MEMENTO EXPERTO
FRANCIS LEFEBVRE

Ciberseguridad

Fecha de edición: 29 de enero de 2021

Es una obra realizada por iniciativa
y bajo la coordinación
de la Redacción de
Francis Lefebvre
sobre la base de un estudio técnico
cedido a la editorial por

Francisco Pérez Bes (Coordinador)
Abogado. Ex Secretario General del Instituto Nacional de Ciberseguridad (2014-2019). Socio en Ecix Group. Miembro de la Junta Directiva de la Asociación de Expertos Nacionales de la Abogacía TIC (ENATIC). Miembro de la Comisión Jurídica del Consejo General de la Abogacía Española. Profesor Honorífico de Derecho Público en la Universidad de León.

Carlos Galán, PhD
Licenciado y Doctor en Informática. Licenciado en Derecho y Abogado. Profesor de la Universidad Carlos III de Madrid. Asesor del Centro Criptológico Nacional (CNI). Auditor Técnico de la Entidad Nacional de Acreditación (ENAC). Miembro del Grupo de Expertos de la Estrategia Nacional de Ciberseguridad

Francisco Martínez Vázquez
Abogado. Letrado de las Cortes Generales. Profesor de Derecho Constitucional. Exsecretario de Estado de Seguridad (2013-2016)

Jorge Villarino Marzo
Abogado y Doctor en Derecho. Letrado de las Cortes Generales. Socio de Vinces Consulting.

Eloy Velasco
Magistrado en la Audiencia Nacional.

Rafael Ansón Peironcely
Abogado y Doctor en Derecho. Socio en Bufete Mascalvet.

Fernando Sánchez Gómez
Director del Centro Nacional para la Protección de las Infraestructuras y la Ciberseguridad (CNPIC).

Margarita Robles
Profesora titular de Derecho Internacional en la Universidad de Granada.

Vicente Moret Millás
Abogado. Letrado de las Cortes Generales. Of Counsel en Andersen. IE Law School professor

Pedro Agudo Novo
Inspector Jefe de Policía Judicial de la Unidad Adscrita a los Tribunales y la Fiscalía.

Jorge Bermudez
Fiscal adscrito a la unidad de apoyo de la Fiscalía General del Estado y responsable de ciberseguridad. Exdelegado en Guipúzcoa para la criminalidad informática.

Jerónimo Domínguez-Bascoy
General auditor del Cuerpo Jurídico Militar

Enrique Cubeiro Cabello
Capitán de Navío. Jefe de Operaciones del Mando Conjunto de Ciberdefensa (MCCD)

Rafael García del Poyo
Abogado. Socio Director del Departamento de Derecho IT/IP. Osborne Clark España

Mercedes Fuertes
Catedrática de Derecho Público en la Universidad de León (ULE)

Lefebvre-El Derecho, S. A.
Monasterios de Suso y Yuso, 34. 28049 Madrid. Teléfono: (91) 210 80 00. Fax: (91) 210 80 01
www.efl.es
Precio: 38,48 € (IVA incluido)

ISBN: 978-84-18405-43-3
Depósito legal: M-3703-2021

Impreso en España
por Printing'94
C/ Orense, 4 (2ª planta) – 28020 Madrid

Plan general

Abreviaturas

ABE	Autoridad Bancaria Europea
AENOR	Asociación Española de Normalización y Certificación
AEPD	Agencia Española de Protección de Datos
AGNU	Asamblea General de Naciones Unidas
ALAC	At-Large Advisory Comité
AP	Audiencia Provincial
APT	Advanced persistant threats
art.	artículo
ASO	Address Supporting Organization
BCE	Banco Central Europeo
BOE	Boletín Oficial del Estado
CCN	Centro Criptológico Nacional
CCN-STIC	Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones
ccNSO	Country Code Names Supporting Organization
CEPD	Comité Europeo de Protección de Datos
CERT	Computer Emergency Response Team
CICR	Comité Internacional de la Cruz Roja
Circ	Circular
CIS	Communication and Information Systems
CNMC	Comisión Nacional de los Mercados y la Competencia
CNI	Centro Nacional de Inteligencia
CNPIC	Centro Nacional de Protección de Infraestructuras y Ciberseguridad
Const	Constitución española
CSIRT	Computer Security Incident Response Team
C	Mando y Control
DCE	Directiva de Comercio Electrónico (Dir 2000/31/CE)
DDoS	Denegación Distribuida de Servicio
DGA	Algoritmo de Generación de Dominio
DIH	Derecho Internacional Humanitario
Dir	Directiva
Directiva NIS	Dir (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión
DoS	Denegación de Servicio
DPD	Delegado de Protección de Datos
DSN	Departamento de Seguridad Nacional
EBA	European Banking Authority (Autoridad Bancaria Europea)
ECB	European Central Bank (Banco Central Europeo)
ECSN	Estrategia de Ciberseguridad Nacional de 2013
EEE	Espacio Económico Europeo
EIPD	Evaluación de Impacto de Protección de Datos
EMAD	Estado Mayor de la Defensa
ENAC	Entidad Nacional de Acreditación
ENCS	Estrategia Nacional de Ciberseguridad 2019
ENI	Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (RD 4/2010)
ENISA	European Union Agency for Network and Information Security (Agencia Europea de la Ciberseguridad)
ENS	Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (RD 3/2010)

ESPDEF-CERT	Equipo de Respuesta ante Emergencias Informáticas del Ministerio de Defensa
EW	Electronic War (Guerra Electrónica)
FAS	Fuerzas Armadas
FGE	Fiscalía General del Estado
GDPR	General Data Protection Regulation
GEG	Grupos de Expertos Gubernamentales
GNSO	Generic Names Supporting Organization
ICANN	Internet Corporation for Assigned Names and Numbers (Corporación para la Asignación de Números y Nombres en Internet)
IoT	Internet of the Things
ISACA	Asociación de Auditoría y Control de los sistemas de información
ITS	Instrucción Técnica de Seguridad
ITU	International Telecomunication Union
I3D	Infraestructura Integral de Información para la Defensa
JEMAD	Jefe del Estado Mayor de la Defensa
JM	Juzgado de lo Mercantil
JMC	Jefatura de Mando y Control
JSCD	Jefatura de Sistemas de Ciberdefensa
JTEW	Jefatura de Telecomunicaciones y Guerra Electrónica
L	Ley
LCS	Ley de Contrato de Seguro (L 50/1980)
LEC	Ley de Enjuiciamiento Civil (L 1/2000)
LECr	Ley de Enjuiciamiento Criminal
LGDCU	Ley General para la Defensa de los Consumidores y Usuarios (RDLeg 1/2007)
LJCA	Ley 29/1998 de Jurisdicción contencioso-administrativa
LO	Ley Orgánica
LOPD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales
LPI	Ley de Propiedad Intelectual (RDLeg 1/1996)
LSSI	L 34/2002 de servicios de la sociedad de la información y de comercio electrónico
MCCD	Mando Conjunto de Ciberdefensa
MCCE	Mando Conjunto del Ciberespacio
MOC	Mando Operativo Ciberespacial
MOPS	Mando de Operaciones
OCC	Oficina de Coordinación Cibernética
OF	Orden Foral
OM	Orden ministerial
ORECE	Organismo de Reguladores Europeos de las Comunicaciones Electrónicas
OSE	Operador de Servicio Esencial
OTAN	Organización del Tratado del Atlántico Norte
PCSD	Política Común de Seguridad y Defensa
PESC	Política exterior y de seguridad común
PIC	Protección de Infraestructuras Críticas
PSD	Proveedor de Servicios Digitales
RAE	Real Academia Española
RD	Real Decreto
RDL	Real Decreto Ley
RDL-NIS	RDL 12/2018 de seguridad de las redes y sistemas de información
RDLeg	Real Decreto Legislativo
RGPD	Reglamento (UE) 2016/679 General de Protección de datos
Rgto	Reglamento
SCA	Strong Customer Authentication (Autenticación Reforzada de Clientes)
SEAP	Secretaría de Estado de la Administración Pública

SEFP	Secretaría de Estado de Función Pública
SEGINFOSIT	Seguridad de la Información en los Sistemas de Información y Telecomunicaciones
SES	Secretaría de Estado de Seguridad
SGSI	Sistema de gestión de la seguridad de la información
SOT	Sistemas de Observación de la Tierra
TCo	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TIC	Tecnologías de la Información y las Comunicaciones
TIJ	Tribunal Internacional de Justicia
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
UE	Unión Europea
UIT	Unión Internacional de Telecomunicaciones
WWW	World Wide Web

CAPÍTULO 1

Consideraciones generales

100

A. Conceptos

Definición de ciberseguridad Según la Asociación de Auditoría y Control de los sistemas de información (ISACA) debemos entender por ciberseguridad la **protección** de los **activos de la información** (cualquier dato con valor) a través del tratamiento de amenazas que pongan en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados. 105

Lo anterior supone proteger los **activos de una organización** (componentes o funcionalidades de un sistema de información susceptibles de ser atacados deliberada o accidentalmente con consecuencias para la organización) frente a vulnerabilidades (debilidades que pueden ser aprovechadas por una amenaza), amenazas (explotación dañina de las vulnerabilidades) y riesgos (probabilidad de aprovecharse de esas vulnerabilidades y sufrir amenazas) y los **programas** con la **información o datos** que se tratan en ellos (privacidad, protección, propiedad...).

También la **Unión Internacional de Telecomunicaciones** (UIT) ha desarrollado una definición de ciberseguridad en su Resolución 181. En esta, se aprobó una definición de ciberseguridad, siguiendo lo ya recogido en la Recomendación UIT-T X.1205, que considera a la ciberseguridad como a un conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. 106

En este sentido la UIT entiende que los **activos de la organización y los usuarios** son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno.

Así, la ciberseguridad garantiza que se alcancen y mantengan las **propiedades de seguridad** de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes. Las propiedades de seguridad incluyen una o más de las siguientes:

a) Disponibilidad.

b) Integridad, que puede incluir la autenticidad y el no repudio.

c) Confidencialidad.

También la Dir (UE) 2016/1148 (**Directiva NIS**) nos ofrece una definición que, si bien no es del término «ciberseguridad», es sobre el concepto de **«seguridad de las redes y sistemas de información»**. En este caso, el art.4.2 de la Directiva NIS se refiere a aquella desde una óptica de resiliencia, al entenderla como la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos. 107

Esta definición va en línea con la que recoge la **norma ISO/IEC 27032:2012**, cuando dice que ciberseguridad es *preservation of confidentiality, integrity and availability of information in the Cyberspace*.

108 Así las cosas, podemos **definir a la ciberseguridad** como un conjunto de procesos dirigidos a prevenir y gestionar incidentes de seguridad.

111 Términos y conceptos utilizados en ciberseguridad En España, el Anexo IV del RD 3/2010, por el que se aprueba el Esquema Nacional de Seguridad (ENS), recoge un **glosario** con las definiciones de los principales términos y conceptos utilizados en ciberseguridad, y que si bien solo resultan de aplicación en el ámbito de aplicación del dicho esquema, se hace extensivo al resto de aspectos y supuestos en otros ámbitos de esta materia.
Entre estas definiciones, podemos destacar algunas que, por su relevancia y uso, son especialmente importantes:

112 • **Análisis de riesgos**: utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.
• **Autenticidad**: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
• **Confidencialidad**: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
• **Disponibilidad**: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
• **Firma electrónica**: conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
• **Gestión de incidentes**: plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.
• **Gestión de riesgos**: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

113 • **Incidente de seguridad**: suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.
• **Integridad**: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
• **Medidas de seguridad**: conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.
• **Política de firma electrónica**: conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.
• **Política de seguridad**: conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.
• **Principios básicos de seguridad**: fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

114 • **Proceso**: conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.
• **Proceso de seguridad**: método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.

• **Requisitos mínimos de seguridad**: exigencias necesarias para asegurar la información y los servicios.
• **Riesgo**: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
• **Seguridad de las redes y de la información**: es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.
• **Servicios acreditados**: servicios prestados por un sistema con autorización concedida por la autoridad responsable, para tratar un tipo de información determinada, en unas condiciones precisas de las dimensiones de seguridad, con arreglo a su concepto de operación.

• **Sistema de gestión de la seguridad de la información** (SGSI): sistema de gestión **115**
que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.
• **Sistema de información**: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
• **Trazabilidad**: propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
• **Vulnerabilidad**: una debilidad que puede ser aprovechada por una amenaza.

B. Normativa aplicable

La ciberseguridad es una materia que se encuentra regulada, entre otras, en las **120**
siguientes normas:

Estrategia Europea de Ciberseguridad La Comunicación conjunta al Parla- **123**
mento europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones. Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro (52013JC0001), es el documento donde se recogen las **principales líneas de acción**, marcadas por la **Comisión Europea** de cara al desarrollo de la política pública comunitaria en materia de ciberseguridad, y sobre la cual se basan las estrategias nacionales de ciberseguridad desarrolladas por los distintos estados miembros.

Estrategia Nacional de Ciberseguridad Tras la publicación de la Estrategia **126**
de Ciberseguridad Nacional (ECSN) del año 2013, el Gobierno español publicó, en el año 2019 (BOE 30-4-19), la OM PCI/487/2019, por la que se publica la **Estrategia Nacional de Ciberseguridad 2019**, aprobada por el Consejo de Seguridad Nacional (ENCS). Ver nº 3305.
Este documento **desarrolla** las previsiones de la **Estrategia de Seguridad Nacional 2017** (ver nº 130) en el ámbito de la ciberseguridad, considerando los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas para conseguirlo.
Ante el desarrollo y evolución de la digitalización, como clara tendencia global ya identificada en la Estrategia de Seguridad Nacional de 2017, la ENCS trata a la ciberseguridad como un aspecto que se extiende más allá del campo meramente de la protección del patrimonio tecnológico para adentrarse en las esferas política, económica y social.
A raíz de esta nueva aproximación, la Estrategia establece un **esquema novedoso**, con **cinco objetivos** generales que resultan transversales a todos los ámbitos. La gestión de crisis, la cultura de Seguridad Nacional, los espacios comunes globales, el desarrollo tecnológico y la proyección internacional de España conforman una

matriz estratégica donde la ciberseguridad está llamada a abrir nuevas vías hacia el modelo de presente y futuro de la seguridad en España.

127 Además de las acciones para causar efectos en los sistemas digitales, se debe tener en cuenta la concepción del **ciberespacio** como un **vector de comunicación estratégica**, que puede ser utilizado para influir en la opinión pública y en la forma de pensar de las personas a través de la manipulación de la información, las campañas de desinformación o las acciones de carácter híbrido. Su potencial aplicación en situaciones muy diversas, donde se incluyen los procesos electorales, genera un elevado grado de complejidad.

130 Estrategia de Seguridad Nacional Mediante RD 1008/2017, se aprueba la Estrategia de Seguridad Nacional 2017, que sustituye a la estrategia de 2013, y que se desarrolla con el **objetivo** de configurarse como el marco político estratégico de referencia de la política de seguridad nacional.
El fundamento de dicha estrategia la encontramos en la L 36/2015, de seguridad nacional, que establece que la **política de seguridad nacional** es una política pública en la que bajo la dirección del presidente del Gobierno y la responsabilidad del Gobierno, participan todas las Administraciones públicas, de acuerdo con sus respectivas competencias, y la sociedad en general, para responder a las necesidades de la seguridad nacional.
Como resumen, podemos afirmar que la Estrategia de Seguridad Nacional es el marco de referencia para la política de seguridad nacional, una política de Estado que parte de una **concepción amplia de la seguridad**. La estrategia actual profundiza en algunos de los conceptos y líneas de acción definidos en 2013 y avanza en la adaptación de dicha política ante nuevos desarrollos de un entorno de seguridad en cambio constante.

133 Esquema Nacional de Seguridad (ENS) Aprobado mediante RD 3/2010. En él se fija la política de seguridad en el uso de los medios electrónicos para las Administraciones, señalando los principios fundamentales y bases mínimas de una adecuada protección de la información. Ver nº 1185.

136 Protección de infraestructuras críticas La L 8/2011, de protección de las infraestructuras críticas, desarrollada por su Reglamento a través del RD 704/2011, establece un marco de control y una serie de medidas de seguridad a aplicar a las infraestructuras críticas, que son aquellas encargadas de asegurarnos los **servicios más esenciales** de la sociedad. Ver nº 1250 s.

139 Seguridad en redes y sistemas de información La Dir (UE) 2016/1148, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea (**Directiva NIS**), fue traspuesta al ordenamiento jurídico español a través del RDL 12/2018, y el Rgto ejecución (UE) 2018/151 –para los proveedores de servicios digitales–, que pretenden aportar seguridad a las redes y sistemas de información en los **servicios esenciales digitales**, respecto del desarrollo de capacidades y de planificación, intercambio de información, cooperación y seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales, con especial atención a la prevención y acción ante los incidentes de ciberseguridad.
Posteriormente, el RDL 14/2019, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, incorpora, en su Capítulo V, medidas para reforzar la **coordinación** en materia de seguridad de las redes y sistemas de información, para lo cual efectúa una modificación en el citado RDL 12/2018.
Más recientemente, mediante RD 43/2021 (BOE 28-1-21), se ha publicado el **desarrollo reglamentario** del RDL 12/2018, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información y al cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los provee-

dores de servicios digitales y a la gestión de incidentes de seguridad. Esta norma ha entrado en vigor el 29-1-2021. Ver nº 1006.

Reglamento europeo de ciberseguridad Aprobado por el Rgto (UE) 2019/881 (comúnmente conocido como *Cybersecurity Act*), que, además de establecer las **funciones de ENISA** (Agencia de Ciberseguridad de la UE), fija los criterios comunes para el sistema de **certificación de ciberseguridad** en sistemas de información y comunicación. **142**

Medidas restrictivas contra los ciberataques El Rgto (UE) 2019/796, relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros, y la Decisión (PESC) 2019/797 del Consejo, que establece un marco para unas medidas restrictivas específicas con el fin de prevenir y responder a los ciberataques con un efecto significativo que constituyan una amenaza externa para la Unión o sus Estados miembros. **145**

Protección penal: ciberdelicuencia A la ciberseguridad en sentido estricto –protección de las infraestructuras, redes y sistemas– se le debe añadir la referida a los **contenidos**, obligándonos a contemplar además la protección penal, esto es: la ciberdelincuencia. **148**

Desde esta vía se protege tanto **sistemas** como **información** (ataques a sistemas, datos, propiedad intelectual, menores y seguridad), así como otras protecciones trasversales que pretenden incorporar el respeto de los derechos fundamentales en el diseño y uso de las nuevas tecnologías, y de entre los que destacan el de la **protección del dato** (con temas afectantes a la seguridad como la seudonimización, cifrado, confidencialidad, integridad, disponibilidad, resiliencia, etc.) y el de los secretos empresariales.

El **Código Penal** incorpora este concepto de ciberdelincuencia estableciendo responsabilidades penales y civiles derivadas de las infracciones tecnológicas más graves, afectantes tanto a las personas físicas como a las jurídicas. Ver nº 2750 s.

Protección de datos personales El Rgto (UE) 2016/679 General de Protección de datos (**RGPD**) establece los estándares comunes a los 27 países en materia de protección de la información, señalando los **principios** que deben regir el **tratamiento de datos** (RGPD art.5; LOPD art.4 a 10). Ver nº 615 s. **151**

El citado Reglamento se complementa por la LO 3/2018, de protección de datos y garantía de derechos digitales (**LOPD**), que desarrolla los derechos de los usuarios de los mismos (LOPD art.11 a 18).

A esto se debe añadir, en materia de datos personales para la prevención, investigación, detección o enjuiciamiento de **infracciones penales** o de ejecución de sanciones penales, la Dir (UE) 2016/680.

Protección de información corporativa confidencial La Dir (UE) 2016/943, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas, transpuesta en lo que se refiere a la protección de información corporativa confidencial por la L 1/2019, de **secretos empresariales**, que protege los datos pertenecientes a las corporaciones normalmente desconocidos por la competencia, que, aportando valor empresarial, se suelen mantener razonablemente en secreto. **154**

C. Clasificación de las ciberamenazas

Con independencia de las tipologías penales relacionadas con los ciberdelitos provocados a través de algún tipo de práctica ilícita, los incidentes de seguridad (comúnmente conocidos como «ciberataques») pueden agruparse: **160**

- en función de su objetivo; o
- en función de las características de la amenaza (ver nº 168).

163 **En función del objetivo del ciberataque** Distinguimos los siguientes ciberataques:

A) Contra la **información** (espionaje):

• Acceso a la información (datos de identidad, bancarios, médicos...)

– A datos propios confidenciales.

– A datos ajenos confidenciales (perfil del cliente).

• Revelación (fuga) información.

B) Contra la **integridad** de las redes y sistemas de información:

• Dañado de programas, aplicaciones, páginas webs, datos... (p.e., la realización de una alteración del diseño original de una página web, conocido como *defacement*, al objeto de incluir algún tipo de mensaje reivindicativo. Esta técnica es muy utilizada por organizaciones terroristas y por *hacktivistas*).

• Interrupción de un sistema a través de un ataque de denegación distribuida de servicio (DDoS).

• *Ransomware*.

• *Exploits malwares, rootkits*.

Precisiones Un ejemplo de **ciberataque** contra la integridad de las redes informáticas se produjo en enero de 2010, contra la **página web del Ministerio de la Presidencia** español, que vio alterada su página web con una imagen de Mr. Bean.

164 **C)** Contra la **identidad** de personas:

• Suplantación de identidad digital corporativa (Web, Red social)

• Registro abusivo de nombre de dominio (ver supuesto de *Cibersquatting*: JM Valencia núm 1, 22-5-19, EDJ 659679, caso «Aboga2»).

• *Spoofing*.

D) Contra la **propiedad**:

• Venta de datos robados.

• Robo de propiedad intelectual, industrial (signo distintivo).

• *Phising*, *Pharming*.

E) Contra el **prestigio** de individuos y empresas:

• Reputacionales (prensa, red social, informaciones negativas).

• Información que no desaparece en la red.

165 **F) Otros** riesgos:

• **Internos**:

– Referidos a la propia **entidad o a sus integrantes**: socios, directivos, empleados, etc. con la aparición de agentes internos delatores (*insider*) al albur de cuestiones como la estabilidad laboral, fuga de talentos, etc.

– Infección a través del **Internet de las Cosas**. Con relación a esta tipología y de los problemas de intimidad y privacidad que plantea esta tecnología, en julio de 2020 el Reino Unido prohibió a sus funcionarios tener reuniones en salas en las que hubiera algún tipo de asistente virtual, del tipo Cortana, Siri o Alexa.

• **Externos**:

– Ataques de *hacktivismo* (por desacuerdos respecto de clientes, estrategias o líneas de actuación).

– Acceso de terceros a estrategias propias o ajenas.

168 **En función de las características de la amenaza** La Agencia Europea de la Ciberseguridad (**ENISA**) publica anualmente una relación de las **principales amenazas cibernéticas** que circulan por Internet, en función de una serie de parámetros, tales como su peligrosidad o nivel de incidencia (*Threat Taxonomy report* o taxonomía de las ciberamenazas).

En función de las características de la amenaza, podemos definir los principales riesgos a los que se enfrenta una persona que accede a Internet:

169 **A) Difusión de contenido abusivo:**

• **SPAM**: correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.

• **Delito de odio**: el usuario recibe o tiene acceso a un contenido difamatorio o discriminatorio. Sería el caso del ciberacoso o amenazas dirigidas contra un colectivo concreto.
• **Contenido ilegal o inadecuado**: por ejemplo, la pornografía infantil, entendida como material que represente de manera visual contenido relacionado con imágenes de contenido sexual en las que aparezcan menores de edad; apología de la violencia, etc.

B) Distribución de contenido dañino: **170**
• **Sistema infectado**: sistema infectado con software malicioso o *malware*. La instalación de este tipo de programas pone en peligro la seguridad del dispositivo y de la información que contiene. Por ejemplo: terminal infectado con un *rootkit*.
• **Servidor C (Mando y Control)**: cuando un sistema está infectado por determinado *malware*, un tercero puede tomar el control sobre nuestro sistema o dispositivo, a través de su conexión al servidor de Mando y Control. Así ocurre en el caso de las redes de ordenadores *zombies* o *botnets*.
• **Malware dominio DGA**: esta técnica consiste en crear un nombre de dominio generado mediante un Algoritmo de Generación de Dominio (DGA), que será el empleado por un malware para contactar con un servidor de Mando y Control (C).

C) Obtención ilícita de información: **171**
• **Escaneo de redes** (*scanning*): esta técnica consiste en enviar peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ejemplos: peticiones DNS, ICMP, SMTP, escaneo de puertos.
• **Análisis de paquetes** (*sniffing*): observación y grabación del tráfico de redes.
• **Ingeniería social**: recopilación de información personal o profesional de terceros (p.e., empleados de una organización) empleando la tecnología como canal de comunicación con las víctimas. En esta categoría podríamos incluir el *phishing* o el fraude del CEO.

> Precisiones El **fraude del CEO** tiene como objetivo engañar a empleados que tienen acceso a los recursos económicos para que paguen una factura falsa o haga una transferencia desde la cuenta de la compañía. Para más información, ver nº 2855.

D) Intento de intrusión: **172**
• **Explotación de vulnerabilidades conocidas**: esta práctica consiste en un intento de comprometer un sistema o interrumpir un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado. Como ejemplos de este tipo de prácticas encontramos el «desbordamiento de buffer», «puertas traseras», *cross site scripting* (XSS).
• **Intento de acceso con vulneración de credenciales**: esta técnica consiste en llevar a cabo múltiples intentos de vulnerar credenciales. Este sería el caso de intento de ataque por fuerza bruta o el ataque de diccionario.
• **Ataque desconocido o de día cero** (*0 day*): este es el ataque más temido, ya que se explota una vulnerabilidad no conocida por el sector ni por el mercado, por lo que todavía no existe solución para subsanar tal problema.

E) Acciones de intrusión: **173**
• **Compromiso de cuenta con privilegios**: el objetivo de este tipo de ataque es el de comprometer un sistema con tal de que el atacante pueda adquirir privilegios (permisos).
• **Compromiso de cuenta sin privilegios**: en este caso, el objetivo es el de comprometer un sistema empleando cuentas sin privilegios.
• **Compromiso de aplicaciones**: consiste en comprometer una aplicación mediante la explotación de vulnerabilidades de software. Este sería el caso de un ataque mediante «inyección SQL».
• **Robo**: consiste en una intrusión física. También el robo de dispositivos y terminales se considera como incidente de seguridad, que debe notificarse a la correspon-

diente autoridad de control en el caso de que cumpla con los requisitos establecidos en la Ley.

174 **F) Acciones que ponen en peligro la disponibilidad:**
• **Denegación de servicio** (DoS): consisten en un ataque de denegación de servicio que se lleva a cabo a través de un envío masivo y coordinado de peticiones a un servidor que aloja una aplicación, para provocar intencionadamente la interrupción o ralentización en la prestación del servicio.
• **Denegación distribuida de servicio** (DDoS): ataque de denegación distribuida de servicio.
• **Sabotaje**: acciones de sabotaje físico, que incluyen cortes de cableado o incendios provocados, entre otros.
• **Interrupciones**: interrupciones del servicio normal debido a causas externas, imprevisibles o inevitables. Este podría ser el caso de un desastre natural.

175 **G) Acciones que compromete la información:**
• **Acceso no autorizado a información**: un tercero, sin autorización, accede de manera no consentida a información custodiada por la empresa. Este podría ser el caso de un acceso a través de un robo de credenciales logrado mediante interceptación de tráfico o mediante el acceso a documentos físicos.
• **Modificación no autorizada de información**: un tercero, de manera no autorizada, modifica información custodiada por la empresa.

176 **H) Comisión o intentos de fraude:**
• **Infracción de derechos de autor**: consiste en el ofrecimiento o instalación de software carente de licencia o infringiendo los derechos de autor. Organizaciones tales con la *Business Software Alliance* (BSA) monitorizan la red de cara a localizar organizaciones que utilizan software sin licencia.
• **Suplantación**: se trata de un tipo de ataque en el que una entidad suplanta a otra, con el objetivo de obtener beneficios de forma ilícita.
• **«Phishing»**: suplantación de una persona u organización, usando el engaño con tal de convencer a un usuario para que revele sus credenciales privadas o información de naturaleza privada o confidencial.

177 **I) Aprovechamiento de vulnerabilidades existentes:**
• **Criptografía débil**: se trata de servicios accesibles públicamente, que son vulnerables a accesos externos por carecer de criptografía robusta.
• **Sistema vulnerable**: sistemas no actualizados o con versiones obsoletas o desfasadas, con una deficiente configuración del proxy, etc.

178 **J) Otros:**
• **APT** (*advanced persistant threats*): se trata de ataques dirigidos contra organizaciones concretas, sustentados en mecanismos sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas híbridas en las que mezcla ataques de ingeniería social con el uso de procedimientos originales.
• **Ciberterrorismo**: en este tipo de situaciones se utilizan las redes o los sistemas de información con fines de naturaleza terrorista.

D. Ciberatacantes

185 El Manual de Tallinn del año 2013 incluía una definición de **«hacker»** como a aquella persona que trata de obtener un acceso no autorizado al software y/o al hardware con fines de investigación. Y podemos añadir que puede conseguirlo gracias a su habilidad y altas capacidades técnicas.
Este perfil no debe confundirse con el de aquella persona que utiliza tales habilidades para cometer actos de naturaleza delictiva, y que son comúnmente conocidos como **«crackers»**, *black hat hackers* o **ciberdelincuentes**.

Tipología Podemos distinguir los siguientes tipos de ciberatacantes: **188**

• **Servicios de inteligencia de otros Estados**: en este caso, el origen de la amenaza proviene de organización patrocinadas por un Estado, o bien directamente por los servicios de inteligencia de este, quien tiene interés en obtener algún tipo de información confidencial de otro Estado o secretos industriales de una empresa en particular.

• **Ciberterroristas**: son aquellas personas que llevan a cabo actuaciones ilegales a través de la red con la finalidad de crear confusión e incertidumbre en un Estado o en parte del mismo, con finalidades políticas, económicas o ideológicas. A estos efectos, persiguen promover el miedo y la violencia utilizando internet como canal.

• **Organizaciones criminales**: son grupos de personas que de manera concertada y coordinada se distribuyen distintas funciones al objeto de cometer delitos a través de Internet. Esta estructura de funcionamiento, cada vez más sofisticada (y que en ocasiones funciona como una auténtica estructura empresarial, que ha acuñado el concepto de *Crime As A Service*) viene sancionada en el Código Penal. Los principales objetivos son los de lucrarse con la comisión de delitos utilizando o aprovechándose de Internet.

• **«Hacktivistas»**: se trata de personas u organizaciones que utilizan Internet para difundir mensajes de protesta o reivindicativos.

• **«Script kiddies»**: es un término utilizado para describir a aquellos usuarios más jóvenes que tratan de *hackear* sistemas y redes con tal de demostrar sus habilidades y ganar reputación entre la comunidad hacker. También se utiliza despectivamente para referirse a aquellos usuarios que, al carecer de habilidad para desarrollar sus propios *exploits*, utilizan programas desarrollados por terceros para realizar ataques a sistemas ajenos.

• **«Insider»**: con este término se refieren a aquellas personas, empleados de una organización, que por determinados motivos (descontento, chantaje, soborno, etc.) ayudan a un cibercriminal a infiltrarse en los sistemas de su compañía.

CAPÍTULO 2

Políticas públicas y regulación en materia de ciberseguridad

250

1. Regulación del ciberespacio

255

La sociedad contemporánea ha experimentado en los últimos años un profundo proceso de transformación, en el que todavía estamos inmersos, calificado como **«cuarta revolución industrial»**, que se caracteriza por el impacto de una acelerada transformación tecnológica que ha alcanzado todos los ámbitos de la actividad humana, desde la vida cotidiana hasta los más complejos procesos industriales, económicos o políticos.

Esta transformación social impulsada por la rápida penetración de los cambios tecnológicos nos permite hablar de un **mundo digital** en el que buena parte de las relaciones se desarrollan en un entorno que llamamos ciberespacio, que constituye un mundo virtual construido sobre interconexiones electrónicas en red que permiten posibilidades de interacción inalcanzables en el mundo físico, incluidos el conflicto o el crimen.

En el ciberespacio interactúa casi un 60% de la población mundial, más de 4.500 millones de personas que se relacionan en un **entorno sin fronteras**, que se resiste a cualquier definición con categorías jurídicas tradicionales. Las **redes sociales** reúnen más usuarios que los países más poblados del planeta y empresas que desarrollan toda su actividad en Internet y que hace tan solo unas décadas eran, sencillamente, inconcebibles se sitúan entre las principales compañías del mundo.

En este entorno virtual se desarrolla la comunicación personal y el acceso a información con una velocidad y un alcance sin precedentes, el comercio internacional, los servicios públicos, las relaciones internacionales y también el crimen y la guerra.

Como señala la primera conclusión del «Informe de la Ponencia para el estudio de diversas cuestiones relativas a la ciberseguridad en España», aprobado por la Comisión Mixta de Seguridad Nacional de las Cortes Generales (BOCG núm 277, 13-3-19): «La profundidad y relevancia de los cambios que la disrupción digital está produciendo en los sistemas económicos, los sistemas políticos, los modelos comerciales y, en general, en las relaciones sociales, supone una **transformación integral de la realidad** que conocemos».

258

Concepto de ciberespacio La Estrategia de Seguridad Nacional aprobada por RD 1008/2017 –en adelante, Estrategia de Seguridad Nacional (2017)– describe este entorno afirmando que «el ciberespacio es un **escenario** con **características propias** marcadas por:

- su componente tecnológico;
- fácil accesibilidad;
- anonimidad;
- alta conexión; y
- dinamismo.