre sus vulnerabilidades y sobre el impacto de cualquier ataque en los intereses nacionales.
– Aprovechar las oportunidades en el ciberespacio mediante la obtención de inteligencia que apoye las políticas nacionales y actué contra los adversarios.
– Incrementar las actividades de concienciación, desarrollar una doctrina sobre el ciberespacio y sus políticas derivadas y mejorar las capacidades humanas y técnicas.

El documento considera que al igual que en el siglo XIX para alcanzar la seguridad nacional se tuvieron que asegurar los mares y en el XX el aire, en el XXI se debe asegurar la ventaja en el ciberespacio y ése es el objetivo al que apunta esta estrategia.

Asimismo, implícitamente se considera que actualmente las misiones en este campo se encuentran dispersas en diversos organismos que no están coordinados entre sí. Así se pueden destacar los siguientes:

– La Oficina del Consejo de Ministros (29). En ella se encuentra la Secretaría de Seguridad Nacional así como otros organismos relacionados con ciberamenazas entre los que destaca el jefe de la información gubernamental.

(28) Cyber Security Strategy of the United Kingdom. June 2009. Cabinet Office. www.cabinetoffice.gov.uk
(29) Cabinet Office. www.cabinetoffice.gov.uk

– El Centro Nacional de Protección de Infraestructuras Críticas (CPNI)(30) que proporciona asesoramiento en seguridad a empresas y organizaciones que gestionan infraestructuras críticas. Este centro depende del Servicio de Seguridad Interior (MI5) (31) que actúa contra cualquier amenaza organizada contra la seguridad nacional.
– La agencia de inteligencia en las comunicaciones y de aseguramiento de la información (GCHQ (32) / CEGS(33)) con la misión de obtención de inteligencia de señales y de protección de las redes gubernamentales.
– El Ministerio del Interior (Home Office (34)) con la misión de luchar contra el uso del ciberespacio por parte de cualquier actividad criminal. Dispone de la oficina de seguridad y contraterrorismo que lucha específicamente contra el uso terrorista del ciberespacio.
– El Ministerio de Defensa (35) con misiones relacionadas con el uso militar del Ciberespacio.
– El Servicio de inteligencia (36) con la misión de proporcionar inteligencia exterior de fuentes humanas para defender la seguridad nacional y el bienestar económico del Reino Unido.
– La Policía Metropolitana (37) con sus unidades de cibercrimen.
– La Agencia del crimen organizado (SOCA) (38) para el uso del ciberespacio por parte del crimen organizado.

Por ello, se propone que se establezca un programa que afecte a todo el gobierno para alcanzar los objetivos estratégicos incrementando los fondos que desarrollen nuevas tecnologías para proteger las redes nacionales, incrementando la formación para conseguir personal con perfiles adaptados a esta actividad y trabajando coordinadamente con el sector público, la industria, los grupos de defensa de las libertades civiles, los ciudadanos y los aliados internacionales.

(30) Centre for the Protection of National Infrastructure (CPNI) www.cpni.gov.uk
(31) British Security Service(BSS-MI5) www.mi5.gov.uk
(32) Government Communications Head Quarter (GCHQ) www.gchq.gov.uk
(33) CEGS Communications-Electronics Security Group www.cegs.bov.uk. Creado en 1969.
(34) Home Office / Office for Security and Counter-Terrorism (OSCT) www.homeoffice.gov.uk
(35) Ministry of Defence www.mod.uk
(36) Secret Intelligence Service (SIS-MI6). www.sis.gov.uk
(37) Metropolitan Police www.met.police.uk
(38) Serious Organised Crime Agency (SOCA) www.soca.gov.uk

Asimismo, con la misión de coordinar todos los esfuerzos, se crean los siguientes organismos:

– Oficina de Ciberseguridad (OCS) (39) dentro de la Oficina del Consejo de Ministros encargada del desarrollo de esta estrategia que debe impulsar las acciones parciales de otros organismos. Su objetivo es proporcionar liderazgo y coherencia en la aplicación de la misma. Asimismo se fijan 8 líneas de acción. Esta oficina se ha unificado con la de Aseguramiento de la Información también existente en este organismo pasándose a denominarse OCSIA (40). El personal destinado es aportado por los diferentes organismos con responsabilidades en el ciberespacio.
– El Centro de operaciones en ciberseguridad (CSOC) (41) liderado por el GCHQ y ubicado en su sede institucional. Está constituido por las diferentes agencias con responsabilidades en este terreno con la misión de proporcionar el estado de alerta, analizar tendencias y mejorar la coordinación en la respuesta técnica ante ciberincidentes. De la actividad de este organismo se informará a un panel interdepartamental que se organizará en el CEGS que es la autoridad y el brazo ejecutor de las políticas de aseguramiento de la información (Information Assurance).

La dotación presupuestaria recibida asciende a 650 millones de libras en 4 años (42) en un momento en que se están anunciando los mayores recortes de inversiones desde la segunda guerra mundial.

> *De esta estrategia se destaca la importancia que se otorgan a las implicaciones de seguridad del ciberespacio, la voluntad del gobierno británico de coordinar los esfuerzos de sus diferentes agencias, y la determinación de invertir presupuesto para adquirir capacidades en un campo que considera estratégico para adquirir ventaja en futuros conflictos.*
>
> *La estructura y división de funciones en ciberseguridad existentes actualmente en el Reino Unido es en muchos casos similar a la existente en España.*

(39) Office of Cyber Security (OCS) www.cabinetoffice.gov.uk
(40) Office of Cyber Security and Information Assurance (OCSIA). www.cabinetoffice.gov.uk
(41) Cyber Security Operation Centre (CSOC).
(42) Anuncio del Nuevo presupuesto y de la estrategia Nacional de Ciberseguridad. http://direct.gov.uk/produc_consum_dg/groups/dg_digitalassets/

Canadá

La Estrategia de Ciberseguridad en Canadá (43) fue publicada en 2010 y resalta la importancia del ciberespacio para el modo de vida de los canadienses. Destaca la facilidad y efectividad de los ataques y señala como principales riesgos el ciberespionaje y las actividades militares de otros estados, el uso terrorista de Internet y el cibercrimen. Además resalta la continua evolución de las amenazas lo que requiere una defensa que se adapte a esta circunstancia.

La estrategia se basa en tres pilares:

– Securización de los sistemas gubernamentales. Para ello se deben articular las estructuras, herramientas y personal necesarios para cumplir este objetivo.
– Cooperación con los gobiernos provinciales y regionales y con el sector privado para apoyar iniciativas que mejoren la resistencia de los sistemas nacionales haciendo especial énfasis en las infraestructuras críticas.
– Ayudar a los canadienses a proteger sus actividades en el ciberespacio reforzando las capacidades contra el cibercrimen de las fuerzas de seguridad del Estado.

La estrategia resalta además, la necesidad de trabajar conjuntamente con la comunidad académica, las organizaciones no gubernamentales y el sector privado para intentar mejorar la seguridad de los sistemas canadiense.

Posteriormente la estrategia desarrolla los tres pilares. Se designa al Ministerio de seguridad pública de Canadá (44) y a su Centro de Respuesta ante Ciberincidentes (45) que debe continuar con la misión de monitorizar y apoyar a los diferentes organismos ante cualquier incidente de seguridad informático.

En apoyo de este organismo la Agencia de Seguridad de las Comunicaciones (46), el servicio de inteligencia (47), la policía montada (48), el

(43) Canada´s Cyber Security Strategy. www.publicsafety.gc.ca/prg/em/cbr/ccss-scc-eng.aspx
(44) Public safety Canada. www.publicsafety.gc.ca
(45) Canadian Cyber Incident Response Centre. www.publicsafety.gc.ca/prg/ccirc
(46) Communications Security Establishment. www.cse-cst.gc.ca
(47) Canadian Security Intelligence Service. www.csis-scrs.gc.ca
(48) Royal Canadian Mounted Police. www.rcmp-grc.gc.ca

secretariado del tesoro (49), el Ministerio de Asuntos Exteriores y tratados internacionales (50) y finalmente, el Departamento de Defensa Nacional y las Fuerzas Armadas Canadienses (51) le proporcionaran toda la información disponible sobre la amenaza.

Además se establece la necesidad de mejorar la arquitectura de seguridad de los sistemas gubernamentales y la reducción de las interconexiones con Internet. Se recuerda la necesidad de que los diferentes departamentos monitoricen y aseguren sus operaciones electrónicas como se establece en la política de seguridad publicada en 2009.

En el desarrollo del segundo y tercer pilar se dan ejemplos de la necesidad de cooperación y se alerta sobre los riesgos de los sistemas SCADA y se propone la realización de ejercicios para depurar la coordinación entre los diferentes gobiernos y compañías. Además se realizarán acciones que mejoren la cultura de seguridad de los canadienses y se creará el centro de fusión del cibercrimen con el que se espera mejorar la capacidad de la policía montada en este campo.

Esta estrategia destaca que la ciberseguridad es una responsabilidad compartida y para el desarrollo de los tres pilares es fundamental el trabajo coordinado. La implantación de esta estrategia tiene una asignación presupuestaria inicial de 90 millones de dólares en cinco años y 18 millones adicionales.

> *Canadá al igual que Estados Unidos, Reino Unido y Australia ha considerado crítica esta actividad publicando una estrategia que aborda el problema de forma global y concentrando las misiones en el Ministerio de seguridad pública. No define claramente los mecanismos de coordinación con el resto de organismos.*

Francia

La estrategia francesa sobre ciberseguridad la establece el libro blanco de la seguridad y Defensa Nacional (52) aprobado por el Presidente de la República en junio de 2008 donde se resalta que la ciberamenaza

(49) Treasury Board Secretariat. www.tbs-sct.gc.ca
(50) Foreign Affaire and International Trade Canada. www.international.gc.ca
(51) Department of National Defence. www.forces.gc.ca
(52) Livre blanc sur la défense et la sécurité nationale. www.livreblancdefenseetsecurite.gouv.fr/information

tiene una probabilidad muy alta de que se produzca y su impacto en las infraestructuras críticas y en los sistemas gubernamentales es considerado alto.

Este libro blanco contempla cinco funciones estratégicas que las fuerzas de defensa y seguridad francesas deben dominar que son: el conocimiento y la previsión (con la necesidad de mejora de las capacidades técnicas de las Agencias de Inteligencia), la prevención (con la necesidad de una defensa proactiva en profundidad que realice una vigilancia permanente), la disuasión, la protección y la respuesta.

Anteriormente a esta estrategia se había desarrollado un plan de mejora de la Seguridad de los Sistemas de Información del Estado (53) desde el 2004 al 2007.

En Francia la Secretaria General de la Seguridad y Defensa Nacional (54) dependiente del primer Ministro y recientemente reestructurada, es la encargada de tratar todos los asuntos de ciberdefensa y dentro de ésta en julio de 2009 se creó la Autoridad Nacional de Seguridad de los Sistemas de Información (ANSSI) (55) con las siguientes misiones:

- La detección y reacción urgente ante ciberataques mediante la vigilancia continua de las redes gubernamentales sensibles y la implementación de mecanismos de defensa en estas redes.
- El desarrollo de productos y servicios de confianza para su uso en los gobiernos y en los sectores críticos.
- Proporcionar asesoramiento de seguridad a organismos gubernamentales y operadores de infraestructuras críticas.
- Proporcionar información a empresa y ciudadanos sobre las nuevas amenazas a la seguridad de la información y el procedimiento de protección mediante una política activa de comunicación.

Entre los organismos subordinados destacan la subdirección de estrategia y reglamentación, el centro de formación y el centro operacional

(53) Consultar en Cuadernos Cátedra ISDEFE-UPM. Nº 6 Seguridad Nacional y Ciberdefensa. Octubre 2009. Anexo A. Punto 1.4.2.

(54) Secrétariat général de la défense et de la sécurité nationale SGDSN www.sgdsn.gouv.fr/

(55) Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n° 2009-834 du 7 juillet 2009 (Journal officiel du 8 juillet 2009). www.ssi.gouv.fr

de la seguridad de los sistemas de información (COSSI) (56), en disponibilidad permanente, que aglutina misiones de desarrollo de productos de cifra, realización de inspecciones y auditorías de seguridad a sistemas gubernamentales, realización de ejercicios que evalúen la seguridad, despliegue de sistemas de detección y, en caso de crisis, coordinación de la respuesta gubernamental.

En el COSSI se encuentra además el centro de expertos del gobierno en el tratamiento de ataques informáticos (CERTA) (57) creado en 1999 y que hacía las funciones de CERT gubernamental y los observatorios regionales de seguridad de los sistemas de información (OzSSI) (58) que facilitan la aplicación de buenas prácticas y mejoran la atención a los usuarios en todo el territorio.

> *Con la nueva orgánica de la SGDSN y la creación de la ANSII en 2009 en Francia se han centralizado todas las actividades críticas relacionadas con la ciberdefensa en busca de una respuesta más eficaz y operativa ante ciberataques. Asimismo la ANSII ha recibido una importante dotación presupuestaria.*

Alemania

No está disponible ninguna estrategia de ciberseguridad alemana. No obstante en 1990 se creó la Oficina federal de Seguridad de la Información (BSI) (59) dependiente del Ministerio Federal de Interior (BMI) (60). Anteriormente estas funciones las realizaba el servicio de inteligencia (BND) (61).

Las misiones del BSI son la de protección de las redes del gobierno federal (incluye el CERT-Bund, el centro de situación de las tecnologías de información, el centro de gestión de crisis y los sistemas de alerta temprana), el desarrollo de productos de cifra, el análisis de nuevas tecnologías, la seguridad de los productos software (SW) y la protección de infraestructuras críticas.

---

(56) Centre opérationnel de la sécurité des systèmes d'information (COSSI). www.ssi.gouv.fr

(57) CERTA Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques www.certa.ssi.gouv.fr/

(58) OzSSI Observatoires zonaux de la sécurité des systèmes d´information

(59) BSI www.bsi.bund.de

(60) BMI www.bmi.bund.de

(61) BND. www.bnd.bund.de

El BSI opera el CERT-Bund (62) como CERT gubernamental desde 2001 e impulsa una alianza de todos los equipos de respuesta ante incidentes alemanes denominada CERT-Verbund (63). Además el BSI soporta el CERT para ciudadanos y pequeñas y medianas empresas denominado Bürger-CERT (64).

También tienen misiones en la protección de infraestructuras críticas la Oficina Federal de protección civil y asistencia ante desastres (BBK (65)) y la agencia federal de policía criminal (BKA (66)).

En el BMI se ha organizado un grupo de trabajo interministerial de infraestructuras críticas (AG KRITIS (67)) que establece los escenarios de riesgo, realiza análisis de vulnerabilidades en sectores críticos, propone contramedidas y supervisa los sistemas de alerta temprana.

El Plan nacional de protección de infraestructuras de la información (68) se marca como objetivos la prevención (las actividades críticas son divulgar información sobre riesgos y posibilidades de protección o empleo de productos y sistemas confiables), la preparación (las actividades críticas son recolectar y analizar información y proporcionar alertas y avisos) y de reacción (mejorar las capacidades técnicas propias y desarrollar productos con tecnología nacional).

> *Aunque no dispone de estrategia de ciberseguridad publicada todas las misiones defensivas ante ciberataques se concentran en el BSI que dispone de varios equipos de respuesta ante incidentes para proporcionar este servicio. No se espera que se publique más normativa. Durante los últimos años se han incrementado sus recursos humanos y económicos para proporcionar nuevos servicios tanto a Administraciones Públicas y ciudadanos como a empresas que gestionan infraestructuras críticas.*

---

(62) CERT-Bund. www.bsi.bund.de/certbund/

(63) CERT.Verbund. www.cert-verbund.de/

(64) Bürger-CERT (2007). www.buerger-cert.de

(65) BBK. www.bbk.bund.de

(66) BKA. www.bka.bund.de

(67) No hay informes publicados sobre AG KRITIS. Se encuentra una versión en borrador (alemán) //userpage.fu-berlin.de/~bendrath/Kritis-12-1999.html.

(68) Federal Ministry of the Interior. «National Plan for Information Infrastructure Protection» (Berlin, 2005). www.bmi.bund.de/cln_012/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National__Plan__for__Information__Infrastructure_ Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.

Estonia

Este país dispone de una estrategia de seguridad publicada en mayo de 2008 (69). En la que se plantea como objetivo reducir las vulnerabilidades de su ciberespacio a través de la implementación de los planes nacionales específicos (entre 2008-2013) y de la colaboración internacional. Planea sobre el documento el ataque generalizado recibido en abril-mayo en 2007. El comité que desarrolló la estrategia, liderado por el Ministerio de Defensa contaba también con expertos del sector privado.

La misión de desarrollar esta estrategia es del Ministerio de Defensa en cooperación con el Ministerio de Educación e Investigación, el Ministerio de Justicia, el Ministerio de Economía, el Ministerio del Interior y el Ministerio de Asuntos Exteriores. No obstante el consejo de ciberseguridad supervisa estas actividades.

Los objetivos estratégicos a conseguir son:

– Aplicar de forma gradual un conjunto de medidas de seguridad. Este objetivo afecta a infraestructuras críticas (se fijan 10 sectores), Internet y sistemas SCADA. Se deben mejorar las capacidades de detección y respuesta ante incidentes así como la coordinación entre agencias nacionales.
– Desarrollar conocimiento técnico mediante el desarrollo de normativa que mejore la formación en seguridad, la realización de ejercicios y el impulso a iniciativas de investigación y desarrollo en ciberseguridad.
– Desarrollar el marco normativo y legal que soporte el empleo seguro de los sistemas de información y la protección de infraestructuras críticas.
– Promover la colaboración internacional para fortalecer la ciberseguridad de tal forma que se condenen los ciberataques por el daño que ocasionan a derechos humanos y a las libertades democráticas. Para ello se intentarán impulsar acuerdos internacionales contra ciberataques y cibercrimen.
– Concienciación en seguridad de la información a todos los niveles pero con especial atención a ciudadanos y pequeña y mediana empresa.

(69) Cyber Security Strategy for 2008–2013. Cyber Security Strategy Committee. Ministry of Defence. ESTONIA. Tallinn 2008. http://www.mod.gov.ee/en/national-defense-and-society

Para asegurar el cumplimiento de los objetivos se establecen plazos muy concretos para el desarrollo de los planes específicos y se ha creado un consejo de ciberseguridad dependiente del Comité de Seguridad del Gobierno de la República que informa del estado de cumplimiento mediante informes anuales.

> *Se han concentrado en el Ministerio de Defensa la responsabilidad de desarrollar esta estrategia aunque hay otros cinco ministerios involucrados y un consejo de ciberseguridad al más alto nivel que vigila su aplicación... Destaca el detalle de las medidas específicas a desarrollar para cumplir con los objetivos estratégicos y el plazo de cinco años para conseguirlos.*

Australia

Este país dispone de una estrategia de seguridad publicada el 23 de noviembre 2009 (70) como resultado de la revisión estratégica del gobierno electrónico realizada en 2008 y presentada por el Primer Ministro en el Parlamento en diciembre de 2008.

Esta estrategia se basa en unos principios básicos, unos objetivos y unas prioridades estratégicas.

Los principios básicos son:

– **Liderazgo nacional** para afrontar la escala y complejidad del desafío de la ciberseguridad.
– **Responsabilidad compartida** de todos los ciudadanos para mantener sus equipos seguros.
– **Colaboración** del sector público, el sector privado y de todos los ciudadanos.
– **Compromiso de colaboración internacional.** Debido a la naturaleza transnacional de Internet se requiere una acción global para conseguir un acuerdo en ciberseguridad.
– **Gestión de riesgos**. Al tener un ciberespacio interconectado, la vulnerabilidad de los sistemas ante ciberataques hace que una protección completa sea imposible. Por ello se debe realizar una aproximación basada en la gestión de riesgos para priorizar las actividades a realizar.
– **Protección de los valores y libertades fundamentales**. Se debe perseguir que las políticas en ciberseguridad sean respetuosas con estos valores individuales y colectivos.

(70) Cyber Security Strategy. www.ag.gov.au/cybersecurity.

Los objetivos del gobierno australiano con esta política de ciberseguridad son:

1. Que todos los australianos sean conscientes de los riesgos, aseguren sus equipos y protejan su privacidad, identidad y gestiones financieras en sus actividades on-line.
2. Que las compañías australianas operen de forma segura y que sus sistemas de información y comunicaciones protejan la integridad de sus operaciones y la identidad y privacidad de sus clientes.
3. Que el gobierno australiano asegure su información y que sus sistemas de información y comunicaciones sean seguros y resistentes.

Para conseguir estos objetivos, las prioridades estratégicas son:

– Mejorar la capacidad de detección, análisis y respuesta ante ciberataques sofisticados centrándose en sistemas gubernamentales, de infraestructuras críticas y otros de interés nacional.
– Concienciar y ayudar a los australianos proporcionando información y herramientas prácticas para su protección on-line (71).
– Colaborar con el sector privado para promover la seguridad y resistencia de sus infraestructuras, redes, productos y servicios (72).
– Implantar las mejores prácticas en los sistemas gubernamentales priorizando aquellos que proporcionen servicios on-line. Entre las medidas de desarrollo destaca el estudio para la reducción de los accesos a Internet y la colaboración activa con los gobiernos locales y regionales para que los requisitos de interconexión sean comunes.
– Promover un entorno electrónico seguro, resistente y de confianza que proteja los intereses nacionales.
– Mantener un marco legal y unas capacidades en las fuerzas de seguridad que permitan la persecución efectiva del cibercrimen.
– Promover el desarrollo de una comunidad de investigación en ciberseguridad que permita el desarrollo de soluciones innovadoras en este campo mediante la estrategia nacional de seguridad en ciencia e innovación.

Para abordar estas prioridades, la estrategia establece que se deben potenciar dos organizaciones, ya existentes, que deben alcanzar una capacidad operativa completa en 2010.

---

(71) www.staysmartonline.gov.au
(72) Foro de intercambio de información sobre infraestructuras críticas. www.tisn.gov.au

El primero de ellos es el CERT nacional (CERT Australia (73)) que pasa a depender de la Fiscalía General (74) y que unificará todas las capacidades en este campo en torno al anterior CERT gubernamental (GovCERT.au (75)). Será el que proporcione toda la información necesaria en ciberseguridad (en especial sobre amenazas y vulnerabilidades) a la comunidad nacional y actuará como punto de contacto para las relaciones internacionales. Deberá establecer canales seguros para el intercambio de información entre el sector público y privado y tendrá la misión de coordinar nacionalmente cualquier incidente de seguridad crítico.

El segundo de ellos es el Centro de Operaciones en Ciberseguridad (CSOC (76)) perteneciente a la agencia de inteligencia de señales (DSD (77)). Este centro reúne personal de diferentes agencias de seguridad. Dispone de un amplio conjunto de fuentes en todos los dominios; inteligencia, seguridad, fuerzas policiales, equipos de respuesta ante incidentes (nacionales y del sector privado) que le permiten disponer de una visión completa de los sistemas de información australianos. Coordina la respuesta ante incidentes complejos entre las diversas agencias del gobierno y proporciona el nivel de alerta nacional.

Además la estrategia involucra a los siguientes organismos que deben proporcionar toda la información necesaria a las dos organizaciones arriba apuntadas:

– El Departamento del Fiscal General que proporciona las políticas en ciberseguridad y contra el cibercrimen.
– La Autoridad Australiana de comunicación y medios (78) responsable de la regulación de las telecomunicaciones y canal de enlace con los proveedores de servicios para actuar contra amenazas como el spam, el robo de identidades o la infecciones de ordenadores.

(73) CERT Australia. www.cert.gov.au

(74) Attorney-General's Department. www.ag.gov.au/. Agencia que lidera la política de ciberseguridad para todo el gobierno australiano. Preside el comité de coordinación y políticas en ciberseguridad (Cyber Security Policy and Coordination (CSPC) Committee) que es el comité interdepartamental encargado de coordinar el desarrollo de las políticas de ciberseguridad.

(75) Australian Government Computer Emergency Readiness Team (GovCERT.au). www.cert.gov.au.

(76) Cyber Security Operations Centre (CSOC).

(77) Defence Signals Directorate (DSD). www.dsd.gov.au/

(78) Australian Communications and Media Authority (ACMA). www.acma.gov.au

– La Policía federal australiana (79) que está encargada de todos los crímenes tecnológicos complejos y que coordina en este campo a todas las fuerzas policiales australianas y se relaciona con los organismos internacionales en este campo.
– Las Agencias de inteligencia y seguridad (80) que según las funciones establecidas en su ley (81) de 1979 debe, entre otras misiones, investigar los ataques electrónicos con propósitos de espionaje, sabotaje o terrorismo; recolectar inteligencia sobre ciberataques contra sistemas del gobierno e infraestructuras críticas o proporcionar la correspondiente evaluación de la amenaza en este campo.
– La agencia de inteligencia de señales (DSD) que según las funciones establecidas en su ley (82) es la autoridad nacional de seguridad para los sistemas de información gubernamentales proporcionando consejo y orientación en las mejores prácticas de seguridad (mantiene el manual de seguridad de los sistemas de Información y Comunicaciones gubernamentales y proporciona productos de cifra certificados) y, a través del CSOC, es responsable de los servicios ya enumerados en éste.
– El departamento de economía digital y comunicaciones (83) responsable de potenciar el empleo de la economía digital alineando las iniciativas privadas de ciberseguridad con las gubernamentales.
– La Oficina de gestión de información del Gobierno en el departamento de economía (84).

En mayo de 2008 se ha realizado una asignación presupuestaria de 125,8 millones de dólares en cuatro años para incrementar la seguridad en el plan de seguridad cibernética (www.dbcde.gov.au) para la protección contra delitos de cibercrimen. En el presupuesto de 2009 se ha realizado una asignación presupuestaria de 100 millones de dólares (dentro de los 685 dedicados a seguridad nacional) (85) para impulsar los obje-

(79) Australian Federal Police **(**AFP). www.afp.gov.au
(80) Australian Security Intelligence Organisation**'s** (ASIO). www.asio.gov.au
(81) *Australian Security Intelligence Organisation Act 1979*
(82) *Intelligence Services Act 2001.* www.dsd.gov.au/
(83) Department of Broadband, Communications and the Digital Economy (DBCDE). www.dbcde.gov.au/
(84) Department of Finance and Deregulation's Australian Government Information Management Office (AGIMO). www.finance.gov.au/agimo/
(85) Información sobre el presupuesto (fecha consulta 11.10.2010) www.ag.gov.au/www/agd/agd.nsf/Page/Publications_Budgets_Budget2009_MediaReleases_StrengtheningOurNationalSecurity.htm

tivos y prioridades marcados en la estrategia como la concentración de todas las capacidades de CERT (dotado con 8,8 millones).

> *Esta estrategia nacional considera la ciberseguridad una de las prioridades nacionales, marca unos objetivos y prioridades a conseguir y reforma las responsabilidades nacionales concentrando en la Fiscalía general (CERT Australia) y en la agencia de inteligencia de señales (CSOC) los esfuerzos de protección activa contra ciberataques.*
>
> *La estrategia está acompañada de una importante dotación presupuestaria y el resto de departamento tiene la obligación de colaborar y apoyar con todos los medios necesarios en su consecución.*

Organizaciones Internacionales

La organización y actividades de OTAN y UE se han tratado en otros capítulos de este cuaderno.

En la UE resalta el dictamen del Comité Económico y Social Europeo sobre «Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia» (86) que propone un plan de acción basado en 5 pilares; preparación y prevención, detección y respuesta (mecanismos de alerta temprana), mitigación y recuperación, cooperación internacional e identificación de infraestructuras críticas.

En este documento la UE exhorta a las naciones a la creación de equipos de respuesta ante incidentes nacionales y su adhesión al grupo de CERT gubernamentales europeos (EGC (87)).

Conclusiones

Del análisis de estas estrategias se extraen las siguientes conclusiones:

– Se realiza una aproximación global al problema tratando de forma conjunta todos los niveles sobre los que se debe actuar en ciberdefensa:
  • Gobiernos centrales, regionales y locales.
  • Infraestructuras críticas
  • Fuerzas y cuerpos de seguridad del Estado
  • Ciudadanos

(86) [COM(2009) 149 FINAL] (2010/C 255/18) Dictamen. C/255 de 22.09.2010.
(87) European Government CERT http://www.egc-group.org/

– Se reconoce que es un problema emergente, que el escenario es incierto, que es una de las prioridades para la seguridad nacional y como tal, se debe abordar.
– En las naciones analizadas, se centralizan las responsabilidades en ciberdefensa en uno o dos organismos o en un una oficina de coordinación cuya dependencia es del presidente o primer ministro o, en su caso, se fortalece de forma explícita la posición de los organismos a los que se asigna esta misión.
– Se potencian las capacidades de monitorización y alerta temprana, se concentran y se fortalecen los equipos de respuesta ante incidentes (especialmente las gubernamentales) por considerarlos los mejor posicionados para resolver el problema de las nuevas amenazas de forma más eficiente.
– Se impulsan esquemas nacionales de seguridad (requisitos de seguridad mínimos a implantar en las redes gubernamentales) y se intentan disminuir las interconexiones con Internet.
– Se priorizan y fortalecen las capacidades de inteligencia por el mejor conocimiento que poseen de la amenaza con el objetivo de hacer frente a ataques complejos.
– Se declara como necesidad estratégica la formación y concienciación de servidores públicos, empresas y ciudadanos. Se presentan diversas soluciones para conseguir este objetivo.
– Se impulsan las actividades de investigación e innovación en este campo mediante alianzas con Universidades y centros de investigación.
– Se proporciona una dotación presupuestaria para la implantación de las estrategias con la vocación política de mantenerla en el tiempo.

ESPAÑA. RESPONSABILIDADES EN EL CIBERESPACIO

Tras el análisis de las soluciones propuestas por los diferentes países y como distribuyen las responsabilidades en el ciberespacio. Se analizan éstas en los siguientes organismos:

– Ministerio de Industria, Turismo y Comercio (88).
– Ministerio del Interior(89).
  • Secretaría de Estado de Seguridad. CNPIC (90).

(88) Ministerio de Industria Turismo y Comercio. www.mityc.es
(89) Ministerio del Interior. www.mir.es/
(90) Centro Nacional de Protección de Infraestructuras Críticas (CNPIC). www.cnpic-es.es/

  - Unidades de investigación tecnológica de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).
- Ministerio de Política Territorial y Administración Pública (91).
  - Consejo Superior de Administración Electrónica (CSAE (92)).
- Centro Nacional de Inteligencia (93)
  - Autoridad Nacional de Seguridad Delegada (94)
  - Centro Criptológico Nacional (95)
- Ministerio de Defensa (96).
  - Dirección General de Infraestructuras
  - Estado Mayor de la Defensa
  - Cuartes Generales de Tierra, Armada y Aire.

Ministerio de Industria Turismo y Comercio

Este Ministerio a través de su Secretaría de Estado de Telecomunicaciones y Sociedad de la Información tiene entre otras misiones, la de relacionarse con los operadores de telecomunicaciones, la gestión de nombres del dominio.***es***, la capacidad de dictar normas sobre interceptación legal de comunicaciones y el desarrollo de la sociedad de la información con el plan Avanza (impulsa el empleo de las tecnologías de información en la sociedad). En el RD (97) que define su estructura básica se referencia alguna misión genérica en seguridad de la información.

Dispone de organismos con responsabilidades en desarrollo de sociedad de la información como Red.es (98) y en seguridad, accesibilidad y calidad como INTECO (99) que a su vez disponen de sendos equipos de respuesta ante incidentes que se describirán posteriormente.

---

(91) Ministerio de la Política Territorial y Administración Pública. www.mpt.es
(92) Consejo Superior de Administración electrónica (CSAE). www.csae.map.es/
(93) Centro Nacional de Inteligencia (CNI). www.cni.es
(94) Autoridad Nacional de Seguridad Delegada (ANS-D). Ver funciones en página Web CNI. www.cni.es
(95) Centro Criptológico Nacional (CCN). www.ccn.cni.es
(96) Ministerio de Defensa. www.mde.es/
(97) RD 1620/2010 el que se regula su estructura básica del MITYC. www.mityc.es
(98) RED.ES. Empresa pública empresarial adscrita al M. Industria, Turismo y Comercio a través de la Secretaria de Estado de Telecomunicaciones y Sociedad de la Información que tiene por misión impulsar la sociedad en red en España. www.red.es
(99) Instituto Nacional de Tecnologías de la Comunicación (INTECO). www.inteco.es

Ministerio del Interior

La Secretaria de Estado de Seguridad es el organismo en este ministerio con competencias en el ciberespacio a través del CNPIC y de las unidades encargadas de la ciberdelincuencia en las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

El CNPIC tiene responsabilidades en la protección de estas infraestructuras con las salvedades especificadas en el borrador de legislación que se encuentra en elaboración (Protección Civil, MINISDEF, FCSE, Aviación Civil, Consejo de Seguridad Nuclear y funciones del CNI que se complementarán con este centro). Tiene la responsabilidad de custodiar, mantener y actualizar el Plan Nacional de Protección de Infraestructuras Críticas y el Catálogo Nacional de Infraestructuras Estratégicas.

El CCN-CERT (100) colabora con el CNPIC en el tratamiento de los ciberataques sobre infraestructuras críticas y en la actualización de información sobre vulnerabilidades SCADA e incidentes de seguridad informáticos relacionados con infraestructuras críticas. Se debe esperar a la aprobación de su legislación y la elaboración de normativa de detalle para definir responsabilidades ante ciberincidentes en estas infraestructuras.

Respecto a las FCSE con responsabilidad en la ciberdelincuencia existen 2 unidades que desarrollan esta tarea, el Grupo de delitos telemáticos (101) de la Guardia Civil y la Brigada de Investigación Tecnológica (BIT) (102) de Cuerpo Nacional de Policía. En las policías autonómicas (País Vasco, Navarra y Cataluña) existen unidades que tratan este tipo de delitos.

Ministerio de Política Territorial y Administración Pública

Este ministerio (103) preside el Consejo Superior de Administración Electrónica (104) y a través de éste, debe promover la colaboración y cooperación con las comunidades autónomas y las entidades locales para

(100) Capacidad de respuesta ante incidentes gubernamental. www.ccn-cert.cni.es
(101) Grupo de Delitos telemáticos (DGT). www.gdt.guardiacivil.es/
(102) Brigada de Información Tecnológica (BIT). www.policia.es/bit/
(103) Estas funciones han sido desarrolladas por el anterior Ministerio de Administraciones Públicas y posteriormente en el Ministerio de Presidencia. En la última remodelación del gobierno de octubre de 2010 estas competencias se han traspasado al Ministerio de Política territorial y Administración Pública.
(104) Consejo Superior de Administración Electrónica (CSAE). www.csae.map.es/

la puesta en marcha de servicios públicos interadministrativos. Para ello preside la conferencia sectorial de las AAPP que reúne a todas las CCAA y la conferencia nacional de la Administración local (para ayuntamientos de más de 140.000 habitantes).

Además debe impulsar las actividades de cooperación de la Administración General del Estado con la Unión Europea, con las organizaciones internacionales y, especialmente, con Iberoamérica, en materia de tecnologías de la información y Administración electrónica, en colaboración con el Ministerio de Asuntos Exteriores y de Cooperación. Por otro lado, gestiona la red SARA (105).

Consejo Superior de Administración Electrónica

El Consejo Superior de Administración Electrónica (106) es el órgano encargado de la política y estrategia del Gobierno en materia de tecnologías de la información y la implantación de la Administración Electrónica en la Administración General del Estado. Dispone de una comisión permanente cuyas funciones se detallan en el Real Decreto 589/2005, de 20 de mayo.

En colaboración con el Centro Criptológico Nacional el CSAE realizará las siguientes acciones:

– Elaboración de medidas de seguridad de las tecnologías de la información y comunicaciones,
– Adquisición coordinada de material de cifra
– Formación de personal especialista en seguridad de los sistemas

Dispone de un Observatorio de la Administración Electrónica (107) que analiza el nivel de implantación de ésta en las AAPP.

---

(105) Sistemas de Aplicaciones y Redes para las Administraciones (SARA). Artículo 43. Ley 11/2007 de 22 junio. Acceso de los ciudadanos a los servicios públicos. Establece la interconexión de las diferentes Administraciones para intercambio de información y servicios y para la interconexión con la Unión Europea y otros Estados miembros. www.ctt.map.es/web/proyectos/redsara

(106) El Consejo Superior de Administración Electrónica, «es el órgano colegiado adscrito al Ministerio de Administraciones Públicas –hoy Ministerio de la Presidencia- encargado de la preparación, la elaboración, el desarrollo y la aplicación de la política y estrategia del Gobierno en materia de tecnologías de la información» (Art. 3 del Real Decreto 589/2005, de 20 de mayo, por el que se reestructuran los órganos colegiados de la Administración Electrónica).

(107) Observatorio de la Administración electrónica. www.obsae.map.es/

Centro Nacional de Inteligencia

El CNI depende orgánicamente del Ministerio de Defensa pero en la seguridad de la información clasificada y en el ámbito de la ciberdefensa tiene encuadrados a organismos que tienen misiones que afectan a todas las Administraciones Públicas.

El Secretario de Estado Director del CNI es Autoridad Nacional de Seguridad Delegada (ANS-D) por el Ministro de Defensa y Ministro de Asuntos Exteriores para la protección de información clasificada Nacional e Internacional. Tiene como órgano de trabajo para esta actividad a la Oficina Nacional de Seguridad (ONS) (108) y por la ley 11/2002, de 6 de mayo, reguladora del CNI es Director del Centro Criptológico Nacional.

Oficina Nacional de Seguridad

La ONS se crea en 1983. Tiene por misión fundamental la de velar por el cumplimiento de la normativa relativa a la protección de la Información Clasificada tanto nacional como aquella que es entregada a la Administración o a las empresas en virtud de Tratados o Acuerdos internacionales suscritos por España.

Destacan las siguientes funciones:

- Realización de Acuerdos para protección de la Información Clasificada a nivel internacional.
- Participación en Comités y Grupos de Trabajo sobre protección de información clasificada de Unión Europea, OTAN, acuerdos internacionales y programas clasificados.
- Relaciones con otras Autoridades Nacionales de Seguridad.
- Expedición de Habilitaciones Personales de Seguridad.
- Expedición de Habilitaciones de Empresa.
- Acreditación y autorización de los Órganos, Instalaciones y Sistemas que manejan Información Clasificada.

En la acreditación de sistemas para manejar información clasificada trabaja conjuntamente con el CCN en apoyo de la ANS-D.

Centro Criptológico Nacional

Fue creado en el año 2004, a través del Real Decreto 421/2004. Comparte con el CNI medios, procedimientos, normativa y recursos. A su vez,

(108) Oficina Nacional de Seguridad (ONS). www.cni.es/es/ons/

y tal y como contempla el Real Decreto citado anteriormente, al CCN están adscritos el Organismo de Certificación (OC (109)) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) y la capacidad de Respuesta a Incidentes de Seguridad de la Información en las Administraciones Públicas (CCN-CERT).

Las funciones establecidas en el RD 421/2004 son:

- Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de las TIC en la Administración
- Formar al personal de la Administración especialista en el campo de la seguridad de las TIC
- Constituir el organismo de certificación del Esquema Nacional de Evaluación y Certificación de aplicación a productos y sistemas de su ámbito
- Valorar y acreditar la capacidad de productos de cifra y Sistemas de las TIC (que incluyan medios de cifra) para manejar información de forma segura
- Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los Sistemas antes mencionados
- Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia (Sistemas de las TIC)
- Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países.

El RD 3/2010 por el que se regula el Esquema Nacional de Seguridad reitera estas funciones, esta vez, para los sistemas sujetos a la Ley 11/2007 de Administración Electrónica. Destacando el desarrollo de normativa en apoyo al esquema (Artículo 29) y las misiones encomendadas al CERT Gubernamental (Artículos 36 y 37).

Ministerio de Defensa

Además de las misiones que tiene asignada el CNI este Ministerio dispone de un elevado número de sistemas clasificados y gestiona diversos sistemas de intercambio de información y mando y control con OTAN. Dispone de una política de seguridad con responsabilidades sobre sistemas que manejan información clasificada.

(109) Organismo de Certificación. www.oc.ccn.cni.es

Las responsabilidades se encuentran distribuidas en Dirección General de Infraestructuras (DIGENIN(110)), en el Estado Mayor de la Defensa (EMAD) y en los Cuarteles Generales de los tres Ejércitos.

Dirección General de Infraestructuras

Destaca la misión de dirigir y coordinar la planificación, obtención y gestión de los sistemas de información y telecomunicaciones, así como la política de seguridad de la información. Entre sus unidades destacan la Inspección General del Plan Director de Sistemas de Información y Telecomunicaciones y la Subdirección General de Servicios Técnicos y Telecomunicaciones que gestiona entre otras la red corporativa del Ministerio.

Estado Mayor de la Defensa

El Estado Mayor de la Defensa es responsable del planeamiento, dirección y control del Sistema de Mando y Control Militar de las FAS, y de las telecomunicaciones que lo soportan. Es Autoridad Delegada de Acreditación para los sistemas conjuntos que manejen información nacional clasificada.

Cuarteles Generales

Son responsables de los sistemas propios. Son Autoridades Delegadas de Acreditación para los sistemas propios que manejen información nacional clasificada.

Equipos de Respuesta ante Incidentes

Actualmente, los equipos de respuesta ante incidentes se consideran los organismos con mayor capacidad técnica y con la estructura más adecuada para luchar contra el mayor espectro de ciberamenazas. El modo de actuación es muy colaborativo y sus relaciones son informales y flexibles pero guiadas por criterios de máxima eficiencia y rapidez en la actuación.

La descripción que se refleja a continuación no es exhaustiva y solo intenta proporciona una visión general de los campos de actuación de los equipos que se encuentran operando. Se relacionan a continuación:

(110) Dirección General de Infraestructuras (DIGENIN). www.mde.es/organizacion/organigramaMinisterio/secretariaEstado/

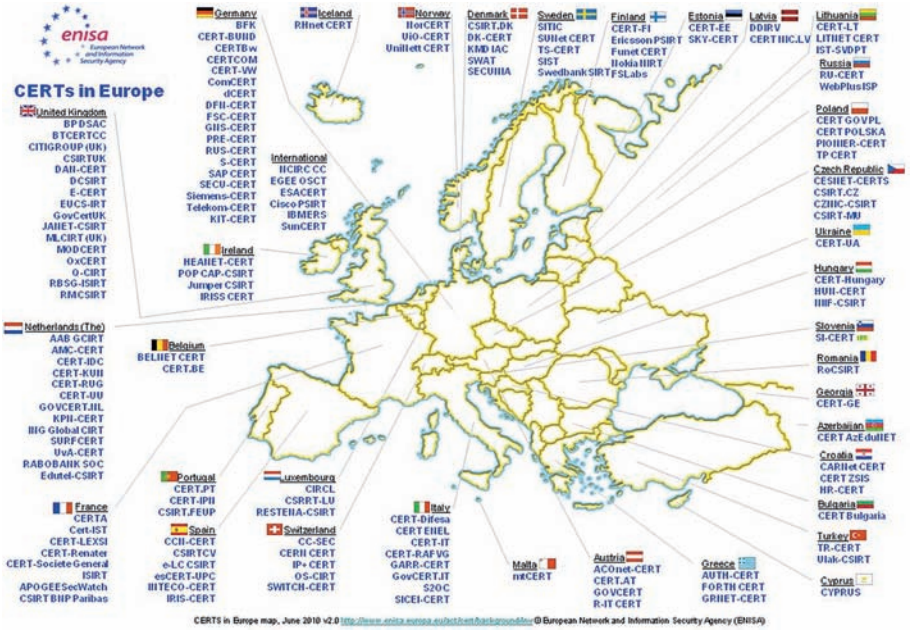
– **CCN-CERT** (111)**.** (Organismo adscrito al CCN-CNI). Tiene responsabilidades en ciberataques sobre sistemas clasificados, sistemas de la Administración General, Autonómica y Local y, en coordinación con el CNPIC, sobre sistemas que gestionen infraestructuras críticas. Proporciona el estado de la amenaza en ciberseguridad para Presidencia de Gobierno. Este CERT es el CERT gubernamental/nacional. Tiene esta responsabilidad reflejada en el RD 3/2010 de 8 de enero que desarrolla el Esquema Nacional de Seguridad. En los artículos 36 y 37 se asigna a este CERT el papel de coordinador público estatal.
– **INTECO-CERT** (112) (Instituto Nacional de Tecnologías de Comunicación adscrito al Ministerio de Industria, Turismo y Comercio). Tiene responsabilidades de seguridad y respuesta ante incidentes de seguridad en los entornos de ciudadanos y pequeñas y medianas empresas (PYMES) según la definición de la comunidad sobre la que actúa este CERT. En su creación 2004 se le traspasó el CATA (Centro de Alerta Temprana Antivirus) desde Red.es, empresa pública también adscrita al Ministerio de Industria.
– **CERT en comunidades autónomas (CCAA).** Existe creado y reconocido el CSIRT-CV (113) de la Generalitat Valenciana y están en fase de despliegue / desarrollo, el CESICAT (114) (CERT de la Generalitat Catalana) y el ANDALUCIA-CERT. Estos organismos dependen de sus CCAA respectivas. Las responsabilidades de estos CERT,s es diferente pudiéndose referir a los sistemas de la administración autonómica y/o local así como tener otras misiones de asistencias a empresas y ciudadanos. Se debe consultar su misión y objetivos en las páginas Web correspondientes.
– **IRIS-CERT** (115)**.** Organismo adscrito al Ministerio de Industria, Turismo y Comercio. Tiene responsabilidades de seguridad en la red IRIS que da servicio a la comunidad universitaria y a los centros de investigación.
– **Otros CERT.** Existen otros CERT y centros operativos de seguridad que ofrecen servicios a otros sectores. Entre ellos destacan por su actividad los siguientes:

(111) CCN-CERT. www.ccn-cert.cni.es
(112) INTECO-CERT. http://cert.inteco.es
(113) Computer Security Incident Response Team (equipo de respuesta ante incidentes de seguridad informática) de la Comunidad Valenciana CSIRT-CV. www.csirtcv.es/
(114) Centro de Seguridad de la Información de Cataluña (CESICAT). www.cesicat.cat/
(115) IRIS-CERT. www.rediris.es/cert/

– **e-La Caixa-CSIRT** (116). Respuesta ante incidentes de seguridad de este banco.
– **S21Sec-CERT** (117). Este CERT proporciona servicios de gestión de incidentes para las diferentes entidades, fundamentalmente, del sector bancario).
– **esCERT-UPC** (118). Decano de los CERT,s nacionales. Fundado en 1994. Proporciona servicios de CERT a la Universidad Politécnica de Cataluña.
– **Hispasec** (119). Empresa de seguridad que proporciona servicios de CERT.

Todos los CERT se coordinan a través del grupo de trabajo de CERT,s nacionales (CSIRT.es) (120) y a su vez, en el foro ABUSES(121) se relacionan con los principales proveedores de servicios de Internet.

En la figura adjunta se muestran los CERT,s recogidos por ENISA (122).



(116) E-La Caixa-CSIRT. www.lacaixa.es
(117) S21Sec-CERT. www.cert.s21sec.com
(118) EsCERT-UPC. http://escert.upc.edu/
(119) Hispasec. www.hispasec.com
(120) CSIRT.es. www.csirt.es
(121) Foro abuses. www.abuses.es/
(122) European Network and Information Security Agency (ENISA). www.enisa.europa.eu/

Relaciones internacionales

En el ámbito internacional existen foros de colaboración entre los organismos responsables de ciberseguridad preferentemente entre los equipos de gestión de incidentes de seguridad de los diferentes países entre los que destacan los siguientes:

- **FIRST** (123). Esta organización relaciona los CERT,s reconocidos de los diferentes países resaltando su misión y la comunidad a la que proporciona servicio. La adscripción a este foro requiere un procedimiento que culmina con una auditoría realizada por uno de los CERT,s que patrocinan la adhesión del nuevo equipo. Los CERT,s nacionales reconocidos por orden de ingreso son Iris-CERT (1997), e-La Caixa-CERT (2005), CCN-CERT (2007), EsCERT-UPC (2007), e INTECO-CERT (2008).
- **TF-CSIRT** (124)**. Grupo de trabajo de TERENA (Trans-European Research and Education Network Association).** Es el foro de CERT,s europeos. Los CERT,s nacionales reconocidos por orden de ingreso son EsCERT-UPC, Iris-CERT, CCN-CERT, INTECO-CERT y CSIRT-CV. Por otro lado, S21Sec-CERT y CESICAT están en proceso de acreditación.
- **European Government CERT** (125)**.** Es el grupo de trabajo de CERT,s gubernamentales/nacionales europeos. La adhesión a este grupo requiere una auditoria formal sobre el mandato legal, la capacidad técnica y los procedimientos empleados por el CERT. En principio solo se admite un único equipo por país. El representante nacional es el CCN-CERT.
- **NCIRC** (126)**. Capacidad de respuesta ante incidentes de OTAN.** Es la capacidad equivalente a los equipos citados anteriormente para OTAN. Identifica al CCN-CERT como CERT nacional para la coordinación de incidentes de seguridad principalmente asociado con ataques o fugas de información sensible. El CCN-CERT participa en los ejercicios de ciberdefensa organizados por este organismo conjuntamente con el Estado Mayor de la Defensa (EMAD).
- **Sistema de Alerta Temprana de la Unión Europea.** Está en proceso de definición desde principios de 2010. Identifica a los CERT,s

(123) Forum for Incident Response and Security Teams (FIRST). www.first.org/
(124) TERENA. www.trusted-introducer.nl/
(125) European Government CERT www.egc-group.org/
(126) NATO Computer Incident Response Capability (NCIRC). www.ncirc.nato.int/

gubernamentales para realizar el intercambio de información y para solicitar colaboración en caso de la detección de un ataque que afecte a más de una nación.

– **Directorio MERIDIAN** (127)**.** Directorio internacional de organismos y agencias gubernamentales con responsabilidad en la protección de infraestructuras críticas. No es específico de los equipos de respuesta ante incidentes aunque en los diversos aspectos que cubre el directorio aparecen estos equipos. En este directorio tienen responsabilidades las siguientes organizaciones; Secretaría de Estado de Seguridad (CNPIC) del Ministerio del Interior, CNI/CCN, Secretaría de Estado de Telecomunicaciones y Sociedad de la Información (SETSI) del Ministerio de Industria Turismo y Comercio, Dirección de Infraestructura y Seguimiento de Situaciones de Crisis (DISCC) de Presidencia del Gobierno y Ministerio de Defensa.

ESPAÑA. SITUACIÓN ACTUAL

Con el panorama citado en el apartado anterior se puede ver que las responsabilidades de seguridad en el ciberespacio están distribuidas en varios organismos tanto en la Administración General de Estado como en la autonómica.

La posibilidad de solapes y sistemas que puedan depender de diversos organismos es muy alta. Además, la respuesta eficaz a las nuevas amenazas que se tienen que afrontar hace necesaria un intercambio de información muy ágil y una coordinación muy estrecha entre los diferentes organismos con responsabilidades.

En los siguientes apartados se amplía información de la problemática asociada a los siguientes ámbitos:

– Actuación de CERT,s
– Sistemas clasificados
– Sistemas de la Administración. Esquema Nacional de Seguridad
– Protección de datos personales
– Sistemas asociados a infraestructuras críticas

(127) International Critical Information Infrastructure Protection Directory. Meridian conference Issue 24. Agosto 2010. No disponible en enlace público. www.meridianprocess.org/

Ámbitos de actuación en ciberseguridad

Por ámbitos la actuación de estos equipos de respuesta ante incidentes sería:

- **Sistemas relacionados con Seguridad y Defensa**. En este ámbito por lo establecido en el RD 421/2004 la responsabilidad recae en el CCN y la respuesta ante incidentes de seguridad en el CCN-CERT. Los sistemas aquí contemplados pertenecen fundamentalmente al Ministerio de Defensa, Ministerio del Interior, Presidencia de Gobierno, Ministerio de Política Territorial y Administración Pública y Ministerio de Asuntos Exteriores y Cooperación. Preferentemente se trata de sistemas que manejan información clasificada. Disponen de regulación propia y se tratarán en apartado correspondiente.
- **Sistemas de las Administraciones Públicas**. Las responsabilidades no se encuentran completamente definidas aunque el RD 3/2010 por el que se regula el Esquema Nacional de Seguridad determina que las responsabilidades de actuación ante cualquier incidente contra estos sistemas se ubican en el CCN-CERT, especialmente para los sistemas recogidos en el ámbito de la ley 11/2007 de Administración electrónica. Iris-CERT da servicio a la comunidad académica.
- **Ciudadano y PYME**. Las actuaciones en estos ámbitos en materia de prevención y respuesta están lideradas por el Ministerio de Industria, Turismo y Comercio (MITYC). La capacidad de respuesta ante incidentes se articula a través del INTECO-CERT aunque los CERT,s de las Comunidades Autónomas también se atribuyen competencias en su demarcación territorial sobre esta comunidad.
- **Operadores de Telecomunicaciones y Proveedores de Servicios**. Los principales operadores y proveedores disponen de centros de operación de seguridad (SOC) orientados hacia la prevención y respuesta ante incidentes de seguridad, fraudes y ataques a sus infraestructuras.
- **Sectores estratégicos / Infraestructuras críticas**. La responsabilidad sobre estos sistemas recae en el CNPIC con las salvedades expuestas en el proyecto de legislación. Existen algunos CERT de carácter privado que dan servicio a alguno de los sectores estratégicos.

Muchos de estos ámbitos de actuación se superponen y, en la gestión de incidentes de seguridad, se detectan solapes y redundancias.

Sistemas Clasificados

Los sistemas que manejan información clasificada tanto nacional como de la OTAN, Unión Europea (UE) o sujeta a acuerdos internacionales disponen de una normativa muy completa y de la obligatoriedad de someterse a un proceso de acreditación en el que se verifican mediante las auditorias correspondientes todos los aspectos relacionados con la seguridad del sistema.

Existe un completo conjunto normativo de requisitos de seguridad según el nivel de clasificación de la información cuando es manejada en estos sistemas, recogido en las series CCN-STIC publicadas por el CCN según lo establece el RD 421/2004 donde se desarrollan las funciones de este organismo.

Tanto en la OTAN como en la UE la interconexión de los sistemas nacionales con los propios requiere una declaración de conformidad firmada de la Autoridad Nacional de Seguridad que debe ejecutar las inspecciones o las auditorias necesarias para la verificación del cumplimiento de todos los requisitos de seguridad establecidos.

A diferencia de lo establecido para la información clasificada de OTAN y UE, España adolece de una normativa de alto nivel que cubre todos los niveles de clasificación. Así en España la ley 9/1968, de secretos oficiales se establecen los niveles de SECRETO y RESERVADO, las clasificaciones de CONFIDENCIAL y DIFUSIÓN LIMITADA solo se han adoptado fruto de los acuerdos internaciones en el reconocimiento de información recibida de organizaciones internacionales. Por ello, solo el Ministerio de Defensa dispone de legislación de detalle que fije los estándares de protección de estos niveles de clasificación.

En el cuadro adjunto (128) se muestran las equivalencias entre las diferentes clasificaciones de seguridad (OTAN, UE, Nacional, Ley Orgánica de Protección de Datos y Esquema Nacional de Seguridad) aunque no se pueden equiparar si puede servir de orientación aproximada del nivel de protección.

(128) CCN-STIC 001 Seguridad de las Tecnologías de Información y comunicaciones que manejan información nacional clasificada en la Administración. Diciembre 2006. www.ccn-cert.cni.es

<table>
<tr><th>NACIONAL</th><th>OTAN</th><th>UE</th><th>LOPD(1)</th><th>ENS</th><th>OTROS(5)</th></tr>
<tr><td>SECRETO</td><td>COSMIC TOP SECRET</td><td>TRES SECRET UE</td><td></td><td></td><td></td></tr>
<tr><td>RESERVADO</td><td>NATO SECRET</td><td>SECRET UE</td><td></td><td></td><td></td></tr>
<tr><td>CONFIDENCIAL</td><td>NATO CONFIDENTIAL</td><td>CONFIDENTIEL UE</td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">DIFUSION LIMITADA</td><td rowspan="2">NATO RESTRICTED</td><td rowspan="2">RESTREINT UE</td><td rowspan="2">ALTO(2)</td><td>ALTO(4)</td><td rowspan="3">USO INTERNO</td></tr>
<tr><td rowspan="2">MEDIO</td></tr>
<tr><td>SIN CLASIFICAR</td><td>NATO UNCLASSIFIED</td><td>-----</td><td>MEDIO(3)
BASICO(3)</td><td>BAJO</td></tr>
</table>

1) Reglamento de aplicación de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal
2) Puede incluir algunas protecciones consideradas para información CONFIDENCIAL
3) Entre Básico y Medio existe un nivel intermedio de aplicación
4) No incluye protecciones criptográficas
5) Uso Interno Administración equivalente a DL

Estos sistemas manejan la información más sensible por lo que las medidas de seguridad que deben incorporar deben ser máximas y la vigilancia de los mismos extrema.

Esquema Nacional de Seguridad

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos establece la obligatoriedad de proporcionar los diferentes servicios de la Administración en el Ciberespacio. La ley contempla la creación de sedes electrónicas desde las que los diferentes organismos deben proporcionar el máximo de servicios en línea al ciudadano.

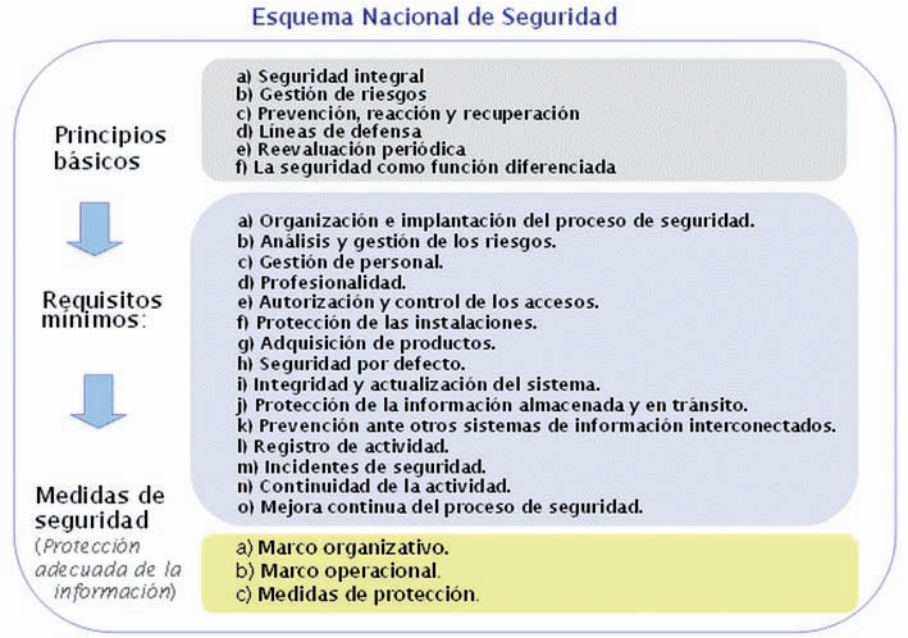
Asimismo establece que las Administraciones Públicas utilizarán las tecnologías de la información asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

Esta ley, en su artículo 42, regula la creación de un Esquema Nacional de Seguridad que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos y está constituido por unos princi-

pios básicos y requisitos mínimos que permitan una protección adecuada de la información. Este esquema ha sido publicado en el RD 3/2010 y por primera vez establece un conjunto de medidas de seguridad de obligado cumplimiento según el nivel de la información o sistema (ALTO, MEDIO o BAJO).

Asimismo, como aspectos interesantes del RD resaltan; la obligatoriedad de la realización de auditorías, la recomendación del empleo de productos certificados y la articulación de una capacidad de respuesta ante incidentes de seguridad para las Administraciones Públicas.

En la figura adjunta (129) se muestran estos principios básicos y requisitos mínimos.



Asimismo, en el cuadro adjunto se muestran los diferentes servicios previstos y los organismos responsables de proporcionarlos en el ENS:

(129) RD 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE nº 25 (29.10.2010).

Se considera, por tanto, que esta norma es un conjunto homogéneo y compacto de medidas de seguridad que, una vez que se apliquen mejorarán considerablemente los niveles de seguridad de los distintos organismos de la Administración.

No obstante, el ENS adolece de algunas deficiencias fruto del consenso en su desarrollo entre la Administración General, Autonómica y Local. Así la revisión de las auditorias y la corrección de las posibles deficiencias detectadas no están supervisadas por ningún organismo que vele porque todas las AAPP mantengan el mismo nivel de seguridad en sus sistemas.

Además, aunque para sistemas de nivel ALTO se establece en las medidas de protección asociadas con la monitorización de sistemas, en el Real Decreto esta actividad no está contemplada con la importancia que sería necesaria para hacer frente a las amenazas actuales.

De todas formas, el esquema en su artículo 29 establece que el CCN elaborará y difundirá guías de seguridad que desarrollen éste. Se espera que estas guías aclaren y subsanen las posibles deficiencias del mismo. En la tabla adjunta se muestra las guías previstas hasta el momento en la serie CCN-STIC 800.

800 – Esquema Nacional de Seguridad	801	Responsabilidades en le ENS
	802	Auditoria del Esquema Nacional de Seguridad
	803	Categorización de los sistemas en el ENS
	804	Implementación de Medias en el ENS
	805	Modelo de política de seguridad
	806	Modelo de Plan de Adecuación al ENS
	807	Criptología de empleo en el ENS
	808	Verificación del cumplimiento de las medidas en el ENS
	809	Declaración de conformidad con el ENS
	810	Guía de Creación de CERT,s
	811	Interconexión en el ENS
	812	Herramientas de seguridad en el ENS

Protección de Datos personales

La Ley Orgánica 15/1999 (130), de 13 de diciembre, de Protección de Datos de Carácter Personal tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas.

Sus normas de desarrollo, determinan las medidas para la protección de los datos de carácter personal y aportan criterios para establecer la proporcionalidad entre las medidas de seguridad y la información a proteger.

Esta normativa fue la primera de obligado cumplimiento para sistemas dentro de su ámbito de actuación. Normalmente sus medidas de seguridad están asociadas al fichero y no al sistema por lo que la seguridad proporcionada no es integral.

Además de la Agencia Española de Protección de Datos (131), existen en algunas CCAA (Madrid (132), Cataluña (133) o País Vasco (134)) otras agencias con misión similar en su entorno geográfico.

(130) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Título VI con rango de ley ordinaria)

(131) AEPD Agencia Española de Protección de Datos. www.agpd.es. Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos

(132) En Madrid. creada artículo 6 de la Ley 9/1990, de 8 de noviembre, Reguladora de la Hacienda de la Comunidad de Madrid. Estatuto aprobado por el Decreto 40/2004 de 18 de marzo. www.madrid.org/cs/Satellite?language=es&pagename=PortalAPDCM%2FPage%2FPAPD_home

(133) Agencia Catalana de Protección de Datos. www.apdcat.net/ca/index.php

(134) Agencia Vasca de Protección de Datos. www.avpd.euskadi.net/s04-5213/es

Sistemas asociados a Infraestructuras críticas

Actualmente, el anteproyecto de ley asociado a la protección de infraestructuras críticas está en su fase final de aprobación por lo que no se puede determinar el nivel de seguridad de los sistemas asociados a las mismas.

Existen sectores que proporcionan muchos servicios en el ciberespacio y por subsistencia de su negocio implementan unos niveles de seguridad aceptables como puede ser el sector financiero pero existen otros de los que se desconoce realmente el nivel de seguridad que tienen.

Se deberá esperar al desarrollo de esta normativa en el campo de la ciberdefensa para poder valorar realmente el nivel de seguridad de estas infraestructuras.

ESTRATEGIA ESPAÑOLA DE CIBERSEGURIDAD

De lo expuesto en los capítulos 5 y 6 se observa que las responsabilidades en ciberseguridad se encuentran muy disgregadas en diferentes organismos que además no tienen las mismas prioridades desde el punto de vista de seguridad.

Se detecta un posible solape por un lado y una disgregación de funciones por otro que impide un tratamiento completo de los nuevos desafíos de seguridad que nos presenta el ciberespacio.

Por otro lado, y tras analizar cómo se está abordando el problema en otros países de nuestro entorno, se hace necesario desarrollar una estrategia nacional sobre ciberseguridad que trate de forma completa el problema, que permita alcanzar una visión de conjunto sobre el mismo, establezca estructuras que aseguren la coordinación de las iniciativas de cada uno de los organismos con responsabilidades en este ámbito y promueva la adopción de unas líneas estratégicas de acción.

Se describe a continuación una posible aproximación a esta estrategia.

Objetivos

La Estrategia Nacional de Ciberseguridad persigue conseguir un ciberespacio más seguro a través de los siguientes objetivos:

1. Establecer una línea de defensa común y homogénea. Para ello se debe desarrollar con la máxima rapidez el Esquema Nacional de Seguridad y mejorar el intercambio de información de alertas, vulnerabilidades y amenazas que se detecten en las redes de la administración.
2. Mejorar las capacidades de detección y reacción. Para ello se deben mejorar o desarrollar sistemas de alerta temprana e incrementar la seguridad de los productos y tecnologías desde su fase de diseño.
3. Colaborar con la Administración autonómica y local y con el sector privado para apoyar iniciativas que mejoren la seguridad de los sistemas nacionales haciendo especial énfasis en los que gestionan infraestructuras críticas. Extender las acciones de formación y concienciación en ciberseguridad a todos ellos.
4. Concienciar y proporcionar apoyo a los ciudadanos para hacer más segura su actividad en línea (on-line) así como reforzar la capacidad de las fuerzas y cuerpos de seguridad del Estado para combatir el cibercrimen.
5. Fortalecer el entorno futuro de ciberseguridad. Para ello se debe incrementar el número de especialistas en seguridad de las TIC, impulsar y coordinar los esfuerzos de investigación y desarrollo de productos de seguridad nacionales y definir estrategias que disuadan la actividad hostil o dañina en el ciberespacio.

Al igual a lo realizado por otras naciones, para conseguir estos objetivos se deben incrementar los presupuestos de las agencias encargadas de la seguridad de la Administración y las unidades encargadas del ciberdelito en las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

Líneas estratégicas de acción

Para conseguir estos objetivos se plantean algunas líneas estratégicas que se deben considerar y dotar presupuestariamente:

1. **Desarrollar el Esquema Nacional de Seguridad**, reforzando su aplicación y la realización de auditorías que verifiquen el estado de seguridad de los sistemas de la Administración. El RD no contempla dotación presupuestaria que impulse su aplicación.
2. **Gestión homogénea de las redes de las Administraciones Públicas** minimizando y optimizando sus conexiones a Internet (deben cumplir los mismos requisitos de seguridad) y centralizando las capacidades de Monitorización y respuesta.

3. **Despliegue de sistemas de alerta y protección de las redes de las AAPP y sus interconexiones** para la detección rápida de incidentes y anomalías dentro de éstas. Estos sistemas, basado en el análisis y correlación de registros (logs) generados por las herramientas de seguridad instaladas, permite detectar de manera proactiva cualquier anomalía o ataque analizando el tráfico que circula dentro, entre y en las salidas de los diferentes Ministerios y Organismos.
4. **Desarrollo del Plan de Protección de infraestructuras críticas (PPIC) ante ciberamenazas**. Con el objetivo de gestionar de incidentes de seguridad relacionados con ciberataques sobre infraestructuras críticas; actualizar la información sobre vulnerabilidades (especialmente en sistemas SCADA); impulsar el cumplimiento por parte de los operadores de los estándares de seguridad que se definan como mínimos; realizar análisis de riesgos y ejecutar auditorias de seguridad que revisen el cumplimiento. Sería del máximo interés que estos operadores que manejan infraestructuras críticas se acojan a servicios de alerta temprana similares a los del punto anterior.
5. **Elaborar un programa de concienciación y formación para crear una sólida cultura de seguridad** en el desarrollo y el uso de sistemas de información y comunicaciones a todos los niveles ciudadanos, sector privado (infraestructuras críticas) y Administraciones públicas.
6. **Mejorar los mecanismos de coordinación y respuesta ante incidentes** y realizar ejercicios que demuestren su efectividad. Por ello, se deben crear estructuras de ciberdefensa similares a las de otras naciones en las que se integren las capacidades de respuesta ante incidentes de seguridad existentes actualmente.
7. **Coordinación de esfuerzos en investigación y desarrollo de tecnologías de seguridad** especialmente centrada en el desarrollo de productos de cifra. Se debe evitar el empleo de tecnologías de terceros países en aspectos tan críticos como la protección de la información. En esta acción se debe involucrar al sector privado por su papel en muchas de las infraestructuras críticas nacionales.
8. **Potenciar la colaboración internacional**. Por la naturaleza transnacional de la amenaza y del ciberespacio hace necesario una cooperación internacional para hacerle frente. Se deben impulsar la firma de acuerdos en materia del ciberdelito y crear unas normas

de comportamiento en el ciberespacio consensuadas por todas las naciones que pueda facilitar la atribución de los ataques.

9. **Promover el uso de estándares de seguridad y la certificación de seguridad de los productos TIC**. Es necesario que las tecnologías y productos hayan sido revisadas desde el punto de vista de seguridad. Estos procesos son costosos y difíciles de abordar especialmente para pequeñas y medianas empresas. Esta acción permitiría además, que los productos desarrollados nacionalmente puedan competir en el ámbito internacional.
10. **Mejorar de seguridad en las redes clasificadas**. Estas redes manejan la información clasificada y sensible de la Administración para conducir Operaciones de Mantenimiento de Paz, Operaciones Militares, actividades diplomáticas, actividades contraterroristas, actividades de las FCSE o de inteligencia así como las actividades de seguridad interior. La integridad de estas redes es crítica y cualquier incidente declarado en las mismas puede dañar de forma grave la soberanía nacional. Se debe reforzar por tanto las medidas de seguridad de estos adaptando las salvaguardas y procedimientos existentes a la evolución de los ciberataques.

Se describen con mayor detalle estas posibles líneas de acción en el anexo A.

Posible estructura de la ciberseguridad

Del análisis de las responsabilidades en el ciberespacio se determina que esta actividad está siendo realizada por diferentes Ministerios y se detecta que existen solapes en sus diferentes actividades. Asimismo no están definidos canales de colaboración formales entre las capacidades de respuesta ante incidentes de seguridad.

Por ello, para poder afrontar el reto de la ciberdefensa se considera necesario un organismo (oficina o centro de coordinación) con responsabilidades transversales en este asunto y con una visión global que pueda impulsar todas las líneas de acción.

Puede ser una solución la creación de una **Oficina de Ciberseguridad (OCS)** responsable de desarrollar la política para la defensa cibernética, garantizar su cumplimiento, definir y establecer la estructura funcional necesaria para esta defensa en las Administraciones públicas, apoyar a los operadores privados que gestionen infraestructuras críticas y coordinar las iniciativas de concienciación a los ciudadanos.

Dentro de esta oficina se tiene que articular un organismo de planeamiento que debe ser un órgano colegiado cuyas funciones pueden ser las de implementar y revisar la política de ciberdefensa, revisar las amenazas emergentes con respecto a los planes de defensa e inversiones, revisar las medidas de defensa implementadas en los diferentes organismos, desarrollar el programa de trabajo establecido, aprobar los programas de formación y concienciación y validar y aprobar los informes de evaluación de amenazas, vulnerabilidades y riesgos de seguridad.

Asimismo será necesario disponer de un Centro de Coordinación Técnica en ciberseguridad (CCTCS) con la función principal coordinar las actividades operativas de ciberdefensa de todos los organismos nacionales implicados en la misma, así como con los organismos internacionales que se determinen.

Las misiones de este CCTCS pueden ser:

– Alertar y prevenir los incidentes de seguridad en el ciberespacio y, llegado el caso, responder de forma rápida y eficiente ante cualquier ataque cibernético que se pueda producir.
– Ser punto de contacto para la recepción, valoración y distribución de información de seguridad cibernética.
– Realizar cualquier tipo de coordinación a nivel internacional y ejecutar las acciones necesarias para la mitigación y neutralización de ataques cibernéticos recibidos por otros países.

Dependiendo de CCTCS se deben concentrar las capacidades de respuesta ante incidentes gubernamental en un Centro de Coordinación de Respuesta ante Incidentes de Seguridad (CCRIS).

El ámbito de actuación del CCRIS debe comprender los sistemas clasificados nacionales y aquellos internacionales que por acuerdo o convenio le corresponda proteger al Estado español, los sistemas de la Administración y, en coordinación con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), los sistemas que gestionen infraestructuras críticas.

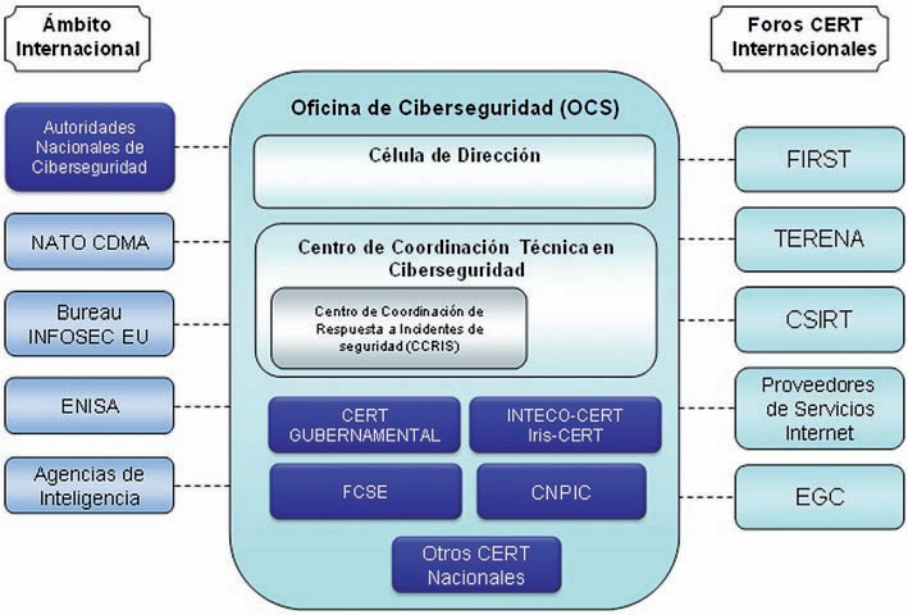
La articulación de una adecuada respuesta ante incidentes en sistemas que gestionan infraestructuras críticas es una actividad crítica que debería realizarse con la mayor celeridad.

El CCRIS debe estar compuesto por representantes del CERT gubernamental, de los distintos CERT,s de ámbito nacional (IRIS-CERT e INTECO-CERT), de los CERT,s autonómicos (CESICAT, CSIRT-CV, Anda-

lucía-CERT), de la Brigada de Investigación Tecnológica (BIT) del Cuerpo Nacional de Policía, del Grupo de Delitos Telemáticos (GDT) de la Guardia Civil, de la División de Investigación Criminal de los Mozos de Escuadra (Mossos d´Esquadra), de la Sección de Delitos Informáticos de la Unidad de Investigación Criminal y Policía Judicial de la Policía Autónoma Vasca (Ertzaintza), de la Unidad Técnica de Policía Judicial de la Guardia Civil entre otros posibles representantes.

No obstante, estará abierto a la adhesión de otros organismos cuando la naturaleza de la amenaza cibernética requiera de su asesoramiento para hacer frente a la misma.

En la figura adjunta se muestran las posibles relaciones de la estructura propuesta.



CONCLUSIONES

Los ciberataques son muy rentables en términos de esfuerzo necesario para su ejecución, riesgos que se asumen y beneficios económicos o políticos que se pueden obtener y afecta transversalmente tanto al sector público, al sector privado como a los ciudadanos. Además no existe una legislación armonizada que permita una lucha efectiva contra estas amenazas.

Todas las naciones de nuestro entorno están desarrollando iniciativas para intentar controlar las amenazas que vienen del ciberespacio. La mayoría de ellas está apostando por estructuras similares a la propuesta en este documento.

En España las responsabilidades en el ciberespacio están muy fragmentadas en diferentes organismos que abordan el problema de forma parcial.

Es necesario por tanto impulsar actuaciones en este sentido fortaleciendo las capacidades de respuesta ante incidentes y de inteligencia ante este tipo de amenazas. La dotación presupuestaria se considera crítica si se quieren llevar a cabo las líneas de acción que se plantean como posibles soluciones para reducir la amenaza.

Por ello, la estrategia propone que se establezca un programa que afecte a todo la nación para alcanzar los objetivos estratégicos planteados incrementando los fondos que desarrollen nuevas tecnologías para proteger las redes nacionales e incrementando la formación en perfiles críticos para esta actividad y fomentando el trabajo coordinado entre el sector público, la industria, los ciudadanos y los aliados internacionales.

BIBLIOGRAFÍA

14th Annual, CSI Computer Crime and Security Survey, diciembre de 2009.

A human capital crisis in cybersecurity. *Technical Proficiency Matters,* Center for Strategic & International Studies, July 2010. [disponible en www.csis.org]

Ataques DDoS 2010. Últimas motivaciones y métodos utilizados, *Informe de Amenazas CCN-CERT IA-05/10,* 10.09.2010, [disponible en www.ccn-cert-cni.es (parte privada del portal)]

CCN-CERT IA-03/10 Ciberamenazas 2009 y Tendencias 2010, *Informe de amenazas del CCN-CERT,* 15 de marzo de 2010, [disponible en www.ccn-cert-cni.es (parte privada del portal)]

Cyber Threats and Trends, *An iDefense® Topical Research Paper,* The VeriSign® iDefense® Intelligence Operations Team, 18 de diciembre de 2009

Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations, Swedish Defense Research Agency (FOI), marzo 2010, [disponible en www2.foi.se/rapp/foir2970.pdf], [consulta 7-10-2010]

ENISA Country Reports, European Network and Information Security Agency (ENISA), enero 2010, [disponible en www.enisa.europa.eu]

International Critical Information Infrastructure Protection Directory, Meridian conference, Issue 24. Spain (page 110), agosto 2010

Jihadist and the Internet. 2009 Update, *National Coordinator for Counterterrorism,* mayo 2010, [disponible en english.nctb.nl/current_topics/reports], [consulta 7-10-2010]

La inteligencia, factor clave frente al terrorismo internacional, Cuadernos de Estrategia nº 141, Ministerio de Defensa, 2009

La Sociedad de la Información en España 2009, *Fundación Telefónica,* 21 de diciembre de 2009, [disponible en e-libros.fundacion.telefonica.com/sie09/aplicacion_sie/ParteA/datos.html y

www.fundacion.telefonica.com/prensa/noticias/noticia.php?prog=debateyconocimiento&noticia=21_12_2009_esp.htm]

MOLINA MATEOS José María, *Aspectos jurídicos de la protección criptológica de la información y las comunicaciones,* Universidad Complutense, Madrid, 1999

Online as soon as it happens, *Informe ENISA*, 8 de febrero de 2010, [disponible en www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens]

PASTOR Oscar, PÉREZ José Antonio, ARNÁIZ Daniel, TABOSO Pedro, *Seguridad Nacional y* Ciberdefensa, Cuadernos Cátedra ISDEFE-UPM, octubre de 2009.

Toward a general policy on the fight against cyber crime, Committee from the Commission to the European Parliament, the Council and the Committee of the Regions, 22 de mayo de 2007

Legislación

Borrador de legislación por el que se establecen medidas para la protección de las infraestructuras críticas. Ministerio del Interior, [disponible en www.cnpic-es.es], [consulta 11-6-2010]

Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, *BOE* nº 109 de 7 de mayo de 2002

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, *BOE* nº 150 de 23 de junio de 2007

Ley 9/1968, de 5 de abril, sobre Secretos Oficiales, *BOE* nº 84 de 6 de abril de 1968

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, *BOE* nº 298 de 14 de diciembre de 1999

Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, *BOE* nº 230 de 25 de septiembre de 2007

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, *BOE* n. 17 de 19/1/2008

Real Decreto 263/1996, de 16 de Febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, *BOE* nº 52, de 29 de febrero de 1996

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, *BOE* nº 25 de 29 de enero de 2010

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, *BOE* nº 25 de 29 de enero de 2010

Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, *BOE* nº 68 de 19 de marzo de 2004

Reino Unido

CORNISH Paul, HUGHES Rex and LIVINGSTONE David, *Cyberspace and the National Security of the United Kingdom*, Chatham House, March 2009

Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space. Cabinet Office, June 2009, [disponible en www.cabinetoffice.gov.uk]

Estados Unidos

Cybersecurity. Continued Attention is needed to Protect Federal Information Systems from Evolving Threats, United States Government Accountability Office. GAO-10-834T, 16 de junio de 2010, [disponible en www.gao.gov], [consulta 7-10-2010]

Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure, 29 de mayo de 2009, [disponible en www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf], [consulta 7-10-2010]

National Infrastructure Protection Plan, Homeland Security Department, 2006, [disponible en www.dhs.gov], [consulta 7-10-2010]

Privacy Impact Assessment for EINSTEIN 2, United States Computer Emergency Readiness Team (US-CERT), 19 de mayo 2008, [disponible en www.dhs.gov], [consulta 7-10-2010]

The Comprehensive National Cybersecurity Initiative, White House, 2010, [disponible en http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative], [consulta 7-10-2010]

The National Strategy to Secure Cyberspace., White House. Washington

February 2003, [disponible en www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf], [consulta 7-10-2010]

Canadá

Canada's Cyber Security Strategy. For a stronger and more prosperous Canada. 2010, [disponible en www.publicsafety.gc.ca/prg/em/cbr/ccss-scc-eng.aspx], [consulta 7-10-2010]

Estonia

Cyber Security Strategy. Cyber Security Strategy Committee, Ministry of Defence. Estonia, Tallinn 2008, [disponible en [www.mod.gov.ee/en/national-defense-and-society],[consulta 22-10-2010]

Francia

Défense et Sécurité nationale. Le Livre Blanc, Editorial Odile Jacob/ La Documentation Française, junio 2008, [disponible en www.livreblanc-defenseetsecurite.gouv.fr], [consulta 22-10-2010]

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) decreto n° 2009-834 de 7 de julio de 2009, Journal officiel du 8 juillet 2009, [disponible en www.ssi.gouv.fr], [consulta 22-10-2010]

*Plan de Renforcement de la Sécurité des Systèmes d´Information de L'état, m*arzo 2004, [disponible en www.ssi.gouv.fr], [consulta 22-10-2010]

Alemania

Act to Strengthen the Security of Federal Information Technology of 14 August 2009, Act on the Federal Office for Information Security, BSI Act – BSIG, [disponible en www.bsi.bund.de], [consulta 1-10-2010]

Improving IT Security, BSI Annual Report 2008/2009, Federal Office for Information Security BSI, [disponible en www.bsi.bund.de], [consulta 1-10-2010]

National Plan for Information Infrastructure Protection, octubre 2005, [disponible en www.bmi.bund.de], [consulta 1-10-2010]

Australia

Cyber Security Strategy, Attorney General's Department, 23 de noviembre de 2009, [disponible en www.ag.gov.au/cybersecurity], [consulta 7-10-2010]

E-Security Review 2008, Discussion Paper for public consultation, [disponible en www.ag.gov.au/agd/agd.nsf], [consulta 7-10-2010]

Protecting Yourself Online. What Everyone Needs to Know, Australia 2010, [disponible en www.staysmartonline.gov.au], [consulta 7-10-2010]

Security of Infrastructure Control Systems for Water and Transport, Victorian Government Printer, October 2010, [disponible en www.audit.vic.gov.au], [consulta 5-10-2010]