ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

65/2013 09 diciembre de 2013

Mª José Caro Bejarano

ESTRATEGIA DE CIBERSEGURIDAD NACIONAL

ESTRATEGIA DE CIBERSEGURIDAD NACIONAL

Resumen:

El pasado 5 de diciembre el Consejo de Seguridad Nacional aprobó la Estrategia de Ciberseguridad Nacional, junto con la Estrategia de Seguridad Marítima. Este documento se adopta al amparo y alineada con la Estrategia de Seguridad Nacional de 2013, que contempla la ciberseguridad dentro de sus doce ámbitos de actuación.

Es el documento estratégico que sirve de fundamento al Gobierno de España para desarrollar las previsiones de la Estrategia de Seguridad Nacional en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección y respuesta frente a las ciberamenazas.

La Estrategia de Ciberseguridad Nacional es el marco de referencia de un modelo integrado basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado, en la colaboración público-privada, y en la participación de la ciudadanía. Asimismo, dado el carácter transnacional de la ciberseguridad, la cooperación con la Unión Europea y con otros organismos de ámbito internacional o regional con competencias en la materia, forma parte esencial de este modelo.

Abstract:

On 5th December, the Spanish Security Council approved the Spanish Cyber Security Strategy, together with the Maritime Security Strategy . This document is adopted under and aligned with the National Security Strategy of 2013, which provides cyber security in twelve areas.

This is the strategic document which underpins the Spanish Government to develop the National Security Strategy provisions for cyberspace protection in order to implement in a coherent and structured way the prevention, defense, detection and response actions to cyber threats. The Spanish Cyber Security Strategy is the framework of an integrated model based on the involvement, coordination and harmonization of all State actors and resources, public- private partnerships, and participation of the citizenry. Also, given the transnational nature of cyber security, the cooperation with the European Union and other international or regional organizations competent in the matter, are an essential part of this model.

Palabras clave:

Estrategia, Ciberseguridad, Tecnologías de la Información y Comunicación, TIC, seguridad nacional, ciberamenazas, infraestructuras críticas.

Keywords:

Strategy, cyber security, Information and Communication Technology, ICT, national security, cyber threats, critical infrastructures.

ESTRATEGIA DE CIBERSEGURIDAD NACIONAL

El pasado 5 de diciembre el Consejo de Seguridad Nacional[1] se reunió por segunda vez en el Palacio de la Moncloa presidido por el jefe del Gobierno, Mariano Rajoy. Este Consejo es un órgano colegiado que forma parte de la estructura del Sistema de Seguridad Nacional definido en la Estrategia de Seguridad Nacional[2], ESN. En esta segunda reunión se aprobó la Estrategia de Ciberseguridad Nacional[3], junto con la Estrategia de Seguridad Marítima[4].

De los doce riesgos y amenazas para la seguridad nacional identificados en la ESN, la ciberamenaza es una de las más recientes pero se ha convertido en una de las más preocupantes. El ciberespacio es un nuevo ámbito de relación que ha proporcionado el desarrollo de las nuevas tecnologías de la información y las comunicaciones, pero también ha diluido las fronteras, permitiendo una globalización sin precedentes, que propicia nuevas oportunidades, pero conlleva serios riesgos y amenazas.

La creciente dependencia de la sociedad del ciberespacio y su fácil accesibilidad hacen que cada vez sean más comunes y preocupantes las intromisiones en este ámbito. En buena medida, el ciberespacio es un medio para la materialización de otros riesgos y amenazas. Los ciberataques, en sus diversas modalidades de ciberterrorismo, ciberdelito, ciberespionaje o activismo en la red, se han convertido en un potente instrumento de agresión contra particulares e instituciones públicas y privadas. El bajo coste y mínimo riesgo que suponen para el atacante y su fácil empleo, efectividad y accesibilidad, son factores que explican la extensión del fenómeno.

Estos ataques ilícitos proceden -y cada vez más frecuentemente- de grupos terroristas, redes de crimen organizado, empresas, Estados o individuos aislados. También la ciberseguridad se puede ver comprometida por causas técnicas o fenómenos naturales.

---

[1] La estructura del Sistema de Seguridad Nacional se asienta sobre dos nuevos organismos: el Consejo de Seguridad Nacional y los Comités especializados. El consejo es un órgano colegiado, con reuniones periódicas, con una composición amplia y flexible, y como órganos de apoyo los Comités especializados. Su primera reunión se celebró el pasado 17 de julio.

[2] El pasado 31 de mayo de 2013, el Consejo de Ministros aprobó la nueva "Estrategia de Seguridad Nacional. Un proyecto compartido". El documento, que actualiza la anterior versión fechada en junio de 2011, articula la Seguridad Nacional como Política de Estado y contiene directrices con el fin de reasignar todos los recursos disponibles del Estado de manera eficiente para la preservación de la Seguridad Nacional. Véase en: http://www.lamoncloa.gob.es/NR/rdonlyres/0BB61AA9-97E5-46DA-A53E-DB7F24D5887D/0/Seguridad_1406connavegacionfinalaccesiblebpdf.pdf .

[3] Véase la Estrategia de Ciberseguridad en: http://www.lamoncloa.gob.es/NR/rdonlyres/680D00B8-45FA-4264-9779-1E69D4FEF99D/255433/20131332_completo_05dic13_0955h.pdf.

[4] Véase la Estrategia de Seguridad Marítima en: http://www.lamoncloa.gob.es/NR/rdonlyres/680D00B8-45FA-4264-9779-1E69D4FEF99D/255435/20131333_completo_05dic13_1130h.pdf

Estas circunstancias explican que sea un objetivo prioritario garantizar la integridad, confidencialidad y disponibilidad de los sistemas que soportan la prestación de servicios ampliamente utilizados, así como la gestión de las infraestructuras críticas.

La ausencia de una legislación armonizada en materia de ciberseguridad, así como el hecho de que Internet fuera diseñado como un canal de comunicación accesible, sencillo y útil, sin considerar la dimensión de su seguridad, son elementos que incrementan las posibilidades de que las ciberamenazas se materialicen.

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

Para contrarrestar estas ciberamenazas se define un ámbito de actuación con un objetivo y unas líneas de acción estratégicas. Este ámbito es el de la ciberseguridad cuyo objetivo es *el* de garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques. Este objetivo se conseguirá a través de seis líneas de acción que enmarcarán las actuaciones concretas necesarias para la preservación de la Ciberseguridad Nacional.

Para alcanzar el objetivo de la Ciberseguridad Nacional se aprueba esta nueva estrategia que detalla además del objetivo y las líneas de acción anteriores, el propósito y los principios rectores y define un marco de coordinación mediante la creación de un órgano colegial.

DETALLES DE LA CIBERESTRATEGIA

Con este documento España se pone a la altura de otros países de nuestro entorno y algunas organizaciones internacionales, que tras presentar o revisar sus estrategias nacionales han avanzado su definición con la presentación de una estrategia de segundo nivel que aborda la ciberseguridad nacional. Es de destacar los casos de EE.UU. Alemania, Reino Unido, Francia, Holanda, entre los países, y entre las organizaciones internacionales señalemos la OTAN y la UE.

Aunque España ha sido más tardía en incorporar un documento de ciberseguridad, ya existía anteriormente un tratamiento de este ámbito desde las distintas Administraciones Públicas como lo indica la existencia de diversos órganos en ministerios como Presidencia, Defensa, Interior e Industria, que ahora se coordinarán de forma explícita con el nuevo órgano que se crea con esta Estrategia.

El documento se organiza en cinco capítulos.

El primero, "El ciberespacio y su seguridad", define el ciberespacio y sus características como un nuevo dominio global y dinámico que está compuesto por las infraestructuras TIC (Tecnologías de la Información y la Comunicación). Estas características de los ciberataques incluyen su bajo coste, la ubicuidad y fácil ejecución, su efectividad e impacto, y el reducido riesgo para el atacante. Además identifica como riesgos y amenazas a la Ciberseguridad Nacional un amplio espectro proveniente de: individuos aislados, hacktivistas, amenazas internas, delincuentes, terroristas, estados extranjeros que se suman a los problemas causados por causas técnicas o fenómenos naturales.

El segundo capítulo, "Propósito y principios rectores de la ciberseguridad en España", establece el propósito respetando el objetivo de ciberseguridad marcado en la ESN, así fija las directrices generales de un uso seguro del ciberespacio, con una visión integradora a través de la adecuada coordinación y cooperación de todas las Administraciones Públicas, contando además, con el sector privado y con los ciudadanos. Todo esto teniendo presente el máximo respeto al ordenamiento jurídico interno e internacional y alentando la presencia española en los organismos y foros de carácter internacional que canalizan las iniciativas y esfuerzos en defensa del ciberespacio.

Como principios rectores se recogen cuatro que están en sintonía con los principios informadores de la ESN: unidad de acción; anticipación y prevención; eficiencia y sostenibilidad en el uso de los recursos; y resiliencia o capacidad de resistencia y recuperación. Estos principios rectores son: el liderazgo nacional y la coordinación de esfuerzos; la responsabilidad compartida; la proporcionalidad, racionalidad y eficacia; y la cooperación internacional.

Estos principios se establecen respetando la protección de los derechos fundamentales constitucionales consagrados y con el compromiso por parte del Gobierno de España de desarrollar políticas que mejoren la seguridad de los Sistemas de Información y Telecomunicaciones que emplean todos los sectores de la sociedad: los ciudadanos, profesionales y empresas.

El tercer capítulo "Objetivos de la ciberseguridad", define un objetivo global y seis objetivos específicos. Este objetivo global recoge el objetivo planteado en la ESN en el ámbito de la ciberseguridad "Garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques". Este fin será recogido en la futura Política de Ciberseguridad Nacional. Esta Política estará alineada con iniciativas similares a las de los países de nuestro entorno, así

como con las organizaciones europeas e internacionales competentes, en particular, con la Estrategia de Ciberseguridad de la Unión Europea[5]. Para garantizar la protección de los sistemas y la resiliencia de los servicios de las Administraciones Públicas y las Infraestructuras Críticas, así como la disponibilidad de productos confiables, será necesario potenciar, impulsar y reforzar las capacidades nacionales de investigación y desarrollo en ciberseguridad de las TIC. Para ello se velará por la utilización de componentes que estén certificados conforme a normas internacionalmente reconocidas.

Los otros seis objetivos específicos se refieren a:

Ámbito	**Objetivo**
Administraciones Públicas	garantizar que los Sistemas de Información y Telecomunicaciones utilizadas por éstas poseen el adecuado nivel de seguridad y resiliencia
Empresas e infraestructuras críticas	impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular
Ámbito judicial y policial	potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio
Sensibilización	concienciar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio
Capacitación	alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad
Colaboración internacional	contribuir a la mejora de la ciberseguridad, apoyando el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales, así como colaborar en la capacitación de Estados que lo necesiten a través de la política de cooperación al desarrollo

El objetivo global se detalla en estos seis objetivos específicos y a su vez el sexto objetivo específico de colaboración internacional tendrá repercusión en los otros cinco.

El capítulo 4, “Líneas de acción de la ciberseguridad Nacional”, se centra en detallar las líneas de acción que habrán de articularse para alcanzar los objetivos señalados en el capítulo anterior.

[5] Véase la estrategia de febrero de 2013 en http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Nº	Línea de acción	Medidas
1	Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas	• Ampliar y mejorar las capacidades de detección y análisis de ciberamenazas que permitan la identificación de procedimientos y orígenes de ataque, y la elaboración de la inteligencia necesaria para una defensa y protección más eficaz de las redes nacionales. • Ampliar y fortalecer las capacidades de detección y respuesta ante ciberataques dirigidos contra objetivos de carácter nacional, regional o sectorial, incluyendo a ciudadanos y empresas. • Garantizar la coordinación, la cooperación y el intercambio de información entre la Administración General del Estado, las Comunidades Autónomas, las Entidades Locales, el sector privado y los organismos competentes de la UE e internacionales para asegurar la permanente concienciación, formación y capacidad de respuesta a través del Sistema de Intercambio de Información y Comunicación de Incidentes. • Asegurar la cooperación de los organismos con responsabilidades en ciberseguridad, en especial entre el CERT de la Administración Pública del Centro Criptológico Nacional (CCN-CERT), el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) y el CERT de Seguridad e Industria. Los CERT de las Comunidades Autónomas, los de las entidades privadas y otros servicios de ciberseguridad relevantes deberán estar coordinados con los anteriores en función de las competencias de cada uno de ellos, articulando los instrumentos adecuados a tal efecto. • Desarrollar y mantener actualizadas las instrucciones de prevención y detección, incluyendo procedimientos de respuesta frente a situaciones de crisis y planes de contingencia específicos ante incidentes de ciberseguridad de ámbito nacional, asegurando su integración en el Sistema de Seguridad Nacional. • Desarrollar y ejecutar un Programa de Ejercicios de Simulación de Incidentes de Ciberseguridad, para evaluar y perfeccionar las acciones llevadas a cabo en este ámbito. • Ampliar y mejorar permanentemente las capacidades de Ciberdefensa de las Fuerzas Armadas que permitan una adecuada protección de sus Redes y Sistemas de Información y Telecomunicaciones, así como de otros sistemas que afecten a la Defensa Nacional. Se

		consolidará la implantación del Mando Conjunto de Ciberdefensa y se potenciará su cooperación con los diferentes órganos con capacidad de respuesta ante incidentes cibernéticos en aspectos de común interés. • Potenciar las capacidades militares y de inteligencia para ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.
2	Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas	• Asegurar la plena implantación del Esquema Nacional de Seguridad y articular los procedimientos necesarios para conocer regularmente el estado de las principales variables de seguridad de los sistemas afectados. • Ampliar y mejorar las capacidades del CERT de las Administraciones Públicas-CCN-CERT- y particularmente de sus Sistemas de Detección y de Alerta Temprana. • Reforzar las estructuras de seguridad y la capacidad de vigilancia de los Sistemas de Información, en particular los que manejan información clasificada. • Optimizar el modelo de interconexión de los organismos de las Administraciones Públicas españolas a las redes públicas de voz y datos, maximizando su eficacia, disponibilidad y seguridad. • Reforzar la implantación y seguridad de la infraestructura común y segura en la Administración Pública española (Red SARA), potenciando su uso y sus capacidades de seguridad y resiliencia. • Desarrollar nuevos servicios horizontales seguros, de acuerdo con directrices de la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado, organismo responsable de la coordinación, dirección y racionalización del uso de las TIC en la Administración General del Estado. • Incrementar las actividades nacionales para el desarrollo y evaluación de productos, servicios y sistemas a fin de obtener su certificación apoyando específicamente aquellas que sustenten necesidades de interés nacional. • Potenciar la creación, difusión y aplicación de las Mejores Prácticas en materia de Ciberseguridad en el ámbito de las Administraciones Públicas.
3	Seguridad de los Sistemas de Información y Telecomunicaciones que	En este ámbito, el Gobierno de España adoptará, entre otras, las siguientes medidas: • Asegurar la implantación de la normativa sobre

	soportan las Infraestructuras Críticas	Protección de las Infraestructuras Críticas con el fin de conseguir una seguridad que abarque tanto el ámbito físico como el tecnológico. Para ello, se evaluará la inclusión de las medidas de ciberseguridad oportunas en los distintos planes que se establezcan. • Ampliar y mejorar las capacidades del CERT de Seguridad e Industria, potenciando la colaboración y coordinación con el Centro Nacional para la Protección de Infraestructuras Críticas, con los diferentes órganos con capacidad de respuesta ante incidentes y con las unidades operativas de las Fuerzas y Cuerpos de Seguridad del Estado. • Impulsar la participación del sector privado en los Programas de Ejercicios de simulación de incidentes de Ciberseguridad. • Desarrollar modelos de simulación que permitan analizar las dependencias entre las diferentes Infraestructuras Críticas y los riesgos acumulados por éstas.
4	Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia	• Integrar en el marco legal español las soluciones a los problemas que surjan relacionados con la ciberseguridad para la determinación de los tipos penales y el trabajo de los departamentos competentes. • Ampliar y mejorar las capacidades de los organismos con competencias en la investigación y persecución del ciberterrorismo y la ciberdelincuencia así como asegurar la coordinación de estas capacidades con las actividades en el campo de la ciberseguridad, a través del intercambio de información e inteligencia por los canales de comunicación adecuados. • Fortalecer la cooperación policial internacional y fomentar la colaboración ciudadana, articulando los instrumentos de intercambio y transmisión de información de interés policial. • Asegurar a los profesionales del Derecho el acceso a la información y a los recursos que les proporcionen el nivel necesario de conocimientos en el ámbito judicial para la mejor aplicación del marco legal y técnico asociado. En este sentido, es especialmente importante la cooperación con el Consejo General del Poder Judicial, la Abogacía del Estado, la Fiscalía General del Estado, la Fiscalía Coordinadora de la Criminalidad Informática y el Consejo General de la Abogacía Española.

5	Seguridad y resiliencia de las TIC en el sector privado	El Gobierno desarrollará, entre otras, las siguientes medidas: • Impulsar la cooperación entre los sectores público y privado, promoviendo el intercambio de información sobre vulnerabilidades, ciberamenazas y sus posibles consecuencias, especialmente en lo relativo a la protección de los sistemas de interés nacional. • Promover la cooperación con los sectores de la industria y los servicios de la ciberseguridad, con el fin de mejorar conjuntamente las capacidades de detección, prevención, respuesta y recuperación frente a los riesgos de seguridad del ciberespacio, impulsando la participación activa de los proveedores de servicios así como el desarrollo y adopción de códigos de conducta y buenas prácticas. • Impulsar el desarrollo de estándares en ciberseguridad a través de los organismos y entidades de normalización y certificación nacionales e internacionales, y promover su adopción.
6	Conocimientos, Competencias e I+D+i	• Desarrollar un marco de conocimientos de ciberseguridad en los ámbitos técnico, operativo y jurídico. • Programas de captación de talento, investigación avanzada y capacitación en ciberseguridad en cooperación con Universidades y centros especiali-zados. • Establecer mecanismos de identificación temprana de las prioridades y demandas de los poderes públicos en materia de ciberseguridad. • Fomentar el desarrollo industrial de productos y servicios en materia de ciberseguridad por medio de los instrumentos disponibles. • Impulsar la coordinación nacional y la dinamización del sector industrial y de servicios de ciberseguridad para la mejora de la competitividad, la internacionalización, la identificación de oportunidades, la eliminación de barreras y la orientación normativa, entre otras actividades. • Impulsar las actividades de certificación de ciberseguridad de acuerdo con las normas y estándares de reconocimiento internacional... • Impulsar modelos y técnicas de análisis de ciberamenazas y medidas de protección de productos, servicios y sistemas, así como su especificación, evaluación y certificación.

7	Cultura de ciberseguridad	• Impulsar las actividades de sensibilización entre ciudadanos y empresas con acceso a información relativa a vulnerabilidades, ciberamenazas e información sobre cómo proteger mejor su entorno tecnológico. • Propiciar el desarrollo de programas de Concienciación en Ciberseguridad, en colaboración con agentes del sector público y privado potenciando. • Fomentar los mecanismos para apoyar a empresas y profesionales en el uso seguro de las TIC, reforzando los conocimientos en materia de seguridad, promoviendo la adopción de herramientas, la difusión de normativa y el uso de buenas prácticas. • Asesorar y dar soporte al desarrollo de módulos educativos de sensibilización en ciberseguridad, dirigidos a todos los niveles de la enseñanza.
8	Compromiso Internacional	• Potenciar la presencia de España en organizaciones y foros internacionales y regionales sobre ciberseguridad. • Promover la armonización legislativa y la cooperación judicial y policial internacionales en la lucha contra la ciberdelincuencia y el ciberterrorismo. • Propiciar la suscripción de acuerdos en el seno de organizaciones internacionales y con los principales socios y aliados. • Impulsar el establecimiento de canales internacionales de información, detección y respuesta. • Promover la participación coordinada de instituciones públicas y del sector privado en simulacros y ejercicios internacionales. • En el ámbito de la UE, colaborar en la armonización de legislaciones nacionales, la implantación de la Estrategia de Ciberseguridad de la UE y el impulso de una política internacional en el ciberespacio. • Fomentar la cooperación con la OTAN en materia de Ciberdefensa.

El quinto y último capítulo, ”La ciberseguridad en el Sistema de Seguridad Nacional”, establece la estructura orgánica al servicio de la ciberseguridad que responde a la visión integral del documento con objeto de dar una respuesta conjunta y adecuada para preservar la ciberseguridad. Esta estructura orgánica está formada por tres componentes, los dos últimos de nueva creación, bajo la dirección del Presidente del Gobierno: a) el Consejo de

Seguridad Nacional; b) el Comité Especializado de Ciberseguridad; c) el Comité Especializado de Situación, único para el conjunto del Sistema de Seguridad Nacional.

El Comité Especializado de Ciberseguridad dará apoyo al presidente del Gobierno y al propio Consejo de Seguridad Nacional para coordinar la Política de Seguridad Nacional en el ámbito de la ciberseguridad. Se encargará, además, de reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privados, y facilitará la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.

Este Comité estará compuesto por representantes de los distintos ámbitos de las Administraciones Públicas afectados, amén de otros actores pertenecientes al sector privado y especialistas en ciberseguridad.

Según algunas fuentes publicadas[6] la presidencia de este Comité será rotatoria, y tendrá periodicidad anual. La rotación se hará entre representantes de los ministerios de la Presidencia, del Interior, de Industria, Energía y Turismo, de Defensa y de Asuntos Exteriores y de Cooperación.

Por otra parte el Comité Especializado de Situación, único para el conjunto del Sistema de Seguridad Nacional, será convocado para gestionar las situaciones de crisis de ciberseguridad que, por su transversalidad o su dimensión, desborden las capacidades de respuesta de los mecanismos habituales. Contará con el apoyo del Centro de Situación del Departamento de Seguridad Nacional para garantizar su interconexión con los centros operativos implicados y dar una respuesta adecuada en situaciones de crisis, facilitando su seguimiento y control y la trasmisión de las decisiones.

Los dos Comités Especializados actuarán de forma complementaria, cada uno en su ámbito de competencias, con una misma dirección estratégica y política del Consejo de Seguridad Nacional presidido por el Presidente del Gobierno.

Mª José Caro Bejarano
Analista Principal IEEE

[6] Agencia EFE, 5 de diciembre de 2013