U-tad
CENTRO UNIVERSITARIO
DE TECNOLOGÍA Y ARTE DIGITAL

Estado de la Ciberseguridad 2015

Índice

Prólogo

La Ciberseguridad está cada día más presente en nuestras vidas digitales, la cantidad y tipología de ciberataques que pueden sufrir ciudadanos, empresas e instituciones aumenta exponencialmente cada año y mantener la visión de conjunto de la situación es cada vez más difícil.

Por eso, desde **U-tad** hemos querido hacer un ejercicio de síntesis de las principales fuentes y estudios para que los ciudadanos y las empresas puedan disponer de una visión actualizada y agregada de este complejo mundo.

En las siguientes páginas abordamos las **principales amenazas que los ciberdelincuentes** emplean en sus ataques, las técnicas de respuesta –que por desgracia siempre surgen como reacción al ingenio desplegado por los atacantes, pero la verdad es que con mejoras en los paradigmas que empiezan a dar su frutos en prevención y detección temprana de amenazas-, y la estimación del perjuicio económico que estos ataques provocan.

Sobre este análisis de situación general, desde U-tad, como **Universidad surgida de la industria tecnológica y especializada en Economía y Sociedad Digital**, no podíamos dejar de reflejar el **mercado y la evolución que las tecnologías y servicios de ciberseguridad** están suponiendo y el **mercado laboral altamente especializado que genera.** En esta línea, CISCO apunta a un déficit de un millón de nuevos profesionales de la ciberseguridad. Los profesionales de la ciberseguridad requieren de conocimientos y competencias muy avanzadas que sólo se obtienen tras una práctica intensa en los diferentes campos de la ciberseguridad tales como en análisis de *malware*, la detección de intrusiones o la reacción de los equipos de respuesta a incidentes de ciberseguridad ante ciberataques.

Dadas las significativas pérdidas que se derivan de los ciberataques, las Administraciones Públicas han impulsado Estrategias Nacionales de Ciberseguridad que se empiezan a coordinar a nivel europeo e internacional. En mi etapa en el Ministerio de Industria pude participar en los trabajos como miembro del nuevo Consejo Nacional de Ciberseguridad, Comité Especializado dependiente del Consejo de Seguridad Nacional que preside Su Majestad el Rey o, en su ausencia, el Presidente del Gobierno, y pude comprobar el **significativo liderazgo que el Gobierno de España está demostrando en la implicación de las principales empresas y operadores de infraestructuras críticas** y en la sensibilización y concienciación de los ciudadanos. Muchas de esas iniciativas se encuentran detalladas en la Estrategia de Ciberseguridad Nacional que también recogemos en el presente informe.

Nuestro compromiso de formar a los profesionales de la economía digital con un alto grado de especialización nos obliga a mantenernos siempre actualizados sobre las últimas tecnologías y tendencias en ámbitos tan cambiantes como la ciberseguridad, una muestra de este compromiso es el presente informe y una prueba de sus resultados es la **incorporación en nuestras aulas de las más modernas tecnologías de formación** en ciberseguridad, como el simulador para retos y ciberejercicios iPhalanx de Indra que nuestros alumnos ya utilizan en sus entrenamientos.

Como la ciberseguridad debe ser un compromiso de todos, les invito a leer el presente informe para tener una perspectiva general inmejorable del estado de situación de la ciberseguridad.

Juan Corro
Director Académico del Área
de Ingeniería de Software de U-tad

Resumen ejecutivo

El traslado de la actividad de todos los actores de la sociedad al **ciberespacio**, ha aumentado drásticamente su **exposición a nuevos riesgos y amenazas**. Por ello el concepto **ciberseguridad**, cuyo objetivo es la protección de las organizaciones y las instituciones contra los **ataques** que los **cibercriminales** lanzan para comprometer sus sistemas de información a nivel de hardware o software y contra el robo o destrucción de la información que almacenan o gestionan.

La ciberseguridad ya es una prioridad en la agenda de los gobiernos y de las empresas de todo el mundo. En 2014, **nueve grandes organizaciones sobre diez han tenido algún tipo de brecha de seguridad[1] con un coste medio anual para las organizaciones que se sitúa cerca de los 15 millones de dólares[2].** Un 46% de las organizaciones espera sufrir un ataque a lo largo del 2015[3].

La profesionalización de los atacantes y la sofisticación y violencia de los ataques hacen que **la simple protección ya no sea suficiente**, sino que sea necesario poner en marcha medidas de monitorización constante orientadas a la **detección y prevención de los ataques,** mucho antes de que estos tengan lugar, así como de **mecanismos de respuestas** adecuados.

Estos mecanismos deben tener un enfoque multidisciplinar, en cuanto que la ciberseguridad trasciende de la dimensión puramente tecnológica y depende de muchos más factores internos y externos, siendo el factor humano uno de los más importantes: **el 75% de las grandes organizaciones han sufrido incidentes de seguridad relacionados con acciones o comportamientos de sus empleados[4].**

El mercado global de la ciberseguridad está en continuo crecimiento y se espera que alcance los **170 mil millones de dólares en 2020[5]**, a una tasa de crecimiento compuesta anual del 9,8%. La seguridad gestionada, los servicios basados en la nube, la protección de datos en movilidad, el BYOD, las amenazas persistentes avanzadas (APT), Internet de las cosas y la seguridad en smart grid son algunos de los segmentos que experimentarán más crecimiento.

Para hacer frente a las ciberamenazas, **el 37% de las organizaciones planea emplear más profesionales de ciberseguridad a lo largo de 2015**, aunque el 92% de ellas espera encontrar dificultades en encontrar candidatos con las competencias adecuadas[6]. A nivel global se ha estimado un **déficit de más de un millón de profesionales de ciberseguridad[7].**

1 PwC, 2015 Information security breaches survey, http://www.pwc.co.uk/industries/insurance/insights/2015-information-security-breaches-survey.html
2 Ponemon Institute Cost of Cyber Crime Study, http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/index.html?jumpid=va_fwvpqe387s
3 ISACA, 2015 Global Cybersecurity Status Report, http://www.isaca.org/Pages/Cybersecurity-Global-Status-Report.aspx
4 PwC, ibíd.
5 MarketsandMarkets, Cyber Security Market by Solution http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html
6 ISACA, 2015 Global Cybersecurity Status Report, http://www.isaca.org/Pages/Cybersecurity-Global-Status-Report.aspx
7 http://globalnewsroom.cisco.com/es/es/release/Los-ataques-avanzados-y-el-tr%C3%A1fico-malicioso-experimentan-un-crecimiento-sin-precedentes-1881684

También los inversores tienen un enorme interés en este sector: en los últimos 5 años se han invertido **7,3 mil millones de dólares en más de 1000 *startups*** de ciberseguridad[8].

Las **principales riesgos** actuales en ciberseguridad son representados por los dispositivos móviles y el BYOD, las infraestructuras críticas y los sistemas de control industrial SCADA, las *smart grid*, el Internet de las cosas y las vulnerabilidades del *software*, en particular las de día cero.

En cuanto a **amenazas**, las principales tendencias son la intensificación del ciberespionaje, la profesionalización del crimen y su oferta "como servicio", el *hacktivismo*, el *malware* de tipo *Ransomware* y *Cryptoware* y el *spear-phishing*.

Frente a los riesgos y las amenazas a la ciberseguridad, **compartir información** se revela fundamental, bien sea entre organizaciones, o entre organizaciones y las administraciones públicas o entre ciudadanos. En este sentido, **la Administración puede jugar un papel fundamental** en apoyo a las empresas, en la coordinación nacional e internacional y en proporcionar un marco legislativo que permita perseguir a los criminales.

Entre las **principales técnicas de respuesta y prevención** frente a las ciberamenazas destacan los sistemas corporativos de gestión de dispositivos y aplicaciones móviles, los servicios de seguridad gestionada, la seguridad como servicio, el Big Data Analytics, la autenticación avanzada, el hacking ético y la simulación de incidentes de ciberseguridad.

8 https://www.cbinsights.com/blog/cybersecurity-startup-financing/

La emergencia de la ciberseguridad

Los continuos avances en las **tecnologías y servicios digitales,** su libre puesta a disposición y su rápida adopción por parte de la sociedad están aportando grandes beneficios, ofreciendo nuevas posibilidades de desarrollo humano, político y económico y afectando desde la vida diaria de las personas hasta el funcionamiento de industrias enteras, así como de los gobiernos y de las administraciones públicas.

Internet, las **redes sociales** y los **dispositivos móviles** conectados, rompen barreras y ofrecen a los individuos nuevas maneras más rápidas y efectivas de comunicación y de acceso global a la información y servicios. Además, revolucionan la forma en que las instituciones y las organizaciones se relacionan con las personas, ya que la comunicación se hace más fluida y, sobre todo, bidireccional.

Por otro lado, el **Cloud Computing** facilita a las organizaciones el acceso a la capacidad de computación, al software y a las aplicaciones de forma online y escalable, reduciendo drásticamente las inversiones necesarias en tecnología.

El uso masivo de las aplicaciones y de los servicios conectados por parte de las personas y de las organizaciones multiplica exponencialmente la cantidad de información intercambiada y almacenada en la red, generando ingentes cantidades de datos que pueden ser procesados y analizados para evidenciar tendencias y realizar predicciones, fenómeno que se denomina **Big Data.**

El traslado de la actividad de todos los actores de la sociedad al **ciberespacio,** también aumenta drásticamente su **exposición a nuevos riesgos y amenazas.**

Los mismos mecanismos de amplificación de beneficios y oportunidades descritos, también hacen que las denominadas ciberamenazas a la seguridad de las personas y organizaciones:

- tengan una **dimensión global,** ya que pueden provenir desde – y ser dirigidos hacia – cualquier persona, institución u organización conectada a Internet con independencia de su ubicación física;
- generen **más impacto,** al poder alcanzar al mismo tiempo más cantidad de personas de forma directa, o de forma indirecta comprometiendo servicios e infraestructuras críticos;
- sean **difíciles de prever, identificar, controlar y erradicar**, ya que los mecanismos tradicionales de vigilancia y aplicación de las leyes pierden efectividad en el ciberespacio;
- **evolucionen** a una velocidad típica del mundo digital, al beneficiarse de la disponibilidad de tecnología avanzada y a bajo coste y del libre acceso y distribución de información.

Alentados por la rentabilidad que ofrecen las acciones delictivas en el ciberespacio, bien en términos económicos, políticos o de adquisición de ventajas competitivas, protegidos por el anonimato que ofrece el ciberespacio y armados de herramientas y tecnología de coste relativamente bajo, los **ciberdelincuentes** – *hackers*, terroristas, activistas, pero también empresas y gobiernos – llevan a cabo acciones delictivas en el ciberespacio con incidencia creciente. Los llamados **ciberataques** – es decir un conjunto de acciones perpetradas a través de Internet y vueltas a destruir o comprometer los sistemas informáticos de una entidad, infraestructuras o gobierno – y las acciones de **ciberespionaje** – el acceso masivo ilegal o no ético a datos sensibles o personales – se aprovechan de las **vulnerabilidades** de las aplicaciones o bien de los **errores humanos** a la hora de no identificar correctamente una amenaza.

Por todas estas razones, emerge el concepto de seguridad aplicada al ciberespacio, o de **ciberseguridad**, cuyo objetivo es la protección de los sistemas de información contra el daño que se pueda infligir a su funcionamiento a nivel de hardware o software y contra el robo o destrucción de la información que almacenan o gestionan.

La ciberseguridad requiere ser gestionada por todos los actores afectados, es decir, desde los gobiernos hasta las personas, pasando por las organizaciones y las empresas privadas, de la misma forma que se hace con la seguridad física. Sin embargo, a diferencia de ella, su gestión no puede ser compartimentada sino que requiere de un enfoque integral y de una colaboración entre todo los actores en forma de partenariados público-privados, cooperación internacional y educación a las personas, ciudadanos o trabajadores de las organizaciones.

La ciberseguridad, prioridad de gobiernos y empresas

La ciberseguridad ya es una prioridad en la agenda de los gobiernos y de las empresas de todo el mundo. Esto porque el uso de las nuevas tecnologías y de Internet comporta unos riesgos en términos de seguridad que pueden poner en peligro no solamente la privacidad de la información, sino a enteras industrias estratégicas de un país, a sus infraestructuras críticas y, en última instancia, a su estabilidad.

El ministro del Interior español, Jorge Fernández Díaz, ha recordado[9] recientemente que **"el ciberdelito supone ya la tercera forma delictiva y criminal más importante a nivel mundial"** y ha asegurado que "las Fuerzas y Cuerpos de Seguridad son plenamente conscientes de esta realidad".

El ministro ha destacado también algunas cifras significativas: **18.000 ataques cibernéticos registrados en 2014 por el CERT de Seguridad e Industria**; 80 incidentes de operadores de infraestructuras críticas y más de 40 comunicaciones relativas a la ciberseguridad, el ciberdelito y el ciberterrorismo gestionados por la Oficina de Coordinación Cibernética del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC).

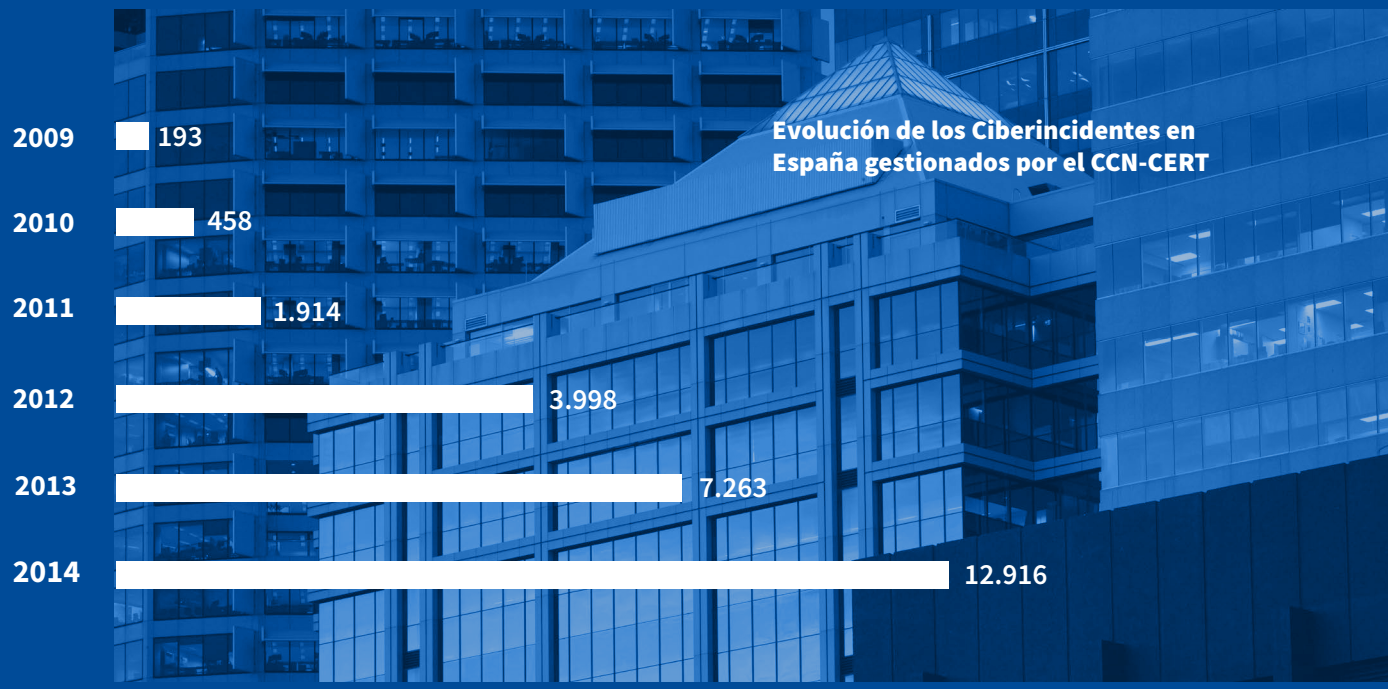
A los cuales, se añade la actividad del CERT Gubernamental del Centro Criptológico Nacional, que en 2014 abordó **12.916 incidentes, de los cuales, 132 fueron catalogados como críticos**, es decir, aquellos que pueden causar degradación de los servicios para un gran número de usuarios, implicar una grave violación de la seguridad de la información, pueden afectar

a la integridad física de las personas, causar importantes pérdidas económicas, ocasionar daños irreversibles a los recursos de la organización, se puede incurrir en delitos y/o sanciones reglamentarias u ocasionar un daño muy grave en la imagen de la organización.

La **dimensión política y militar** de la ciberseguridad es también importante: en su informe de actividad de 2014[10], el CERT Gubernamental Nacional destaca como varios Ministros y Secretarios de Estado del Gobierno Español sufrieron diversas campañas de ataque dirigidas contra los móviles y ordenadores personales de altos cargos del Ejecutivo, a través de un correo electrónico dañino.

9 http://www.interior.gob.es/es/web/interior/noticias/detalle/-/journal_content/56_INSTANCE_1YSSI3xiWuPH/10180/4059909

10 CCN-CERT IA-09/15 CIBERAMENAZAS 2014 TENDENCIAS 2015, https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/795-ccn-cert-resumen-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html



También hay que destacar los recientes ciberataques lanzados en contra de la red del Ejercito de EEUU[11] que han llevado a Obama a impulsar un nuevo paquete legislativo[12], en un contexto de crecientes ataques informáticos hacia EEUU, que además han afectado también a grandes empresas como Sony, Target, Home Depot y JPMorgan[13].

El caso de Sony[14] fue particularmente relevante, sospechándose la involucración de Corea del Norte y forzando al Presidente a comparecer antes los medios.

El ataque informático contra la multinacional Sony Pictures Entertainment ha demostrado como un ciberataque puede, además de causar daños económicos, llegar a poner en peligro las libertades civiles fundamentales de una sociedad, como lo es la libertad de expresión.

La multinacional, tras sufrir un robo de información y consecuente chantaje de que se publicara en Internet, decidió la retirada de una película de 44 millones de dólares, "*The interview*". La película era una parodia del líder norcoreano Kim Jong, lo que llevó todas las hipótesis de culpabilidad hacia Corea del Norte.

> *"No podemos tener una sociedad en la que un dictador de otra parte empiece a imponer la censura en Estados Unidos"*

Declaró el presidente de Estados Unidos Barack Obama a los medios[15].

11 http://www.elmundo.es/internacional/2015/01/12/54b40d0d268e3e97718b4578.html
12 http://www.elconfidencial.com/ultima-hora-en-vivo/2015-01-14/obama-impulsa-reformas-en-ciberseguridad-tras-los-ataques-a-sony-y-pentagono_466335/
13 http://www.abc.es/economia/20141003/rc-jpmorgan-sufre-ciberataque-afecta-201410030006.html
14 http://www.abc.es/economia/20141003/rc-jpmorgan-sufre-ciberataque-afecta-201410030006.html
15 http://internacional.elpais.com/internacional/2014/12/19/actualidad/1419009199_719868.html

La probabilidad de sufrir un ciberataque es hoy en día muy alta para cualquier tipo de organización. Un estudio de PwC[16] realizado en el Reino Unido enseña como en 2014, **9 grandes empresas sobre 10 han tenido algún tipo de brecha de seguridad,** con una media por organización de 14 incidentes anuales.

Otra encuesta global de PwC[17] destaca como en 2015 **los incidentes de ciberseguridad detectados por las empresas crecieron un 38%** con respecto al año anterior, dentro de los cuales los robos de propiedad intelectual se incrementaron un 56% en el mismo periodo.

Las empresas son conscientes de ello, de hecho el **83% de ellas cree que los ciberataques son una de las tres amenazas más importantes** que afronta su organización a día de hoy y un **46% espera sufrir un ataque a lo largo del 2015**, según un estudio de ISACA[18].

Más allá de los problemas relacionados con la seguridad de la información, de los ciudadanos y de las infraestructuras críticas de un país, los ciberataques representan también **un coste muy elevado** para las organizaciones que los sufren.

En su último informe[19], Ponemos Institute destaca como **el coste medio anual de estos ataques para las organizaciones ya se sitúa cerca de los 15 millones de dólares**, habiéndose incrementado en casi un 20% respecto al año anterior y un 82% en los últimos seis años. Cada ataque recibido representaría ya un coste medio de 1,9 millones de dólares.

Según las recientes declaraciones del Secretario de Estado de Seguridad, Francisco Martínez[20], **las empresas españolas tuvieron el año pasado pérdidas por valor de 14.000 millones de euros** a causa de los ciberdelitos.

16 PwC, 2015 Information security breaches survey http://www.pwc.co.uk/industries/insurance/insights/2015-information-security-breaches-survey.html
17 PwC, The Global State of Information Security® Survey 2016, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
18 ISACA, 2015 Global Cybersecurity Status Report, http://www.isaca.org/Pages/Cybersecurity-Global-Status-Report.aspx
19 Ponemon Institute Cost of Cyber Crime Study, http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/index.html?jumpid=va_fwvpqe387s
20 http://www.interior.gob.es/es/web/interior/noticias/detalle/-/journal_content/56_INSTANCE_1YSSl3xiWuPH/10180/4215949

Agenda de la ciberseguridad: los próximos eventos

CyberCamp 2015[21]

Organizado por INCIBE, se celebrará del 26 al 29 de noviembre de 2015, en el Barclaycard Center de Madrid. Durante los cuatro días de duración del evento los visitantes disfrutarán de un conjunto de actividades formativas y lúdicas relacionadas con el mundo de la ciberseguridad y asistirán a conferencias y talleres impartidos por importantes figuras y expertos de la comunidad de la ciberseguridad. Asimismo, las empresas y organizaciones más representativas del mundo de la ciberseguridad y de las redes de comunicación ofrecerán actividades destinadas a promover el interés por los estudios, la especialización profesional y el emprendimiento en el ámbito de la ciberseguridad.

IX Jornadas de Seguridad TIC[22]

Organizadas por el CCN-CERT, se celebrarán en Madrid el 10 y 11 de diciembre de 2015 con el objetivo de sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio.

Securmática[23]

SECURMÁTICA, el Congreso global español de Ciberseguridad, Seguridad de la Información y Privacidad, que organiza la revista SIC, tendrá su próxima cita en abril de 2016. Su objetivo es ofrecer una visión panorámica, actualizada y exclusiva del estado del arte de la ciberseguridad, la protección de la información y la privacidad en sus aspectos técnicos, organizativos y legales, con especial incidencia en la exposición de proyectos de referencia en la materia, expuestos al alimón por las compañías copatrocinadoras y los usuarios corporativos.

ENISE[24]

En 2016 se celebrará la 10 edición del Encuentro Internacional de Seguridad de la Información, ENISE. Organizado por INCIBE, el evento es un punto de encuentro para analizar colectivamente los avances más significativos en el sector de la Ciberseguridad. Su edición 2015 se celebró en León los días 20 y 21 de octubre y acogió a más de 2.000 asistentes.

21 https://cybercamp.es

22 https://www.ccn-cert.cni.es/sobre-nosotros/jornadas-stic-ccn-cert/ix-jornadas-de-seguridad-tic-del-ccn-cert.html

23 http://www.securmatica.com/

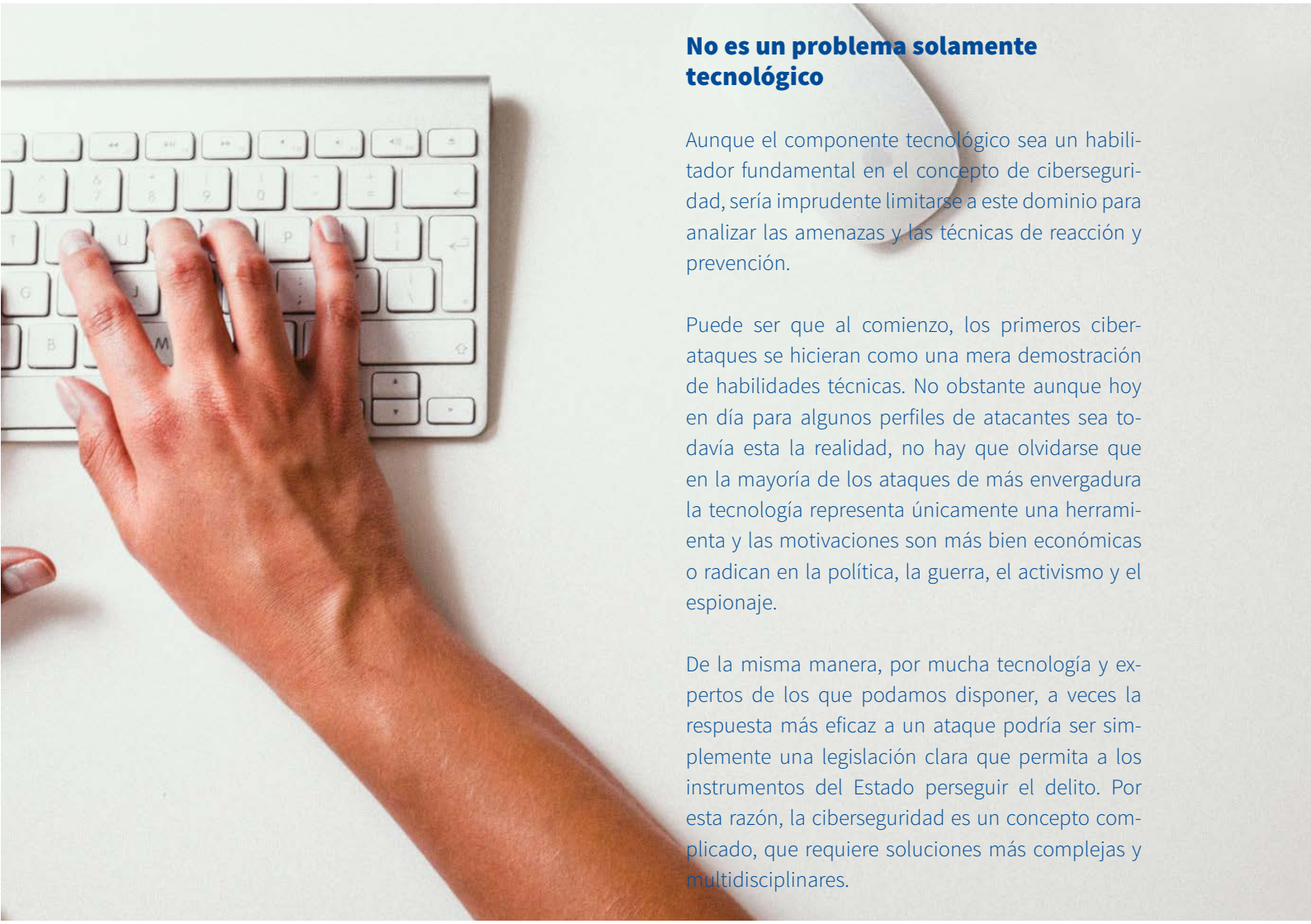
24 https://www.incibe.es/enise

Gestionar la ciberseguridad: un enfoque multidisciplinar

De la protección hacia la prevención

Un estudio llevado a cabo por EMC[25] evidencia que la mayoría de las empresas todavía no se sienten preparadas frente al reto de la ciberseguridad, de hecho **el 75% de las organizaciones opina estar significativamente expuestos a los ciberriesgos.** Esto a pesar de que, según el mismo estudio, las empresas se declaren bastante preparadas en la protección frente a las amenazas. Sin embargo, hoy en día la profesionalización de los atacantes y la sofisticación y violencia de los ataques hacen que **la simple protección ya no sea suficiente**, sino que sea necesario poner en marcha medidas de monitorización constante orientadas a la **detección y prevención de los ataques**, mucho antes de que estos tengan lugar, así como de **mecanismos de respuestas** adecuados.

De hecho, estas capacidades aparecen en los últimos lugares del ranking de preparación de las empresas encuestadas.



No es un problema solamente tecnológico

Aunque el componente tecnológico sea un habilitador fundamental en el concepto de ciberseguridad, sería imprudente limitarse a este dominio para analizar las amenazas y las técnicas de reacción y prevención.

Puede ser que al comienzo, los primeros ciberataques se hicieran como una mera demostración de habilidades técnicas. No obstante aunque hoy en día para algunos perfiles de atacantes sea todavía esta la realidad, no hay que olvidarse que en la mayoría de los ataques de más envergadura la tecnología representa únicamente una herramienta y las motivaciones son más bien económicas o radican en la política, la guerra, el activismo y el espionaje.

De la misma manera, por mucha tecnología y expertos de los que podamos disponer, a veces la respuesta más eficaz a un ataque podría ser simplemente una legislación clara que permita a los instrumentos del Estado perseguir el delito. Por esta razón, la ciberseguridad es un concepto complicado, que requiere soluciones más complejas y multidisciplinares.

25 RSA Cybersecurity Poverty Index, https://www.emc.com/campaign/rsa/cspi.htm

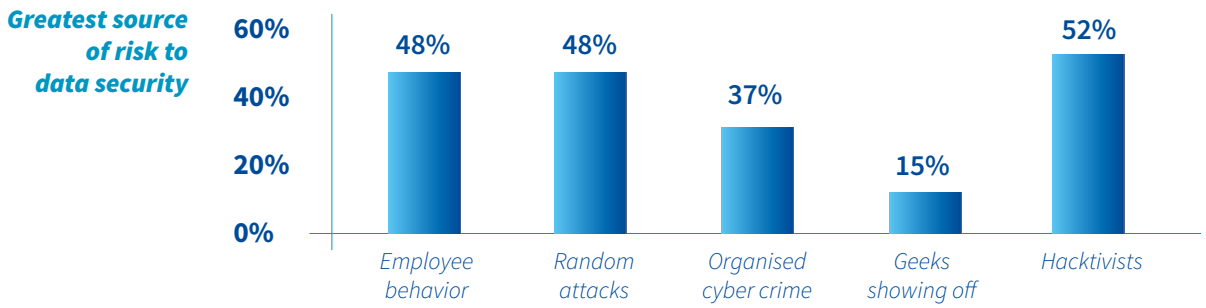
El factor humano

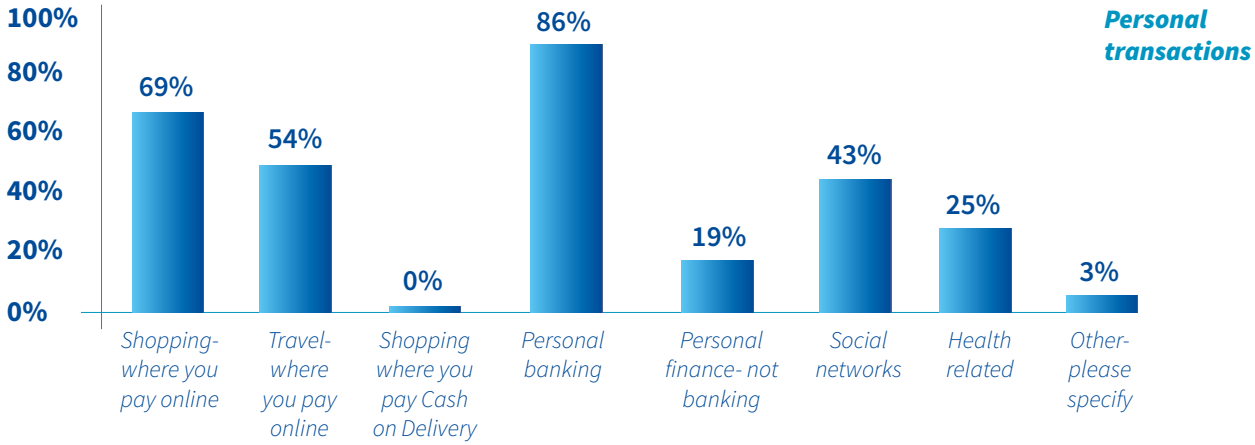
Como se suele decir, la seguridad de una cadena es la de su eslabón más débil y en la ciberseguridad ese eslabón no es la tecnología, sino el factor humano. La mayoría de las veces, el riesgo existe simplemente al ser los empleados de las organizaciones usuarios de múltiples sistemas tecnológicos y servicios digitales, lo cual les convierte en el objetivo de los ataques y a menudo a su vez y sin saberlo, colaboradores de ataques orquestados sin que tengan consciencia de ellos.

El estudio de PwC[26] realizado en el Reino Unido confirma esta alarmante realidad, mostrando que en 2014 **el 75% de las grandes organizaciones han sufrido incidentes de seguridad relacionados con acciones o comportamientos de sus empleados.**

Además, la mitad de las empresas afirma que su peor brecha de seguridad fue causada por un error humano. Esto, a pesar de que ya el 72% de las grandes empresas proporciona a sus empleados formación en temas de seguridad.

Según un estudio realizado en España por Cisco[27], los trabajadores identifican su propio comportamiento como el segundo mayor riesgo para la seguridad de los datos corporativos, únicamente precedido por la actividad de los hackers. Todos los empleados consultados declaran utilizar la red corporativa para realizar transacciones personales, como gestiones de sus cuentas bancarias, compras *on line*, reservas de viajes o redes sociales.





Cisco, Ciberseguridad en las empresas españolas

26 PwC, 2015 Information security breaches survey, http://www.pwc.co.uk/industries/insurance/insights/2015-information-security-breaches-survey.html
27 Cisco, Ciber-seguridad en las empresas españolas, http://www.cisco.com/web/ES/ciberseguridad/index.html

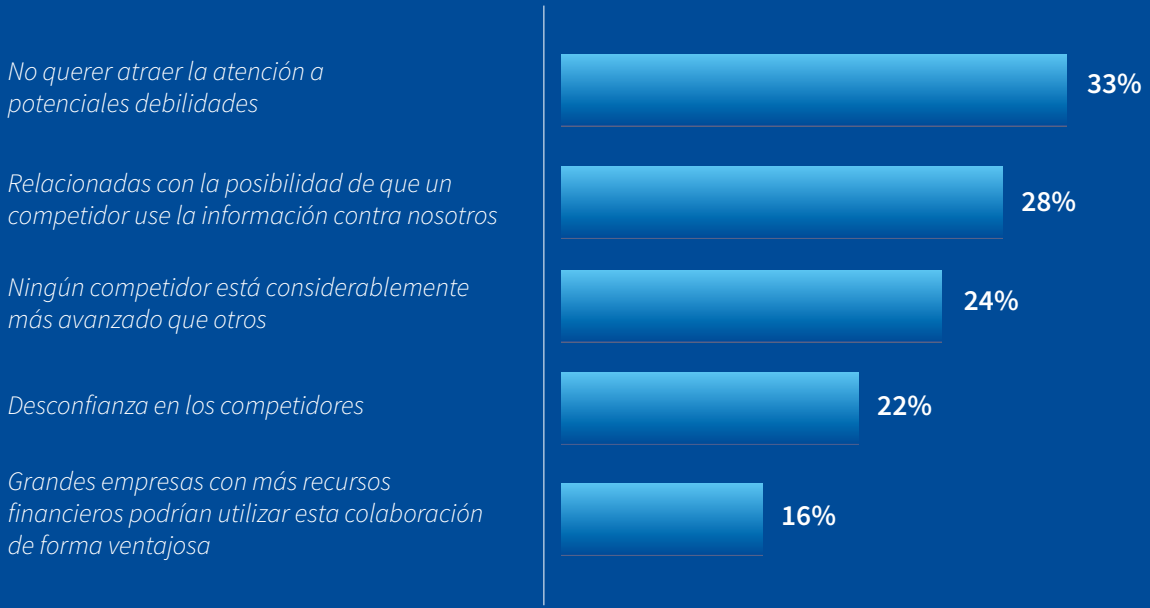
La importancia de compartir

Frente a la complejidad de las amenazas y a la fragilidad de las organizaciones debido a sus vulnerabilidades internas, se hace necesario aunar esfuerzos desde diferentes ámbitos. En este sentido, el compartir información sobre los riesgos y amenazas se revela fundamental, bien sea entre organizaciones, o entre organizaciones y las administraciones públicas o entre ciudadanos.

Aunque en realidad a menudo las empresas son reticentes en elegir este camino, bien por miedo a perder ventaja frente a sus competidores o imagen frente a sus clientes, o a causa muchas veces de una legislación no clara que se volvería en su contra (como por ejemplo la legislación en materia de protección de datos personales).

Consciente de ello, el presidente de EEUU, Barack Obama, a principios de 2015 firmó una orden ejecutiva para fomentar la colaboración entre organizaciones públicas y privadas mediante la creación de Organizaciones de Intercambio y Análisis de Información (ISAOs)[28], con el objetivo de permitir a las empresas y organismos del sector público compartir información sobre ciberamenazas específicas en industrias concretas.

PwC, Temas candentes de la Ciberseguridad. Razones para no colaborar en material de seguridad de la información



28 http://www.reuters.com/article/2015/02/13/us-usa-cybersecurity-exclusive-idUSKBN0LG2GR20150213

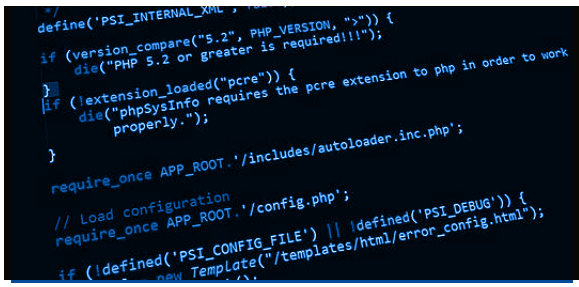
El **Gobierno de Estados Unidos** anunció[29] a comienzos de 2015 la creación del **Centro de Integración de Inteligencia contra la Amenaza Cibernética** (CTIIC) una agencia que, inspirada en la lucha antiterrorista, coordinará las actuaciones ante un ataque cibernético. La agencia recopilará información de inteligencia entre varios departamentos gubernamentales, que la obtienen por separado. La asesora de seguridad nacional y para la lucha antiterrorista de la Casa Blanca, **Lisa Monaco**, apuntó que:

> *"Tenemos que compartir información más ampliamente y coordinar acciones. Podemos hacer más en evaluar las amenazas que se mueven rápidamente."*

Un reciente informe de ESADEGeo y Zurich[30] aboga por **incrementar la colaboración entre países para reforzar la ciberseguridad**. Entre las medidas propuestas, destaca la creación de organismos internacionales que incluirían un **Consejo de Ciberestabilidad** y que tendrían que mantenerse aislados de las tensiones geopolíticas. También se propone la creación de un **sistema de alerta cibernética** basado en el modelo de trabajo de la Organización Mundial de la Salud (OMS) para mejorar la gestión de las crisis.

Javier Solana, ex alto representante de Política Exterior y Seguridad Común en la UE, ha afirmado[31] al respecto que:

> *"La fragmentación del mundo físico dificulta que los Gobiernos colaboren y compartan información sobre sus amenazas y los ataques que sufren. Y que la ciberseguridad no es un asunto del que se pueda hablar desde una perspectiva nacional. Hacerlo nos llevaría a lo que ocurre en China. Las estrategias nacionales crean fragmentación. Y una Red que es global, neutral, libre… no puede estar fragmentada."*



29 http://internacional.elpais.com/internacional/2015/02/11/actualidad/1423610572_212199.html
30 Zurich, Risk Nexus Global cyber governance: preparing for new business risks, http://knowledge.zurich.com/cyber-risk/global-cyber-governance/
31 http://tecnologia.elpais.com/tecnologia/2015/10/09/actualidad/1444393079_943595.html

El papel de la Administración

En el ecosistema de la ciberseguridad, quizás el rol más importante sea el de la Administración.

El objetivo principal de las empresas es de competir en sus mercados con productos y servicios innovadores y además tienen que dotarse de mecanismos de prevención, protección y reacción antes las ciberamenazas. Si embargo, poco pueden contra ciertos tipos de ataques detrás de los cuales hay organizaciones criminales profesionalizadas o hasta gobiernos de países hostiles. En todos estos casos, la Administración tiene el poder de apoyar a las empresas, coordinarlas para acciones conjuntas y dotarlas de un marco legislativo para protegerse y perseguir a los criminales.

En este sentido, la actividad de la Administración se agrupa en cuatro roles principales:

- **Impulsor** de iniciativas en el campo de la ciberseguridad. En España ha habido mucho esfuerzo en este sentido con la creación del Instituto Nacional de Ciberseguridad – INCIBE[32], el Centro Nacional para la Protección de las Infraestructuras Críticas – CNPIC[33], el Centro Criptológico Nacional – CCN[34] y el Mando Conjunto de Ciberdefensa[35].

- **Coordinador**, estableciendo los foros y mecanismos adecuados para la puesta en común de la información, a nivel nacional e internacional. En esta línea se crearon en España los CERT, centros de respuesta ante incidentes del INCIBE, y del Centro Criptológico Nacional.

- **Regulador,** implementando un marco legislativo adecuado que permita perseguir los ciberdelitos. En España destaca la aprobación del Esquema Nacional de Seguridad (ENS)[36], la formulación de la Estrategia Nacional de Ciberseguridad[37] y la Ley 8/2011 de protección de infraestructuras críticas[38].

- **Protector**, desplegando los cuerpos y fuerzas de seguridad del Estado y los servicios de Inteligencia para la defensa contra las ciberamenazas. En nuestro país destacan el Grupo de Delitos Telemáticos de la Guardia Civil[39] y la Brigada de Investigación Tecnológica de la Policía Nacional[40].

32 https://www.incibe.es/
33 http://www.cnpic.es/
34 https://www.ccn.cni.es/
35 http://www.emad.mde.es/CIBERDEFENSA/
36 https://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf
37 Gobierno de España, Estrategia de Ciberseguridad Nacional, http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf
38 http://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf
39 https://www.gdt.guardiacivil.es/webgdt/home_alerta.php
40 http://www.policia.es/org_central/judicial/udef/bit_alertas.html

La ciberseguridad, un mercado en crecimiento

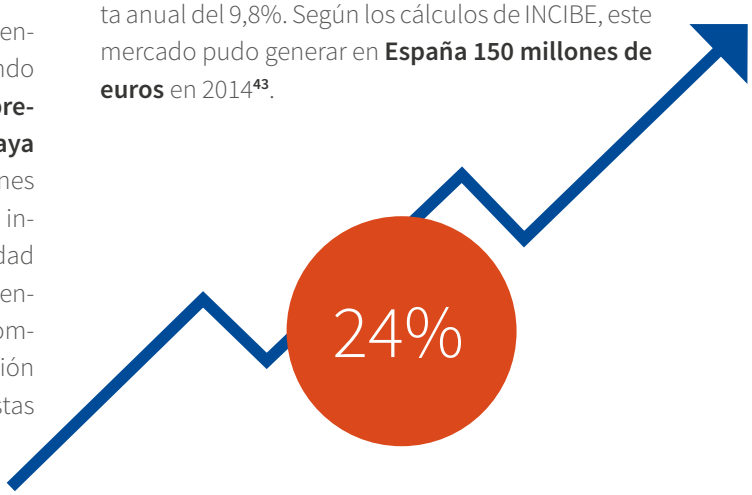
El mercado de la ciberseguridad está en continuo crecimiento. Las organizaciones y las instituciones necesitan soluciones que les ayuden a identificar las ciberamenazas, así como a protegerse y a defenderse de ellas.

Según una encuesta de PwC[41], frente el crecimiento de las amenazas, las empresas están invirtiendo más en seguridad, lo que se refleja en que **el presupuesto para seguridad de la información haya crecido en media de un 24%**. Entre las soluciones más elegidas, están la adopción de tecnologías innovadoras como los servicios de ciberseguridad basados en la nube, el Big Data Analytics y la autenticación avanzada, además de la tendencia a compartir con sus colaboradores externos información sobre detección de riesgos y técnicas de respuestas a amenazas.

También, internamente, las organizaciones están repensando los roles de los ejecutivos clave y el Consejo de Administración, apuntando un Chief Information Security Officer (CISO) o Chief Security Officer (CSO) en la dirección del programa de seguridad.

Un 91% de las empresas ha implantado un marco de ciberseguridad, como la norma ISO/IEC 27001 o el Cibersecurity Framework del NIST.

Según datos de MarketsandMarkets[42], se espera que el mercado global de la ciberseguridad crezca de 106 mil millones de dólares en 2015 hasta **170 mil millones de dólares en 2020**, a una tasa compuesta anual del 9,8%. Según los cálculos de INCIBE, este mercado pudo generar en **España 150 millones de euros** en 2014[43].



También los inversores tienen un enorme interés en este sector, como demuestra el hecho de que en los últimos 5 años se han invertido a nivel global **7,3 mil millones de dólares en más de 1000 *startups*** de ciberseguridad[44].

41 PwC, The Global State of Information Security® Survey 2016, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
42 MarketsandMarkets, Cyber Security Market by Solution http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html
43 INCIBE, Análisis y caracterización del mercado de la Ciberseguridad, https://www.incibe.es/extfrontinteco/img/File/empresas/blog/20150331_caracterizacion_mercado_ciberseguridad_Espa%C3%B1a/incibe_caracterizacion_mercado_ciberseguridad.pdf
44 https://www.cbinsights.com/blog/cybersecurity-startup-financing/

Entre las *startups* que últimamente consiguieron más financiación[45] destacan: **Tanium**, con sede en California, que obtuvo 90 millones de dólares de Andreeseen Horowitz; **Lookout**, que captó 150 millones de inversores como Khosla Ventures, Morgan Stanley, Goldman Sachs y Andreessen Horowitz; por otro lado, **Illumio** fue valorada en 1.000 millones en una ronda de 100 millones liderada por Accel Partner.

Adallom, una *startup* israelí especializada en ciberseguridad, fue recientemente adquirida por Microsoft por 250 millones de dólares[46]. La *startup* había captado ya unos 50 millones de dólares de los fondos de capital riesgo Sequoia Capital, Index Ventures u Rembrandt Fund, así como de empresas tecnológicas como EMC y HP.

En España, **Telefónica**, tras crear a su filial **Eleven Paths** hace tres años, ha realizado distintas adquisiciones en este segmento entre las cuales Informática 64, SmartAcces y GesConsultor. De igual forma, Telefónica ha invertido en empresas del sector como Alice Devices y Blueliv, y ha establecido alianzas con grupos como RSA, Alien Vault, Intel Security, Vaultive o Palo Alto Networks. La compañía factura en ciberseguridad en todo el mundo cerca de 400 millones de euros anuales[47].

Sectores y mercados principales

La ciberseguridad es una de las preocupaciones principales dentro de algunos sectores críticos como el **aeroespacial,** la **defensa**, la **inteligencia**, la **banca** y los servicios financieros y de seguros, los **gobiernos** y la **industria manufacturera.** En particular, la industria aeroespacial y de defensa representan la mayor cuota de mercado debido a las necesidades de proteger la información sensible en relación con los gobiernos y sus principales contratistas y proveedores.

45 https://www.cbinsights.com/blog/cybersecurity-industry-startup-funding-trends/
46 http://techcrunch.com/2015/09/08/microsoft-confirms-purchase-of-cloud-security-firm-adallom/
47 http://cincodias.com/cincodias/2015/10/08/empresas/1444299985_779701.html

Por otro lado, la difusión de las prácticas de **gobierno electrónico** a través de Internet, incrementa las amenazas cibernéticas en los organismos gubernamentales. Por lo tanto, as administraciones de todo el mundo están impulsando regulaciones y leyes estrictas en materia de seguridad de datos.

La ciberseguridad también están ganando interés en las PYMES sobre todo en lo que concierne a **soluciones de seguridad basadas en la nube.**

Otro campo de gran desarrollo es representado por la **seguridad móvil**, debido a la disponibilidad creciente de servicios en movilidad y el utilizo de los datos para diversos fines, como el marketing social.

Finalmente la implementación de **Internet de las cosas,** la creciente difusión de prácticas **BYOD** *(bring your own device)*, la sofisticación de las **amenazas persistentes avanzadas** (APT) están impulsando la demanda de soluciones de ciberseguridad, abriendo grandes oportunidades para la industria.

Casi todos los diferentes mercados relacionados con la ciberseguridad presentan **previsiones de crecimiento** en los próximos años con tasas anuales entre el 15 y el 33%:

- El mercado de la **seguridad gestionada** se espera que crezca de 14,32 mil millones de dólares en 2014 a 31,86 mil millones de dólares en 2019, a una tasa anual del 17,3%[48].
- Los **servicios de seguridad basados en la nube** podrían ver crecer su mercado de 4,2 mil millones de dólares en 2014 a 8,71 mil millones de dólares en 2019, a una tasa anual del 15,7%[49].
- El mercado de la **protección e datos en movilidad y BYOD** se espera que crezca de 1.29 mil millones de dólares en 2014 a 3,54 mil millones de dólares en 2019, a una tasa anual del 22,4%[50]
- El mercado de **protección de las amenazas persistentes avanzadas** (APT) podría llegar de 3.9 mil millones de dólares en 2015 a 8,7 mil millones de dólares en 2020, a una tasa anual del 17%[51]
- La seguridad relacionada con **Internet de las cosas** se espera que genere un mercado de 28,90 mil millones de dólares en 2020, creciendo desde los 6,89 mil millones de dólares en 2015 a una tasa anual del 33,2%[52]
- El mercado global de la ciberseguridad en ***smart grid*** tendrá un enorme crecimiento, pasando de 7,8 mil millones de dólares en 2011 hasta 79 mil millones de dólares en 2020, con una tasa anual del 29,5%[53].
- Finalmente, siempre más empresas deciden optar por un **seguro de ciberseguridad** para ayudar a mitigar el impacto financiero de los delitos cibernéticos que no han podido evitar. De hecho, se trata de uno de los sectores de más rápido crecimiento en el mercado de los seguros: se prevé que este mercado triplicará su tamaño actual para 2020, cuando alcanzará los 7,5 mil millones de dólares, a partir de los 2,5 mil millones de dólares registrados en 2015[54].

Se necesitan un millón de profesionales de ciberseguridad

La sofisticación de las tácticas y de la tecnología utilizada por los cibercriminales y sus continuos intentos de vulnerar redes y robar datos han superado la capacidad de los departamentos de TI y profesionales de seguridad para responder a dichas amenazas. La mayoría de organizaciones no cuentan con el personal o los sistemas necesarios para monitorizar las redes de manera constante, detectar amenazas y establecer protecciones a tiempo y de forma efectiva.

Según un estudio de ISACA[55], **el 37% de las organizaciones planea emplear más profesionales de ciberseguridad a lo largo de 2015**, aunque el 92% de ellas espera encontrar dificultades en encontrar candidatos con las competencias adecuadas. En general, **el 86% de las organizaciones cree que existe una falta de profesionales con competencias en ciberseguridad**. Recientemente CISCO ha dimensionado **el déficit de profesionales de ciberseguridad a nivel global en más de un millón de expertos[56].**

Por otro lado, según datos de INCIBE[57], **en España hay ya más de 42.500 profesionales** trabajando en el ámbito de la seguridad en la red y el sector crecerá exponencialmente en los próximos años.

48 MarketsandMarkets, Managed Security Services Market by Services - Global Forecast (2014 - 2019), http://www.marketsandmarkets.com/Market-Reports/managed-security-services-market-5918403.html

49 MarketsandMarkets, Cloud Security - Global Advancements, Forecasts & Analysis (2014-2019) http://www.marketsandmarkets.com/Market-Reports/cloud-security-market-100018098.html

50 http://www.marketsandmarkets.com/Market-Reports/mobile-data-protection-market-175123782.html

51 http://www.marketsandmarkets.com/Market-Reports/advanced-persistent-threat-protection-market-7303302.html

52 http://www.marketsandmarkets.com/Market-Reports/iot-security-market-67064836.html

53 http://www.prnewswire.com/news-releases/smart-grid-cyber-security-market--electrical-energy-storage-technology-in-the-intelligent-grid-analyzed-in-new-market-research-reports-170005586.html

54 PwC, Insurance 2020 & beyond: Reaping the dividends of cyber resilience, http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf

55 http://www.isaca.org/Pages/Cybersecurity-Global-Status-Report.aspx

56 http://globalnewsroom.cisco.com/es/es/release/Los-ataques-avanzados-y-el-tr%C3%A1fico-malicioso-experimentan-un-crecimiento-sin-precedentes-1881684

57 https://www.incibe.es/pressRoom/Prensa/Actualidad_INCIBE/NP_Foro_de_Empleo_Cybercamp

El Instituto Nacional de Ciberseguridad, INCIBE, ha lanzado un **programa de becas de estudios de especialización en ciberseguridad[58].**

Las becas pretenden contribuir a la generación de talento en ciberseguridad en España, con el objetivo final de dar respuesta a las necesidades de las empresas, que demandan perfiles expertos.

Para ello, INCIBE ha destinado en 2015, 400.000€ para la formación de expertos en ciberseguridad. Los fondos han ido dirigidos íntegramente para la ayuda a las matrículas de los alumnos presentados a las convocatorias de becas que han ofrecido las entidades seleccionadas en colaboración con INCIBE.

El director de la empresa de seguridad **S21sec, Xabier Mitxelena**, reconoce[59] que:

> *"Existe un déficit importante de mano de obra especializada. Crece la demanda y hay pocos expertos."*

En la misma línea, **Jorge López**, jefe del Grupo de Investigación en Seguridad de **Indra**, otra de las grandes compañías de seguridad españolas, apunta que:

> *"Los currículums de los candidatos que nos llegan presentan flaquezas en temas de hacking."*

Un estudio de la Fundación ESYS[60] señala que **el 22,73% de los ingenieros TIC españoles tienen un nivel de formación "inadecuado"** y "falta de formación práctica" en el ámbito de la ciberseguridad.

58 https://www.incibe.es/excelencia/becas_estudios/
59 http://economia.elpais.com/economia/2014/10/24/actualidad/1414175965_509685.html
60 Fundación ESYS, Necesidades de formación en el sector de la seguridad, http://www.fundacionesys.com/index.php?option=com_content&view=article&id=56%3Aestudio-fundacion-esys-qnecesidades-de-formacion-en-el-sector-de-la-seguridadq&catid=7%3Anoticias&Itemid=43&lang=es

Tendencias en ciberseguridad

Principales riesgos

Seguridad en dispositivos móviles, BYOD

El uso de dispositivos móviles para acceder a los datos corporativos es una tendencia creciente entre los empleados, tanto si se trata de dispositivos de propiedad de las mismas empresas, como de sus empleados, fenómeno este último conocido como *bring your own device*, o BYOD.

El auge del BYOD está relacionado con los beneficios que aporta, entre los cuales se encuentran: el ahorro de costes, al no tener que adquirir la organización estos dispositivos; la actualización constante a los últimos modelos; la mejora de la productividad y una mayor satisfacción de los empleados debido a las mejores condiciones de trabajo ya que se fomenta la flexibilidad laboral y el teletrabajo.

Sin embargo **el BYOD introduce unos riesgos importantes para las organizaciones**, sobre todo debido a los dispositivos móviles como tabletas y *smartphones*, que están resultando especialmente sensibles a los ciberataques tanto por su uso masivo, como por la ausencia de medidas de seguridad por parte de sus usuarios.

Además, las *apps* no suelen emplear adecuadamente mecanismos de seguridad, realizan conexiones no autorizadas y recopilan información privada sin autorización expresa del usuario. A través de ataques a los dispositivos móviles, los atacantes pueden fácilmente introducirse en las redes de las organizaciones.

Desde el punto de vista de la seguridad, según CCN-CERT[61], **son muchas las amenazas y vulnerabilidades principales asociadas al fenómeno BYOD:**

- Riesgos derivados de la **movilidad:** robo o manipulación.
- Uso de **dispositivos, aplicaciones y contenidos no confiables:** los mismos dispositivos tienen problemas de seguridad en si mismos o debido a su uso no seguro, como, por ejemplo, tras operaciones de *rooting* o *jailbreaking*; además, las aplicaciones instaladas en el dispositivos son difíciles de detectar, aplicaciones que podrían provenir de

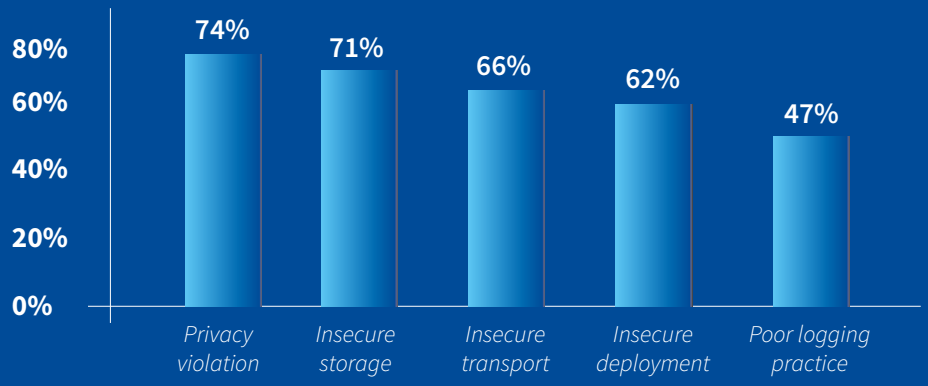
61 CCN-CERT IA-09/15 CIBERAMENAZAS 2014 TENDENCIAS 2015,
https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/795-ccn-cert-resumen-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html

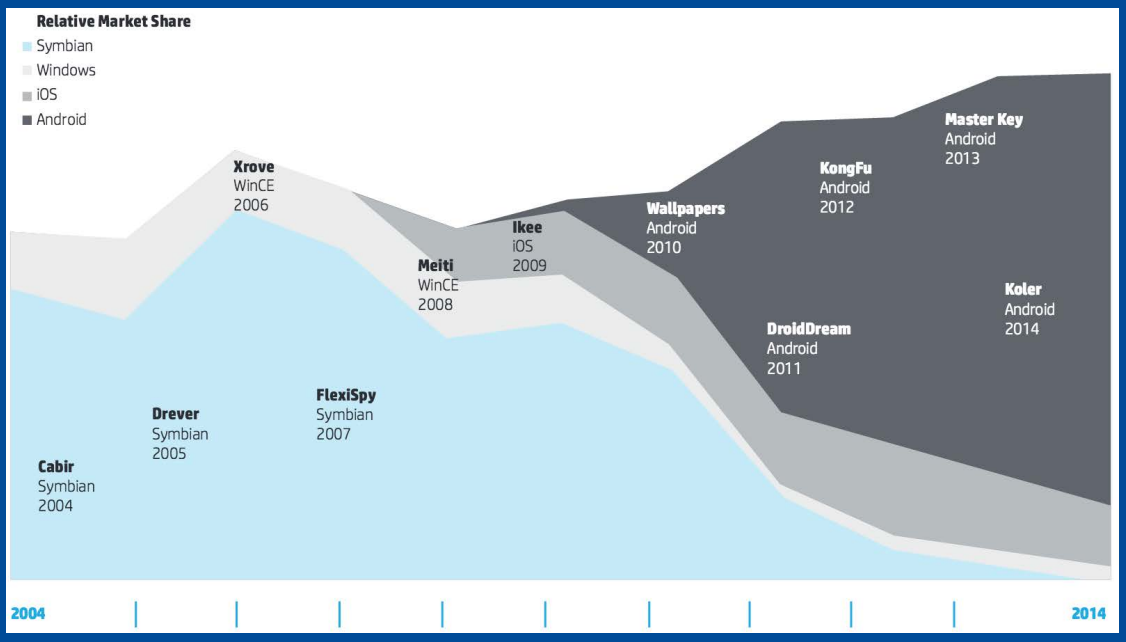
fuentes no seguras u oficiales; por último los dispositivos pueden acceder a URLS de páginas web dañinas sin que se puedan bloquear.

- Uso de **redes inseguras** y por tanto no inmunes a interceptaciones y otros ciberataques.
- **Interconexión con otros sistemas** a través de cables USB y las posibilidades derivadas de intercambio de datos y perdida del control sobre los mismos, así como de la posibilidad de transmisiones de código dañino.
- Uso de **servicios de localización**, con el riesgo de que se pueda acceder a la ubicación del usuario y de su actividad.
- **Riesgos de tipo legales,** por ejemplo todo lo que concierne al termino de la relación laboral y el tratamiento de los datos almacenados por el ex empleado.

Las 5 vulnerabilidades más frecuentes en aplicaciones móviles. HP Cyber Risk Report 2015

Según el CCN-CERT, en los próximos años se duplicará el número de amenazas a Android y las vulnerabilidades en los dispositivos móviles, plataformas y aplicaciones. Los datos comprometidos se usarán para otros ataques o para su venta en el mercado negro.





10 años de *malware* en dispositivos móviles. HP Cyber Risk Report 2015

Apple, una de las empresas que más presumen de sus estrictos controles de seguridad en sus aplicaciones, ha sufrido recientemente **el mayor ciberataque de su historia**[62]. El ataque consistió en un software malicioso que simula ser Xcode, el programa utilizado por los programadores para crear aplicaciones para dispositivos de Apple. Las aplicaciones creadas con este software falso – entre las cuales destacan WeChat, Didi Kuadi, o los juegos Angry Birds 2 y CarrotFantasy – estaban programadas para recoger información sobre los dispositivos infectados, como las contraseñas y datos de acceso a banca *on line,* transmitirla y permitir controlar estos dispositivos a distancia.

Seguridad de las Infraestructuras críticas

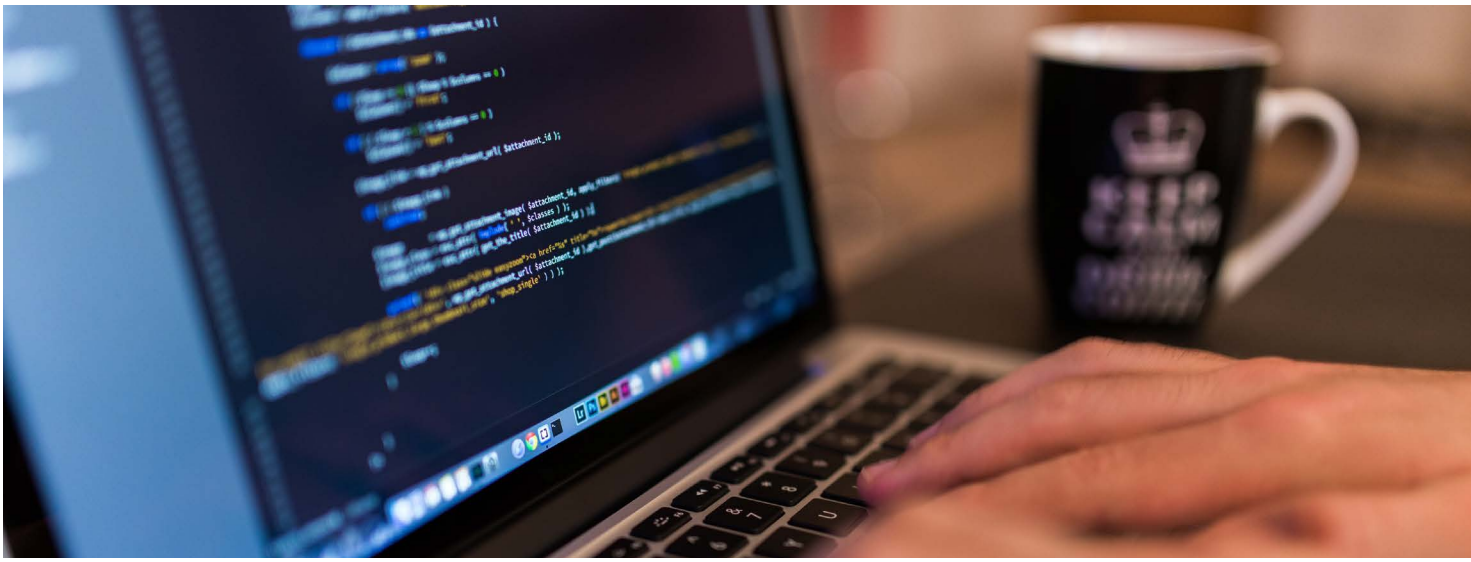
En España, la **Ley 8/2011**[63] establece una definición oficial de lo que debe ser considerado como Infraestructura Crítica:

> *"Las infraestructuras estratégicas (es decir, aquellas que proporcionan servicios esenciales) cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales."*

Las infraestructuras críticas – como centrales y redes de energía, transportes, sistema financiero, etc. – son recursos fundamentales y 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.

Al ser controladas por sistemas informáticos, pueden ser objeto de ciberataques, con consecuencias desastrosas. Estos sistemas de control industrial, en particular los sistemas **SCADA** (Supervisión, Control y Adquisición de Datos) están en el foco de atención por sus problemas de seguridad, debidos a su amplia difusión y a la escasa protección del software que los gestiona, a menudo anticuado y sin actualizar.

En España, el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC), creado en 2007, es el Órgano del Ministerio del Interior encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad en relación con la Protección de Infraestructuras Críticas en el territorio nacional.



62 http://tecnologia.elpais.com/tecnologia/2015/09/21/actualidad/1442823415_104653.html
63 http://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf

Gracias a la colaboración con el Ministerio de Industria, Energía y Turismo se ha puesto en marcha un Centro de Respuesta a Incidentes de Seguridad TIC (CERT) que conciernen también a estas infraestructuras.

Recientemente, el ministro del Interior, Jorge Fernández Díaz aseguró[64] que España se encuentra "en el momento más complicado desde el 11-M, desde los atentados de 2004" tras la reciente decisión de elevar el nivel de alerta a 4 sobre 5. Ante la amenaza terrorista, el Ministerio del Interior ha señalado 54 nuevos "operadores críticos"[65], empresas que dan servicios esenciales en los sectores del agua y el transporte. El mapa de alto riesgo de España está formado hoy por 93 infraestructuras críticas.

Seguridad en *smart grid*

Dentro del concepto de infraestructura crítica cobran bastante relevancia las *smart grid*, o redes eléctricas inteligentes y su protección de los ciberataques. Ya que el flujo bidireccional de información que se produce amenaza la privacidad y pone en peligro los datos personales de los usuarios.

Los *hackers*, por ejemplo, **pueden tomar el control de las aplicaciones y de los servidores y acceder a información confidencial.**

Por lo tanto, las *smart grid* requieren medidas de seguridad no sólo para manejar los sistemas y equipos, sino también para asegurar el intercambio de información entre sistemas.

Un informe[66] del Real Instituto de Asuntos Exteriores de Reino Unido alerta de **la escasa precaución contra los ciberataques que ejercen las centrales nucleares.** Contra las creencias habituales, las centrales nucleares de los países avanzados están indirectamente conectadas a Internet y por tanto presentan vulnerabilidades.
El primer ciberataque del que se tiene constancia, en 1992, llevó al Consejo Ruso de Seguridad a afirmar que podría haber acarreado **"un desastre similar al de Chernóbil".**

Recientemente tuvo mucha repercusión el ataque[67] mediante un gusano informático, ***Stuxnet*,** a dos centrales nucleares iraníes, Bushehr y Natanz, ocurrido en 2010. El ataque había podido acceder al sistema SCADA controlando indirectamente las centrifugadoras que se utilizan para enriquecer el uranio y provocar consecuencias altamente peligrosas. El mismo virus protagonizó un incidente en una central nuclear rusa en torno a 2010, hecho público por el dueño de la empresa antivirus **Kaspersky Lab.**

64 http://politica.elpais.com/politica/2015/07/05/actualidad/1436123811_079164.html
65 http://www.interior.gob.es/es/web/interior/noticias/detalle/-/journal_content/56_INSTANCE_1YSSI3xiWuPH/10180/4597486
66 Chatham House, Cyber Security at Civil Nuclear Facilities,
https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneExecSum.pdf
67 http://www.elmundo.es/elmundo/2010/11/23/navegante/1290510462.html

Seguridad en Internet de las cosas

El Internet de las cosas, se refiere a la creciente interconexión de objetos inteligentes –electrodomésticos, sensores, dispositivos– a través de Internet. IDC[68] prevé que **para 2020 haya 30 mil millones de dispositivos conectados en la red.**

Los dispositivos de este tipo generalmente carecen de las medidas de seguridad adecuadas, lo cual permite que **malintencionados externos puedan penetrar estos sistemas,** monitorizando los datos y la actividad de los usuarios o intentando interrumpir o poner en peligro la integridad de los productos y servicios. Si además consideramos que muchos proyectos de ciudades inteligentes (Smart city) se basan en el Internet de las cosas, es posible entender el alcance que pueden llegar a tener incidentes de seguridad en estos sistemas.

La división estadounidense de **Fiat Chrysler Automobiles** (FCA) ha llamado recientemente a revisión 7.810 vehículos en Estados Unidos, después de la posibilidad de que el software de sus radios pueda ser sensible a ataques inform áticos.

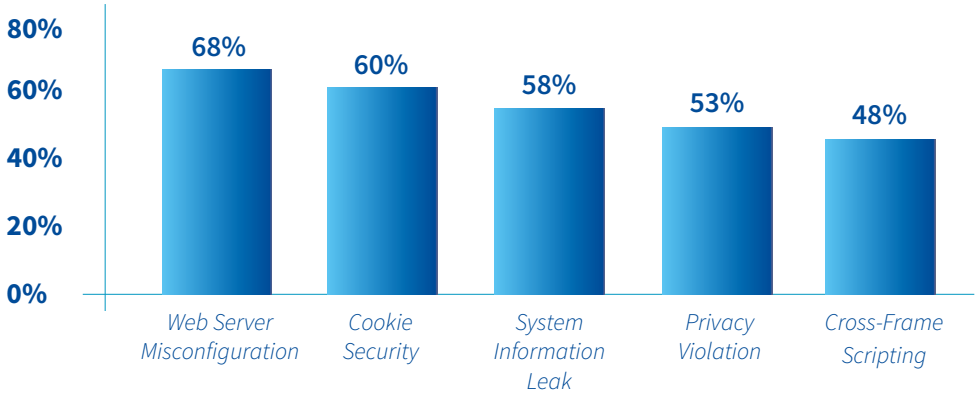
Algunos investigadores demostraron que es posible manipular el coche de forma remota, llegando hasta a apagar el vehículo mientras se está conduciendo. La noticia[69] aumenta las preocupaciones sobre los vehículos conectados a internet.

Vulnerabilidades técnicas

Las vulnerabilidades son **debilidades en el *software*** –sistema operativo, navegador web o aplicaciones– que permiten a un atacante comprometer la integridad, disponibilidad o confidencialidad del propio *software* o de los datos que procesa. Algunas de las vulnerabilidades más peligrosas permiten a los atacantes **ejecutar código dañino en el sistema comprometido.**

Según un informe de HP[70], la mayoría de las vulnerabilidades encontradas son relacionadas con una **mala configuración del servidor.**

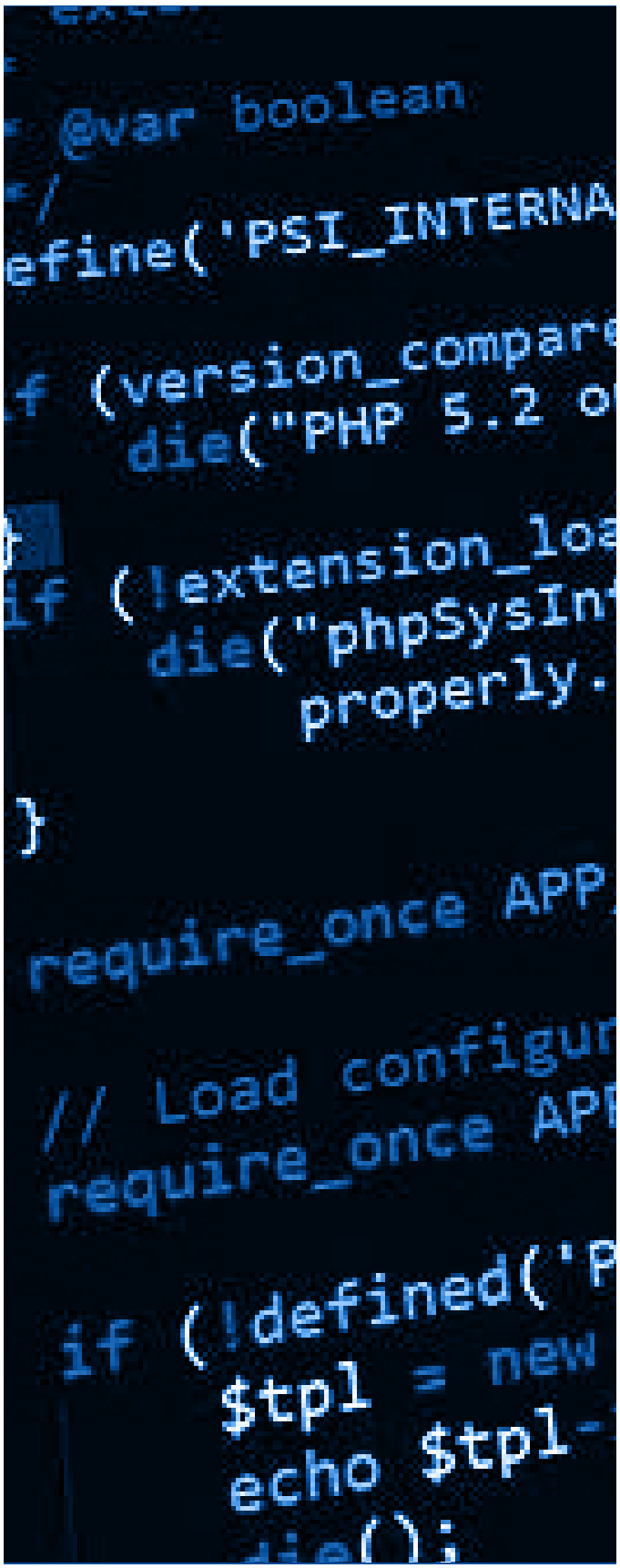
Las 5 vulnerabilidades más recurrentes en las aplicaciones, HP Cyber Risk Report 2015



68 http://www.idc.com/infographics/IoT/ATTACHMENTS/IoT.pdf

69 http://www.eleconomista.es/ecomotor/coches/noticias/6894507/07/15/Fiat-Chrysler-llama-a-revision-a-14-millones-de-vehiculos-tras-el-hackeo-de-un-Jeep.html

70 HP Cyber Risk Report 2015, http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/



Se define vulnerabilidad día cero a un fallo en un *software* no conocido por su fabricante por lo que no dispone de actualización de seguridad y puede permitir la ejecución de código en el ordenador víctima y su infección.

Ligado al concepto de vulnerabilidad se encuentran los ***exploit***, programas que explotan o aprovechan una vulnerabilidad de un sistema informático en beneficio propio. En particular, generan especial preocupación los llamados ***exploit* de día cero** (zero-day), es decir, aquellos que todavía no se han publicado y, por tanto, no disponen todavía de soluciones. También en el caso de los *exploit* existe un mercado negro en la *deep web*.

Hay algunas vulnerabilidades que últimamente provocan particular preocupación:

- **Vulnerabilidades en software y protocolos habituales,** como la recientes Shellshock,Heartbleed y OpenSSL.
- Explotación de **vulnerabilidades de Linux y OS-X,** fomentado por el incremento en su uso, la desactivación de determinadas medidas de seguridad por defecto (al objeto de permitir la instalación de software pirata) y el escaso desarrollo de herramientas de seguridad para estos sistemas.
- Ataques contra **cajeros automáticos,** máquinas expendedoras de tiquets y puntos de ventas (POS).

Tendencias en ciberseguridad

Principales amenazas

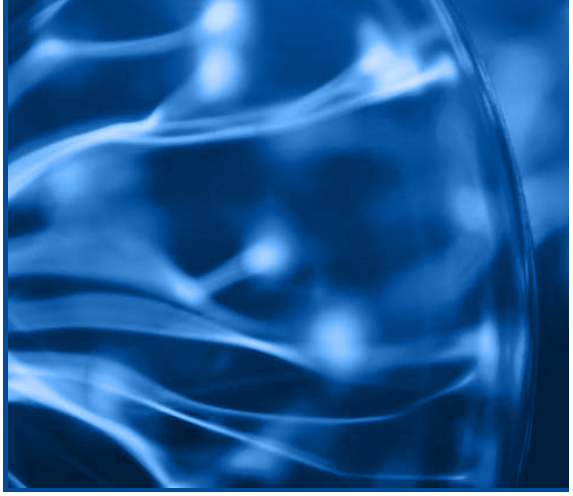
Ciberespionaje

Aunque después del "caso *Snowden*" el ciberespionaje esté más asociado a gobiernos y agencias gubernamentales como la NSA, no hay que olvidar que **puede ser llevado a cabo por empresas privadas** – fabricantes de dispositivos, proveedores de servicios de Internet, buscadores, etc.

Según indica el CCN-CERT[71], la amenaza del ciberespionaje originado en los propios estados o por las empresas ha alcanzado, durante 2014, **la máxima intensidad conocida hasta la fecha** y ha supuesto, sin duda, la mayor amenaza para la ciberseguridad de los intereses nacionales. Utilizando técnicas conocidas como **APT (Advanced Persistent Threat),** los ataques se han dirigido contra determinados departamentos de las administraciones públicas españolas, la industria de la Defensa, aeroespacial, energética, farmacéutica, química, TIC, así como los dispositivos móviles del personal directivo de estos sectores.

Siempre según el CCN-CERT, **la tendencia a recurrir a ciberespionaje se incrementará** por todos los países de nuestro entorno debido a su eficacia y dificultad de atribución.

71 CCN-CERT IA-09/15 CIBERAMENAZAS 2014 TENDENCIAS 2015,
https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/795-ccn-cert-resumen-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html



Crime-as-a-service

Otra tendencia es representada por el "crimen como servicio", un modelo en el que **terceras partes desarrollan los ciberataques.** Este fenómeno es debido a que los grupos criminales se han profesionalizado tanto que ya pueden ofrecer sus servicios como modelo de negocio. A través de la que se denomina la *deep web*, o la **Internet oculta,** es posible contratar los servicios de estos grupos para organizar ataques o comerciar con datos robados, como números de tarjeta o datos de acceso a la banca por Internet.

Hacktivismo

En paralelo con el activismo en el mundo real, se definen como hacktivistas a personas o grupos, más o menos organizados que para promover su causa o defender sus posicionamientos políticos o sociales llevan a cabo ciberataques de algún tipo. Se suelen centrar en ataques de nivel bajo (como desfiguración de páginas web, o ataques de denegación de servicio).

Tras la fragmentación de Anonymous –el grupo hacktivista más publicitado de los últimos años– las acciones de hacktivistas se han llevado a cabo en paralelo a los **grandes conflictos sociales y políticos de la actualidad,** como Siria, Ucraina, Israel, Turquía, entre otros.

Malware

Según un informe de HP[72], ***"Malware"* fue la palabra clave más buscada por los responsables de seguridad en 2014,** superando incluso "seguridad".

Unos de los *malware* más famosos hoy en día son el llamado ***Ransomware*** y **el *Cryptoware***, cuyas apariciones han ido en aumento. Su funcionamiento consiste en el secuestro del ordenador en el primer caso o en el cifrado de sus archivos en el caso de *Cryptoware*, pidiendo el pago de una cantidad de dinero para poder liberar la máquina.

Según el CCN-CERT[73], aumentarán las incidencias de *Ransomware* en las organizaciones, especialmente en sus variantes más agresivas, incluyendo grandes empresas e instituciones.

Otro ejemplo de malware es representado por ***Scareware***, que se presenta bajo el aspecto de un software de seguridad legítimo, y genera alertas erróneas o engañosas, dirigidas a atraer a los usuarios a participar en transacciones fraudulentas.

Spear-phishing

Difundido desde hace mucho tiempo, el *Phishing* consiste en **una estafa en forma de correo electrónico** dirigido con el objetivo de conseguir datos personales – como contraseñas de internet *banking* – que puedan ser utilizados posteriormente en beneficio del atacante.

Una forma particular de phishing, el llamado spear phishing, consiste en utilizar técnicas de **ingeniería social** – recopilación de información de la victima desde su actividad en Internet y sus perfiles en redes sociales – para obtener mayor verosimilitud.

72 HP Cyber Risk Report 2015, http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/
73 CCN-CERT IA-09/15 CIBERAMENAZAS 2014 TENDENCIAS 2015,
https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/795-ccn-cert-resumen-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html

Tendencias en ciberseguridad

Principales técnicas de respuesta y prevención

Seguridad en movilidad: MDM y MAM

En reacción a los riesgos del BYOD y con el objetivo de mantener la seguridad de su información, las empresas adoptan soluciones tecnológicas que permitan **la gestión de los dispositivos móviles a nivel corporativo** (*mobile device management*, o MDM) así como de las **aplicaciones** instaladas en ellos (*mobile application management*, o MAM).

Existen dos tipologías de soluciones MDM. La primera se basa en la gestión completa de la plataforma o del dispositivo móvil; la segunda, de tipo contenedor, proporciona una aplicación segura a través de la cual es posible acceder a los datos y servicios corporativos.

Esta última es la solución mas utilizada por la industria ya que permite una implantación y eliminación sencilla y mantiene la separación entre datos personales y corporativos.

En cuanto a las soluciones MAM, proveen menor control sobre los dispositivos, pero un gran control sobre las distintas aplicaciones. Proporcionan funcionalidades de entrega de las aplicaciones, licenciamiento del *software*, configuración, autorización, *tracking* de uso y borrado remoto.

Servicios de Seguridad Gestionada (MSS)

Las empresas están en una lucha constante para hacer frente a los nuevos retos de seguridad introducidos por la virtualización, el BYOD y las amenazas del cibercrimen organizado. Para muchas de ellas, la complejidad de las amenazas les está obligando a contratar los servicios de **proveedores de servicios de seguridad gestionada (MSSP)**. Estos tipos de proveedores de servicios externos permiten a las organizaciones mantener un alto nivel de seguridad y al mismo tiempo mejorar la eficiencia de negocio y minimizar los costes.

Los servicios que ofrecen los MSSP incluyen el bloqueo de virus, bloqueo de spam, detección de intrusos, protección de ataques de denegación de servicio, *firewalls,* la gestión de redes privadas virtuales (VPN) y también la gestión de las modificaciones y actualizaciones de los sistemas, entre otros.

Security as a Service

Otra tendencia es representada por la demanda creciente, sobre todo entre las PYMES, de **servicios de seguridad basados en la nube**, para hacer frente a la falta de personal o de habilidades, reducir los costes, o para cumplir de forma rápida con las normas de seguridad. Estos servicios se aprovechan de la escalabilidad del modelo de *cloud computing* permitiendo a las organización dimensionar los esfuerzos a su capacidad actual.

Estos servicios incluyen, entre otros, correo electrónico seguro, *gateways web*, administración de identidades y accesos (*Identity and Access Management* - IAM), evaluación en remoto de la vulnerabilidad, encriptación y prevención de perdidas de datos.

Según una encuesta de PwC[74], **un 69% de las empresas ya utiliza servicios de ciberseguridad basados en la nube.**

74 PwC, The Global State of Information Security® Survey 2016, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

Big Data Analytics

El Big Data implica la existencia de grandes cantidades de datos almacenadas, lo cual representa uno de los riesgos principales de la ciberseguridad. Por otro lado, el B**ig Data es también parte de la solución**: un número creciente de empresas están aprovechando el Big Data Analytics para analizar y modelar las ciberamenazas y poder responder rápidamente a incidentes.

Un enfoque basado en datos permite utilizar información en tiempo real para predecir los incidentes de seguridad. La ciberseguridad basada en datos permite identificar actividad anómala – tanto proveniente del exterior como de los mismos empleados – y rápidamente poner en marcha una respuesta.

Sin embargo, el Big Data Analytics requiere inversiones en términos de tecnologías y de recursos humanos competentes, por lo cual muchas empresas optan por soluciones basadas en la nube.

Una encuesta de PwC[75] asegura que **el 59% de las empresas ya están utilizando técnica de Big Data Analytics aplicadas a la ciberseguridad.**

Autenticación avanzada

Muchos de los incidentes de ciberseguridad tienen que ver con **la suplantación de identidad**, obtenida mediante el robo de contraseñas o a causa de una seguridad insuficiente. Por esto, siempre más organizaciones están recurriendo a métodos de autenticación avanzada aplicados a sus clientes – como por ejemplo hace el sector bancario – o a sus empleados y colaboradores.

Entre las soluciones más comúnmente adoptadas, se encuentran las contraseñas de un solo uso y enviadas a teléfonos móviles, la autenticación de dos factores, las combinaciones de token físicos con plataformas de autenticación basadas en la nube, o la biometría.

Según una encuesta de PwC[76], **el 91% de las empresas utiliza algún sistema de autenticación avanzada.**

75 PwC, The Global State of Information Security® Survey 2016, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
76 PwC, The Global State of Information Security® Survey 2016, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

Hacking ético

Se suele diferenciar entre dos tipologías de hackers, los de sombrero negro (*black hat*) y los de sombrero blanco (*white hat*). La diferencia entre los dos grupos reside en la finalidad de sus acciones: los primeros buscan beneficios económicos, políticos o estratégicos, mientras que los segundos buscan encontrar vulnerabilidades con el objetivo de prevenirlas. Los hackers de sombrero blanco son los que se asocian a hacking ético, que se ha vuelto **una herramienta importante de protección de la ciberseguridad.**

Los hackers éticos suelen realizar ***pen test* (test de penetración)** a los sistemas informáticos de organizaciones por cuenta propia o directamente empleados por estas organizaciones.

Simulación de incidentes de ciberseguridad

Un estudio de llevado a cabo por RSA[77], la división de seguridad de EMC, evidencia que las organizaciones que tuvieron que lidiar con un mayor número de incidentes de ciberseguridad en los pasados 12 meses son 2,5 veces más preparadas en sus estrategias de defensa que aquellas organizaciones que tuvieron menos incidentes. Lo que demuestra **la importancia de la experiencia previa para desarrollar capacidades de respuestas adecuadas.**

Por esto, cada vez más organizaciones recurren a las simulaciones de ciberseguridad con el objetivo de poner a prueba la capacidad tecnológica de sus herramientas y sobre todo la reacción de los recursos humanos en los procesos y actividades en caso de crisis. Gracias a las simulaciones es posible conocer de primera mano lo que sucedería y a qué decisiones complejas habría que hacer frente en caso de un ataque.

Entre las soluciones disponibles en el mercado, destaca **iPhalanx[78] de Indra**, diseñada para abordar el entrenamiento efectivo de fuerzas y cuerpos de seguridad y personal técnico de administraciones públicas y empresas. Permite la capacitación y adiestramiento en técnicas y tácticas de prevención, defensa y recuperación ante ciberataques, adaptados al nivel del alumno y el contexto operacional donde éste se desenvolverá en la realidad. También posibilita el entrenamiento de personal civil y militar que deba desarrollar actividades de hacking ético o ciberoperaciones.

77 RSA Cybersecurity Poverty Index, https://www.emc.com/campaign/rsa/cspi.htm
78 http://www.indracompany.com/sector/seguridad/oferta/ciberseguridad

Coordinación y regulación de la Ciberseguridad

Estrategia de Ciberseguridad Nacional

Las Estrategias Nacionales de Ciberseguridad (ENC) son documentos que recogen la visión del gobierno de una nación a la hora de enfrentarse al problema de la gestión de la Ciberseguridad en el ámbito global. Los objetivos de estas estrategias no se limitan únicamente a garantizar la seguridad de los ciudadanos y de las infraestructuras críticas del país, sino también incluyen **instaurar un ecosistema que fomente la cooperación público-privada y la cooperación internacional.**

En los últimos años los principales países desarrollados, especialmente en Europa, Norteamérica y en la órbita de la Unión Europea y de la OTAN, han venido publicando sus ENC. Desde 2013, también España cuenta con su documento[79], muy en línea con las estrategias de los demás países.

La Estrategia de Ciberseguridad Nacional 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.

La ENC representa una guía para los diferentes responsables y actores del sistema nacional que controla y gestiona la ciberseguridad, y, como tal, proporciona una respuesta a las siguientes cuestiones:

- **¿Qué preocupa?** Identificar los diferentes riesgos y amenazas relacionados con el ciberespacio.
- **¿Quién se preocupa?** Hay que definir el conjunto de órganos y organismos responsables de la dirección y gestión de la seguridad en el ciberespacio nacional.
- **¿Cómo se responde a esa preocupación?** Determinando una política y fijando unos objetivos y prioridades.

En cuanto al último punto, la Estrategia Nacional de Ciberseguridad para España fija las siguientes líneas de acción:

- Incrementar las **capacidades** de prevención, detección, respuesta y recuperación ante ciberamenazas.
- Garantizar la **seguridad de los sistemas de información y telecomunicaciones** que soportan las administraciones públicas y las infraestructuras críticas, reforzando las capacidades de detección y mejorando la defensa de los sistemas clasificados.
- Potenciar la capacidad de investigación y persecución del ciberterrorismo y de la ciberdelincuencia, sobre la base de un **marco jurídico y operativo eficaz.**
- Impulsar la seguridad y resiliencia de las infraestructuras, redes, productos y servicios empleando **instrumentos de cooperación público-privada.**
- Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales, mediante la **cooperación internacional.**
- **Concienciar** a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.
- Promover la **capacitación de profesionales**, impulsar el desarrollo industrial y reforzar el **sistema de I+D+i** en materia de ciberseguridad.

79 Gobierno de España, Estrategia de Ciberseguridad Nacional, http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

Directiva Europea sobre Ciberseguridad

La Directiva Europea sobre Ciberseguridad[80], denominada *Network and Information Security* (NIS) propuesta por la Comisión en 2013 y actualmente en la etapa final de las negociaciones entre el Parlamento Europeo y el Consejo, tiene como objetivo **garantizar un alto nivel común de ciberseguridad en la UE,** a través de:

- La mejora de las **capacidades** de ciberseguridad nacionales de los Estados miembros.
- La mejora de la **cooperación** entre los Estados miembros, y entre los sectores público y privado.
- Requerir a las empresas en sectores críticos como la energía, el transporte, la banca y la salud, así como a los principales servicios de Internet a que adopten **prácticas de gestión de riesgo y reporten los incidentes mayores a las autoridades nacionales.**

Una vez acordado y ejecutado en los Estados miembros, la Directiva pretende traer muchos beneficios:

- Los ciudadanos y los consumidores tendrán más confianza en las tecnologías.
- Los gobiernos y las empresas confiarán más en las redes e infraestructuras digitales para proporcionar sus servicios esenciales en su país y entre países.
- La economía de la UE cosechará los beneficios de servicios más fiables y una cultura de gestión del riesgo sistemático y de comunicación de informes de incidentes, –creando condiciones más equitativas y estables para cualquier organización que compita en el mercado único digital.

Entidades y organismos nacionales con competencias en ciberseguridad

INCIBE

El Instituto Nacional de Ciberseguridad, INCIBE[81], sociedad dependiente del Ministerio de Industria, Energía y Turismo (MINETUR) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.

Como centro de excelencia, INCIBE es **un instrumento del Gobierno para desarrollar la ciberseguridad** como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

CERT de Seguridad e Industria

El CERT de Seguridad e Industria, **centro de respuesta a incidentes de ciberseguridad operarado por INCIBE**, trabaja para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, aumentar la ciberresiliencia de las organizaciones y el diseño de medidas preventivas para atender a las necesidades de la sociedad en general y, en virtud del Convenio de Colaboración suscrito entre la Secretaría de Estado de Seguridad del Ministerio del Interior y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, a las necesidades de seguridad de las infraestructuras críticas, de apoyo en la investigación y lucha frente a ciberdelitos y ciberterrorismo.

80 http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive
81 https://www.incibe.es

CCN-CERT

El CCN-CERT[82] es **la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional**, CCN. Este servicio se creó a finales del año 2006 como el CERT gubernamental/nacional, y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad.

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de la Administración y de empresas pertenecientes a sectores designados como estratégicos.

La misión del CCN-CERT es, por tanto, contribuir 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 las Administraciones Públicas y a las empresas estratégicas, y a afrontar de forma activa las nuevas ciberamenazas.

Acuerdos internacionales

SOG-IS

El acuerdo SOG-IS[83] ha sido creado en respuesta a la Decisión del 31 de marzo de 1992 (92/242/EEC) del Consejo de la Unión Europea en el campo de la seguridad de los sistemas de información, y de la posterior Recomendación del Consejo del 7 de abril (1995/144/EC) sobre criterios comunes en la evaluación de seguridad de tecnología de la información.

Los participantes de este acuerdo son **organizaciones o agencias gubernamentales de países de la Unión Europea** o de AELC (Acuerdo Europeo de Libre Comercio).

Los participantes trabajan juntos en:

- Coordinar la estandarización de los perfiles de protección Common Criteria y de las políticas de certificación entre los Organismos Europeos de Certificación, para lograr una posición común en el seno del CCRA, el cuál está experimentando un rápido crecimiento.
- Coordinar el desarrollo de perfiles de protección cuando la Comisión Europea lance un directiva que tuviera que ser implementada en leyes nacionales y que involucre a la seguridad de los sistemas de la información.

Proceso Meridian

El Proceso Meridian[84], tiene como objetivo el intercambio de ideas y de acciones para la **cooperación de los organismos gubernamentales, encargados de la Protección de las Infraestructuras Críticas de la Información** (CIIP), sobre las cuestiones que se plantean a nivel mundial. Explora los beneficios y oportunidades de cooperación entre los gobiernos y proporciona una oportunidad única para compartir las experiencias con todo el mundo.

El Proceso de Meridian busca crear una comunidad de políticas gubernamentales de alto nivel en CIIP fomentando la colaboración. El Proceso Meridian reconoce que sólo mediante el trabajo conjunto podemos avanzar en cada una de las metas y objetivos nacionales.

La participación en el Proceso Meridian está abierta a todos los países / economías, y está dirigido a los altos responsables de las políticas gubernamentales que participan en las cuestiones relacionadas con la CIIP. Se invita a que cada país / economía pueda tomar parte en el proceso Meridian, y se anima a asistir a la conferencia anual de Meridian.
Las Conferencias Meridian están dirigidas a los altos responsables de las políticas gubernamentales, involucrados en la CIIP.

La primera conferencia fue organizada en el Reino Unido en 2005 y las conferencias posteriores se celebraron en Hungría, Suecia, Singapur, Estados Unidos, Taiwán, Qatar, Alemania, Argentina, y la última en Japón en el año 2014. El país anfitrión cambia cada año, y el objetivo es hacer rotar la Conferencia Meridian entre los diferentes territorios para aumentar la participación de la Comunidad Meridian.

82 www.ccn-cert.cni.es
83 http://sogis.org/
84 http://www.meridianprocess.org/default.aspx

Convenio sobre la Ciberdelincuencia

Firmado en 2001 en Budapest, este documento, inicialmente de ámbito europeo, pretende dar cabida a una **estructura uniforme de actividades que debían considerarse delictivas**, sobre las que sería preciso establecer una legislación uniforme. De este modo se pretende facilitar la persecución internacional del ciberdelito. En la actualidad ha sido firmado por unos 50 países, incluidos, entre otros, España, EEUU, Japón y la mayoría de los países de América Latina.

Partnering for Cyber Resilience

Esta iniciativa[85] del Foro Económico Mundial fue lanzada en 2012 en respuesta a la creciente importancia de la ciberseguridad. A día de hoy **más de 100 organizaciones están activamente involucradas**. La fase actual del proyecto se centra en cuantificar el impacto de las ciberamenazas y en la exploración de la viabilidad de los modelos de evaluación de riesgos en toda la industria.

Desde el principio, se establecieron los principios básicos de Alianzas del Foro Económico Mundial para la iniciativa de ciberresiliencia para crear conciencia de los ciberriesgos y construir el compromiso con respecto a la necesidad de enfoques más rigurosos a su mitigación.

International Watch and Warning network (iWWn)

Esta red se estableció en 2004 para fomentar la colaboración internacional a la hora de abordar las amenazas cibernéticas, ataques y vulnerabilidades. Proporciona un **mecanismo para que los países participantes compartan información** encaminada a la concienciación mundial de la situación cibernética y a facilitar la respuesta a incidentes.

Los países participantes son: Alemania, Australia, Canadá, Estados Unidos, Finlandia, Francia, Holanda, Hungría, Italia, Japón, Nueva Zelanda, Noruega, Reino Unido, Suecia, Suiza.

FIRST - Forum of Incident Response and Security Teams

FIRST[86] se estableció en 1990. Es una **red de equipos de respuesta a incidentes de seguridad informática** individuales que trabajan juntos de manera voluntaria para hacer frente a problemas de seguridad informática y su prevención. Estos equipos son de organismos tan diversos como gobiernos, policías, universidades, empresas privadas y otras organizaciones con interés justificable según lo determinado por su Comité Directivo.

85 http://www.weforum.org/projects/partnership-cyber-resilience
86 https://www.first.org/

Bibliografía

CCN-CERT IA-09/15 CIBERAMENAZAS 2014 TENDENCIAS 2015
https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/795-ccn-cert-resumen-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html

CCN-CERT IA-21/13 Riesgos y amenazas del BYOD
https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/677-ccn-cert-ia-21-13-riesgos-y-amenazas-del-byod-1/file.html

Cisco, Ciber-seguridad en las empresas españolas
http://www.cisco.com/web/ES/ciberseguridad/index.html

Fundación Esys, informe anual de la seguridad en españa 2012
http://www.fundacionesys.com

Gobierno de España, Estrategia de Ciberseguridad Nacional
http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

HP Cyber Risk Report 2015
http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/

INCIBE, Análisis y caracterización del mercado de la Ciberseguridad
https://www.incibe.es/extfrontinteco/img/File/empresas/blog/20150331_caracterizacion_mercado_ciberseguridad_Espa%C3%B1a/incibe_caracterizacion_mercado_ciberseguridad.pdf

ISACA, 2015 Global Cybersecurity Status Report
http://www.isaca.org/Pages/Cybersecurity-Global-Status-Report.aspx

MarketsandMarkets, Advanced Persistent Threat Protection Market by Solution - Global Forecast to 2020
http://www.marketsandmarkets.com/Market-Reports/advanced-persistent-threat-protection-market-7303302.html

MarketsandMarkets, Cloud Security - Global Advancements, Forecasts & Analysis (2014-2019)
http://www.marketsandmarkets.com/Market-Reports/cloud-security-market-100018098.html

MarketsandMarkets, Cyber Security Market by Solution
http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html

MarketsandMarkets, Internet of Things (IoT) Security Market by Technologies - Global Forecast to 2020
http://www.marketsandmarkets.com/Market-Reports/iot-security-market-67064836.html

MarketsandMarkets, Managed Security Services Market by Services - Global Forecast (2014 - 2019)
http://www.marketsandmarkets.com/Market-Reports/managed-security-services-market-5918403.html

MarketsandMarkets, Mobile Data Protection Market by Solutions - Global Forecast to 2019
http://www.marketsandmarkets.com/Market-Reports/mobile-data-protection-market-175123782.html

Ponemon Institute Cost of Cyber Crime Study
http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/index.html?jumpid=va_fwvpqe387s

PwC, Insurance 2020 & beyond: Reaping the dividends of cyber resilience
http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf

PwC, Temas candentes de la Ciberseguridad
http://www.pwc.es/es/publicaciones/gestion-empresarial/temas-candentes-ciberseguridad.html

PwC, The Global State of Information Security® Survey 2016
http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

PwC, 2015 Information security breaches survey
http://www.pwc.co.uk/industries/insurance/insights/2015-information-security-breaches-survey.html

RSA Cybersecurity Poverty Index
https://www.emc.com/campaign/rsa/cspi.htm

Zurich, Risk Nexus Global cyber governance: preparing for new business risks
http://knowledge.zurich.com/cyber-risk/global-cyber-governance/

www.u-tad.com info@u-tad.com

900 373 379

Centro adscrito a

UNIVERSIDAD CAMILO JOSÉ CELA

Proyecto confinanciado por el Ministerio de Economía y Competitividad

GOBIERNO DE ESPAÑA MINISTERIO DE ECONOMIA Y COMPETITIVIDAD

La Suma de Todos

Madrid Network

U-TAD

CENTRO UNIVERSITARIO DE TECNOLOGÍA Y ARTE DIGITAL