

BUENAS PRÁCTICAS EN GESTIÓN DE RIESGOS



LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Ciberseguridad

Una guía de supervisión

El INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA es una asociación profesional fundada en 1983, cuya misión es contribuir al éxito de las organizaciones impulsando la Auditoría Interna como función clave del buen gobierno. En España cuenta con más de 3.200 socios, auditores internos en las principales empresas e instituciones de todos los sectores económicos del país.

LA FÁBRICA DE PENSAMIENTO es el laboratorio de ideas del Instituto de Auditores Internos de España sobre gobierno corporativo, gestión de riesgos y Auditoría Interna, donde participan más de 150 socios y profesionales técnicos expertos.



AUDITORÍA INTERNA



BUENAS PRÁCTICAS EN GESTIÓN DE RIESGOS



OBSERVATORIO SECTORIAL



PRÁCTICAS DE BUEN GOBIERNO

El laboratorio trabaja con un enfoque práctico en la producción de documentos de buenas prácticas que contribuyan a la mejora del buen gobierno y de los sistemas de gestión de riesgos en organizaciones de habla hispana. Además de desarrollar contenido, fomenta el intercambio de conocimientos entre los socios.



Ciberseguridad

Una guía de supervisión

Octubre 2016

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN: Israel Martínez Lacabe, CISA. GRUPO SANTANDER

Josep Castells Rafel, CISA. CAIXABANK

José Antonio Castrillo, CISA, CISM, CGEIT. MAZARS

Jordi Civit Vives, CISA, CCSA. MELIÁ HOTELES

Oliver Crespo Romero, CISA, CISM. SANITAS

Sandra Fernández Moreno, CISA. MAPFRE

Gregorio Hernández Manso, CISA, CISM. RED ELÉCTRICA DE ESPAÑA

Juan José Huerta Díaz, CIA, CISA, CISM, CGEIT, CDPP. BBVA

Eduardo Iglesias Cordero. LIBERBANK

Daniel Martínez Villegas. CIMPRESS

Raúl Mateos Martín, CISA, CISSIP, CRISC. BBVA

Marc Muntañá Vergés, CISA, CISM. MUTUA UNIVERSAL

Felipe Pastor Fornieles, CISA, CISM. ERNST & YOUNG, S.L.

Fernando Picatoste Mateu, CIA, CISA, CISM, CGEIT, CRISC, CISSP. DELOITTE

Albert Sans I Feliu, CISA. INDITEX

El avance de las nuevas tecnologías ha propiciado un cambio sin precedentes que ha influido en la forma de operar de las organizaciones, cuyas actividades se desarrollan cada vez más en el ciberespacio.

Este hecho propicia un gran desarrollo económico y social, pero a la vez la aparición de nuevos retos y amenazas que es imprescindible gestionar. No en vano el Foro Económico Mundial incluye varios riesgos asociados a la ciberseguridad en su *ranking* de Riesgos Globales desde hace años. A modo de ejemplo, en 2016 el coste medio de un ataque informático para las compañías ronda los 75.000 euros, lo que hace que solo los ciberdelitos cuesten a las empresas españolas unos 14.000 millones de euros al año.

Los ciberataques y su naturaleza se han multiplicado en los últimos años, y cada vez son más complejos y más difíciles de prevenir y detectar, lo que hace que los órganos de gobierno de las organizaciones deban incrementar y mejorar la supervisión sobre la ciberseguridad.

LA FÁBRICA DE PENSAMIENTO, el *think tank* del Instituto de Auditores Internos de España, aborda en este documento –parte de un manual editado también por el IAI– las principales cuestiones relativas a la ciberseguridad y un completo análisis de buenas prácticas de Auditoría Interna para la evaluación y revisión de los controles en esta materia.

También se incluyen los 20 Controles Críticos de Seguridad que todas las organizaciones deben implementar y cuál es el papel de Auditoría Interna en la revisión de cada uno de ellos.

El valor que aporta esta guía de supervisión va más allá de los auditores internos de sistemas o de las Direcciones de Auditoría Interna. Las Comisiones de Auditoría y otros comités de la empresa encontrarán en estas páginas un importante aliado que les ofrecerá información completa y precisa para permitirles tomar decisiones sobre la estrategia, organización y operaciones para evitar que este riesgo se materialice en las organizaciones.

Un documento tan exhaustivo y a la vez de fácil comprensión como éste, incluso para los profanos en auditoría de TI, solo podía estar firmado por expertos auditores internos como los que han formado parte de la Comisión Técnica. Les felicito por haber puesto su experiencia y conocimiento al servicio de todos los socios y por mantener el nivel de excelencia y sencillez al que nos tienen acostumbrados las publicaciones de LA FÁBRICA DE PENSAMIENTO.

Ernesto Martínez

Presidente del Instituto de Auditores Internos de España



Índice

INTRODUCCIÓN	06
PRINCIPALES CUESTIONES RELATIVAS A LA CIBERSEGURIDAD	07
Riesgos, amenazas y vulnerabilidades	09
De la seguridad de TI a la ciberseguridad: el cambio de paradigma	16
Ciberejercicios y ciberseguros	21
Metodologías y estrategias de control y gestión de ciberriesgos	24
Regulación y normativa	28
BUENAS PRÁCTICAS DE AUDITORÍA INTERNA PARA LA EVALUACIÓN Y REVISIÓN DE CONTROLES DE CIBERSEGURIDAD	32
El rol de Auditoría Interna	32
20 Controles Críticos de Seguridad que todas las organizaciones deberían implementar	35
CERTIFICACIONES PROFESIONALES	42
BIBLIOGRAFÍA RELEVANTE	46



Introducción

La protección frente a los ciberriesgos se ha convertido en una prioridad debido a las nuevas amenazas procedentes de Internet, el crecimiento del número de ataques y la mayor complejidad de las amenazas.

La economía internacional, la prestación de servicios por parte de las administraciones, empresas y profesionales, el acceso a la información, la educación, el comercio, el ocio o la salud de los ciudadanos, al igual que casi todos los ámbitos de nuestra sociedad, se sustentan hoy más que nunca (y cada vez más) en el ciberespacio¹.

Las tecnologías de la información y las comunicaciones (TIC) propician el desarrollo económico de la sociedad de manera integrada dentro de las empresas y organizaciones, que usan en su actividad el amplio abanico de dispositivos electrónicos y redes de comunicaciones disponibles.

Sin embargo, de la mano de dicha expansión tecnológica y el aumento del uso de servicios de Internet surgen nuevos retos y desafíos para las organizaciones. Así, una de las principales amenazas que han traído consigo estos avances es la proliferación de acciones delictivas en el ciberespacio.

Ningún dispositivo hardware o software existente en la actualidad –desde el sistema más complejo instalado en una infraestructura estratégica, como una central nuclear, hasta la más sencilla aplicación informática instalada en un teléfono móvil– está exento de ser atacado.

Así, la ciberseguridad representa actualmente una de las principales preocupaciones de todas las empresas e instituciones, con independencia del sector o ámbito al que pertenezcan.

La protección frente a los ciberriesgos se ha convertido por tanto en una prioridad de las mismas, fruto de la proliferación de nuevas amenazas procedentes de Internet, el enorme crecimiento durante los últimos años del número de ataques recibidos por las organizaciones, y el aumento en la complejidad y sofisticación de estas amenazas.

1. Se entiende por ciberespacio el entorno virtual común que comprende la interconexión del conjunto global de sistemas, activos de información y redes de comunicaciones (incluyendo Internet), así como los usuarios de estos servicios y tecnologías.





Principales cuestiones relativas a la ciberseguridad

Los ciberataques no sólo se han multiplicado en los últimos años, extendiendo su incidencia a todo tipo de organizaciones y a todos los sectores económicos, sino que su naturaleza ha cambiado drásticamente en términos de frecuencia, complejidad y finalidad, dentro de un proceso de continua evolución y sofisticación que los hace cada vez más complejos y peligrosos.

En pocos años, las tradicionales amenazas de la seguridad (virus, gusanos, troyanos,...) han evolucionado hacia ataques de denegación de servicios (DoS²) y sofisticados softwares maliciosos (*malware*) hasta llegar a las amenazas persistentes avanzadas (APTs) o ataques dirigidos, que combinan múltiples técnicas de ataque y explotación de diferentes tipos de vulnerabilidades, incluyendo el uso de técnicas de ingeniería social (por ejemplo *spear-phishing*), así como una fase previa de estudio y recolección de información del objetivo que los hace mucho más eficaces y dañinos.

Son numerosos los ataques recibidos por grandes corporaciones y multinacionales durante los últimos años, como JPMorgan, Sony,

Target, Apple, Home Depot, o Google, entre otras. También administraciones públicas y gobiernos de todo el mundo están entre los damnificados que han sufrido robos de información de sus bases de datos de clientes, elevadas pérdidas económicas, prolongadas indisponibilidades en sus sistemas, daños reputacionales o sabotajes de sus servicios online; como consecuencia del denominado cibercrimen.

Sirvan como ejemplos de lo anterior las siguientes ciberamenazas que han provocado algunas de las mayores infecciones y trastornos recientes en materia de seguridad informática:

- **Zeus.** *Malware*³ orientado al robo de información personal de los usuarios: credenciales de cuentas de correo electrónico, redes sociales, datos de servicios financieros, etc.
- **Flame y Agent BTZ.** Software espía con gran capacidad de propagación capaz de obtener capturas de pantalla, pulsaciones de teclado, control del *bluetooth*, *webcam* o grabación de llamadas. Asimismo, posee la capacidad de transmitir la información reco-

Empresas, administraciones públicas y gobiernos han sufrido robos de información, pérdidas económicas o sabotajes como consecuencia del denominado cibercrimen.

2. DoS: Del inglés *Denial of Service*.

3. Si bien no existe un criterio de clasificación estricto de las diferentes tipologías de *malware*, se entiende de manera general que esta palabra incluye todo tipo de software o código malicioso que tiene el objetivo de infiltrarse y dañar un sistema de información, abarcando virus, gusanos, troyanos, *rootkits*, *spyware*, *keyloggers*, *botnets*, etc.

pilada ocultándola mediante técnicas de cifrado.

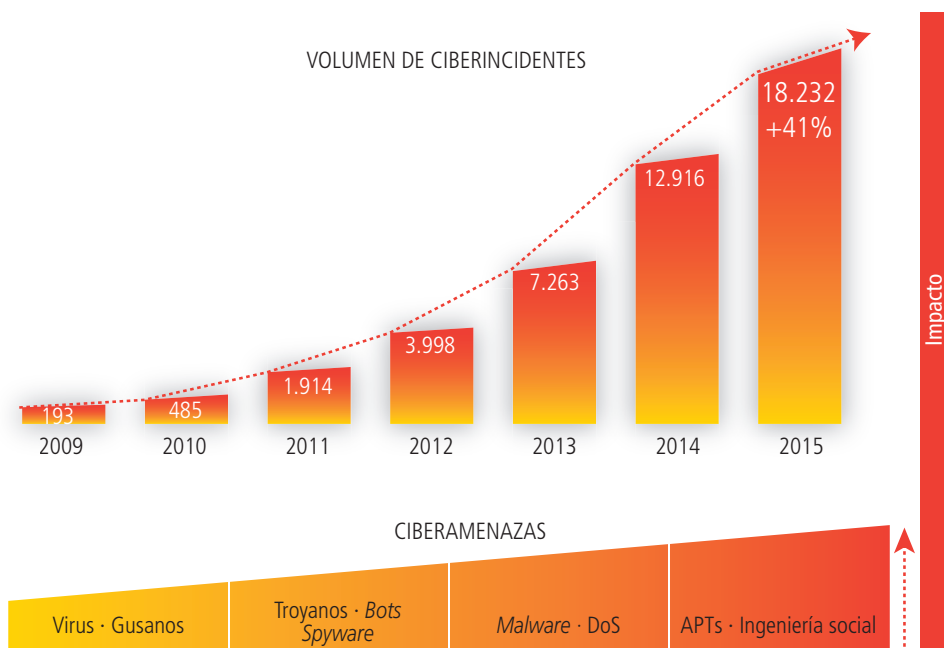
- **Carbanak.** Ataque Persistente Avanzado (APT) diseñado y dirigido al sector bancario, capaz de alterar y manipular el funcionamiento de las redes y software de control de los cajeros automáticos.
- **Ransomware.** También conocido como el “virus de la policía”, cifra la información contenida en el sistema del usuario infectado, solicitando una compensación económica para su desbloqueo.
- **Stuxnet.** Software malicioso descubierto en 2010, capaz de controlar y manipular software de control y supervisión de procesos industriales (SCADA).

Actualmente la ciberseguridad representa un problema global y sistémico, como lo demues-

tra también el hecho de que el *World Economic Forum* lo incluya desde el año 2014 en la lista de los 5 principales riesgos globales, en términos de probabilidad, junto al cambio climático, el desempleo, las catástrofes naturales y la desigualdad económica.

Los principales vectores y razones que han propiciado esta situación actual son:

- La creciente expansión del acceso a Internet y el proceso de digitalización global (actualmente existen más de 2.800 millones de personas con acceso –más del 40% de la población mundial– y 10.000 millones de dispositivos conectados), así como la popularización de nuevos dispositivos (*smartphones*, *tablets*), nuevas tecnologías de procesamiento de datos (*cloud computing*, virtualización de sistemas) y posibilidades de conexión remota y/o móvil (Wifi, VPN, 4G,



Fuente: elaboración propia a partir de datos de CCN-CERT

satélite), con sus consiguientes riesgos y debilidades de seguridad asociados.

- La velocidad de los cambios tecnológicos y la adopción de tecnologías emergentes, en ocasiones no suficientemente maduras desde el punto de vista de seguridad.
- La crisis económica de carácter global (gran recesión) que se inició durante los años 2007-2008 y que, en mayor o menor medida, sigue vigente en muchos países y geografías.
- Las importantes carencias existentes en las legislaciones transfronterizas, laxa normativa y escasa regulación en algunos países, y dificultad legal de perseguir el cibercrimen, de manera general.
- La creciente actividad que presentan los movimientos activistas antisistema y anti-globalización.

- La posibilidad de utilizar fuentes y sistemas anónimos, que amplía la cantidad de gente dispuesta a cometer este tipo de delitos.

Se estima que el cibercrimen tiene un impacto global en la economía de entre 300.000 millones y un billón de dólares al año, cifra que equivale a cerca del 1% del PIB mundial, alcanzando un nivel similar al de amenazas criminales convencionales como el narcotráfico y/o la piratería⁴.

Más aún, los riesgos cibernéticos tienen una naturaleza sustancialmente superior a éstas últimas, en la medida que pueden tener diferentes objetivos simultáneamente: la rentabilidad que ofrece su explotación, la facilidad y el bajo coste de las herramientas utilizadas para la consecución de ataques, así como la facilidad de ocultación del atacante; hacen posible que estas actividades se lleven a cabo de forma anónima y desde cualquier lugar del mundo, con lo que su trazabilidad y seguimiento resulta sumamente complejo.

El concepto de riesgo cibernético proviene de la amenaza continua y a escala industrial por parte de terceros sobre los activos digitales, las operaciones y la información corporativa.

RIESGOS, AMENAZAS Y VULNERABILIDADES

Riesgos cibernéticos

El concepto de riesgo cibernético proviene de la amenaza continua y a escala industrial sobre los activos digitales, las operaciones y la información corporativa, por parte de terceros. Para entender mejor el contexto actual, es necesario conocer los principales riesgos a los que se exponen las organizaciones:

FRAUDE DINERARIO

El robo económico representa una de las principales motivaciones de la gran mayoría

de atacantes. Debido a ello, las instituciones y entidades financieras son uno de los principales objetivos de los ciberdelincuentes.

ROBO DE INFORMACIÓN

La filtración pública o pérdida de la información confidencial representa un elevado riesgo para cualquier organización, cuyos impactos o pérdidas pueden resultar especialmente significativos. Debido a ello, la información de carácter personal o documen-



4. McAfee (2013): *The Economic Impact of Cybercrime and CyberEspionage*. Center for Strategic and International Studies.

La pérdida de reputación es una de las principales consecuencias de los ataques y el objetivo de gran parte de los ciberataques, con efectos altamente significativos.

tos clasificados son algunos de los principales activos de información que deben ser especialmente protegidos.

INDISPONIBILIDAD DE SERVICIOS

Interrupción puntual o prolongada de los servicios online ofrecidos por una organización (correos, pagos financieros, cobro de impuestos, registros públicos).

SABOTAJE DE INFRAESTRUCTURAS

Ataques contra los servicios o infraestructuras críticas de un país o estado (abasteci-

mientos, comunicaciones, etc) con el objetivo de provocar una interrupción puntual o prolongada de los mismos.

PÉRDIDA DE REPUTACIÓN

Más que un riesgo en sí mismo, es una de las principales consecuencias de los ataques y el objetivo de gran parte de los ciberataques, cuyos efectos en una organización pueden resultar altamente significativos.



PRINCIPALES RIESGOS

- Fraude dinerario.
- Robo de información.
- Indisponibilidad de servicios.
- Sabotaje de infraestructuras.
- Pérdida de reputación.



PRINCIPALES AMENAZAS

- Contra la información.
- Contra la infraestructura TIC.



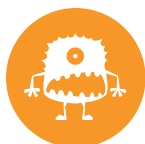
PERFIL DE LOS ATACANTES

- Hacking.
- Cibercrimen.
- Hacktivism.
- Ciberespionaje y ciberterrorismo.
- Insiders.



PRINCIPALES TÉCNICAS DE ATAQUE

- Ingeniería social.
- Fingerprinting.
- Enumeración y escaneo.
- Ataques de días cero (0-Day).
- Spam y Phishing.
- Hijacking.
- DoS (Denegación de Servicios).
- SQL Injection.
- Cross-site scripting (XSS).
- Virus, malware, gusanos y troyanos.
- Botnet (Redes zombis).
- Rootkits.
- APT (Amenaza Persistente Avanzada).



Amenazas

Al igual que la naturaleza se adapta, las amenazas que en un principio eran puntuales y muy concretas en cuanto a objetivos, con técnicas muy simples y consecuencias para el

usuario más molestas que dañinas, se están convirtiendo en sofisticadas herramientas potencialmente dañinas. De este modo, las principales amenazas relacionadas con el ciberes-

pacio se pueden agrupar en las amenazas contra la información y las amenazas contra la infraestructura TIC⁵.

AMENAZAS CONTRA LA INFORMACIÓN

Aquellas cuya materialización provocan una pérdida, manipulación, publicación o uso inadecuado de la misma. Entre otras destacan:

- Espionaje, desde el ámbito del espionaje de Estado al espionaje industrial.
- Robo y publicación de información clasificada o sensible (datos personales, datos bancarios).
- Robo de identidad digital.
- Fraude.

AMENAZAS CONTRA LAS INFRAESTRUCTURAS TIC

Son aquellas cuya materialización pueden provocar la interrupción temporal, parcial o total de determinados servicios o sistemas, entre las que se encuentran:

- Ataques contra infraestructuras críticas.
- Ataques contra las redes y sistemas.
- Ataques contra servicios de Internet.
- Ataques contra sistemas de control y redes industriales.
- Infecciones con *malware*.
- Ataques contra redes, sistemas o servicios a través de terceros.

Perfil de los atacantes

Si bien el anonimato y la deslocalización son algunas de sus máximas señas de identidad, los principales actores que componen el perfil de los atacantes se pueden clasificar en los siguientes grupos:

HACKING

Individuos que generalmente trabajan de manera individual con el objetivo de provocar trastornos o daños puntuales, si bien no suelen resultar de gran impacto.

CIBERCRIMEN

Organizaciones y/o grupos de ciberdelincentes/*hackers* que cuentan generalmente con los recursos, conocimientos, motivación y respaldo o apoyo financiero necesarios para la obtención de sus objetivos (princi-

palmente el fraude económico y el robo de información confidencial).

HACKTIVISMO

Grupos de *hackers* que actúan en base a una serie de principios y/o creencias políticas, sociales o religiosas, principalmente con fines reivindicativos. Sus principales objetivos suelen incluir multinacionales, gobiernos y organismos oficiales.

Algunos ejemplos conocidos de grupos *hacktivistas* son: "Anonymous", "Legion of Doom", "Milw0rm" y "LulzSec".

CIBERESPIONAJE Y CIBERTERRORISMO

Uso de tecnologías de la información y comunicación electrónica con el propósito de apoderarse de información confidencial de



5. Spanish Cyber Security Institute (2014): *La Ciberseguridad Nacional, un compromiso de todos*.

La información es una de las armas estratégicas más letales en un nuevo escenario de riesgo para las organizaciones.

gobiernos, naciones u otros organismos, e incluso generar el miedo o terror en una población o Estado.

Este objetivo puede perpetrarse a través del sabotaje de infraestructuras críticas, infiltración en redes de alta seguridad, reclutamiento de personal a través de Internet y/o publicación de contenidos violentos o amenazadores.

INSIDERS

Personal de las propias organizaciones que, aprovechando su conocimiento o acceso a información confidencial en los sistemas, realiza igualmente acciones delictivas (principalmente de fraude) asociadas al cibercrimen.

Las **motivaciones** son diversas y pueden variar desde la perpetuación de un fraude financiero sobre los ingresos de la organización o de sus clientes; la producción de un quebranto económico directo a una compañía, el entorpecimiento de sus operaciones o el sabota-

je/destrucción de infraestructuras críticas; hasta la sustracción de información corporativa estratégica como la relativa a la propiedad industrial o intelectual, datos personales de clientes y empleados, inteligencia de mercado, etc., con objeto de lucro; el daño de la imagen o reputación de una entidad; la reivindicación político-social; e incluso la simple notoriedad o amenaza, entre otras⁶.

Los **objetivos** son muy heterogéneos y los ataques van dirigidos a cualquier tipo de organización —pública o privada, con ánimo de lucro o sin él— afectando a empresas de todos los sectores de actividad, gobiernos y organizaciones de cualquier tipo.

Así las cosas, los recientes eventos de fuga de información y fallos en la seguridad cibernética de algunas organizaciones evidencian un nuevo escenario de riesgo donde la información se convierte en una de las armas estratégicas más letales, comprometiendo la estabili-

	ACTORES	MOTIVACIÓN	OBJETIVOS
	HACKING.	Personal.	Notoriedad, pequeños disturbios, ...
	CIBERCRIMEN.	Ekonomica/lucro.	Robo dinerario o de informaci3n.
	HACKTIVISMO.	Ideol3gica.	Daño reputacional, divulgaci3n de informaci3n, ...
	CIBERESPIONAJE.	Política.	Trastornos graves, robo de informaci3n crítica, ...
	INSIDERS.	Varias.	Varias

Fuente: elaboraci3n propia

6. Deloitte (2015): *12º Programa para el Desarrollo de Directores Financieros*.

dad o continuidad de cualquier persona u organización.

En efecto, algunos ataques cibernéticos recientes han puesto en riesgo naciones e industrias. Un ejemplo fue la operación "Aurora", en 2009, que vulneró los sistemas de seguridad de hasta 34 compañías de EEUU (Google, Yahoo, Symantec y Adobe, entre muchas otras)⁷. O el ciberataque sufrido por Sony en 2014, cuando se filtraron en Internet los datos personales, números de identificación fiscal e información médica de los más de 3.800 trabajadores de la empresa, así como varios contenidos de producciones cinematográficas

aún sin estrenar⁸. Otros ejemplos relevantes fueron las filtraciones de Edward Snowden, cuando se comprometió la información de más de 40 delegaciones de países en suelo estadounidense⁹, o el robo de datos de 83 millones de clientes a la entidad bancaria JP Morgan Chase.

Estos hechos demuestran que los objetivos de los atacantes son cada vez más ambiciosos, se manifiesten sus acciones en el terreno de la ciberdelincuencia o en los entornos del ciberespionaje (estados, empresas, personas) y del ciberterrorismo.

Los principales ataques son los producidos en forma de DDoS, *hacking*, ataques fuera del perímetro, ataques a activos intangibles y los basados en el fraude económico y la fuga de información confidencial.

Principales técnicas de ataque y vulnerabilidades

Nos encontramos con ataques a plataformas propias en forma de DDoS, *hacking* o de explotación de vulnerabilidades en el hardware y software corporativo; ataques fuera del perímetro, como los dirigidos a clientes (*phishing*, *malware*, credenciales robadas); ataques a ac-

tivos intangibles (reputación de la marca o los directivos); a activos físicos o infraestructuras críticas; y ataques basados en el fraude económico y en la fuga de información confidencial (filtraciones, robos o pérdidas de dispositivos).



INGENIERÍA SOCIAL

Técnicas y habilidades sociales o psicológicas para obtener información confidencial a través de la manipulación de las personas o usuarios.

FINGERPRINTING

Búsqueda y recolección de todo tipo de información del objetivo, principalmente en Internet, y realizada de manera pasiva, que pueda ser utilizada en la perpetración de un ataque.

Puede incluir tanto la recolección de información de fuentes públicas (OSINT: Open-Source Intelligence), como de fuentes privadas o de pago.

7. El Economista (2010): *Operación Aurora, el ciberataque más sofisticado de la historia*.

8. CNet (2014): *Sony encabeza la lista de los peores 'hackeos' del año*.

9. Onemagazine (2014): *La ciberseguridad en 2013: un año marcado por Snowden*.

ENUMERACIÓN Y ESCANEEO

Identificación de sistemas, equipos y dispositivos existentes en la red. Obtención de nombres de equipos, usuarios, recursos compartidos, etc.

También incluye habitualmente la identificación de posibles vulnerabilidades.

ATAQUES DE DÍAS CERO (0-DAY)

Ataques contra aplicaciones o sistemas que aprovechan nuevas vulnerabilidades, desconocidas por los fabricantes del producto y/o software, y para los que no se han desarrollado aún “parches” o soluciones que las corrijan.

Estos ataques pueden tener un grave impacto, y el código para explotar dichas vulnerabilidades se vende a menudo por elevadas cantidades de dinero en el denominado mercado negro de los *exploits*.

SPAM Y PHISHING

Ataques a través del servicio de correo electrónico, ya sea buscando la indisponibilidad del mismo o la suplantación de identidad para obtener información confidencial de los usuarios.

Durante los últimos años las técnicas de *phishing* han evolucionado enormemente dada su simplicidad y alta efectividad, y es habitual hablar de ataques concretos de *smishing*, *vis-hing*, *spear phishing*, etc.

HIJACKING

Técnicas ilegales utilizadas por los atacantes para adueñarse o tomar el control de diferentes recursos: navegador, credenciales de sesión, conexiones TCP/IP, páginas web, etc.

DoS (DENEGACIÓN DE SERVICIOS)

Ataques de desbordamiento con el objetivo de provocar la parada o interrupción de un servicio crítico, típicamente realizados a través de una inundación de peticiones a páginas web.

SQL INJECTION

Técnica de ataque sobre páginas web que a través de la ejecución de comandos SQL, permite la obtención y/o manipulación de información de la base de datos del servidor.

CROSS-SITE SCRIPTING (XSS):

Técnicas de inyección de código (principalmente Javascript y PHP) que, aprovechando errores de programación en las páginas web, provocan un comportamiento anormal del sistema pudiendo afectar a la integridad del mismo.

VIRUS, MALWARE, GUSANOS Y TROYANOS

Software o código malicioso que tiene como objetivo infiltrarse o dañar un sistema o equipo, estando además normalmente diseñados para su rápida propagación en una red de ordenadores. Especialmente extendido se encuentra el uso de *troyanos*, cuya apariencia simula la de un programa benigno o inocuo que, tras ser ejecutado por el usuario, ocultan y liberan el virus contenido en él.

BOTNET (REDES ZOMBIS)

Conjunto de ordenadores (conectados a Internet) infectados que se ejecutan y controlan de manera autónoma y automática. Estas redes son usadas principalmente para aumentar la capacidad de procesamiento necesaria para perpetrar un ataque, así como para ocultar el origen y autoría del mismo.

ROOTKITS

Herramientas y programas usados para esconder la presencia del intruso, obteniendo privilegios de administración que permitirán la manipulación futura del sistema.

APT (AMENAZA PERSISTENTE AVANZADA)

Ataques especialmente diseñados y dirigidos contra una organización o entidad concreta. Por lo general requieren de un elevado tiempo de preparación y combinan diferentes técnicas y vulnerabilidades de entre las ya comentadas anteriormente.

El 80% de los ataques podrían prevenirse con buenas prácticas como el uso de contraseñas seguras, configuraciones de seguridad adecuadas, un correcto control de accesos a aplicaciones y datos, y la actualización de sistemas.

Con carácter general, todas estas técnicas o amenazas se basan en la detección y existencia de errores en la configuración de seguridad de los sistemas, obsolescencia o falta de actualización de las infraestructuras tecnológicas, y fallos de programación o diseño en las arquitecturas de seguridad y comunicaciones, cuya identificación y mitigación debe considerarse una prioridad por las entidades y organizaciones.

Por otro lado, a las facilidades derivadas de una mayor superficie de explotación por parte de los atacantes (móviles, *cloud*, redes sociales, etc.) o la existencia de un mercado negro de vulnerabilidades 0-Day, poco ayuda una realidad en la que la mayor parte de los ata-

ques sufridos por las empresas evidencian fallos ocasionados por la ausencia de medidas de seguridad, métodos, procedimientos, productos y herramientas debidamente implementados y certificados.

A este hecho se suma la escasa concienciación y cultura de seguridad dentro de las organizaciones, y la escasez de personal sólidamente formado y especializado dedicado a la ciberseguridad. El 80% de los ataques cibernéticos podrían prevenirse mediante una serie de sencillas buenas prácticas en redes y equipos, que suelen incluir el uso de contraseñas seguras, configuraciones de seguridad adecuadas, correcta gestión del control de acce-

El cibercrimen se ha convertido en un negocio, siendo posible contratar a través de Internet la realización de un ataque DoS, spam, phishing, el alquiler de una botnet o los servicios de un hacker.

tos a aplicaciones y datos, y un apropiado nivel de actualización de los sistemas¹⁰.

De hecho, según estudios recientes publicados por el CCN-CERT (Centro Criptológico Nacional-Centro de Respuesta a Incidentes de

Seguridad), el mayor porcentaje de ataques tienen su origen en vulnerabilidades ya conocidas y para las que se dispone de soluciones y medidas de detección y mitigación.

DE LA SEGURIDAD DE TI A LA CIBERSEGURIDAD: EL CAMBIO DE PARADIGMA

Es importante señalar el incremento en el número de ataques directos a personas (empleados, clientes, simples usuarios de Internet), puesto que representan el eslabón más débil de la cadena de seguridad. La popularización y extendido uso de Internet en casi todos los ámbitos de la sociedad actual (público, profesional, compras, comunicación, noticias, viajes, cultura,...) ha incrementado notablemente la superficie de ataque disponible para los cibercriminales; y debido a su alta efectividad y la falta de medidas de protección adecuadas que en muchas ocasiones presentan los dispositivos (*smartphones, tablets, ordenadores personales*,...) son cada vez más habituales este tipo de ataques, habiendo crecido su impacto de manera exponencial durante los últimos años.

Se puede afirmar incluso que el cibercrimen se ha profesionalizado, contando actualmente los atacantes con elevados conocimientos y recursos, tanto humanos como técnicos y financieros. Se trata, por tanto, de grupos bien organizados y preparados.

Hasta tal punto es así, que también el cibercrimen se ha convertido en un negocio (Cybercrime as a Service), siendo posible actualmente contratar a través de Internet (principalmente en la *Deep-web / Dark-Web*¹¹) la realización de un ataque de DoS, spam, phishing, el alquiler de una botnet o los servicios de un hacker.

Este nuevo entorno de evolución, sofisticación e incremento de los ataques y amenazas está produciendo un cambio relevante en la manera de gestionar la seguridad en las organizaciones.

Tradicionalmente la seguridad de la información ha sido siempre una de las materias mayormente olvidadas, cuya percepción general se aproximaba más a un impedimento o traba en el desarrollo de los negocios y las tecnologías, que a una auténtica necesidad.

Desde un enfoque histórico, la gestión de la seguridad de la información consistía en un enfoque principalmente reactivo: las revisiones de configuración de seguridad de los sis-

10. National Audit Office (2013): *The UK cyber security strategy: Landscape review*

11. Parte oculta de Internet, utilizada por los cibercriminales/delincuentes, no accesible desde los motores de búsqueda tradicionales, y dotada de complejos sistemas de comunicación y reenvío del tráfico y contenidos para ocultar su origen, acceso y mantener el anonimato.





Fuente: elaboración propia

temas y revisión de *logs* o registros de eventos eran ejecutadas casi única y exclusivamente por exigencias de cumplimiento o auditorías, entre otros motivos por la carencia de cultura de seguridad en las organizaciones, así como por la escasez de recursos y personal dedicado a estas tareas.

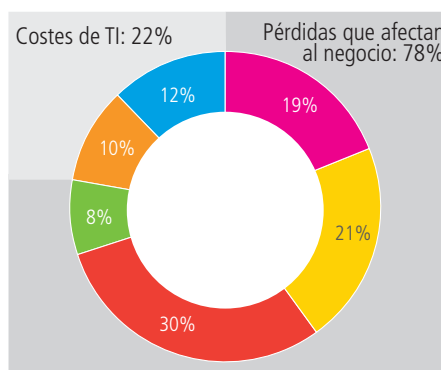
El contexto actual ha hecho necesario evolucionar hacia una gestión proactiva de la seguridad, la identificación anticipada de los riesgos y la gestión continua de las amenazas que pueblan el ciberespacio. En otras palabras, es necesario evolucionar de la actual cultura reactiva a una de prevención y resiliencia.

Por otra parte, las funciones de seguridad de la información, prevención de fraude y continuidad de negocio, están pasando a un primer plano corporativo porque se imbrican en el conjunto de responsabilidades de la alta dirección de las organizaciones. Especialmente en empresas cotizadas, que han de ser ejemplares de cara a sus accionistas en el buen gobierno de sus sociedades y en el cumplimiento legal, por lo que deberían invertir adecuadamente en la gestión de riesgos de ciberseguridad como uno de los elementos clave

de sus planes de transformación a la economía digital.

Un ciberataque dirigido a una organización afecta a todas sus áreas, pero se traduce sobre todo en pérdidas que afectan al negocio¹²:

- Pérdida de ingresos (19%).
- Pérdida de productividad (21%).
- Deterioro marca/ reputación y pérdida de la confianza de clientes/accionistas (30%).
- Cumplimiento y sanciones legales (8%).



De hecho, apenas una cuarta parte del impacto de ciberataque son costes TI:

- Costes técnicos de remediación (10%).
- Costes de investigación (12%).

12. IBM (2014): Global Study on the Economic Impact of IT Risk

La ciberseguridad no debe circunscribirse a los departamentos de TI, sino que la Alta Dirección ha de implicarse en su gestión eficiente con un compromiso activo continuo.

De la rapidez y extensión del impacto que tienen las nuevas amenazas en toda la organización se concluye que la ciberseguridad no es una cuestión cuya responsabilidad deba circunscribirse a los departamentos de TI, sino que la Alta Dirección de la empresa ha de estar implicada en su gestión eficiente con un compromiso activo continuo.

Por tanto la seguridad corporativa ya no se identifica únicamente con la seguridad preventiva, ni es responsabilidad exclusiva de un departamento, ni se separa en un escenario interior o exterior o con un enfoque reactivo o preventivo.

De este modo surgen en el seno de las empresas nuevas actividades y tareas relacionadas entre las que cabe destacar:

- **Análisis de la exposición a los ciberriesgos** por parte de las entidades, identificación y clasificación de información crítica existente en una organización y establecimiento de una estrategia de seguridad.
- **Concienciación:** Cualquier persona o área de una entidad puede ser víctima de un ciberataque, por lo que resulta necesario establecer una cultura de seguridad en las organizaciones con el objetivo de cambiar la manera en que la seguridad es percibida por las personas, adoptando entre otras algunas de estas medidas:
 - Divulgación de políticas y manuales de seguridad.
 - Difusión de incidentes y ataques de seguridad, explicando sus causas y orígenes.
 - Establecimiento de cursos y actividades formativas en materia de prevención y

detección de los riesgos de ciberseguridad.

- **Medidas organizativas**, como la difusión de políticas de seguridad en las organizaciones o la concienciación a los usuarios de los riesgos en el uso de las tecnologías de la información.
- **Medidas técnicas** que pueden incluir desde la existencia de herramientas para la gestión centralizada de alertas y eventos de seguridad en los sistemas a técnicas que permitan detectar y prevenir fugas de información confidencial; contratación de servicios de *hacking* ético y auditorías forenses de seguridad; búsqueda de información en Internet, prensa o redes sociales; suscripción a servicios de alertas, incidentes y vulnerabilidades de seguridad; e incluso la contratación de pólizas de los denominados ciberseguros que cubran la pérdidas ocasionadas por un ciberataque, y la participación en ciberejercicios que permitan evaluar las capacidades de organización y resiliencia ante el cibercrimen.

Servicios y sistemas de seguridad

En los últimos años han surgido diferentes servicios avanzados de seguridad para el control y gestión de estos riesgos que cada vez más organizaciones están adaptando e implantando en su operativa diaria, y entre los que cabe destacar:

- **SOC (Security Operations Center).** La existencia de un Centro de Operaciones de Seguridad (24x7) con personal especialista dedicado en exclusiva a la prevención y detección de ciberataques.



- **SIEM (System Information Event Management).** La existencia de herramientas que permitan la correlación e identificación de eventos de seguridad en los diferentes sistemas y dispositivos, así como una gestión centralizada de dichas alertas.
- **DLP (Data Loss Prevention).** La existencia de procedimientos, medidas y herramientas para la prevención y detección de pérdidas, robos y fugas de información confidencial.
- **Antimalware.** Herramientas de detección y prevención de *malware* y otras amenazas avanzadas. Estos sistemas, utilizan técnicas heurísticas y de detección por comportamiento algo más avanzadas que los clásicos anti-virus, normalmente basados en firmas.
- **Hacking ético y pen-testing.** La necesidad de contar con servicios y pruebas periódicas de *hacking* e intrusión en los sistemas, realizados bien sea a través de recursos internos o subcontratados con terceros.
- **Auditorías forenses de seguridad.** Servicios basados en diferentes procesos de investigación, rastreo y recopilación de información con el objetivo de establecer el origen, motivo e incluso autoría de un ciberataque, así como la recolección de evidencias digitales que puedan servir incluso como prueba en posibles litigios o procesos judiciales.
- **Ciberinteligencia.** Observatorio de Internet y servicios de vigilancia digital que incluyan entre otros el seguimiento y análisis de información publicada en redes sociales, foros, portales técnicos, medios de comunicación, etc., como medida de prevención de posibles ataques, identificación de fugas de

información, etc. Incluye la coordinación e intercambio de información con organismos públicos (por ejemplo, Fuerzas de Seguridad del Estado) y otras organizaciones de referencia.

Para llevar a cabo estas actividades, resulta fundamental contar con los recursos y el personal capacitado para realizarlas, adaptándonos por supuesto a las necesidades, nivel de exposición y tamaño de cada entidad. Por este motivo, el personal con conocimientos y habilidades en materia de ciberseguridad es a día de hoy un perfil muy demandado y valorado en el mercado de trabajo actual.

Por otro lado, en el actual contexto globalizado donde empresas y organizaciones de cualquier país y sector son posibles objetivos de los ciberdelincuentes, para combatir estas amenazas resulta casi imprescindible la colaboración, coordinación e intercambio de información entre entidades, gobiernos, instituciones públicas y gubernamentales, y fabricantes y proveedores de software y hardware.

El alcance actual de la ciberseguridad y los riesgos que conlleva excede con creces el ámbito de las infraestructuras y tecnologías de la comunicación, e incluye también la protección de personas.

Debido a ello, su tratamiento requiere de un enfoque transversal e integral en las organizaciones. Cualquier persona o área de una organización puede ser víctima de un ciberataque, por lo que es necesario contar con todas ellas, puesto que la ciberseguridad excede el ámbito, funciones y responsabilidades del personal y áreas de seguridad y tecnología, y nos afecta a todos y cada uno de nosotros.

El tratamiento de la ciberseguridad requiere de un enfoque transversal e integral, ya que ésta excede el ámbito, funciones y responsabilidad del personal y áreas de seguridad y tecnología.

Las organizaciones deben implantar una estrategia de seguridad acorde a su exposición a los riesgos y a las necesidades, posibilidades y recursos.

Actualmente, resulta cada vez más común escuchar en las entidades y medios de comunicación términos como ciberinteligencia, resiliencia o seguridad operacional, que representan perfectamente este cambio de paradigma, y ahondan en la idea del establecimiento de una estrategia global del ciclo de vida de la seguridad y la gestión de incidentes, así como en las capacidades de las organizaciones de defenderse, resistir e incluso responder a un ciberataque.

Para ello, las entidades están adoptando modelos para la gestión de los ciberriesgos, basados en algunos de los estándares y buenas prácticas del mercado, propuestos por las principales organizaciones de referencia (ISO, CobiT, ISACA, ITIL).

La siguiente figura muestra las principales funciones asociadas a la gestión de la ciberseguridad según el modelo de control propuesto por el Instituto Nacional de Estándares y Tecnología Norteamericano (NIST¹³).



Fuente: NIST (National Institute of Standards and Technology) (Feb. 2014): *Framework for Improving Critical Infrastructure Cybersecurity*

Si bien la seguridad no existe al cien por cien (siempre estaremos expuestos en mayor o menor medida), sí es posible hacer nuestras organizaciones más seguras. Para ello, la anticipación es clave. Hay que ir por delante de los ataques siendo capaces de detectarlos y prevenirlos.

Además, se puede limitar de forma significativa el daño si se reacciona de forma rápida y decidida ante cualquier intento de comprometer nuestro entorno. Todo esto requiere continuidad y constancia en la vigilancia pero,

sobre todo, es necesario un cambio de mentalidad.

En este sentido, las organizaciones deben realizar un análisis detallado de la exposición a estos riesgos, e implantar una estrategia de seguridad acorde a la misma, así como a las necesidades, posibilidades y recursos de cada organización, construyendo un modelo de gestión de la seguridad donde, además de las áreas clásicas de la seguridad IT, tengan reflejo capacidades más avanzadas asociadas con los conceptos de ciberseguridad y ciberresiliencia¹⁴.

13. NIST: del inglés "National Institute of Standards and Technology".

14. Deloitte (2015): *Modelo Colaborativo de CiberSeguridad (MCCS)*.

A nivel agregado, el conjunto de medidas y principales actividades para el control y gestión de los ciberriesgos, podría resumirse en:

- **Gobierno** y organización en la entidad para gestionar los riesgos, con una clara asignación de roles y responsabilidades en toda la organización, implantando estructuras de gobierno –procedimientos, políticas de seguridad, estándares, cumplimiento legal, formación y concienciación de directivos y empleados, gestión de proveedores– que permitan mantener y evolucionar sus capacidades de ciberseguridad.
- **Detección** de las amenazas mediante el uso de las múltiples fuentes de ciberinteligencia con el fin de poder gestionarlas proactivamente, análisis de redes y sistemas, análisis del comportamiento de los usuarios, monitorización de eventos de seguridad, etc.

- **Prevención** frente a ciberataques manteniendo y mejorando las herramientas y medidas de seguridad física, de sistemas, redes, y aplicaciones para la protección de sus infraestructuras y sus activos de información.
- **Respuesta** ante incidentes de seguridad y **recuperación** adecuadas, con el fin de poder limitar su impacto sobre la organización y mantener la continuidad del negocio.

Este marco estratégico para la gestión de la seguridad, permitirá a las organizaciones comprender el panorama de las ciberamenazas y los riesgos subyacentes; proteger los datos y activos contra las amenazas cibernéticas; detectar estas a tiempo; y finalmente, responder a los ciberataques y estar mejor preparadas para reaccionar frente a lo inesperado.

La sucesiva realización de ciberejercicios permite a las organizaciones mejorar su desempeño en el ámbito de la ciberseguridad.

CIBEREJERCICIOS Y CIBERSEGUROS

De la misma forma que en el mundo de la continuidad de negocio y la gestión de crisis el modelo de gestión evoluciona principalmente por la realización de sucesivos escenarios de prueba, dentro de la ciberseguridad la sucesiva realización de ciberejercicios permiten a las organizaciones mejorar su desempeño dentro de este ámbito.

Ciberejercicios

Tal y como se recoge en el documento *Taxonomía de Ciberejercicios* desarrollado por el INCIBE (Instituto Nacional de Ciberseguridad), se puede definir el concepto de ciberejercicio como: “...una herramienta que per-

mite evaluar el estado de preparación de los participantes frente a crisis de origen cibernético, facilitando además lecciones aprendidas y recomendaciones para el futuro...”

Con carácter general, y aunque la naturaleza de estos ejercicios es variada, pueden cumplir con los siguientes objetivos:

- Evaluar las medidas de seguridad perimetral, monitorización de seguridad y protección de sistemas y activos de información, mediante ejercicios de *hacking* ético o *pentesting* que simulan y utilizan las técnicas y modos de actuación de los atacantes.
- Evaluar las capacidades de tratamiento y recuperación de las entidades ante un ci-

Los resultados de los ciberejercicios permiten identificar debilidades y ausencias de control en los sistemas y mecanismos de control y seguridad de la información, permitiendo establecer planes y acciones para su resolución y mejora.

berataque, tanto de las medidas organizativas y de gestión (ejercicios *role-play*: toma de decisiones), como desde un punto de vista técnico (capacidades de detección, análisis de la infección e informática forense, contingencia de los sistemas,...).

- Evaluar el nivel de concienciación, formación y cultura de seguridad de los empleados de la organización, típicamente realizado a través de la realización de simulacros (falsas campañas de *phishing*, colocación de dispositivos con información confidencial,...).

Los resultados de estos ejercicios son de gran valor para las entidades, puesto que permiten identificar debilidades y ausencias de control en los sistemas y mecanismos de control y seguridad de la información, permitiendo establecer planes y acciones para su resolución y mejora.

Estas actividades de prueba dentro de la ciberseguridad han sido promovidas y desarrolladas, tradicionalmente, por los ámbitos militares y gubernamentales.

Generalmente las pruebas cuentan con la participación de las fuerzas de seguridad locales, aunque recientemente, y cada vez más, la complejidad de las infraestructuras tecnológicas y la protección de las infraestructuras críticas implican la participación de diferentes organizaciones empresariales de diversos sectores.

Inicialmente, los principales ciberejercicios provenían de organismos gubernamentales de defensa como la OTAN. Dentro de este tipo de iniciativas podríamos encuadrar el *Locked Shields* y la *Cyber Coalition*, que se desarrollan principalmente a nivel europeo aun-

que con la participación de organismos de defensa estadounidenses. La realización de este tipo de ejercicios suele implicar la participación de numerosos organismos gubernamentales incluyendo tanto al ejército como a las fuerzas del orden y seguridad del Estado.

La implicación de múltiples organismos en la preparación de estos ciberejercicios representa un gran dilema a la hora de desarrollar una estrategia continua de pruebas. El alto coste de preparación y coordinación de actividades que exigen estos ejercicios representa un escollo importante a la hora de formalizar un proceso continuo de prueba. Además, suele ser complicado obtener un reaprovechamiento de las actividades desarrolladas anteriormente debido al alto grado de volatilidad y caducidad de las ciberamenazas. Es decir, el escenario preparado un año para la realización del ciberejercicio puede encontrarse obsoleto para el ejercicio del año siguiente, lo que requiere volver a desarrollar y planificar un nuevo escenario de prueba cada ejercicio.

La elevada complejidad de las pruebas, unida al reducido beneficio que estas actividades pueden llegar a proporcionar (teniendo en consideración la constante aparición de nuevas ciberamenazas) han hecho surgir el término *CyberRange*, conocido como "Campo de Maniobras". Este tipo de iniciativas representan una infraestructura tecnológica de virtualización con la suficiente versatilidad como para poder componer multitud de escenarios y situaciones de manera rápida y automatizada. De esta forma, con un esfuerzo menor y de forma ágil se pueden recrear campos de entrenamiento continuo para el personal implicado en la ciberseguridad. Este concepto, con un elevado coste y una alta complejidad de diseño, representa actualmente una ten-

dencia muy interesante para los organismos de defensa de cara a reducir la carga de trabajo que puede representar la preparación y realización de ciberejercicios.

Sin embargo, actualmente la realización y participación de las entidades en ciberejercicios se encuentra ampliamente extendida y ha evolucionado hacia un enfoque menos complejo y más práctico (pequeños simulacros y ejercicios concretos) para las entidades, hasta ser considerada una buena práctica casi imprescindible en ciberseguridad para las organizaciones.

En el ámbito nacional los ejercicios organizados por el INCIBE y el CNPIC (Cyber-Ex), contaron en 2014 con la participación de quince grandes empresas españolas de sectores del transporte, finanzas, energía, servicios, inversiones y seguros; como por ejemplo Banco Santander, Repsol, Mapfre, Metro Madrid, Acciona S.A., y El Corte Inglés, entre otras.

En el año 2015 aumentó el número de entidades participantes, habiéndose realizado ejercicios específicos adaptados a la naturaleza de la actividad de las entidades (diferentes ejercicios por sector), así como la realización del primer Cyber-Ex Internacional, incluido en el marco de los Estados Miembros de la Organización de los Estados Americanos (OEA), con el objetivo de fortalecer las capacidades de respuesta ante incidentes cibernéticos, así como una mejora de la colaboración y cooperación ante este tipo de incidentes.

Otros ejemplos de ciberejercicios relevantes son los promovidos por FS-ISAC¹⁵ y Payments Council (iniciados en 2010 para entidades de Estados Unidos y Canadá, y que por primera

vez en 2015 contó con la participación de instituciones europeas) o los más recientes Proteus (Brasil), CBEST Cyber Exercise (Inglaterra) y Ciber Perseu (Portugal).

Ciberseguros

Otra de las tendencias recientes en el ámbito de la ciberseguridad es la proliferación de los denominados ciberseguros o pólizas para la cobertura de los riesgos relacionados con la ciberseguridad, siendo considerada una de las principales estrategias para la mitigación de riesgos (transferencia del mismo a un tercero).

Las compañías aseguradoras han diseñado productos específicos dentro de este ámbito con coberturas que oscilan desde la protección de las propias infraestructuras a la cobertura de los riesgos, en caso de la declaración de una ciberguerra.

En este tipo de pólizas el tomador de las mismas debe cumplimentar un cuestionario, e incluso el tomador puede verse sometido a un proceso de evaluación en ciberseguridad por parte de un externo contratado por la compañía aseguradora, de cara a establecer el importe de la prima, que dependerá en parte de las medidas de seguridad que el tomador ha implantado en su compañía, así como de las coberturas y franquicias establecidas.

Es importante mencionar que, con carácter general, este tipo de pólizas no suele cubrir las pérdidas económicas directas (robo dinerario) ocasionadas por un cibertaque (las compañías suelen disponer de otro tipo de pólizas y provisiones para cubrir los eventos de fraude tanto interno como externo), sino

La contratación de ciberseguros es tendencia, con coberturas que van desde la protección de las propias infraestructuras a la cobertura de los riesgos en caso de la declaración de una ciberguerra.

15. Financial Services—Information Sharing and Analysis Center. <https://www.fsisac.com/>

Los ciberseguros no suelen cubrir las pérdidas económicas directas de un ciberataque, sino que cubren aquellas relacionadas con fallos en los sistemas, notificación a clientes, investigación forense o impactos reputacionales, entre otras.

que están enfocadas a cubrir las pérdidas y gastos relacionados con fallos en los sistemas, notificación y atención a clientes, investigación forense, extorsión, gastos de consultorías y asesoramiento legal, impactos reputacionales o responsabilidades derivadas de robos de información y publicación de contenidos en medios digitales.

Valga como ejemplo el caso de la cadena de supermercados norteamericana Target, que disponía de un ciberseguro. A finales de 2013 sufrió un cibertaque por el que le fueron sustraídos los números de tarjetas de crédito y débito de 40 millones de clientes, así como los datos personales de 70 millones de personas. El coste del ataque para la compañía fue

de 61 millones de dólares, de los cuales su seguro cubrió 44 millones.

Un reciente estudio de Wells Fargo sobre 100 empresas medianas y grandes de Estados Unidos desveló que el 85% de ellas tenían un ciberseguro. De éstas, el 44% habían sufrido incidentes que fueron cubiertos por su aseguradora.

Según la correduría de seguros Marsh, el mercado de los ciberseguros generó en Estados Unidos 1.000 millones de dólares en 2013, cantidad que se dobló en 2014 y cuya demanda sigue aumentando significativamente en la actualidad. El mercado europeo de ciberseguros es aún pequeño comparado con Estados Unidos, pero crece a buen ritmo.

METODOLOGÍAS Y ESTRATEGIAS DE CONTROL Y GESTIÓN DE CIBER-RIESGOS

En la actualidad existe un buen número de **marcos de control y buenas prácticas** sobre ciberseguridad que pueden ser de gran utilidad para que las organizaciones afronten este reto. Hacer uso de ellos facilitará la comprensión de los riesgos y amenazas existentes y facilitará la implantación de las medidas adecuadas a la realidad de la compañía.

A continuación se muestran algunos de los ejemplos más significativos, incluyendo algunas de las entidades/organismos de referencia en el ámbito de la ciberseguridad, tanto a nivel nacional como internacional.

No hay que olvidar que el sector se encuentra en constante evolución, pudiendo surgir nuevas referencias. Es importante mantenerse activo en la búsqueda de soluciones y nuevas

prácticas si queremos luchar con éxito contra los riesgos asociados a la ciberseguridad.

NIST 02-2014

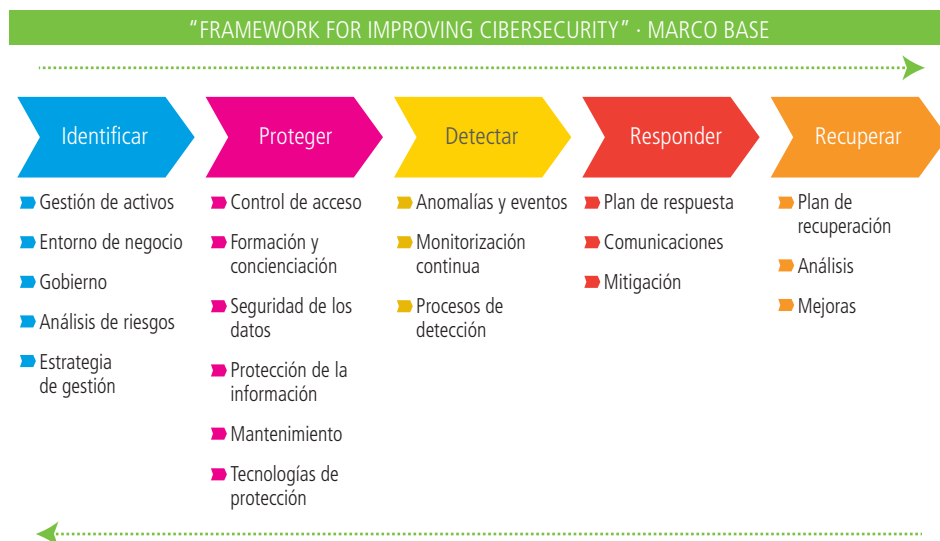
El National Institute of Standards and Technology (NIST) proporciona interesantes referencias y buenas prácticas a través de metodologías y normas, cuyo objetivo no es otro que el de promover la innovación y competitividad industrial.

Dentro de su gran producción de marcos de referencia, cabe destacar por su utilidad en el tema que estamos tratando el correspondiente a ciberseguridad: **"Framework for Improving Cybersecurity"**. Este documento, de carácter público y disponible a través de su página web, muestra un enfoque basado en



riesgos para la gestión de la ciberseguridad y se compone de tres apartados:

- Marco base: Conjunto de actividades para la correcta gestión de la ciberseguridad. Se divide en 5 funciones: identificar, proteger, detectar, responder y recuperar que, a su vez, se dividen en 20 categorías.
- Niveles de implantación del marco y procesos para gestión del riesgo.
- Perfiles del marco: Resultados en base a las necesidades del negocio.



Fuente: National Institute of Standards and Technology (NIST)

ISO / IEC 27032

La organización internacional de normalización no podía ser menos a la hora de ofrecer un estándar internacional con directrices de ciberseguridad.

El alcance de las directrices incluidas en la norma **"Cybersecurity Guideline"** engloba los ámbitos de seguridad de la información, seguridad de la red, seguridad en Internet y en las infraestructuras críticas, así como buenas prácticas en el intercambio de información, manejo de incidentes y colaboración entre las partes interesadas. La norma establece una visión general de ciberseguridad, explicación de la relación entre la misma y otros ti-

pos de seguridad, definición de grupos de interés y sus roles, y guía para hacer frente a los problemas de ciberseguridad.

Es importante tener presente que las buenas prácticas en seguridad de la información, seguridad física, etc., son también aplicables a la ciberseguridad, por lo que se deben tener también presentes otras normas como la ISO 27014 "Gobierno de la seguridad de la información", o el conjunto ISO 27000, entre las que destacan entre otras:

- ISO 27001 "Estándar para la seguridad de la información".
- ISO 27002 "Código de buenas prácticas para la gestión de seguridad de la información".

Normas como la ISO 27032, la ISO 27014 o el conjunto ISO 27000 son importantes para asegurarse buenas prácticas en materia de ciberseguridad.

Según el Instituto SANS, hay 20 controles críticos o acciones clave que las organizaciones deberían implementar para prevenir, detectar y mitigar los ciberataques.

- ISO 27003 "Directrices para la implantación de un SGSI¹⁶".
- ISO 27004 "Métricas para la gestión de la seguridad de la información".
- ISO 27005 "Gestión de riesgos en seguridad de la información".

SANS y CIS

SysAdmin Audit, Networking and Security Institute (SANS) es una conocida organización norteamericana de investigación y educación cooperativa que ofrece recursos y noticias sobre seguridad. Entre sus artículos se puede encontrar mucha información relevante en materia de ciberseguridad. Dentro de sus recursos, se encuentra "Securing The Human", que ofrece herramientas de concienciación gratuitas.

En el año 2008, con el objetivo de minimizar los robos de información sufridos principalmente por organizaciones del ámbito de defensa estadounidense, se inició el proyecto para la elaboración de una guía de buenas prácticas en seguridad de la información: "Critical Security Controls for Effective Cyber Defense", que fue transferido en 2015 al Center for Internet Security (CIS) de Estados Unidos.

Se trata de 20 controles críticos o acciones clave que las organizaciones deberían implementar para prevenir, detectar y mitigar los ciberataques. A la fecha de publicación de este documento, la última versión (6.1) data de agosto de 2016 y será objeto de un mayor análisis en posteriores capítulos del presente documento.

CESG UK GOV

Communications - Electronics Security Group (CESG)) representa la autoridad nacional en el Reino Unido en materia de seguridad de la información.

Entre sus muchas publicaciones destaca "Ten Steps To Cyber Security", una guía sobre cómo las organizaciones pueden protegerse en el ciberespacio en 10 pasos. Inicialmente publicada en septiembre de 2012, a la fecha de publicación de este documento la última versión data de enero de 2015, e incluye como sus 10 principales prioridades la gestión de los siguientes aspectos:

- Modelo de información de los riesgos de ciberseguridad.
- Configuración segura.
- Seguridad de la red.
- Gestión de usuarios privilegiados.
- Formación y concienciación de usuarios.
- Gestión de incidentes.
- Protección ante el *malware*.
- Monitorización de seguridad.
- Control de dispositivos removibles.
- Política de trabajo a distancia (móvil y en el hogar).

ISACA

Information Systems Audit and Control Association (ISACA) se involucra en el desarrollo de buenas prácticas en auditoría y control en sistemas de la información. Dentro de la infinidad de documentación que proporciona a los profesionales cabe destacar la guía para la aplicación del marco NIST (mencionado ante-

16. Sistema de Gestión de Seguridad de la Información.



riormente) para la ciberseguridad: **“Implementing the NIST Cybersecurity Framework”**, desarrollada dentro de su programa CSX (Cybersecurity Nexus), creado en 2015 tras la aprobación de la ley de ciberseguridad estadounidense (Cibersecurity Information Sharing Act of 2015), con el objetivo de proporcionar a los profesionales de seguridad los conocimientos y herramientas necesarios para la realización de su trabajo.

Adicionalmente, y dentro la última revisión de CobiT (Control objectives for Information and related Technology), cuyas guías representan uno de los principales estándares de buenas prácticas para el control y supervisión de tecnología de la información a nivel mundial, ISACA lanzó en junio del 2012 **“COBIT 5 para la seguridad de la información”**, actualizando la última versión de su marco para proporcionar una guía práctica de seguridad de la empresa en todos sus niveles prácticos, y ayudar a las empresas a reducir sus perfiles de riesgo a través de una adecuada administración de la seguridad.

INCIBE

El Instituto Nacional de Ciberseguridad (INCIBE), fundando en España en 2006 bajo el nombre de INTECO (Instituto Nacional de Tecnologías de la Comunicación) y dependiente del Ministerio de Industria, pone a disposición de su público —que abarca desde ciudadanos individuales a grandes empresas— una elevada cantidad de recursos e información relacionada con la ciberseguridad.

Entre muchas otras utilidades, en su página web se puede encontrar un apartado específico denominado **“Protege tu empresa”**, y que incluye por ejemplo las siguientes guías:

- **“Cómo gestionar una fuga de información”**.

- **“Gestión de riesgos”**.
- **“Ciberseguridad en comercio electrónico”**.

Adicionalmente, el Instituto pone a disposición de los usuarios de todo un catálogo de empresas proveedoras de soluciones de ciberseguridad, así como un servicio gratuito para conocer si un equipo está infectado.

En materia de formación y concienciación cabe destacar la actividad de la Oficina de Seguridad del Internauta (www.osi.es), cuyo objetivo es ayudar a los usuarios de Internet a la adopción de buenos hábitos en seguridad, sensibilizando a la comunidad de los riesgos existentes, y contribuyendo a reducir el volumen y gravedad de incidentes de seguridad sufridos por los usuarios.

Otras de las iniciativas lideradas por el INCIBE son CyberCamp y CyberEx, también mencionadas en este documento.

ENISA

La European Union Agency for Network and Information Security (ENISA) ofrece en su página web intercambio de información, buenas prácticas y conocimiento en el campo de la ciberseguridad.

Un reglamento publicado en junio de 2013 encomendaba a ENISA el ámbito de actuación y la autoridad necesarios que les permite la lucha contra el cibercrimen:

- Desarrollo de políticas y legislación de la Unión Europea en materia de ciberseguridad.
- Investigación, desarrollo y estandarización de normativa.
- Prevención, detección y respuesta a ciberamenazas fronterizas.

El español INCIBE pone a disposición de ciudadanos y empresas una elevada cantidad de recursos e información relacionada con la ciberseguridad.

La Estrategia de Ciberseguridad Nacional recoge los puntos fundamentales para la definición de la estrategia española en materia de ciberseguridad.

Aunque sus recomendaciones están enfocadas a estrategias nacionales de ciberseguridad, su lectura puede ayudar a extraer buenas

prácticas aplicables a la realidad de las organizaciones.

REGULACIÓN Y NORMATIVA

Sector Público

El documento más importante en materia de ciberseguridad en el ámbito regulatorio nacional fue el publicado en el año 2013 desde la Presidencia del Gobierno con el título *Estrategia de Ciberseguridad Nacional*. Este documento, conforma el eje central estratégico y recoge los principios fundamentales para la definición de la estrategia española en materia de ciberseguridad.

El documento se encuentra estructurado en los siguientes capítulos:

- **El ciberespacio y su seguridad.** Este capítulo recoge las características del ciberespacio, así como sus principales oportunidades y amenazas.
- **Propósito y principios rectores de la ciberseguridad en España.** Establece una definición de las directrices generales del uso seguro del ciberespacio.

- **Objetivos de la ciberseguridad.** En este apartado se establece el objetivo global de lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones.
- **Líneas de acción de la ciberseguridad nacional.** Define una serie de líneas maestras para alcanzar los objetivos expuestos en el capítulo anterior.
- **La ciberseguridad en el Sistema de Seguridad Nacional.** Define la estructura orgánica al servicio de la ciberseguridad.

En el ámbito del sector público, se puede producir una nueva diferenciación respecto al ámbito de aplicación de esta estrategia nacional. Por un lado, se puede diferenciar el ámbito específico de defensa (militar) y por otro, se puede identificar el ámbito de las administraciones públicas. Aunque la estrategia en materia de ciberseguridad es la misma para estos ámbitos, la aproximación empleada para su desarrollo es diferente.

EN EL ÁMBITO DE LAS ADMINISTRACIONES PÚBLICAS, la principal normativa empleada para la gestión de la ciberseguridad lo conforman las normas internacionales ISO (principalmente ISO27002 e ISO18044).

Estas normas internacionales recogen, por un lado, un conjunto de controles para la gestión de la seguridad de la información (ISO27002)



y, por otro lado, la norma ISO18044 define las medidas de seguridad aplicables para el tratamiento y respuesta a incidentes tecnológicos.

EN EL ÁMBITO DE DEFENSA, como ya se ha mencionado anteriormente, se toma como principal guía el documento *Estrategia de Ciberseguridad Nacional*. Sin embargo, se manejan y toman como documentación adicional los documentos de *benchmarking* elaborados por el CIS (Center for Internet Security) y las guías DISA STIGs (Defense Information Systems Agency - Security Technical Implementation Guides) elaboradas por organismos estadounidenses, que definen medidas de seguridad específicas para diferentes entornos y plataformas. Estas guías definen gran cantidad de medidas de seguridad, algunas de ellas bastante costosas de implementar, pero son una pieza fundamental y muy completa a la hora de bastionar distintas plataformas.

A nivel nacional también se cuenta con un conjunto de guías de la serie STIC (Seguridad de las Tecnologías de la Información y las Comunicaciones). En concreto, cabe destacar la serie 800 relacionada con el ENS (Esquema Nacional de Seguridad). Esta Serie CCN-STIC-800 establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el Esquema Nacional de Seguridad (RD 3/2010).

Adicionalmente, tal y como se ha indicado, dentro del ámbito de las administraciones públicas se pueden destacar las normativas elaboradas por el CCN-CNI (Centro Criptológico Nacional) a través de las series de guías STIC. Estas guías cuentan, en algunas ocasiones, con herramientas propias de desarrollo como son CARMEN (Centro de Análisis de Registros y Minería de Datos), LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) o CLARA (que permite verificar el cumplimiento

desde un punto de vista técnico de los requisitos del ENS en entornos Windows 7 y Windows server 2008 R2.). Estos documentos y herramientas son también empleados dentro del ámbito de defensa para la implantación de medidas de ciberseguridad.

Finalmente, y aunque su ámbito de actuación excede el de la seguridad de las comunicaciones telemáticas y el ciberespacio, abarcando el terreno de la seguridad física y la lucha contra el terrorismo, es relevante mencionar la creación del Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC) –dependiente del Ministerio del Interior– encargado de impulsar, coordinar y supervisar todas las actividades y mecanismos necesarios para garantizar la seguridad de la infraestructuras que proporcionan servicios esenciales a nuestra sociedad, fomentando la participación de todos y cada uno de los agentes del sistema en sus correspondientes ámbitos, con el objetivo de crear un modelo de seguridad basado en la confianza mutua, y creando una asociación público-privada que permita minimizar las vulnerabilidades de las infraestructuras críticas ubicadas en el territorio nacional.

El primer **Plan Nacional de Protección de las Infraestructuras Críticas**, aprobado en mayo de 2007, reconoce que el riesgo de ataques terroristas catastróficos contra infraestructuras críticas está viviendo un aumento, y por ello se ha creado un catálogo de instalaciones sensibles a estos atentados.

Este plan establece que las infraestructuras críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funciona-

La serie de guías de la serie STIC establece las políticas y procedimientos adecuados para la implantación de las medidas contempladas en el Esquema Nacional de Seguridad.

INFRAESTRUCTURAS
CRÍTICAS

PLAN NACIONAL DE PROTECCIÓN

Factores

- Rango
- Escala
- Efectos en el tiempo

Parámetros

- Daños causados
- Impacto económico
- Impacto en servicios esenciales

Áreas estratégicas

- Energía
- Industria Nuclear
- TI
- Transportes
- Suministro de Agua
- Suministro de Alimentos
- Salud
- Sistema Financiero
- Industria Química
- Espacio
- Administración

miento de los gobiernos de los Estados miembros.

Entre estas instalaciones sensibles destacan las centrales y redes de energía, las comunicaciones, las finanzas, el sector sanitario, la alimentación, el agua —embalses, almacenamiento, tratamiento y redes—, los transportes —aeropuertos, puertos, etc.—, monumentos nacionales, así como la producción, almacenamiento y transporte de mercancías peligrosas, como material químico, biológico o nuclear.

El criterio para incluir a dichas instalaciones en el catálogo es una mezcla de diversos factores: rango, escala y efectos en el tiempo; y de parámetros: daños causados, impacto económico e impacto en servicios esenciales; y comprende actualmente más de 3.500 instalaciones e infraestructuras sensibles dentro de las siguientes áreas estratégicas: Energía, Industria Nuclear, Tecnologías de la Información, Transportes, Suministro de Agua, Suministro de Alimentos, Salud, Sistema Financiero, Industria Química, Espacio y Administración.

EN EL ÁMBITO INTERNACIONAL caben destacar otras iniciativas como *La Estrategia de Ciberseguridad de la Unión Europea* (publicada en 2013), o la *Directiva de Seguridad de la Redes y la Información* (NIS), que establece medidas de control y mecanismos de cooperación concretos entre los estados miembros, como la red de equipos de respuesta a incidentes de seguridad (CSIRT) y el grupo de cooperación, compuesto por miembros de autoridades nacionales competentes, la Comisión de la Unión Europea y la ENISA. La Directiva también obliga a diseñar una estrategia de ciberseguridad nacional, y la obligación para empresas que trabajan en sectores críticos tales como energía, transporte y fi-

nanzas, entre otros, a informar a las autoridades nacionales acerca de incidentes de impacto significativo.

Se ha establecido que las 5 estrategias prioritarias a desarrollar son:

- La resiliencia contra ciberataques.
- La reducción drástica de la delincuencia en la red.
- El desarrollo de una política de ciberdefensa y de las capacidades correspondientes en el ámbito de la Política Común de Seguridad y Defensa (PCSD).
- El desarrollo de los recursos industriales y tecnológicos necesarios en materia de ciberseguridad.
- El establecimiento de una política internacional coherente del ciberespacio en la Unión Europea y la promoción de los valores europeos esenciales.

Así pues, son numerosas las iniciativas a nivel internacional que diferentes organismos, reguladores y gobiernos están promoviendo en el ámbito de la ciberseguridad y protección de las infraestructuras críticas, entre las que cabe destacar la aprobación y promulgación de diversas leyes en diferentes países:

- **Cybersecurity Enhancement Act of 2014** (Estados Unidos). Proporciona una asociación permanente público-privada para mejorar y fortalecer la investigación y el desarrollo del personal, educación, preparación y conciencia en materia de ciberseguridad.
- **Cybersecurity Act of 2015** (Estados Unidos). Creada con el objetivo de promover y alentar al sector privado y gobierno de Estados Unidos para intercambiar con rapidez y de manera responsables información sobre las amenazas cibernéticas.

- **IT Security Act** (Alemania). En respuesta, y tras la alarma del ciberataque al parlamento alemán (Bundestag) conocido en junio de 2015, Alemania aprobó una ley de seguridad informática destinada a reforzar los dispositivos de protección a las empresas, debiendo además informar de inmediato acerca de cualquier incidente, anomalía o sospecha de virus.

Sector Privado

Dentro de las compañías de sector privado se debe desarrollar un cuerpo normativo de seguridad que cubra todos los riesgos a los que la compañía se encuentra expuesta, sin olvidar la ciberseguridad. Este cuerpo normativo debe ser debidamente publicado y comunicado a todos los empleados de modo que conozcan los riesgos a los que nos exponemos cuando nos enfrentamos a la ciberseguridad.

Una buena práctica es realizar cuestionarios y actividades de concienciación que permitan a los empleados conocer sus responsabilidades en materia de ciberseguridad y realizar pruebas internas de ingeniería social que nos ayuden a medir el nivel de concienciación implantado en la compañía. Realizar revisiones periódicas de cumplimiento del cuerpo normativo permitirá identificar debilidades y establecer acciones correctoras.

Cabe mencionar la importancia de colaboración con entidades públicas, tal y como establece la *Estrategia de Ciberseguridad Nacional* comentada con anterioridad.

Por supuesto no hay que olvidar que el sector privado deberá realizar un levantamiento de las leyes y regulaciones de los países en los que tiene presencia con objeto de conocer sus obligaciones legales.

Así pues, la regulación en materia de ciberseguridad en el sector privado ha cobrado especial importancia durante los últimos años, como demuestran algunos de estos hechos:

- La creación por parte del NERC (Corporación para la confiabilidad del sector eléctrico norteamericano) de un estándar de buenas prácticas en ciberseguridad y soporte a la industria e infraestructura eléctrica.
- La creciente exigencia a los bancos y entidades financieras en materia de sistemas y para la prevención y detección de amenazas de ciberseguridad por parte de los diferentes reguladores del sistema financiero.

Así lo demuestran las constantes revisiones, auditorías y procesos periódicos de análisis y evaluación de la capacidad de ciberresiliencia de las mismas, realizadas por la FED¹⁷, OCC¹⁸ y FDIC¹⁹ en Estado Unidos, PRA²⁰ y FCA²¹ en Inglaterra, y más recientemente por el Mecanismo Único de Supervisión (MUS) del Banco Central Europeo. A este respecto, es importante mencionar que el BCE inició sus diligencias el pasado año sobre las principales entidades bancarias a nivel europeo, con la realización de un primer proceso de evaluación de ciberseguridad a través del envío de un cuestionario, y seguido por inspecciones *in situ* actualmente en curso.

La realización de cuestionarios, pruebas internas de ingeniería social y actividades de concienciación para que los empleados conozcan sus responsabilidades en materia de ciberseguridad son buenas prácticas a aplicar en el sector privado.

17. Federal Reserve System - <https://www.federalreserve.gov/>

18. Office of the Comptroller of the Currency - <http://www OCC.gov/>

19. Federal Deposit Insurance Corporation - <https://www.fdic.gov/>

20. Prudential Regulation Authority - <http://www.bankofengland.co.uk/>

21. Financial Conduct Authority - <http://www.fca.org.uk/>



Buenas prácticas de Auditoría Interna para la evaluación y revisión de controles de ciberseguridad

A partir de este punto, se profundiza en los aspectos más relevantes que un auditor interno de sistemas o TI deberá tener en cuenta a la hora de abordar una revisión de ciberseguridad.

EL ROL DE AUDITORÍA INTERNA

Una buena aproximación para mitigar los riesgos puede consistir en integrar la ciberseguridad en el Modelo de las Tres Líneas de Defensa, comúnmente implantado en la mayoría de las organizaciones.

La ciberseguridad suscita mucho interés en los órganos de gobierno (comités o consejos directivos, comisiones de auditoría, comités de riesgos, etc...) de las distintas organizaciones, independientemente de su sector y actividad, y cada vez está más presente en las reuniones y en el día a día de dichos órganos.

Los riesgos derivados de ciberseguridad como fugas de información, fraudes, sabotajes, etc., pueden golpear duramente la reputación de las compañías, castigar económicamente en forma de sanciones y pérdidas, o pueden llegar a parar la operativa o prestación del servicio de las compañías, incluso en países con una regulación avanzada pueden conllevar condenas penales.

Tanto el volumen como el impacto de las amenazas están aumentando exponencialmente en los últimos tiempos. Por todo esto hay que extremar las medidas en materia de ciberseguridad y establecer todos los controles necesarios para poder mitigar los riesgos en las organizaciones.

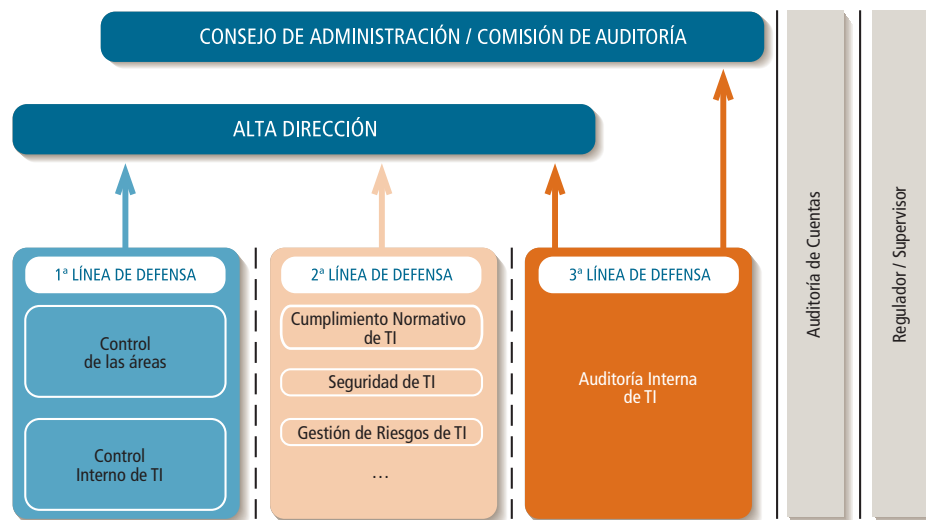
Una buena aproximación puede consistir en integrar la ciberseguridad en el sistema comúnmente implantado en la mayoría de las organizaciones (modelo de las tres líneas de defensa).

La primera línea de defensa

La primera línea de defensa es la propietaria de los riesgos y de su tratamiento en primera instancia. Debe realizar los procedimientos de control interno y de gestión de riesgos en su actividad diaria y tomar las decisiones en cuanto al riesgo con base a su cuantificación cualitativa y cuantitativa, con el objetivo de alcanzar los niveles óptimos en cuanto al coste/beneficio de asumir o no un riesgo.

Debe poner en funcionamiento todas las medidas técnicas y organizativas necesarias. Los empleados y usuarios (o los propietarios de las aplicaciones sean o no desarrolladas internamente por la organización) deben ser conscientes de que son parte primordial de esta primera línea de defensa. Son el primer obje-

Modelo de las Tres Líneas de Defensa* adaptado al riesgo de Ciberseguridad



* European Confederation of Institutes of Internal Auditors/Federation of Risk Management Association-2013. Endorsed by Global Institute of Internal Auditors-2014

tivo y la puerta de entrada más débil para los “malos”.

Deben tener mucho cuidado con correos electrónicos sospechosos, dispositivos móviles, redes Wifi, redes sociales, etc. Un uso adecuado de los mismos y conforme a las políticas de seguridad de la compañía provee una garantía que minimiza el riesgo existente. Pero esto no es suficiente, también se tienen que implantar todas las medidas técnicas (*firewall*, IDS, gestión de accesos, cifrado de la información, etc.) al alcance de la organización y en consonancia con la información que se maneja.

La segunda línea de defensa

La segunda línea de defensa puede estar compuesta por diferentes funciones en la organización tales como Gestión de Riesgos de TI, Seguridad de Sistemas, Cumplimiento Normativo de TI, Asesoría Jurídica, etc. Es evidente que dependiendo de la organización unas

tendrán más presencia que otras, pero todas ellas deberían tener en cuenta la ciberseguridad y sus riesgos.

La relación entre todas ellas debe formar un modelo de aseguramiento en ciberseguridad que facilite que los riesgos y controles en este ámbito se manejan de manera consistente, mediante revisiones proactivas de la seguridad y procesos de detección, corrección y mejora continua, proveyendo de tranquilidad y confianza a la alta dirección de la organización.

Como principales tareas debe:

- Desarrollar e implementar las políticas generales (ciberseguridad) y facilitar el desarrollo e implantación del marco general de riesgos y controles.
- Establecer las metodologías y métricas para evaluar y monitorizar el proceso.
- Reforzar los marcos de control definidos por la primera línea de defensa.

Para definir su Plan de Auditoría, Auditoría Interna de TI debe incorporar la información suministrada por la segunda línea de defensa y sus propios análisis, prestando especial atención a la ciberseguridad.

- Proveer de un mapa de riesgos completo y actualizado de la organización.
- Realizar el seguimiento de la exposición al riesgo y verificación de que está dentro de los márgenes y apetito al riesgo definido en la sociedad.
- Establecer los sistemas de reporting vertical y horizontal en materia de ciberseguridad.

La tercera línea de defensa

La tercera línea de defensa, que suele recaer sobre Auditoría Interna, en nuestro ámbito de ciberseguridad recaería más específicamente sobre Auditoría Interna de Sistemas. Debe ser completamente independiente del resto de líneas de defensa y debe proveer garantías sobre el sistema de control interno a los órganos de gobierno (consejo, comisiones de auditoría...), y la alta dirección.

Auditoría interna debe proporcionar una revisión y evaluación independiente sobre la eficacia de las líneas de defensa inferiores.

La colaboración con la segunda línea de defensa es muy importante facilitando el alineamiento con el modelo de aseguramiento a nivel corporativo y poner en contexto y elevar tanto las bondades del modelo como los *gaps* o deficiencias encontradas en materia de ciberseguridad.

En este punto, Auditoría Interna debería participar de manera pasiva o estar informada puntualmente de las actividades de las áreas

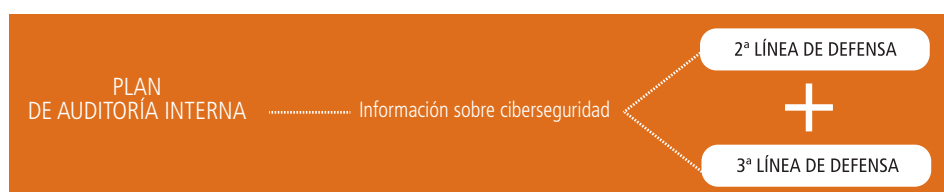
de seguridad de sistemas (encargadas de la ciberseguridad), asistiendo a sus comités o simplemente estableciendo entre ambas una línea de reporting lo suficientemente completa.

Para definir su Plan de Auditoría, Auditoría Interna de TI debería incorporar la información suministrada por la segunda línea de defensa además de sus propios análisis prestando especial atención a la ciberseguridad.

Adicionalmente, Auditoría Interna puede participar en ejercicios de revisión técnica de la seguridad, con el fin de identificar riesgos no identificados en las capas anteriores.

A modo de guía general, el siguiente listado pretende reflejar los principales aspectos en materia de ciberseguridad, que deberían ser preocupación y objeto de revisión por parte de Auditoría Interna:

1. Colaborar con la dirección de la compañía en la creación y desarrollo de una estrategia y política de ciberseguridad.
2. Asegurar que la organización cuenta con un correcto nivel de madurez y capacidad para la identificación y mitigación de los riesgos de ciberseguridad.
3. Verificar los mecanismos para reconocer incidentes de ciberseguridad procedentes de un empleado o proveedor externo.
4. Aprovechar las relaciones con la dirección de la compañía para aumentar el nivel de concienciación con los riesgos de ciberse-



guridad de la Junta y el Consejo, así como su implicación y compromiso con cuestiones clave en esta materia, como la actualización de la estrategia de ciberseguridad de la compañía.

5. La ciberseguridad se encuentra formalmente cubierta e integrada en el Plan de Auditoría Interna.
6. Entender y desarrollar un perfil de riesgo en ciberseguridad de la compañía, teniendo en cuenta las nuevas tecnologías y tendencias emergentes.
7. Evaluar el programa de ciberseguridad de la compañía con el marco de ciberseguridad de la NIST, y otros estándares tales como ISO 27001 y 27002.
8. Identificar y evaluar las capacidades preventivas de control de la ciberseguridad en materia de educación, formación y concienciación de usuarios, así como procesos y herramientas de control y vigilancia digital.
9. Asegurar que la monitorización y gestión de ciberincidentes es considerada una prioridad en la compañía, existiendo un proceso de escalado claro al respecto.
10. Identificar cualquier carencia o falta de personal de IT y Auditoría Interna que pueda representar un impedimento para

alcanzar los objetivos y retos de ciberseguridad de la compañía.

Ciberseguridad en comités y comisiones

Además de las funciones vistas en las tres líneas de defensa, existen multitud de comités y comisiones delegadas dependiendo de las propias características de las organizaciones, para tomar decisiones en cuanto a la estrategia, organización y operación. La ciberseguridad debería estar presente en todos ellos y tomada en consideración como un aspecto relevante en los siguientes:

- Comités de Sistemas, de Seguridad, de Continuidad de Negocio.
- Comités de Cumplimiento, de Riesgos.
- Comités de Dirección.
- Comisiones de Auditoría y Cumplimiento, de Riesgos.

Con esta presencia aseguramos que los máximos responsables de las organizaciones: presidencia, consejeros delegados, consejos de administración, etc., estén informados en todo momento de los riesgos que tienen las organizaciones en materia de ciberseguridad, las medidas adoptadas y las responsabilidades que asumen.

Auditoría Interna debe entender y desarrollar el perfil de riesgo en ciberseguridad de la organización, teniendo en cuenta las nuevas tecnologías y tendencias emergentes.

20 CONTROLES CRÍTICOS DE SEGURIDAD QUE TODAS LAS ORGANIZACIONES DEBERÍAN IMPLEMENTAR

Antecedentes

Los controles de seguridad críticos son un conjunto recomendado de acciones de ciberdefensa, orientados a mitigar los ataques más

comunes y dañinos con la intención de automatizarlos lo máximo posible. Están alineados con el marco de ciberseguridad del NIST y son un subconjunto de los controles definidos de

Los controles de seguridad críticos son acciones recomendadas orientadas a mitigar los ataques más comunes y dañinos para automatizarlos al máximo.

la publicación NIST 800-53, compendio de controles recomendados para las agencias estadounidenses, y sobre el cual se realizan las auditorías de seguridad de las agencias estatales en EEUU.

Los mecanismos de defensa recogidos en estos controles se basan en las experiencias de contención efectiva de ataques reales. Las acciones están priorizadas por orden de mitigación, según la puntuación de la NSA.

En 2009 un consorcio de agencias federales de los Estados Unidos y compañías del sector privado generaron las Directrices Consensuadas de Auditoría (CAG por sus siglas en inglés), un conjunto de 20 controles de seguridad de la información alineados con la publicación NIST 800-53.

SANS Institute ha coordinado la actualización hasta la versión 5.0. En agosto de 2016 se publicó la versión 6.1, ya coordinada desde el Center for Internet Security (CIS). Aunque esta última versión no incorpora cambios relevantes en la redacción y contenido de los controles, incluye una categorización de los mismos en 2 niveles: fundamental y avanzado. Para 2017 se espera la publicación de una herramienta que permitirá evaluar el nivel de implantación de estos controles.

Listado de controles y objetivos de control

La siguiente tabla muestra los 20 Controles Críticos de Seguridad (CSC), así como los objetivos de control necesarios para su correcta implementación:

CSC 1	INVENTARIO DE DISPOSITIVOS AUTORIZADOS Y NO AUTORIZADOS	Gestionar activamente todos los dispositivos hardware en la red, de forma que sólo los dispositivos autorizados tengan acceso a la red.
CSC 2	INVENTARIO DE SOFTWARE AUTORIZADO Y NO AUTORIZADO	Gestionar activamente todo el software en los sistemas, de forma que sólo se pueda instalar y ejecutar software autorizado.
CSC 3	CONFIGURACIONES SEGURAS DE SOFTWARE Y HARDWARE PARA DISPOSITIVOS MÓVILES, PORTÁILES, EQUIPOS DE SOBREMESA Y SERVIDORES	Establecer una configuración base segura para dispositivos móviles, portátiles, equipos de sobremesa y servidores, y gestionarlos activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir a los atacantes explotar servicios y configuraciones vulnerables.
CSC 4	PROCESO CONTINUO DE IDENTIFICACIÓN Y REMEDIACIÓN DE VULNERABILIDADES	Disponer un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.
CSC 5	CONTROL SOBRE PRIVILEGIOS ADMINISTRATIVOS	Desarrollar procesos y utilizar herramientas para identificar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.
CSC 6	MANTENIMIENTO, MONITORIZACIÓN Y ANÁLISIS DE LOGS DE AUDITORÍA	Recoger, gestionar y analizar logs de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.

CSC 7	PROTECCIÓN DEL CORREO ELECTRÓNICO Y DEL NAVEGADOR	Minimizar la posibilidad de que los atacantes manipulen a los empleados a través de su interacción con el correo electrónico y el navegador.
CSC 8	DEFENSAS CONTRA EL <i>MALWARE</i>	Evitar la instalación, difusión y ejecución de código malicioso en distintos puntos, al tiempo que se fomenta la automatización para permitir una actualización rápida en la defensa, recopilación de datos y la corrección.
CSC 9	LIMITAR Y CONTROLAR LOS PUERTOS DE RED, PROTOCOLOS Y SERVICIOS	Gestionar el uso de puertos, protocolos y servicios en los dispositivos que tengan red para reducir las vulnerabilidades disponibles a los atacantes.
CSC 10	CAPACIDAD DE RECUPERACIÓN DE DATOS	Disponer procesos, metodologías y herramientas adecuadas para respaldar la información crítica y realizar pruebas de recuperación.
CSC 11	CONFIGURACIONES SEGURAS DE DISPOSITIVOS DE RED (<i>FIREWALLS, ROUTERS Y SWITCHES</i>)	Establecer una configuración base para los dispositivos de infraestructura de red, y gestionarlas activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir a los atacantes explotar servicios y configuraciones vulnerables.
CSC 12	DEFENSA PERIMETRAL	Desarrollar una estrategia para detectar, prevenir y corregir los flujos de transmisión de información entre redes de distintos niveles de seguridad (confianza).
CSC 13	PROTECCIÓN DE LOS DATOS	Disponer de procesos y herramientas adecuadas para prevenir la fuga de información, mitigar los efectos cuando se ha producido un incidente de fuga de información, y asegurar la confidencialidad e integridad de la información sensible.
CSC 14	ACCESO BASADO EN LA NECESIDAD DE CONOCER (<i>NEED TO KNOW</i>)	El acceso a los activos críticos debe realizarse de acuerdo a una definición formal de que personas, sistemas y aplicaciones tienen la necesidad y el derecho de acceso. Los procesos y herramientas utilizadas en el seguimiento, protección y corrección de estos accesos deben estar alineados con las definiciones.
CSC 15	CONTROL DE ACCESO <i>WIRELESS</i>	Disponer de procesos y herramientas para garantizar una seguridad adecuada en las redes WiFi y en los sistemas clientes, incluyendo seguimiento y corrección de las medidas de seguridad.
CSC 16	CONTROL Y MONITORIZACIÓN DE CUENTAS DE SISTEMA	Gestionar activamente el ciclo de vida de las cuentas de sistema y de aplicación (creación, uso, inactividad y borrado) para reducir su utilización por parte de un atacante.

CSC 17	VERIFICACIÓN DE LAS HABILIDADES DE SEGURIDAD Y FORMACIÓN ADECUADA	Identificar los conocimientos específicos, habilidades y capacidades necesarias en la organización para la defensa de los activos críticos de la compañía, y desarrollar y evaluar un plan para identificar gaps y remediar con políticas, formación y programas de sensibilización.
CSC 18	SEGURIDAD EN EL CICLO DE VIDA DE LAS APLICACIONES	Gestionar el ciclo de vida de todas las aplicaciones, tanto las desarrolladas internamente como las de proveedores para prevenir, detectar y corregir vulnerabilidades técnicas.
CSC 19	GESTIÓN Y RESPUESTA A INCIDENTES	Proteger la información y la reputación de la organización desarrollando e implementando una infraestructura de respuesta a incidentes para detectar un ataque, contener el daño de forma efectiva, expulsar al atacante, y restaurar la integridad de los sistemas y la red.
CSC 20	REALIZAR TEST DE PENETRACIÓN Y EJERCICIOS DE ATAQUE	Probar las defensas de la organización (tecnología, procesos y personas) mediante la simulación de un ataque, utilizando sus mismas acciones y objetivos.

El papel de Auditoría Interna en la revisión de los controles

Para cada uno de los 20 enunciados, existen actividades más concretas que pueden formar parte del programa de trabajo de una auditoría de ciberseguridad.

El propio CIS cuenta con una guía para la medición de la efectividad de estos controles. Esta varía con las amenazas cambiantes. Es necesario contar con procesos de diagnóstico de la efectividad de los controles, utilizando métricas. La automatización de estos es fundamental para alcanzar este objetivo.

Los controles están pensados para organizaciones de cualquier tipo, no obstante, el conocimiento de la organización y la exposición a las amenazas va a condicionar la propia priorización y alcance de la implantación de los controles.

CONTROLES 1 Y 2

La revisión puede realizarse de dos formas:

- Verificar que existe una gestión de inventarios hardware y software, identificando listas blancas y negras y su actualización (al ser una aproximación de “ver que existe un control”, podríamos llamarla, “de capa 2”).
- El auditor interno escanea las redes internas utilizando herramientas automáticas (actúa como *Red Team*, según el control 20, es decir, comportándose como lo haría un atacante), hace una “verificación técnica”, que podríamos llamar “de capa 1”.

En el resto de controles también usaremos estas dos aproximaciones de revisión.

CONTROLES 3 Y 4

Su revisión se puede enfocar, de forma complementaria a los controles 1 y 2, verificando si existe una política de bastionado de todos los dispositivos, aplicaciones y servicios, si esta polí-

tica está alineada con buenas prácticas y si se dispone de un proceso de revisión de las vulnerabilidades que retroalimente la política de bastionado.

Otra aproximación es que el auditor escanee los dispositivos/aplicaciones utilizando herramientas automatizadas, actuando como *Red Team*.

CONTROL 5

Este control nos lleva a que las cuentas de usuarios administradores de aplicaciones, dispositivos y sistemas operativos deben estar identificadas, su uso auditado, eliminando las que no se utilizan y cambiando las que están definidas por defecto. Adicionalmente, deben cumplir con la política de fortaleza de contraseñas.

La revisión de este control puede orientarse a verificar la existencia de una política de alta, baja y mantenimiento de usuarios administradores, y la fortaleza de la contraseña (debería formar parte de la política de bastionado), y las tareas que se desarrollan para comprobar su cumplimiento.

Por otro lado, también podemos solicitar el listado de usuarios definidos en los sistemas y los ficheros de contraseñas cifradas asociados, y comprobar que no disponen de las claves por defecto utilizando herramientas automáticas.

CONTROL 6

Implica que todos los sistemas y aplicaciones deberían tener habilitadas las trazas de auditoría, incluyendo respuestas a desde dónde, quién, qué y cuándo, así como tener definidas acciones de alerta.

Debería existir una política asociada, un formato de *log* corporativo y una tarea de análisis de estos *logs*. En organizaciones con pre-

supuesto y personal suficiente se suele disponer de un SIEM (Security Information and Event Management), sistema que permite disponer en tiempo real de alertas de seguridad.

La verificación pasa por analizar el contenido de los *logs*, y, si actuamos como *Red Team*, las actividades que realicemos, como escanear una red o conectarnos como usuario administrador desde un puesto no habitual, deberían reflejarse en los *logs* y generarse las alertas correspondientes.

CONTROL 7

Nuevo en la versión 6.0, pasa por utilizar clientes de correo y navegadores actualizados y evitar que el usuario pueda añadir extensiones, así como cambiar su configuración. La configuración debe ser la más restrictiva posible para que el usuario pueda trabajar, deshabilitando los *plugins* innecesarios.

De forma complementaria, el control 8 habilita el análisis de *malware* en los equipos, y deben definirse medidas para evitar que el *malware* entre a través de la navegación del usuario o de la lectura de correo (IPS, antivirus de navegación y correo, bloqueo de URLs maliciosas, etc.).

CONTROL 8

El control 8 también recomienda agregar otras medidas contra el *malware* que deben estar recogidas en la política, como el bloqueo de USB y la monitorización continua de los equipos.

Debe existir una política del uso seguro y de configuraciones autorizadas, y tareas de revisión automatizada de los equipos y servidores.

Otra posible verificación pasa por enviar un correo con contenido no autorizado a una

Los controles están pensados para organizaciones de cualquier tipo. El conocimiento de la organización y la exposición a las amenazas condicionará la propia priorización y alcance de la implantación.

El acceso a la información debe seguir el principio de “necesidad de conocer”. Un perfilado adecuado mitiga el riesgo, pero deben implantarse otros controles, ya que un ataque puede obtener credenciales que tengan acceso a la información.

cuenta interna, o navegar por una página dentro de una lista negra.

CONTROL 9

Nos habla de limitar los servicios expuestos a las redes, y separar físicamente las máquinas que tienen esos servicios. Debe existir una política que defina que sólo los servicios y puertos necesarios para la organización estén habilitados, o restringidos a las redes/usuarios que realizan tareas asociadas. El resto debería estar deshabilitado/filtrado.

La aproximación para verificar este control pasa por realizar escaneos automáticos de las diferentes redes, para identificar puertos/servicios que deberían estar restringidos o deshabilitados. Un auditor interno puede realizar esta tarea de forma puntual o verificar si existe un proceso continuo que lo realice.

CONTROL 10

Nos pide que se hagan copias de seguridad de todos los datos críticos, así como que se verifique de forma periódica que estos se pueden recuperar en un tiempo asumible. Asimismo, los sistemas donde se guardan estas copias deben tener acceso restringido, tanto física como lógicamente.

Para probar este control, se pueden solicitar las políticas de *back up* y el resultado de las pruebas de recuperación.

CONTROL 11

Se basa en definir una configuración segura para los dispositivos de comunicaciones (*firewalls, routers, switches*), junto con los procesos de gestión de cambio asociados. Este control es la implantación para estos dispositivos de los controles 3, 4 y 5: configuración base segura, revisión de vulnerabilidades y control

del uso del administrador y, adicionalmente, control de cuentas por defecto (control 16).

El test de este control sería de la misma forma que los controles mencionados.

CONTROL 12

En este control vemos que tenemos que tener una seguridad perimetral basada en aplicar filtros sobre las comunicaciones de nuestra organización hacia y desde fuera, así como desplegar sensores que detecten actividades sospechosas y alimenten a nuestro SIEM, tenemos que protegernos, pero también es importante detectar si están intentando entrar o, si ya lo han hecho, identificarlos.

Por otro lado, tenemos que tener una DMZ, una zona donde los servicios expuestos a Internet estén separados de la red interna.

Si necesitamos acceder a la red interna desde fuera (teletrabajo), debemos implantar un segundo factor de autenticación.

El análisis de las reglas de FW nos permite evaluar este control. De igual forma que en controles anteriores, podemos hacer un escaneo de nuestro perímetro desde Internet para identificar puntos de entrada, servicios accesibles sin autenticación robusta y, testear qué alertas han generado nuestra actividad.

CONTROL 13

Este control confía en el cifrado de la información en reposo y en tránsito para garantizar la privacidad y prevenir una fuga.

CONTROL 14

El acceso a la información debe seguir el principio de “necesidad de conocer”. Un perfilado adecuado mitiga el riesgo, pero aun así debemos implantar otros controles, ya que un ataque puede obtener credenciales que tienen acceso a la información. Debemos emprender

acciones complementarias, y algunos de los controles que hemos visto nos ayudan: limitar el uso de USB, monitorizar las conexiones o la separación entre redes.

La prueba del control tiene que ser empírica, intentar acceder a información a la que no tenemos acceso por perfil.

CONTROL 15

Nos dice que protejamos las redes *wireless*. Un inventario de todas las existentes, junto con revisiones periódicas por parte del área de seguridad de que no existen redes no autorizadas; la comprobación automática de sus vulnerabilidades y de la fortaleza de las contraseñas; y una limitación de las redes internas a las que se puede acceder; completan la revisión del control.

Adicionalmente, se deberían desplegar detectores de intrusos en estas redes para identificar dispositivos no autorizados.

CONTROL 16

Si el control 4 era qué hace el administrador, el 16 es si hay cuentas definidas en los sistemas que sean usuarios por defecto, usuarios que ya han abandonado la organización o si existen otras cuentas definidas en los sistemas.

Por otro lado, se deben establecer bloqueos de cuentas por accesos fallidos (este punto debería estar en la política de seguridad), limitando desde dónde se puede acceder y solicitando un doble factor para acceder a sistemas/datos especialmente sensibles.

Los accesos de terceros deben revisarse especialmente.

Para probar este control, una opción es verificar que exista un proceso de revisión de usuarios. Otra opción es que Auditoría Interna

lance herramientas automáticas para identificar cuentas obsoletas habilitadas.

CONTROL 17

Se basa en que cada puesto funcional tiene que tener una formación específica en seguridad. Deben identificarse posibles carencias y formar a los empleados. Igualmente, la organización debería tener un programa de concienciación dirigido a todos los empleados, adecuado a las funciones que realizan.

Solicitar la formación recibida del personal de seguridad nos permite identificar las carencias.

Una forma de probar la efectividad es, una vez realizada la acción formativa/concienciadora, enviar un correo tipo *phishing* para ver la reacción del empleado y los pasos que realiza para denunciar el evento.

CONTROL 18

El ciclo de vida del software también necesita tener una capa de seguridad, como muestra el control 18. Tanto el desarrollo interno como la compra de software de terceros requieren de una capa de seguridad.

Las redes de desarrollo y producción deberían estar separadas.

Unas directrices de programación segura o plan de formación específica de desarrollo seguro, ayuda a evitar vulnerabilidades en las aplicaciones desarrolladas internamente. Si lo acompañamos de una revisión automática de código por parte de herramientas especializadas, limitamos las vulnerabilidades.

Una revisión final una vez integrado todo el desarrollo nos permite completar el ciclo. Esta última acción puede realizarla Auditoría Interna.

Deben establecerse bloqueos de cuentas por accesos fallidos, limitando desde dónde se puede acceder y solicitando un doble factor para acceder a sistemas/datos especialmente sensibles.

Es fundamental disponer de un plan de gestión y respuesta a incidentes que contemple procedimientos escritos, asignación de tareas y responsabilidades.

Existen productos que filtran/limitan las vulnerabilidades más comunes, que también pueden desplegarse en producción.

Los productos de terceros deberían probarse antes de su implantación.

CONTROL 19

Se enfoca en la gestión de crisis. Es fundamental disponer de un plan de gestión y respuesta a incidentes que contemple procedimientos escritos, asignación de tareas y responsabilidades.

Estos planes deberían ser probados para verificar cómo está preparada la organización frente a un incidente de envergadura, y garantizar una gestión adecuada a la crisis.

CONTROL 20

Nos habla de realizar ciberejercicios. Los tipos de ataques no paran de crecer. Aparecen nuevas técnicas de las que nos tenemos que defender. Una forma de probar si tenemos las defensas adecuadas es comportarnos como un posible atacante utilizando técnicas similares.

La capa 2 puede realizar esta tarea. Auditoría Interna revisaría las situaciones identificadas y las acciones correctoras.

Auditoría Interna también puede realizar la tarea (prueba todos los controles), o contratar los servicios de un externo.



Certificaciones profesionales

Con el aumento del nivel de amenazas y riesgos relacionados con la ciberseguridad experimentado durante los últimos años, existe actualmente una alta demanda de profesionales especializados en estas materias. La Unión Europea prevé la creación de 90.000 nuevos puestos de trabajo en este sector para el año 2020.

Sin embargo, no resulta fácil para las empresas encontrar los perfiles adecuados y especializados en los nuevos riesgos de la seguridad de la información, puesto que no existe todavía demasiada formación reglada.

En este sentido, se lanzaron iniciativas como el Foro de Empleo y Talento en Ciberseguri-

dad de CyberCamp (celebrado los días 27, 28 y 29 de noviembre de 2015 en el Barclaycard Center de Madrid) con el objetivo de dar a conocer la oferta y demanda laboral de diferentes empresas, orientar a los jóvenes acerca de las posibles trayectorias profesionales, así como informar acerca de los diferentes programas y opciones de formación.

En este marco, a las ya tradicionales certificaciones para profesionales de seguridad y auditoría de sistemas: ITIL (Information Technology Infrastructure Library), CobiT (Control Objectives for Information and Related Technology), ISO 27000 (Estándar para la Seguridad de la Información), CISA²² (Certified Inter-

22. Certificación otorgada por ISACA (Information Systems Audit and Control Association).



nal Systems Auditor), CISM (Certified Information Security Manager), CISSP²³ (Certified Information Systems Security Professional), Security+ (certificada por CompTIA²⁴), etc.; se han incorporado otras muchas que han cobrado importancia (especialmente aquellas relacionadas con aspectos de *pentesting* y *hacking* ético, gestión de ciberincidentes o análisis forense), tales como las ofrecidas por las siguientes organizaciones.

ISACA

Ha lanzado el programa Cybersecurity Nexus²⁵ (CSX), que ofrece una serie de certificaciones en diferentes niveles para la formación de profesionales, y alineadas con los principales estándares de ciberseguridad del mercado:

- **Cybersecurity Fundamentals Certificate.** Orientada a la introducción de los conceptos, marcos, guías de buenas prácticas y estándares de ciberseguridad de la industria; ciberseguridad en redes, sistemas, aplicaciones y datos, implicaciones de seguridad de las nuevas tecnologías y respuesta básica ante incidentes.
- **CSX Practitioner.** Certificación orientada a la primera capa de respuesta de seguridad, con el objetivo de conocer e implementar los principales controles de seguridad, realizar análisis y escaneos de vulnerabilidades, definición de procesos y procedimientos de seguridad en los sistemas.

- **CSX Specialist.** Certificaciones avanzadas y especializadas en el conocimiento y habilidades de las siguientes áreas o dominios: Identificación de riesgos, protección de sistemas, detección de amenazas, respuesta y análisis de incidentes, y recuperación de los sistemas.
- **CSX Expert.** Certificación de nivel avanzado para la identificación, análisis, respuesta y mitigación de incidentes de ciberseguridad avanzados, y asociados a empresas con entornos complejos y una alta exposición a ataques.

SANS

El Instituto SANS (SysAdmin Audit, Networking and Security Institute) en colaboración con la entidad certificadora GIAC (Global Information Assurance Certification) ofrece un conjunto de más de 20 certificaciones agrupadas en diferentes niveles en materia de administración y gestión de seguridad, auditoría legal y de seguridad, seguridad del software y análisis forense:

NIVEL INTRODUCTORIO.

- Administración de Seguridad.
 - GISF: Information Security Fundamentals.

NIVEL INTERMEDIO.

- Administración de Seguridad.
 - GSEC: Security Essentials Certification.
- Gestión.
 - GISP: Information Security Professional.
- Forense.
 - GCFE: Certified Forensics Examiner.

23. Certificación otorgada por ISC2 (International Information Security Certification Consortium).

24. Computing Technology Industry Association. <http://certification.comptia.org/>

25. <https://cybersecurity.isaca.org/csx-certifications>

NIVEL AVANZADO.

- Administración de Seguridad.
 - **GPPA**: Certified Perimeter Protection Analyst.
 - **GCIA**: Certified Intrusion Analyst.
 - **GCIH**: Certified Incident Handler.
 - **GCUX**: Certified UNIX Security Administrator.
 - **GCWN**: Certified Windows Security Administrator.
 - **GCED**: Certified Enterprise Defender.
 - **GPEN**: Certified Penetration Tester.
 - **GWAPT**: Web Application Penetration Tester.
- Gestión.
 - **GSLC**: Security Leadership Certification.
 - **GCPM**: Certified Project Manager Certification.
- Seguridad del software.
 - **GSSP-NET**: Secure Software Programmer-NET.
 - **GSSP-JAVA**: Secure Software Programmer - Java.
- Auditoría.
 - **GSNA**: Systems and Network Auditor.
- Forense.
 - **GCFA**: Certified Forensic Analyst.
- Legal.
 - **GLEG**: Law of Data Security & Investigations.

NIVEL EXPERTO

- Administración de Seguridad.
 - **GAWN**: Assessing Wireless Networks.
 - **GXPN**: Exploit Researcher and Advanced Penetration Tester.
- Forense.
 - **GREM**: Reverse Engineering Malware.
- GSE.
 - **GSE**: GIAC Security Expert.

EC-Council2

El Consejo Internacional de Consultores de Comercio Electrónico, ofrece entre otras muchas, las siguientes certificaciones relacionadas con la gestión de la ciberseguridad:

- **CEH (Certified Ethical Hacker)**. Introducción a las habilidades y vulnerabilidades en sistemas utilizando los mismos conocimientos y herramientas que los *hackers* maliciosos y metodología de *pentesting*, con el objetivo de ayudar a la organización a tomar medidas contra estos ataques.
- **ECSA (Certified Security Analyst)**. Curso avanzado en métodos y técnicas de penetración, analizando diferentes herramientas, tecnologías y fases del proceso de *hacking* ético, para identificar y mitigar los riesgos de seguridad de la infraestructura como analista de seguridad y *pentester*.
- **ENSA (Network Security Administrator)**. Certificación dirigida a administradores de seguridad, proporcionando las habilidades para analizar las amenazas (internas y externas), así como las técnicas defensivas para protegerse ante ellas.
- **CHFI (Computer Hacking Forensic Investigator)**. Preparación para la detección ante ataques perpetrados por *hackers*, responder a incidentes de seguridad, e identificación de técnicas de investigación y análisis para rastrear el origen del evento con el fin de determinar diferentes evidencias digitales.
- **ECIH (Certified Incident Handler)**. Diseñada para proveer los conocimientos necesarios en materia detección, gestión y respuesta ante amenazas e incidentes de ciberseguridad.



- **ECES (Certified Encryption Specialist).** Aprendizaje de las diferentes técnicas (simétrico, clave criptográfica), fundamentos y detalle de los algoritmos de cifrado (DES, AES, RSA, MD5, etc.), así como su uso e implementación técnica.

Formación

Ante la demanda y búsqueda de nuevos profesionales en ciberseguridad, y con el objetivo de facilitar una mejor comprensión y gestión de estos riesgos, existe actualmente en el mercado una amplia oferta de opciones de formación (seminarios, cursos presenciales y/o online, cursos de postgrado), entre los que podemos destacar:

- **El Instituto Tecnológico de Massachusetts (MIT²⁶)** reconocido mundialmente como una de las mejores instituciones del sector, dispone de una amplia gama de cursos, certificaciones y seminarios, y cuenta con una completa plataforma online que permite a la inscripción de estudiantes de todo el mundo, y el seguimiento de clases online.
- **La Agencia Europea para la Seguridad de las Comunicaciones y la Información (ENISA²⁷,** por sus siglas en inglés), ofrece también una serie de cursos de formación en

materia de ciberseguridad relacionados fundamentalmente con las siguientes materias: gestión de ciberincidentes, análisis avanzados de amenazas, análisis forense digital y gestión de amenazas en dispositivos móviles.

- **El Instituto Nacional de Ciberseguridad (INCIBE²⁸)** ofrece una serie de cursos online como, por ejemplo: *Seguridad en sistemas de control y automatización industrial, Ciberseguridad para micro-pymes y autónomos, Seguridad avanzada en dispositivos móviles o Ciberseguridad para fuerzas y cuerpos de seguridad.*
- Diferentes Masters en ciberseguridad ofrecidos entre otras por S21sec, Zin Security, CICE (Escuela de Formación de Nuevas Tecnologías), Aocal Business School, y diferentes centros universitarios como la Universidad de León, la Universidad Europea de Madrid, la Universidad Politécnica de Cataluña o la Universidad Camilo José Cela.

²⁶. <http://web.mit.edu/>

²⁷. <https://www.enisa.europa.eu/>

²⁸. <https://www.incibe.es/>

Bibliografía relevante

Estándares, normativa y legislación

- NIST (02/14): Framework for improving Cyber-security.
- ISO27032: Guidance from improving the state of cyber-security.
- Estrategia de Ciberseguridad Nacional (Gobierno de España).
- Ten steps to cyber security (UK GOV: CESG and CPNI).
- Cybersecurity Capability Maturity Model (C2M2) Program (USA Department of Energy).
- CIS Critical Security Controls (SANS Institute & Center for Strategic & International Studies).

Artículos, informes y presentaciones técnicas

- *State of Cybersecurity: Implications for 2015* (Nexus, ISACA y RSA).
- *Temas candentes de la Ciberseguridad - Un nuevo espacio lleno de incógnitas* (IE y PWC).
- *Presente y Futuro de la Ciberseguridad* (CCN-CERT).
- *Ciberamenazas 2014. Tendencias 2015* (CCN-CERT).
- *Guía de gestión de ciberincidentes* (CCN-CERT).
- *Ciberinteligencia: de la reacción a la prevención en Ciberseguridad* (KPMG).
- *Ciberinteligencia aplicada al desarrollo de servicios* (INCIBE).
- *Análisis y caracterización del mercado de la ciberseguridad* (INCIBE).
- *Risk Intelligence Report* (CEB).
- *Informe sobre el estado de la ciberseguridad 2015* (U-TAD).
- *State of the Internet Security Report 2015* (Akamai).
- *System Design Guide for Thwarting Targeted Email Attacks* (IPA, Japan).
- *Controls for Effective Cyber Defense v6.0* (CIS: Center for Internet Security).
- *Cybersecurity, What the Board Directors Needs To Ask* (IIARF & ISACA).
- *Assessing the Top Priorities for Internal Audit Functions* (Protiviti).
- *COSO in the Cyber Age* (Deloitte).
- *2016 Data Protection & Breach Readiness Guide*.
- *Auditing Cybersecurity* (ISACA Journal enero/febrero 2016).

Instituto de Auditores Internos de España

Santa Cruz de Marcenado, 33 · 28015 Madrid · Tel.: 91 593 23 45 · Fax: 91 593 29 32 · www.auditoresinternos.es

Depósito Legal: M-36848-2016

ISBN: 978-84-945594-2-6

Diseño y maquetación: desdezero, estudio gráfico

Impresión: IAG, SL

OTRAS PRODUCCIONES DE LA FÁBRICA DE PENSAMIENTO

COBERTURA DEL RIESGO TECNOLÓGICO: HACIA UNA AUDITORÍA INTERNA DE TI INTEGRADA

El documento destaca la importancia de Auditoría Interna de TI en su apoyo a la organización en la gestión, gobierno y control de los riesgos de TI. Se han estudiado temas relacionados con la gestión de las relaciones entre Auditoría Interna de TI y el área de TI, destinatarios de los informes de Auditoría Interna de TI o las herramientas que habitualmente se utilizan en este tipo de trabajos.

MARCO DE RELACIONES DE AUDITORÍA INTERNA CON OTRAS FUNCIONES DE ASEGURAMIENTO

Ayuda a fijar posiciones sobre la necesidad de mejorar la eficiencia de los recursos de las Direcciones de Auditoría Interna para mantener el nivel adecuado de aseguramiento en coordinación con las distintas funciones encargadas de proporcionarlo. Aborda la necesidad de realizar un mapa de aseguramiento que proporcione una visión global de las actividades de control llevadas a cabo, proponiendo a Auditoría Interna como coordinador principal de todas las funciones de aseguramiento.

GESTIÓN DEL RIESGO DE FRAUDE

Aborda los diferentes procesos para una óptima gestión del riesgo de fraude, que pasa por el establecimiento de un programa eficaz de prevención, detección e investigación de fraudes. La guía, resumen ejecutivo de un estudio más amplio publicado por el Instituto de Auditores Internos, define un enfoque efectivo para la gestión del riesgo de fraude y un análisis profundo sobre las responsabilidades en su prevención, detección e investigación.



LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Prácticamente todos los ámbitos de nuestra sociedad se sustentan hoy más que nunca, y cada vez más, en el ciberespacio propiciado por las tecnologías de la información y las comunicaciones. Una de las principales amenazas que han traído consigo estos avances es la proliferación de acciones delictivas en el ciberespacio, añadiendo nuevos retos y desafíos para las organizaciones.

La ciberseguridad es una de las principales preocupaciones de empresas e instituciones y exige extremar las medidas para establecer todos los controles necesarios para mitigar los riesgos en las organizaciones.

Esta guía establece diversas buenas prácticas, incluyendo los 20 Controles Críticos de Seguridad que todas las organizaciones deben implementar, y cuál es el papel de Auditoría Interna en su revisión.

También aportará gran valor a Comisiones de Auditoría y otros comités, que encontrarán aquí un importante aliado con información completa y precisa para permitirles tomar decisiones sobre la estrategia, estructura y operación de las organizaciones.