III CURSO DE VERANO ADESyD
7-10 julio 2014

"Una visión integral de la Seguridad: nacional, internacional, pública, privada y ciudadana"

"La Estrategia de Ciberseguridad Nacional"

Ana Belén Perianes Bermúdez
Doctoranda en Seguridad Internacional
Experta en Seguridad en el Mediterráneo, Próximo Oriente y Oriente Medio.

7 de julio de 2014

Introducción

* La **ciberseguridad** tiene **carácter global** y afecta a toda la sociedad, tanto a la ciudadanía, a la Administración Pública como al sector privado y económico. Todo el mundo puede ser objetivo de un ciberataque o sufrir un ciberincidente.
* El **paradigma del ciberespacio lo envuelve todo** y cada vez más complejo de administrar. **Creciente internetización** de la sociedad y dependencia total de la tecnología de la información y comunicación. El incremento en la conectividad y la recogida masiva de información aumenta el número de ciberataques y ciberincidentes.
* **Nuevo reto tecnológico, organizativo y administrativo que ha de afrontar España.** Ciberespacio no conoce fronteras ni limite temporal. **Carácter transnacional de la ciberseguridad.**
* **Cloud** o la nube conlleva una concentración de gran cantidad de información. **Objetivo muy rentable para los ciberatacantes.** Vulneración de la confidencialidad, metainformación, big data.

* Nuevas tendencias tecnológicas como el ***bring your own device*** (utilizar el dispositivo personal como smarphone, tablet o portátil en el centro laboral para la actividad corporativa) incorporan un agujero de seguridad. La filtración de información pueden facilitar ciberataques.
* Ciberespacio como **nuevo campo de batalla** en el que tiene lugar la guerra financiera, energética, empresarial, política, mediática, etc.
* **Facilidad y bajo coste del empleo de internet** que produce la globalización.
* **Cambio en el perfil del ciberatacante**. Hasta hace poco era el de hackers, ciberactivistas o redes más o menos organizadas de ciberminales. En la actualidad, cibercomandos de las fuerzas armadas de Estados, cuyos objetivos son militares, políticos y económicos.
* **Firewall y antimalware actualizado no impiden un ciberataque**.
* **La finalidad última de una estrategia de ciberseguridad debe ser la protección activa y pasiva del activo nacional.**

- **Ciberespacio** como **campo de batalla muy tangible**: Tablet; portátil; smartphone conectado a una red corporativa o personal; el router doméstico o de la oficina; un edificio; una destructora de papel que copia; la impresora que se puede hackear; el tendido de telefónico y de fibra óptica por los que circula gran cantidad de información; los sistemas SCADA de la las infraestructuras críticas de producción y distribución de energía que tengan algún punto ciego o conectado a internet; un contador de la energía inteligente; un frigorífico inteligente o una televisión inteligente…
- **El nivel de alerta** en España ante incidentes de la seguridad de la información el 5 de julio de 2014 era: **MUY ALTO**.
- Fuente: Centro Criptológico Nacional.
- https://www.ccncert.cni.es/index.php?option=com_content&view=article&id=1948&Itemid=2&lang=es

Principales agentes de ciberamenazas que pueden afectar a **España**

* El **ciberespionaje** o robo de la propiedad intelectual o información crítica, que afecta tanto a la Administración Pública como a la empresa estratégica y a la ciudadanía.
* El **ciberdelito o cibercrimen**. Tiene como objetivo el robo por ejemplo de tarjetas de crédito, el fraude telemático, el blanqueo de dinero, etc, llevado a cabo principalmente por hackers y el crimen organizado.
* El **ciberactivismo**, que ataca a webs y roba y publica información delicada o de carácter personal. Anonymous.
* El **ciberterrorismo**. Objetivo: el ataque a infraestructuras críticas, la comunicación de su ideario, la obtención de información, propaganda o financiación. Ciberyihad.

Ámbitos que reciben más ciberataques en España: Infraestructuras críticas y sectores estratégicos.

* Administración Pública.
* Industria Nuclear.
* Sector de la defensa.
* Sector energético.
* Sector espacial.
* Sector financiero.
* Sector hídrico.
* Sector de la alimentación.
* Sector del transporte.
* Sector de la sanidad y la industria química y farmacéutica.
* Instalaciones de investigación.
* Tecnologías de la información.
* Derechos humanos.

Nota: Ciberincidentes en estos sectores pueden perjudicar el normal desarrollo de la actividad del país.

1.La Estrategia de Ciberseguridad Nacional Española

* Aprobada el **5 de diciembre de 2013** por el Consejo de Seguridad Nacional, al amparo y alineada con la Estrategia de Seguridad Nacional de España.
* España decimoctavo país europeo que cuenta con una estrategia de ciberseguridad nacional.
* Documento de carácter estratégico mediante el cual el Gobierno fundamenta la implantación de acciones en materia de prevención, defensa, detección y recuperación frente a las amenazas del ciberespacio.
* Ciberseguridad como ámbito de actuación fijado en la Estrategia de Seguridad Nacional.
* España se encuentra plenamente amenazada por ciberataques, que originan tanto un **elevado coste económico** como un **riesgo a la seguridad nacional.**

* El **anonimato** permite planificar y ejecutar un ataque a cualquier punto del ciberespacio desde cualquier parte del mundo.
* La ciberseguridad también puede verse afectada por **elementos fortuitos y no deliberados** como un problema técnico o un fenómeno natural.
* Un óptimo Sistema de Ciberseguridad Nacional exige una **colaboración estratégica público-privada.**
* El avance en ciberseguridad nacional contribuyen, además de a apoyar el Sistema de Seguridad Nacional, el Estado de Derecho y el normal funcionamiento del país, a **incrementar el potencial económico**. La ciberseguridad fundamenta un entorno más fiable para invertir, la generación de empleo y la competitividad de país.

Estructura de la Estrategia de Ciberseguridad Nacional

Cinco capítulos:

* El ciberespacio y su seguridad.
* Propósito y principios rectores de la ciberseguridad en España.
* Objetivos de la ciberseguridad.
* Líneas de acción de la ciberseguridad nacional.
* La ciberseguridad en el Sistema de Seguridad Nacional.

1.1-El ciberespacio y su seguridad.

* La ECN reconoce que la **difuminación de fronteras**, el **alto grado de dependencia del país** en cuanto a la **Tecnología de la Información y la Comunicación** y la **democratización del uso de las nuevas tecnologías** derivada de la globalización ha favorecido la aparición de nuevas oportunidades a la sociedad y, con ello, **nuevos retos y amenazas** en el nuevo espacio, el **ciberespacio**.
* La Estrategia de Ciberseguridad Nacional se configura como una **exigencia para nuestro modelo económico y de país** ya que de la seguridad de las TICs depende en gran medida la estabilidad, la economía, la Administración Pública, la óptima articulación de las infraestructuras críticas y el óptimo funcionamiento del país.
* La ECN caracteriza a los **ciberataques : bajo coste o gratuito; ubicuidad y anonimato del atacante, fácil ejecución, no requieren de un gran conocimiento técnico; efectividad e impacto, falta de concienciación ciudadana y de formación en la materia; bajo riesgo para el atacante, vacío legal.**

Factores que pueden comprometer la ciberseguridad según la ECN

Tres grupos de factores: técnicos, fenómenos naturales o ataques deliberados.

Más concretamente, los riesgos y amenazas a la ciberseguridad y ciberespacio nacional pueden proceder de:

* Estados extranjeros.
* Motivación técnica.
* Hacking.
* Crimen organizado.
* Terrorismo.
* Hacktivismo.
* Delincuencia.
* Terrorismo.
* Espionaje.
* Individuos independientes.
* Sabotaje.
* Amenazas internas.
* Conflictos.
* Fenómenos naturales.

1.2-Propósito y principios rectores de la ciberseguridad en España.

La ECN aboga por la óptima coordinación y cooperación de la Administración Pública con el sector privado y la ciudadanía.

* Los **principios rectores** que contempla la ECN son:
  * **El liderazgo nacional y coordinación**. El presidente del Gobierno dirigirá y controlará la Política de Ciberseguridad Nacional en el marco del Consejo de Seguridad Nacional.
  * Se requiere una gran **coordinación entre la Administración Pública y el sector privado** para intercambiar iniciativas e información. El papel de la ciudadanía como fundamental y se ha de implicar en la ciberseguridad del país.
  * **Proporcionalidad, racionalidad y eficacia**.
  * **Cooperación internacional**. El carácter transnacional de las amenazas a la ciberseguridad lleva a requerir la cooperación global para ganar eficacia.

1.3-Objetivos de la ciberseguridad.

* El **objetivo global** de la ECN será lograr **que España alcance la seguridad en el ciberespacio** fortaleciendo la capacidad de prevención, defensa, detección y de responder a los ciberataques.
* El documento de la ECN indica que promoverá el desarrollo de un **adecuado marco normativo y la coordinación** de toda la Administración Pública con cada agente que detente competencia en la materia.
* Incidencia en la exigencia de garantizar la **Protección del Patrimonio Tecnológico nacional.**
* La ECN aboga por **fortalecer la cooperación judicial y policial internacional,** articulando la colaboración e intercambio de información y la armonización de las legislaciones nacionales.
* **Concienciación** de la ciudadanía, profesionales, empresas y Administración Pública sobre los riesgos derivados del ciberespacio. Se ha de promover una profunda **cultura de la ciberseguridad**.

* **Capacitación** para alcanzar y mantener el conocimiento, habilidad, experiencia y capacidad tecnológica que requiere España para mantener el objetivo de la ciberseguridad. Se debe fomentar y mantener una actividad de **I+D+I** en materia de ciberseguridad de materia efectiva. Debido a la relevancia estratégica de la ciberseguridad, se ha de contar con **personal cualificado tanto a nivel de gobierno, directivo, operativo, técnico y judicial**. Se requiere la **colaboración público-privada** de investigación.
* La **colaboración internacional** debe contribuir a la mejora de la ciberseguridad, apoyando la implementación de una política de ciberseguridad coordinada en la Unión Europea y en el nivel internacional, así como colaborar en la capacitación de Estados que lo requieran a través de la política de cooperación al desarrollo.

1.4-Líneas de acción de la ciberseguridad nacional.

1.4.1 **Capacidad de prevención, detección, réplica y recuperación ante las ciberamenazas.** La línea contempla :

* Permitir la **identificación de procedimientos y origen de ataque** y la **elaboración de la inteligencia** que se requiere para poder proteger y defender la red nacional.
* Obtener la capacidad para poder **detectar y responder ciberataques de objetivo nacional, regional o sectorial,** incluyendo a la ciudadanía y al sector privado.
* 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, la UE y la comunidad internacional para garantizar la permanente concienciación, formación y capacidad de respuesta a través del Sistema de Intercambio de Información y Comunicación de Incidentes.

- Garantizar la **cooperación de las entidades con competencia en ciberseguridad**, sobre todo 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 del sector privado y otras redes de ciberseguridad relevantes deberán estar coordinados con los anteriores.
- Capacidad para hacer frente a **situaciones de crisis y planes de contingencia** específicos ante incidentes de ciberseguridad de ámbito nacional.
- Planificar 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 la capacidad en materia de Ciberdefensa de las Fuerzas Armadas.
- Potenciar la capacidad militar y de inteligencia con el objetivo de garantizar la Defensa Nacional.

1.4.2 **Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas. Se estima:**

* **Ampliar y mejorar la capacidad del CERT de las Administraciones Públicas-CCN-CERT-** y particularmente de sus **Sistemas de Detección y de Alerta Temprana.**
* **Velar por la estructura de la seguridad** que alberga información crítica.
* **Reforzar la implantación y seguridad de la infraestructura común y segura en la Administración Pública española** (Red SARA).
* Potenciar la creación, propagación y aplicación de las **Mejores Prácticas** en materia de Ciberseguridad en el ámbito de la Administración Pública.

1.4.3 **Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas.** La ECN prevé:

* Garantizar la **implantación de la normativa** sobre Protección de las Infraestructuras Críticas con el fin de alcanzar una seguridad que abarque tanto el ámbito físico como el tecnológico.
* Ampliar y mejorar la **capacidad 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 para responder ante incidentes y con Fuerzas y Cuerpos de Seguridad del Estado.
* Fomentar la participación del **sector privado en los Programas de Ejercicios de simulación de incidentes de Ciberseguridad**.
* **Implementar modelos de simulación** que permitan analizar el riesgo acumulado por las Infraestructuras Críticas.

1.4.4 **Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia.** Se plantea:

* **Integrar en el marco legal** español la actualización a los problemas que aparezcan en relación con la ciberseguridad para la determinación de los tipos penales y el trabajo de los departamentos competentes.
* **Ampliar y mejorar la capacidad competencial** que permita investigar y perseguir el ciberterrorismo y la ciberdelincuencia así como garantizar la coordinación e intercambio de información e inteligencia.
* **Fortalecer la cooperación policial internacional y fomentar la colaboración ciudadana,** articulando una instrumentación que permita intercambiar y transmitir información de interés policial.
* **Garantizar 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.

1.4.5 **Seguridad y resiliencia de las TIC en el sector privado.** La ECN explica que se implementarán medidas con el objetivo de:

* **Fomentar** la cooperación entre el sector público y el privado, promoviendo **el intercambio de información de vulnerabilidades y ciberamenazas**, sobre todo de interés nacional.
* **Promover la cooperación con la industria y el ámbito de la ciberseguridad,** con el fin de mejorar conjuntamente la capacidad de detección, prevención, réplica y recuperación frente al riesgo de seguridad del ciberespacio, favoreciendo la participación activa de los proveedores de servicios así como la adopción de un código de conducta y buenas prácticas.
* **Promover la adopción de estándares en ciberseguridad,** de normalización y certificación nacional e internacional y potenciar su adopción.

1.4.6 **Conocimiento, Competencia e I+D+I**. La Estrategia promueve:

* **Implementar un marco de conocimientos de ciberseguridad en el ámbito técnico, operativo y jurídico.**
* **Fomentar programas de captación de talento, investigación avanzada y capacitación en ciberseguridad en cooperación con el mundo académico.**
* Fijar un método de identificación temprana de las prioridades y demandas de la Administración Pública en materia de ciberseguridad.
* Promover la **coordinación nacional y la dinamización del sector industrial** para la mejora de la competitividad, la internacionalización, la identificación de oportunidades, la eliminación de barreras y la orientación normativa.
* Potenciar la **certificación internacional** en materia de ciberseguridad.

1.4.7 **Cultura de ciberseguridad**. Se aboga por:

* **Fomentar concienciación entre la ciudadanía y el sector privado** en cuanto a la información relativa a vulnerabilidades, ciberamenazas e información sobre cómo proteger mejor su entorno tecnológico.
* Fomentar el apoyo al sector privado en cuanto a la utilización segura de las TIC, reforzando el conocimiento en materia de seguridad, promoviendo la adopción de herramientas, difundiendo normativa y buenas prácticas.

1.4.8 **Compromiso Internacional.** La Estrategia de Ciberseguridad Nacional determina:

* **Potenciar el papel de España** en organizaciones, 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 adopción de acuerdos** en el marco de organizaciones internacionales y con los principales socios y aliados.
* **Favorecer la adopción 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 legislación nacional**, la implantación de la Estrategia de Ciberseguridad de la UE y el avance en materia de una política internacional en el ciberespacio.
* **Fomentar la cooperación con la OTAN** en materia de Ciberdefensa.

1.5- La ciberseguridad en el Sistema de Seguridad Nacional.

* La ECN configura la estructura orgánica encargada de velar por la ciberseguridad española. La fija a partir de tres niveles: 1) el Consejo de Seguridad Nacional, 2) el Comité Especializado de Ciberseguridad y 3) el Comité Especializado de Situación.

* En cuanto al **Comité Especializado de Ciberseguridad**, la ECN fija su apoyo al presidente del Gobierno y al Consejo de Seguridad Nacional para coordinar la Política de Seguridad Nacional en el ámbito de la ciberseguridad. También reforzará la coordinación, colaboración y cooperación entre Administración Pública con competencia en ciberseguridad, entre el sector público y el privado. Componen el Comité miembros de la Administración Pública, del sector privado y expertos en la materia.

* Respecto a **Comité Especializado de Situación**, único para el conjunto del Sistema de Seguridad Nacional, será convocado para gestionar y tratar las situaciones de crisis de ciberseguridad que, por su transversalidad o su dimensión, desborden la capacidad 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 coyunturas de crisis, facilitando control y la trasmisión de las noticias.

2.Reflexiones sobre la ECN

* La **intangibilidad de la ciberseguridad** y la **falta de interés** y **conocimiento** prácticamente generalizado entre la ciudadanía dificulta la implementación de una oportuna política de seguridad nacional de protección del ciberespacio tanto a nivel nacional como europeo y global.
* La **complejidad del ciberespacio**, cuyo **carácter transnacional no reconoce las fronteras** estatales, junto con la **facilidad del empleo de la red y su bajo coste, requiere elaborar e implementar una oportuna y adecuada política en materia de ciberseguridad**. Y todo ello racionalmente, sin exagerar ni dramatizar.
* Una oportuna Estrategia de Ciberseguridad Nacional debería permitir al país detectar y actuar, entre otros, ante un ciberincidente no deliberado, ante un ciber-11M, un ciberataque a una infraestructura crítica o un ciberataque que produzca una caída de las comunicaciones

Con el objetivo de avanzar en materia de ciberseguridad nacional, se propone:

* **Voluntad y decidido apoyo político** para implementar en detalle una oportuna y concreta política, marcando prioridades en materia de ciberseguridad.
* **Concienciación en materia de ciberseguridad a nivel político, empresarial y de la población. Hándicap de la limitada cultura en materia de seguridad en España.**
* Incidir muy decididamente en la **formación y la cultura de la seguridad y ciberseguridad en el país**.
* Se requiere un fuerte liderazgo tanto público como privado debido a la falta de percepción de las amenazas tanto a nivel nacional como global. Para ello,
* Dotación de **partidas presupuestarias**. Capacidad económica.
* Se debe **invertir en seguridad informática** a todos los niveles.

* **La ECN debería definir claramente cómo lograr los objetivos en materia de ciberseguridad española** (fines, medios…). También debería **fijar la importancia estratégica del ciberespacio** en el ámbito de la ciudadanía, el económico y político. Analizar profundamente el impacto, alcance y potencial de los ciberataques o ciberincidentes ayudaría a la tarea de concienciación del país en cualquier nivel.
* Legislación. Se debe **cubrir el vacío legal** que supone la falta de legislación armonizada en materia de ciberseguridad. Se requiere así una **armonización legislativa**.
* **Cooperación y colaboración público-privada**. Se necesita materializar un intercambio informativo y de inteligencia, así como una monitorización tanto pública como privada de la amenaza y la garantia de la cadena de suministro y distribución. Potenciar la colaboración Estado-Universidad-Empresa y fomentar el desarrollo de la I+D+I en la materia.

* **Incentivar económicamente al sector privado** para que avance en materia de ciberseguridad.
* **Potenciación y apoyo a la industria nacional** de ciberseguridad.
* **Colaboración internacional.**
* Se ha de actuar preventiva y operativamente cibermaniobrando en entornos virtuales realistas. Realización de c**iberejecicios.**
* Se debe trabajar con el **problema** que conlleva el hecho que **las organizaciones no reconozcan incidentes en materia de ciberseguridad** y no proporcionen información de gran utilidad para poder corregir vulnerabilidades sistémicas.
* **La vigilancia y detección de los *zero days*.**
* **Capacitación en la lucha contra el ciberespionaje.** Los ciberatacantes perfeccionan constantemente su procedimiento, que complica la identificación de ciberataques.

3. El esquema de la ciberseguridad en España. Organismos nacionales.

* La responsabilidad de la **seguridad del ciberespacio nacional** se encuentra **muy fragmentada** en el ámbito de la **Administración General del Estado y las autonomías.**
* La **estructura orgánica española** en materia de ciberseguridad queda configurada así en la Estrategia de Ciberseguridad Nacional:
  * **El Consejo de Seguridad Nacional**. Configurado como Comisión Delegada del Gobierno para la Seguridad Nacional, apoya al presidente del Gobierno en la dirección de la Política de Seguridad Nacional.
  * **El Comité Especializado de Ciberseguridad**. Apoya al órgano anterior para el cumplimiento de sus funciones y, en particular, al presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad.

* **El Comité Especializado de Situación**, único para el conjunto del Sistema de Seguridad Nacional. El Comité será convocado para llevar a cabo la gestión de las situaciones de crisis en el ámbito de la ciberseguridad que desborden los límites de la capacidad de respuesta eficaz previstos, con el objetivo de garantizar una respuesta inmediata y eficaz a través de un único órgano de dirección político-estratégica de la crisis. Contará con el apoyo del Centro de Situación del Departamento de Seguridad Nacional. El Centro podrá ser apoyado por personal especializado procedente de los departamentos ministeriales u organismos competentes, que conformarán la Célula de Coordinación en ciberseguridad.
* # **El Consejo Nacional de Ciberseguridad** celebró a final de febrero de 2014 en el Complejo de La Moncloa su reunión constitutiva como órgano interministerial de apoyo al Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional.

En cuanto a la **coordinación nacional**, cabría apuntar varios niveles:

* **Administración Pública: El CCN-CERT** o Centro Criptológico Nacional es el centro gubernamental con capacidad ante incidentes de seguridad de la información (CERT responde a Computer Emergency Response Team). Coordina la acción de la Administración Pública en materia de procedimiento de cifra, garantiza la seguridad de las Tecnologías de la Información en el ámbito e informa sobre la adquisición coordinada del en este campo. El CCN fue creado en el año 2004, a través del Real Decreto 421/2004, adscrito al Centro Nacional de Inteligencia (CNI). Contribuye a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a la Administración Pública y a la empresa estratégica y afrontar de forma activa las nuevas ciberamenazas.

https://www.ccn-cert.cni.es/

Infraestructuras críticas: CNPIC.

* El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) es el órgano que se encarga fomentar, coordinar y controlar toda la actividad que tiene encomendada la Secretaría de Estado de Seguridad del Ministerio del Interior en relación con la protección de las infraestructuras críticas españolas. Su objetivo es minimizar lavulnerabilidad de las infraestructuras críticas en el territorio nacional. El normal funcionamiento del país depende de una u otra forma, de algún ámbito estratégico de los doce contemplados por la normativa española:
  * Administración, agua, alimentación, energía, espacio, industria química, industria nuclear, centro de investigación, salud, sistema financiero y tributario, tecnologías de la Información y las Comunicaciones (TIC) y transporte.

* En España, la seguridad de las infraestructuras críticas se enmarcan principalmente en el ámbito de la protección contra ataques deliberadas y, especialmente, contra ataques terroristas, resultando por ello lideradas por el Ministerio del Interior.

www.cnpic-es.es/

Ámbito empresarial y ciudadanía: INTECO.

* La actividad del Instituto Nacional de Tecnologías de la Comunicación se apoya en tres pilares fundamentales: la dotación de actividades, la investigación y la coordinación.
  * Servicios: INTECO promueve actividades en el ámbito de la ciberseguridad que permitan el aprovechamiento de las TIC y eleven la confianza digital.
  * Investigación: INTECO cuenta con una importante capacidad para abordar proyectos de gran complejidad y con una fuerte componente innovadora. Con su orientación a la investigación, cuente con capacidad para generar inteligencia en ciberseguridad como motor para abordar su aplicación en nueva tecnología y herramientas que reviertan también en la mejora de su actividad.

* Coordinación: INTECO participa en redes de colaboración que facilitan la inmediatez, globalidad y efectividad a la hora de implementar una actuación en el ámbito de la ciberseguridad. La coordinación y colaboración con entidades, tanto públicas como privadas, nacionales e internacionales, de todo el ámbito de la ciberseguridad se configura un factor fundamental para la actividad de INTECO.
* Las iniciativas de INTECO se dirigen a varios niveles:
  * Al sector privado y empresarial que hacen uso de las TIC. Dedica su actividad a la protección de ámbitos estratégicos, fundamentales para la economía y la sociedad, así como a organizaciones con afiliación a RedIRIS.
  * Expertos en ciberseguridad. A través del equipo especializado en ciberseguridad, INTECO ofrece actividad de información a colectivos y profesionales expertos para mejorar el nivel de ciberseguridad nacional.

* -Ciudadanía: la Oficina de Seguridad del Internauta, OSI es la actuación gratuito que proporciona información y apoyo al usuario final para evitar y solucionar problemas de seguridad que le pueden surgir al navegar por Internet.

www.inteco.es

* Capacidad militar y de defensa. El Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. Es el órgano de la estructura operativa, subordinado al Jefe de Estado Mayor de la Defensa (JEMAD), que realiza el planeamiento y la ejecución de la ciberdefensa militar en la red y sistema de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la responder adecuadamente en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

* El Mando Conjunto de Ciberdefensa participa en **ciberejercicios**:
* **Cyber Europe 2014**: La etapa técnica de Cyber Europe 2014, organizado por la Agencia Europea para la Seguridad de las Redes y la Información (ENISA), se ha realizado recientemente durante los días 28 y 29 de abril. El ejercicio ha contado con la participación de unos 30 naciones y cerca de 400 equipos. España ha contado con cinco equipos, tanto de la Administración General del Estado como del ámbito privado: Iberdrola, el Centro Criptológico Nacional (CCN), el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), el Instituto Nacional de Tecnologías de la Comunicación (INTECO) y el propio Ministerio de Defensa. El ejercicio trabajado en un teatro virtual frente a ciberataques a infraestructuras críticas nacionales, denegación de servicios, infecciones mediante "malware" y ciberespionaje.

* **Ciberejercicio "Locked Shields 14"**: El Mando Conjunto de Ciberdefensa (MCCD) ha liderado el equipo español participante en el ciberejercicio "Locked Shields 14", organizado por el Centro de Excelencia de Ciberdefensa de la OTAN ubicado en Tallin, Estonia; que del 20 al 23 de mayo ha trabajado, de manera conjunta en retos cibernéticos. En el ciberejercicio, los "Blue Teams" (equipos de "hackers buenos" de los países atacados), han debido poner en práctica su conocimiento y habilidad de ciberdefensa. ("Blue Team" como equipo multidisciplinar que incluyen expertos del ámbito técnico, operativo, procedimental y legales del ciberespacio. El ejercicio ha tenido como objeto reforzar las capacidad nacional ante ciberataques y mejorar la coordinación en el contexto multinacional. Tiene lugar en tiempo real, reproduciendo un teatro ficticio y sobre unas infraestructuras controladas que imitan redes y ámbitos estratégicos de los países participantes.

* España ha participado con 30 expertos en ciberseguridad que proceden del Ministerio de la Presidencia, a través del Centro Criptológico Nacional (CCN); Ministerio de Industria, Energía y Turismo, a través del Instituto Nacional de Tecnologías de la Comunicación (INTECO); Ministerio del Interior, a través del Cuerpo Nacional de Policía y la Guardia Civil; y Ministerio de Defensa, a través del Ejército del Aire, el Centro de Operaciones de Seguridad de la Información (COSDEF), el Estado Mayor de la Defensa (EMAD) y el Mando Conjunto de Ciberdefensa.

  www.emad.mde.es/CIBERDEFENSA/

* El Ministerio de Defensa prevé la convocatoria de ciber-reservistas.

4. La dependencia energética de España y la vital importancia de la protección de las infraestructuras críticas

* **El modelo de crecimiento español** se fundamenta en la cada vez mayor **demanda de energía**, sobre todo de petróleo y gas. Nuestra economía depende de la energía como factor clave de la evolución del panorama estratégico tanto nacional como internacional.
* **Reto: La dependencia energética del exterior de España es muy elevada**, ya que el país no cuenta con grandes recursos energéticos.
* La **seguridad energética** se configura para España como un valor de **vital relevancia estratégica.**
* El suministro de gas, el petróleo y la generación de electricidad resultan de **vital importancia** para el país y, con ello, **la protección de sus infraestructuras críticas**, como por ejemplo los gaseoductos y suministros eléctricos. El riesgo derivado de interrumpir el suministro de la energía vital para el país deriva en una grave amenaza tanto por la elevada pérdida tanto económica como ciudadana.

* La **red inteligente** en España irá en aumento paulatinamente ya que se prevé que en el año 2018 habrán recibido un contador inteligente 28 millones de clientes de energía. La medición inteligente del ciudadano puede estar conectada mediante una red inalámbrica con el proveedor de energía. La red inalámbrica puede ser fácilmente interceptada y manipulada por un atacante, quien podría desconectar remotamente viviendas, oficinas y edificios en una gran proporción mediante la conexión alámbrica e inalámbrica. El nivel actual de la seguridad del contador inteligente no cuenta con una oportuna seguridad preventiva ni cuenta con un medio de réplica ante un hipotético y eventual ataque.
* La ciberseguridad se constata como fundamental para un óptimo funcionamiento del modelo actual de suministro eléctrico.

* Apuntar la relevancia de la amenaza que conlleva la **amenaza avanzada permanente** (APT en inglés, *advanced persistent threat)*, que pueden adquirir inteligencia clandestinamente de un modo continuado y permanente sobre una compañía, un sector, una infraestructura crítica o en el nivel particular de la ciudadanía. Se puede utilizar un email fraudulento de un empleado o particular para obtener información o robar credenciales para entrar en el servidor de interés. A través de la inyección de malware y troyanos se puede abrir un canal para que el atacante entre y controle el medio comprometido.
* De este modo, se puede atacar el sistema **SCADA** de una infraestructura crítica. SCADA es el software que permite controlar el procedimiento industrial por remoto y a gran distancia. Proporciona toda la información que se genera en la producción de la infraestructura crítica y permite la intervención. También permite controlar un ciberincidente producido por una eventualidad y sin una deliberada actuación.

* La compañía TrendMicro reportó en el año 2013 en una investigación realizada con el único objetivo de cuantificar ciberataques en un sistema SCADA mal defendido que al poco tiempo de inicio ya recibe ciberataques de modo continuo.
* El monitoreo continuo de SCADA impide normalmente que un ciberataque pueda lograr información, pero la continua evolución del malware evidencia la cada vez mayor amenaza a la que ha de hacerse frente.
* Ejemplo de ataque relevante a una infraestructura crítica: **Stuxnet**. El código malicioso (troyano o malware) fue interceptado en julio de 2010 por una anomalía funcional. Stuxnet fue capaz de espiar, afectar y dañar la infraestructura crítica que controlada sin que la plantilla fuera capaz de reconocerlo a tiempo.

* La complejidad de Stuxnet hace creer que fue muy elevado el valor económico de su programación y que requirió de un equipo de programación con un gran nivel de cualificación y experiencia, de una organización grande o de una entidad estatal de algún país. Se cree que Stuxnet fue creado deliberadamente para retardar el funcionamiento de la planta nuclear de Bushehr en Irán. Stuxnet tiene la facultad de infectar mediante memorias USB (buena parte del equipo de control industrial no es accesible desde internet) y de actualizarse.
* Otro malware de gran complejidad: **Flamer o sKyWIper.** Cuenta con una capacidad muy avanzada para robar información, almacenarla y comunicarla. Puede interceptar el USB, el teclado, la cámara, el bluetooth, el micrófono, la pantalla y la conexión a la red. A partir de ahí, puede enviar toda la información a servidores maliciosos alrededor del mundo. Flamer ha sido utilizado para realizar ciberespionaje en Oriente Medio.
* Otros malware como Duqu, Gauss, Madi, Aurora, Night Dragon y Shady Rat han protagonizado otros ataques de control a infraestructuras críticas.

5. Ciberseguridad y redes WIFI

* El **crecimiento del mercado de los smartphone, tablets y aplicaciones móviles** y la utilización de redes WIFI ha llevado a una cada vez mayor falta de protección e inseguridad de la ciudadanía ante los cibercriminales.
* **La falta de concienciación ciudadana ante el fenómeno que la desprotección WIFI se ha convertido en problema de seguridad muy relevante en la actualidad.**
* La realización de operaciones bancarias, la utilización de Whatsapp, viber o el almacenamiento de fotos y vídeos junto con la desprotección WIFI y la falta de seguridad dentro las aplicaciones para móviles origina multitud de problemas a la ciudadanía.
* Las aplicaciones de móviles transmiten **información no encriptada** y no alertan de la falta de seguridad que pueden suponer para el ciudadano, que no conoce el protocolo de seguridad que utiliza la aplicación. Expertos en seguridad han descubierto que muchas aplicaciones aún utilizan estándares abiertos para la comunicación interna con sus servidores (http en lugar de https), que se pueden hackear facilmente. Por ejemplo, hasta el verano de 2012, Whatsapp transmitió su contenido sin encriptar.

En cuanto a la utilización de aplicaciones móviles, Kaspersky recomienda:

* Utilizar servicios 3G/4G en lugar de WIFI en lugares públicos, cuando sea posible.
* Elegir conexiones WIFI encriptadas (WPA2).
* Utilizar las redes RPV en el dispositivo móvil.
* Evitar realizar operaciones importantes desde el móvil como transacciones bancarias online en lugares públicas y a través de redes no seguras (que en realidad son todas aquellas excepto las configuradas expresamente en el trabajo y en casa).

* La utilización de una red abierta puede llevar a que cualquiera pueda acceder a la navegación de los ciudadanos y ver los datos que se envían o almacenan en el dispositivo. El sistema de cifrado WEP puede ser hackeado en poco tiempo y su seguridad comprometida.
* Analizar el tipo de encriptación que utilizan estas redes y tener mucha precaución a la hora de usar aplicaciones para el móvil. En la medida de lo posible, se aconseja no utilizar red WIFI gratuita en un lugar abierto y público como aeropuertos, cafeterías y hoteles. Cualquiera puede suplantar identidades o crear redes WIFI que simulen ser de confianza para los usuarios.

6. Advanced Threat Report 2013. Fire Eye Labs. February 2014. www.FireEye.com

* En 2013, la plataforma de prevención de amenazas de FireEye interceptó millones de incidentes de malware y los ciberatacantes fueron activos las 24 horas del día.
* FireEye indica que los ataques a la red que interceptó tenían como objetivo principalmente el robo de propiedad intelectual, detectar comunicaciones gubernamentales delicadas y minar la seguridad general de sitios relacionados con la seguridad nacional.
* Los ataques avanzados descritos como Amenazas Avanzadas Persistentes (Advanced Persistent Threats-APTs) implican una actividad apoyada en el tiempo directa o indirectamente por una nación-Estado. FireEye categorizó cerca de 4.000 durante 2013.

* El informe evidencia infección de malware a compañías en un nivel alarmante. También afirma que atacantes avanzados pueden penetrar en patrimonio defensivo fácilmente aunque los sistemas dispongan de firewall o antivirus.
* Durante 2013, FireEye averiguó que Estados Unidos, Canadá y Alemania fueron el objetivo del mayor número de ataques de familias de malware.
* En cuanto a la información obtenida por FireEye, los 10 principales países objetivos de amenazas persistentes avanzadas, cuyo objetivo era la localización de información de seguridad nacional e investigación y desarrollo entre otros elementos, en 2013 fueron:

  Estados Unidos, Corea del Sur, Canadá, Japón, Reino Unido, Alemania, Suiza, Taiwán, Arabia Saudí e Israel.

Los 10 principales sectores objetivos de los ciberataques según FireEye

* **Educación.** La Universidad alberga investigación innovadora y de vanguardia y patentes de tecnología emergente. Lamentablemente, cuenta con un tipo de red amplia y fácilmente infiltrable.
* **Servicio financiero**. La mayoría de las transacciones financieras que llevan a cabo la ciudadanía, los gobiernos y el mundo de los negocios se realizan en la actualidad mediante internet.
* **High-Tech**: cierto tipo de hardware y software es utilizado por millones de ciudadanos y la utilización de dicho soporte por parte de los ciberatacantes puede maximizar el éxito de su actividad, del tiempo y dinero invertido.
* **Gobierno.** Las entidades gubernamentales disponen de información delicada y crítica: organizan naciones, determinan políticas y dirigen la seguridad nacional.
* **Servicios/consultoría**. Una multitud de compañías a menudo manejan asuntos de nivel político, incluyendo a los think tanks.
* **Energía**. La energía permite que un país lleve a cabo su normal actividad.
* **Química**.
* **Telecomunicaciones** (internet, teléfono y cable).
* **Salud/farmacéutica**.
* **Aeroespacial/defensa/aerolíneas**. Desarrollo del espacio tanto de uso comercial como militar.

* FireEye también apunta la **cada vez mayor relevancia de los ataques *zero days*.** En 2013 interceptó once ataques *zero days*, más que cualquier otra compañía de seguridad.

Los objetivos software más frecuentes de este tipo de ataques:

* **Ataques a Java.** Fue el objetivo más común para los ciberatacantes, debido a la mayor facilidad de implementar un ataque contra dicho software.
* **Ataques a los navegadores y exploradores.** Internet Explorer se ha constatado como el vector más importante para los ataques durante 2013, ya que se configura una website muy frecuentada por grupos concretos de interés.

7. Definición de conceptos
Fuente: Glosario de términos del Centro Criptológico Nacional

* **CIBERESPACIO** : Entorno virtual que engloba las TICs.
* **CIBERSEGURIDAD**: Conjunto de actuaciones orientadas a garantizar, en la medida de lo posible, la red que constituye el ciberespacio:
  * detectando y enfrentándose a intrusiones,
  * detectando, reaccionando y recuperándose de incidentes, y
  * protegiendo la confidencialidad, disponibilidad e integridad de la información.
* **CIBERAMENAZA**: Amenaza a las redes que se ubican en el ciberespacio o alcanzables a través de éste.
* **CIBERATAQUE** : Uso del ciberespacio para atacar a las redes que alberga el mismo o alcanzables a través suyo. El atacante pretende acceder sin autorización a información, o alterar o impedir el funcionamiento de los servicios y redes.

* **CIBERDEFENSA**
  * **Activa**: Medida proactiva dirigida a detectar u obtener información, como una ciberintrusión o un ciberataque; impedir una ciberoperación; determinar el origen de una operación que conlleva acción preventiva o ciber-contra operaciones contra una fuente.
  * **Pasiva:** Medida para detectar y mitigar ciberintrusiones y el efecto de los ciberataques que no conllevan una acción preventiva u operaciones contra la fuente. Ejemplos: la instalación de cortafuegos, parches, software anti-virus y herramientas digitales forenses.
* **CIBERDELINCUENCIA**: Actividad delictiva llevada a cabo mediante el empleo del ciberespacio. Ejemplos de ciberdelito: fraude, suplantación de personalidad, robo, crimen organizado, etc.

* **CIBERESPIONAJE**: Ciberataque realizado para obtener secretos de estado, propiedad intelectual, propiedad industrial, información comercial crítica o datos de carácter personal.
* **CIBERTERRORISMO**: Actividad dirigida a originar pánico o catástrofe en la red y sistemas o utilizando éstas como medios.
* **RESILIENCIA**: Capacidad del sistema para continuar operando bajo el efecto de un ciberataque, aunque sea en un modo degradado o debilitado. Incluye la capacidad de reparar con celeridad su función vitales tras un ataque.
* **BOTNET:** Red de equipos infectados por un atacante remoto. Los equipos quedan a su merced cuando pretenda lanzar un ataque masivo, tal como envío de spam o denegación [distribuida] de servicio.
* **SCADA:** Sistema de control industrial. Se ha convertido en crítico en cuanto puede ser objeto de un ciberataque permitiendo atacar infraestructuras críticas.

* **CRIPTOGRAFÍA :** Disciplina que abarca los principios, medios y métodos para la transformación de los datos con el fin de ocultar su contenido de información, impedir su modificación no detectada y/o su uso no autorizado. Encriptar se refiere a "cifrar".
* **DÍA CERO:** Aprovechamiento de una vulnerabilidad inmediatamente después de haber sido reconocida. Se beneficia del intervalo de tiempo requerido por los fabricantes para reparar la vulnerabilidad reportada. Plataformas como Java o Adobe Flash adolecen de una mayor vulnerabilidad y no pueden corregir sus agujeros con suficiente velocidad.
* **GUSANO INFORMÁTICO:** Programa que puede autoaplicarse y enviar copias de si mismo de un ordenador a otro de una red. Tras su instalación en uno de éstos repite el proceso anterior, además de realizar alguna otra tarea indeseable, quizás hasta colapsar el sistema anfitrión

* **INCIDENTE** (Operación del Servicio): Interrupción no planificada de un servicio de tecnología de la información o reducción en la calidad del mismo.
* **PHARMING**: Redirecciona malintencionadamente al usuario a un sitio web ficticio y fraudulento, mediante la explotación del sistema DNS (sistema de nombres de servicio), se denomina secuestro o envenenamiento del DNS.
* **PROXY**: Programa que realiza una acción en representación de otro.
* **TROYANO** : Programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene objetivos dañinos, como permitir intrusiones, borrar datos, etc.

8. Interior activa por primera vez un dispositivo de ciberseguridad para contribuir al normal desarrollo de los actos de proclamación del nuevo Rey de España

* Con motivo de la **proclamación del nuevo Rey de España** el 19 de junio de e2014**, el Ministerio del Interior activó por primera vez en un evento de gran nivel una alerta de ciberseguridad** con el objetivo de contribuir a la normal celebración de la actividad y garantizar la coordinación operativa de todas las instituciones implicadas en la seguridad cibernética.
* La alerta de ciberseguridad fue dirigida a garantizar el correcto transcurrir de la proclamación del nuevo jefe de Estado y a reforzar la protección de la infraestructura crítica española. La activación de la alerta de ciberseguridad actuó junto con la recientemente creada Oficina de Coordinación Cibernética del Ministerio del Interior.

9. Webs interesantes de consulta sobre ciberseguridad

ESPAÑA

-Web de Presidencia del Gobierno. Estrategia Ciberseguridad Nacional

http://www.lamoncloa.gob.es/NR/rdonlyres/2A778417-DABC-4D36-89A2-3B81565C3B82/0/20131332EstrategiadeCiberseguridadx.pdf

-Centro Criptológico Nacional

https://www.ccn.cni.es/

Glosario de términos del Centro Criptológico Nacional:

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-Glosario_y_abreviaturas/401_glosario.pdf

-Mando Conjunto de Ciberdefensa de España

http://www.emad.mde.es/CIBERDEFENSA/

-CNPIC. Centro Nacional de Protección para las Infraestructuras Críticas

http://www.cnpic-es.es/

-INTECO. Instituto Nacional de Tecnologías de la Comunicación

http://www.inteco.es/

-Centro Nacional de Excelencia en Ciberseguridad

http://cnec.icfs.uam.es/

-Think tank Thiber

http://www.thiber.org/

-ISMS. Asociación Española para el fomento de la seguridad de la información

https://www.ismsforum.es/noticias/entrevistas/

INTERNACIONAL

-Centro de Excelencia de Ciberseguridad de la OTAN

https://www.ccdcoe.org/

-Cyber Security Forum Initiative

www.csfi.us

-CERT EU-Computer Emergency Response Team de la UE

http://cert.europa.eu/cert/filteredition/es/CERT-LatestNews.html

-ENISA-European Union Agency for Network and Information Security

http://www.enisa.europa.eu/