

Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

El ecosistema de ciberseguridad nacional y su adaptación a la normativa y estrategias de la UE

Máster Universitario en Dirección TIC para la Defensa

ALUMNO:	Leandro Gobierno López
DIRECTORES:	Aitor Sabino Atorrasagasti Morato
	Isidro Fernández García
	Francisco Javier Rodríguez Rodríguez
CURSO ACADÉMICO:	2023-2024

Universidade Vigo



Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

El ecosistema de ciberseguridad nacional y su adaptación a la normativa y estrategias de la UE

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de la Información

Universidade Vigo

RESUMEN

Este trabajo de fin de máster expone de forma somera el estado de situación global entorno a la ciberseguridad y los elementos esenciales de la misma.

Seguidamente se hace una exposición resumida analítica e interrelacionada de las principales normas, estrategias y estándares en el ámbito internacional, europeo y nacional, que de una forma más o menos directa regulan aspectos de la ciberseguridad.

Todo ello contemplando las diferentes facetas de la ciberseguridad, como la creciente relevancia adquirida en la colaboración público-privada, el engarce de la cibercriminalidad dentro de la ciberseguridad, los nuevos retos y amenazas, así como la especial importancia que adquiere la prevención, protección, recuperación y respuesta de las redes y sistemas de información de las entidades de interés estratégico nacionales, los denominados operadores de servicios esenciales.

Incidiendo en ese último punto, se van a destacar las materias de mayor preeminencia y las novedades establecidas por la reciente Directiva NIS 2 que es la norma nuclear de la ciberseguridad para los estados miembros de la Unión Europea.

PALABRAS CLAVE

Ciberseguridad, estrategias, normas, certificaciones, servicios esenciales, NIS 2.

CONTENIDO

Contenido 3

Índice de Figuras 6

Índice de Tablas....7

1 Introducción....8

1.1 Motivación de este trabajo de fin de máster 8

1.2 Objetivos 8

1.3 Estructura 8

1.4 La revolución de las tecnologías de la información y la comunicación 9

1.5 Concepto de ciberseguridad y aspectos a considerar 10

1.5.1 Definiciones para comprender la ciberseguridad en su conjunto 10

1.5.2 Condicionamientos y aspectos comunes en la regulación de la ciberseguridad....11

1.6 Estadísticas e infografías sobre la situación actual de las tecnologías de la información y la comunicación y la ciberseguridad 13

2 Normas sobre ciberseguridad 18

2.1 Normas internacionales....18

2.1.1 Borrador de las Naciones Unidas de la Convención Internacional amplia contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos 18

2.1.2 Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 .19

2.2 Normas de la Unión Europea 20

2.2.1 Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo 20

2.2.2 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga l Directiva 95/46/CE (Reglamento general de protección de datos) 21

2.2.3 Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación por el que se deroga el Reglamento (UE) 526/2013 (Reglamento sobre la Ciberseguridad)....22

2.2.4 Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales)....23

2.2.5 Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) n 909/2014 y (UE) 2016/1011 (Reglamento DORA)....24

2.2.6 Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en

toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y laDirectiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). Conocida como Directiva NIS 2 26

2.2.7 Reglamento (UE) 2023/588 del Parlamento Europeo y del Consejo de 15 de marzo de 2023 por el que se establece el Programa de Conectividad Segura de la Unión para el período 2023-2027 32

2.2.8 Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión 32

2.2.9 Propuesta del Parlamento Europeo y del Consejo por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos 34

2.3 Normas nacionales 35

2.3.1 Constitución Española 35

2.3.2 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales 36

2.3.3 Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales 36

2.3.4 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico 36

2.3.5 Ley 36/2015, de 28 de septiembre, de Seguridad Nacional 37

2.3.6 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. 37

2.3.7 Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público 38

2.3.8 Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza 38

2.3.9 Ley 11/2022, de 28 de junio, General de Telecomunicaciones 39

2.3.10 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información 39

2.3.11 Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación 44

2.3.12 Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica 45

2.3.13 Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica 45

2.3.14 Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información 46

2.3.15 Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos 51

3 Estrategias sobre ciberseguridad 52

3.1 Estrategias internacionales 53

3.1.1 Organización de Naciones Unidas (ONU).....53
3.1.2 Foro Económico Mundial.....54
3.1.3 Organización para la Seguridad y la Cooperación en Europa (OSCE).....55
3.2 Estrategias de la Unión Europea.....57
3.2.1 Estrategia de ciberseguridad de la UE para la Década Digital.....57
3.2.2 IOCTA 2023.....61
3.3 Estrategias nacionales.....62
3.3.1 Estrategia de Seguridad Nacional 2021.....62
3.3.2 Estrategia Nacional de Ciberseguridad 2019.....64
3.3.3 Estrategia España Digital 2026.....69
3.3.4 Plan Estratégico contra la Cibercriminalidad del Ministerio del Interior.....70
4 Certificaciones de ciberseguridad.....73
4.1 Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad.....73
4.2 ISO/IEC-27001.....75
5 Conclusiones.....78
6 Índice de abreviaturas.....80
7 Bibliografía.....82

ÍNDICE DE FIGURAS

Figura1 Principales ciberamenazas, según el último informe de ENISA de 2022.....14
Figura 2 Porcentaje de ciberincidentes por sectores de 2021 a 2022. 14
Figura 3 Vulnerabilidades de día cero explotadas de a nivel mundial 2012 a 2022 15
Figura 4 Incidentes nacionales de proveedores de servicios digitales en 2022 15
Figura 5 Incidentes nacionales de operadores de servicios esenciales críticos en 2022 16
Figura 6 Incidentes operadores servicios esenciales críticos por sectores en 2022.....16
Figura 7 Ciberdelitos denunciados en España desglosados por tipologías de 2016 a 2022.....17
Figura 8 Principios rectores de la Estrategia Nacional de Ciberseguridad 2019 66
Figura 9 Fases de la ISO/IEC 27001 77

ÍNDICE DE TABLAS

Tabla 1 Sectores de la Directiva NIS 2016/1148 27
Tabla 2 Sectores de la Directiva NIS 2 29
Tabla 3 Comparación de los sectores regulados por la Directiva NIS y por el RD-ley 12/2018.....40
Tabla 4 Autoridades nacionales competentes.....42
Tabla 5 CSIRT nacionales competentes.....43
Tabla 6 Clasificación/Taxonomía de los ciberincidentes.....50
Tabla 7 Ventana temporal de reporte 50

1 INTRODUCCIÓN

1.1 Motivación de este trabajo de fin de máster

En cualquier actividad profesional mínimamente relacionada con las tecnologías de la información y la comunicación (también conocidas como TIC), y más especialmente en el ámbito de la seguridad pública y la seguridad nacional, la necesidad de aplicar estrategias, normas y certificaciones relacionadas con la ciberseguridad resulta fundamental.

Pero esta necesidad se encuentra con el escollo de llegar a conocer no solo qué normas son aplicables, sino cuántas son, hacia donde se dirigen las tendencias de los legisladores, las diferencias entre normas técnicas y certificaciones, hasta qué punto son de obligado cumplimiento los planes estratégicos o como se interrelacionan entre sí.

Y todo ello, teniendo aquí muy presente el artículo 6 de nuestro Código Civil que reza que "la ignorancia de las leyes no excusa de su cumplimiento".

1.2 Objetivos

Este trabajo de fin de máster (de aquí en adelante, TFM) pretende dar respuesta a todas las cuestiones arriba planteadas, para ello se han analizado multitud de normas, estrategias y certificaciones para seleccionar y plasmar aquí todas aquellas que se consideran fundamentales en lo que hemos venido a denominar el ecosistema de la ciberseguridad.

De una forma sistemática el lector va a disponer de todo ese "corpus" tan disperso. Pero no se trata de una mera recopilación, por lo que además va a contar con un análisis específico de todos los aspectos que versan sobre la ciberseguridad en cada una de esas normas, estrategias y certificaciones. Asimismo, se explican las relaciones entre los diferentes preceptos estudiados y los organismos con roles destacados en el ámbito de la ciberseguridad.

Además, dentro de esa exposición sistematizada, a lo largo de todo el documento se presentan de forma diferenciada las normas, estrategias y certificaciones, catalogándolas según pertenezcan al ámbito internacional, europeo o nacional. Ya que, aunque, como se explicará más adelante, una de las tendencias de la ciberseguridad es la homogeneización internacional en el dominio eminentemente digital, se ha de tener en cuenta dentro de ese entorno armonizado la particular idiosincrasia de las jurisdicciones físicas de cada país u organización.

De este modo, se podría entender este TFM como una suerte de guía actualizada para todo aquel que deba conocer los aspectos legales y documentales relacionados con la ciberseguridad sin necesidad de tener conocimientos previos.

Por otro lado, gracias al estudio llevado a cabo para la realización de este TFM se han obtenido unas conclusiones que permiten dar respuesta a uno de los grandes retos en la regulación de la ciberseguridad: cómo adaptar la labor legislativa tradicional, con sus garantías y tiempos considerablemente dilatados, a la necesidad de responder al mundo digital, que evoluciona con gran celeridad.

1.3 Estructura

Este TFM se articula en estos cinco capítulos.

- Introducción: Muestra la necesidad de llevar a cabo este caso de estudio, y da a conocer los elementos básicos que definen y componen la ciberseguridad, así como un somero estudio de situación y los antecedentes a este ecosistema de ciberseguridad actual.

- Normas sobre ciberseguridad: en este TFM se compilan, explican e interrelacionan todos los preceptos legales, con mayor o menor relevancia, para la ciberseguridad en España.

Para una más cómoda comprensión y ordenación de acuerdo con el principio de jerarquía normativa se catalogan en función del ámbito territorial de los organismos que los disponen (ámbito internacional, Unión Europea y normas nacionales).

Entre todas esas normas, hay que destacar por su importancia las encargadas específicamente a la protección de las redes y sistemas informáticos, aglutinadas en la Directiva NIS, Directiva NIS 2, el Real Decreto-ley 12/2018 y el Real Decreto 43/2021.

- Estrategias sobre ciberseguridad: Para lograr una visión global comprensiva de este ecosistema se explican las estrategias sobre ciberseguridad más relevantes, internacionales y nacionales.

Estas estrategias muestran de una forma muy amplia y clara el estado de situación de la ciberseguridad, tras lo cual establecen acciones para responder a los retos detectados. Resultando que en muchas ocasiones son el verdadero motivo de la actividad legislativa, ya que los organismos que las elaboran (la UE, el Gobierno de España, etc.) plasman como líneas de acción la promulgación de normas, que vienen a responder solo a una parte de los retos detectados por esas estrategias.

- Certificaciones de ciberseguridad: el ecosistema de ciberseguridad se fundamenta en sus aspectos más básicos en cuanto a las medidas concretas de seguridad aplicables para dotar a las entidades de herramientas para proteger las dimensiones de la ciberseguridad: la disponibilidad, autenticidad, integridad y confidencialidad.

Para abundar en esta materia se explicarán las certificaciones de mayor implantación, por imperativo legal o de forma voluntaria, en nuestro país, el Esquema Nacional de Seguridad y la serie ISO/IEC-27000.

- Conclusiones: Tras haber puesto de relieve todo lo anterior, estaremos en posición además de obtener unas conclusiones respecto a la regulación del ecosistema mostrado.

1.4 La revolución de las tecnologías de la información y la comunicación

Las tecnologías de la información y la comunicación iniciadas a mediados del siglo XX, están suponiendo un avance vertiginoso en múltiples campos para la humanidad y este avance se está llevando a cabo, no como un mero desarrollo de una ciencia, sino como una verdadera revolución, ya que están efectuando transformaciones profundas en las estructuras y las relaciones sociales de forma perdurable en el tiempo.

Asimismo, dos son los elementos que provocan que esta revolución pueda tener la misma, sino más, relevancia que las revoluciones industriales y sociales acontecidas en los siglos pasados:

- Se está desarrollando de manera global en todos los países del mundo, no solo regionalmente.

- El ritmo de los cambios que las tecnologías de la información y la comunicación ocasionan es sustancialmente más rápido.

Las características particulares de esta revolución conllevan que la regulación de todos sus aspectos sea, como se va a poner de manifiesto a lo largo del presente TFM, de una gran dificultad. A lo que hay que añadir una cuestión que no es baladí, esta revolución dista mucho de haber acabado y estar asentada en el tiempo, por lo que, al estar inmersos en ella, se carece de cierta perspectiva a la hora de afrontar acciones adaptativas o correctoras.

Del mismo modo que hay que entender que esta regulación no se dirige solo a lograr un funcionamiento más idóneo en la sociedad global de las tecnologías de la información y la comunicación, sino que ha de regular las facetas negativas de esta revolución. Hasta mediados del siglo XX la información estratégica de los países, multinacionales o los documentos más preciados y valiosos de los particulares estaba guardada y custodiada en algunos espacios físicos accesibles por unos pocos. En

cambio, con este cambio de paradigma una sola persona de un país en la otra parte del mundo puede acceder indebidamente a esas informaciones en poco tiempo y no solo no ser descubierto, sino en muchos casos, quedar impune a pesar de conocerse su autoría.

Este cúmulo de circunstancias condicionan de tal modo, que la regulación no pueda acometerse desde un punto de vista tradicional. Es necesario afrontar esta desde diferentes jurisdicciones supranacionales y nacionales, así como por distintos órdenes jurisdiccionales y contando en una parte muy relevante con herramientas que parten de la iniciativa privada, como son las certificaciones, ya que sus plazos de implementación son bastante más cortos que la legislación tradicional.

Para tratar de sobreponerse a este escenario es donde están cobrando gran importancia la elaboración y ejecución de estrategias, que analizan las tecnologías de la información y la comunicación desde diferentes ámbitos, estableciendo los estados de situación, retos a los que responder y las medidas para llevarlo a efecto con las herramientas reseñadas más arriba (normas, certificaciones u otras iniciativas), en función del horizonte temporal del que se disponga y la premura para la adopción de medidas.

1.5 Concepto de ciberseguridad y aspectos a considerar

Tras haber puesto sucintamente de relieve la importancia de las tecnologías de la información y la comunicación pasamos a exponer una de sus dimensiones y cuyo desarrollo será el elemento nuclear de este TFM, la ciberseguridad. No obstante, como el resto de las materias de este TFM, se abordará desde un punto de vista normativo y regulatorio, sin entrar a detallar cuestiones tecnológicas de bajo nivel.

1.5.1 Definiciones para comprender la ciberseguridad en su conjunto

Como se verá a lo largo del presente, son multitud las normas, certificaciones, estrategias, iniciativas y órganos los que se encargan de tratar de garantizar la ciberseguridad. Entre todos ellos optamos por recoger estas dos definiciones de las dos normas emanadas de la Unión Europea con mayor preeminencia en el ámbito de la seguridad de las tecnologías de la información y la comunicación.

- Definición de ciberseguridad establecida en el artículo 2.1 del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013; más conocido como Reglamento sobre la Ciberseguridad: "Todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas".

- Definición de seguridad de los sistemas de redes y de información aportada en el artículo 6.2 de la Directiva (UE) 2022/2555 de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión; de aquí en adelante como Directiva NIS 2: "La capacidad de los sistemas de redes y de información de resistir, con un nivel determinado de fiabilidad, cualquier hecho que pueda comprometer la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o de los servicios ofrecidos por tales sistemas de redes y de información o accesibles a través de ellos".

Estas definiciones requieren a su vez que algunos de sus términos más significativos sean explicados, para lo que se acude a las siguientes definiciones referidas en las dos normas antes mencionadas:

- Incidente. También definido en la Directiva NIS 2, artículo 6.6, como "todo hecho que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos". Se valora por el grado de su peligrosidad e impacto.

- Ciberamenaza, según el artículo 2.8 del Reglamento sobre la Ciberseguridad, es cualquier situación potencial, hecho o acción que pueda dañar, perturbar o afectar desfavorablemente de otra manera las redes y los sistemas de información, a los usuarios de tales sistemas y a otras personas.

Por otro lado, para los siguientes términos vamos a recurrir al glosario de la serie de certificaciones ISO/IEC 27000[1], de la que se hablará más adelante:

- Disponibilidad: es, junto a la integridad y confidencialidad, una de las tres dimensiones tradicionales de la seguridad de la información en las tecnologías de la información y la comunicación. Consiste en que la información esté accesible y utilizable cuando lo requiera una entidad autorizada.

- Integridad: la información que obre en los sistemas y se comparta en las redes de comunicación ha sea exacta y completa.

- Confidencialidad: que la información no sea revelada a individuos, entidades o procesos no autorizados.

- Autenticidad: esta es una de las nuevas dimensiones de la información que se están siendo recientemente aceptadas, del mismo modo que la trazabilidad. La autenticidad ya ha sido recogida contemplada en la Directiva NIS 2 y en el Reglamento sobre la Ciberseguridad.

La autenticidad es la garantía de que la entidad emisora de la información, persona física o jurídica es realmente quien es y su identidad no ha sido suplantada.

- Fiabilidad: es la propiedad de que los sistemas y las redes de comunicación se comporten y den unos resultados consistentes previstos.

Tampoco podemos dejar de plasmar aquí, la definición de una de las dimensiones capitales de la ciberseguridad, la ciberdelincuencia o cibercriminalidad, como también es conocida. Esta, aunque ha sido y está siendo permanentemente sujeto de codificación en diferentes normas, no presenta una definición canónica, pese a lo cual la Organización de las Naciones Unidas aporta esta definición[2]: "la ciberdelincuencia es un acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito". Lo que vendría a interpretarse en un lenguaje más coloquial en que la ciberdelincuencia es la comisión de delitos empleando las tecnologías de la información y la comunicación como medio o para atacar los bienes jurídicos que éstas comprenden.

A todo lo anterior hay que añadir los nuevos retos, consustanciales al desarrollo de las tecnologías de la información y la comunicación, que surgen para la ciberseguridad. Podemos resaltar aquí los sistemas de inteligencia artificial (IA), el internet de las cosas (Iota), la tecnología *blockchain*, redes y de comunicaciones de quinta generación (5G), los servicios y el almacenamiento en la nube, etc. Varias de estas tecnologías ya son objeto de regulación, como se verá en el presente, y otras están prontas a ser desarrolladas normativamente, como es el caso de la de inteligencia artificial, por medio de la propuesta de Reglamento del Parlamento Europeo y del Consejo de la Ley de inteligencia artificial que es comentada en este TFM.

1.5.2 Condicionamientos y aspectos comunes en la regulación de la ciberseguridad

Más allá de estas definiciones y términos, hay que tener en consideración otros aspectos esenciales de la ciberseguridad respecto a las tecnologías de la información y la comunicación a la que esta sirve, que afectan sobremanera a la hora de entender esta dentro de ese contexto y sobre todo a la hora de tratar de regularla.

[1] https://www.iso27000.es/glosario.html
[2] https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-in-brief.html

La aportación económica, o de medios personales y materiales, para el desarrollo de proyectos relacionados con las tecnologías de la información y la comunicación se entiende desde el punto del promotor como una inversión que va a producir réditos en un periodo de tiempo estimable.

Sin embargo, en lo que respecta a la implementación de medidas de ciberseguridad ha sido tradicionalmente considerado como poco menos que un obstáculo para esos proyectos o la consecución de los objetivos de la organización ya sea por incrementar el coste y el tiempo de desarrollo de los proyectos, como porque las medidas de seguridad ralenticen y supongan mayor complejidad en la operación y mantenimiento de los sistemas.

No obstante, esta tendencia a denostar, desde esa perspectiva crematística o pragmática, la ciberseguridad en los proyectos y en los ámbitos organizativos donde se aplican las tecnologías de la información y la comunicación está cambiando.

Por una parte, por el incremento de la ciberdelincuencia, que ha supuesto una amenaza para las organizaciones que hace años era residual, tanto por el escaso número de ataques, como por su limitado impacto en los activos digitales. Y por otra, porque el porcentaje de activos de la empresa cuya naturaleza es mayormente digital ha aumentado notabilísimamente.

Las organizaciones se han dado cuenta de que invertir en la seguridad de sus redes y sistemas de las tecnologías de la información y la comunicación, aunque "caro", ciertamente resulta más rentable que afrontar las consecuencias de un ataque o de un evento fortuito pero catastrófico, como puede ser una inundación, incendio, etc.

Asimismo, debido a que esta "cultura de ciberseguridad", como viene siendo conocida la promoción de la implementación de la ciberseguridad en la sociedad, no esté ni mucho menos arraigada, es por lo que las organizaciones con activos digitales se convierten en sujetos obligados a través de mecanismos legales y certificaciones, que tratan de garantizar datos que tras el cambio de paradigma digital del que se ha hablado al inicio del presente.

Tratar de garantizar la seguridad de la información (disponibilidad, autenticidad, integridad y confidencialidad de los datos) de las organizaciones ya no responde únicamente a sus intereses, sino que también ha de comprender a la cantidad ingente de información que estas poseen de sus usuarios, que en muchos casos superan los millones de clientes.

Aquí es donde vuelve a cobrar sentido la supervisión de esas organizaciones por parte de autoridades nacionales e internacionales, de forma que estas puedan comprobar mediante ejercicios, inspecciones, auditorías, etc. que las organizaciones están implementando las medidas de ciberseguridad adecuadas para intentar asegurar la información de esos clientes, ya que su explotación les reporta grandes beneficios, pero las medidas para su seguridad solo costes añadidos.

Otro de los aspectos a considerar son ciertas características comunes que vienen a contemplar los instrumentos regulatorios de la ciberseguridad de las tecnologías de la información y la comunicación.

- La ciberseguridad es un proceso que se aborda a través de diversas fases, que vienen a ser: la prevención, reacción, respuesta y recuperación ante ciberincidentes.

La fase de prevención constituye el primer y más importante paso ya que busca anticiparse a posibles incidentes y minimizar las vulnerabilidades de los sistemas y redes. En esta etapa, se implementan medidas proactivas para reducir el riesgo de incidentes de seguridad mediante la adopción de políticas de seguridad.

A pesar de lo anterior la ciberseguridad total, del mismo modo que la seguridad física, no existe. Por ello la fase de reacción se centra en la detección de incidentes y en la respuesta inmediata ante ellos con medidas de mitigación que limiten su impacto. El rol principal en esta fase es llevado a cabo por los equipos de respuesta a incidentes de seguridad informática, conocidos por sus siglas en inglés como CSIRT.

La fase de respuesta se lleva a efecto tras haberse producido el ciberincidente. Trata de obtener indicios para la acreditar el incidente como un ciberataque y que permita un enjuiciamiento penal.

La última etapa es la de recuperación, que tiene como misión restaurar los sistemas afectados a su estado original y la implementación de medidas correctivas para evitar la repetición de incidentes similares en el futuro.

- Todas las entidades implicadas en la ciberseguridad, como son las autoridades de supervisión, los CSIRT, los sujetos obligados, las fuerzas y cuerpos de seguridad, etc., ven plasmadas en diferentes normas, estrategias y certificaciones la obligación o al menos la promoción o reforzamiento de sus capacidades en materia de ciberseguridad. Estas suponen dotarse de los medios tecnológicos adecuados y el personal con los conocimientos especializados y permanentemente actualizados.

- La coordinación y cooperación, nacional e internacional, entre las entidades implicadas es otra de las piedras de clave en las múltiples normas e iniciativas de ciberseguridad. Estas suelen tener como principal finalidad el intercambio de información, y en menor medida la compartición de capacidades, que de otra forma devendrían inútiles o extemporáneas.

Es una de las formas de tratar de combatir los dos factores más críticos en los ciberincidentes, la velocidad y la deslocalización.

Ante esa velocidad del ataque hay que actuar con urgencia una vez se ha detectado para reducir el impacto en la medida de lo posible. Del mismo modo solicitar ayuda internacional es esencial cuando el atacante y el sistema atacado se encuentran muchas veces en distintos países y afectando por tanto a distintas jurisdicciones.

También esta coordinación persigue la optimización de los canales ya establecidos, tratando de evitar la duplicidad de acciones redundantes innecesariamente.

- Finalmente otras de las cuestiones que siempre se suelen tener en cuenta en estas normas e instrumentos de ciberseguridad es que ante la transversalidad de las tecnologías de la información y la comunicación; donde un único sistema puede implicar a diferentes países, bienes jurídicos y ámbitos sociales y organizativos muy diversos; la norma o instrumento no se circunscriba únicamente así misma ni pretenda ser omnicomprensiva (algo a todas luces demasiado ambicioso e ineficaz), sino que forzosamente se refiera a las normas e instrumentos sectoriales que tratan esas otras materias afectadas.

1.6 Estadísticas e infografías sobre la situación actual de las tecnologías de la información y la comunicación y la ciberseguridad

Se muestran seguidamente algunos datos que ilustran la situación actual de la ciberseguridad a nivel internacional, europeo y en el entorno nacional.



Figura 1 Principales ciberamenazas, según el informe de ENISA de 2022[3]

En esta imagen ENISA destaca en su último informe las últimas amenazas detectadas: el malware, amenazas contras los datos, amenazas usando la ingeniería social, la desinformación, el ransomware, ataques contra la disponibilidad de las redes, ataques de denegación de servicio y ataques a la cadena de suministro.

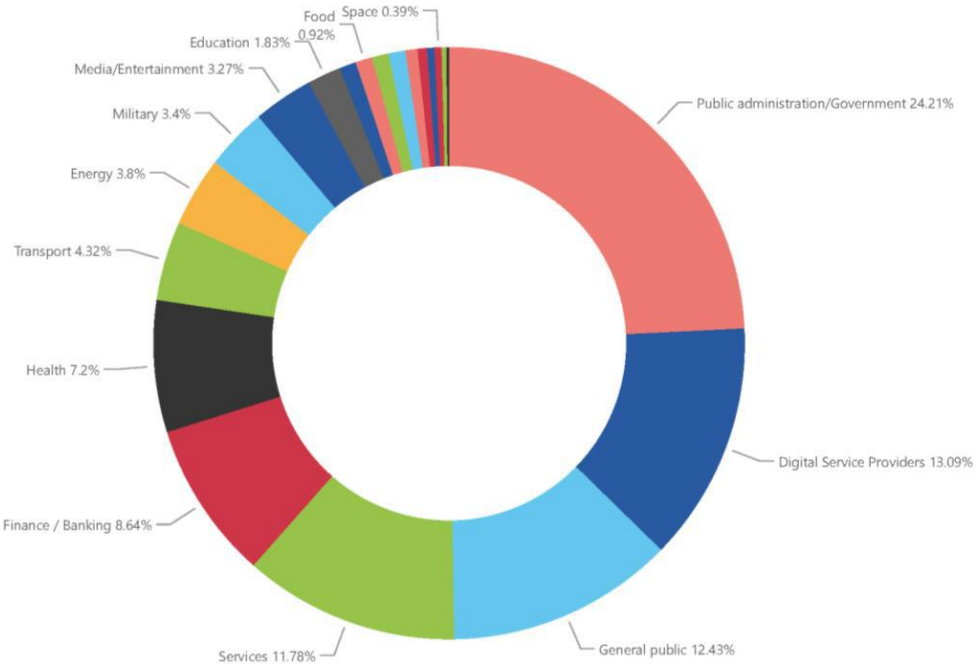

Figura 2 Porcentaje de ciberincidentes por sectores de junio de 2021 a junio de 2022[4]

[3] Fuente: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[4] Fuente: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Aquí ENISA compendia varios sectores en los que los ataques a las administraciones públicas de los estados miembros de la UE promedian más de un 24%, seguidos por un 13% sobre los proveedores de servicios digitales.

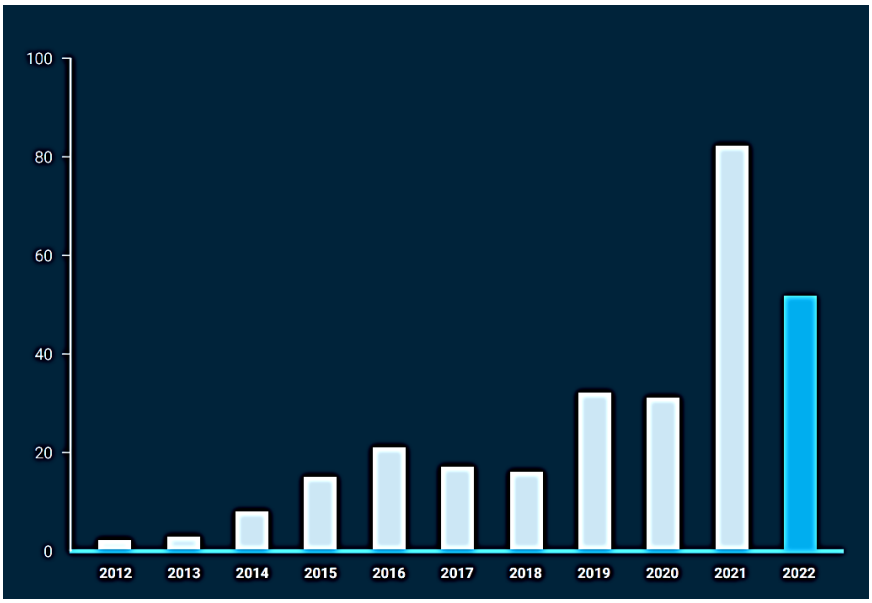

Figura 3 Vulnerabilidades de día cero explotadas de 2012 a 2022 a nivel mundial[5]

Las vulnerabilidades de día cero son aquellas vulnerabilidades de los sistemas y redes que son descubiertas por primera vez por los atacantes, por lo que al poder permanecer ocultas un tiempo prolongado pueden facilitar ataques de un gran impacto. Salvo el descenso en 2022 se aprecia claramente la tendencia ascendente, lo que significa que los ciberdelincuentes se están esforzando en detectar y aprovechar esas vulnerabilidades.

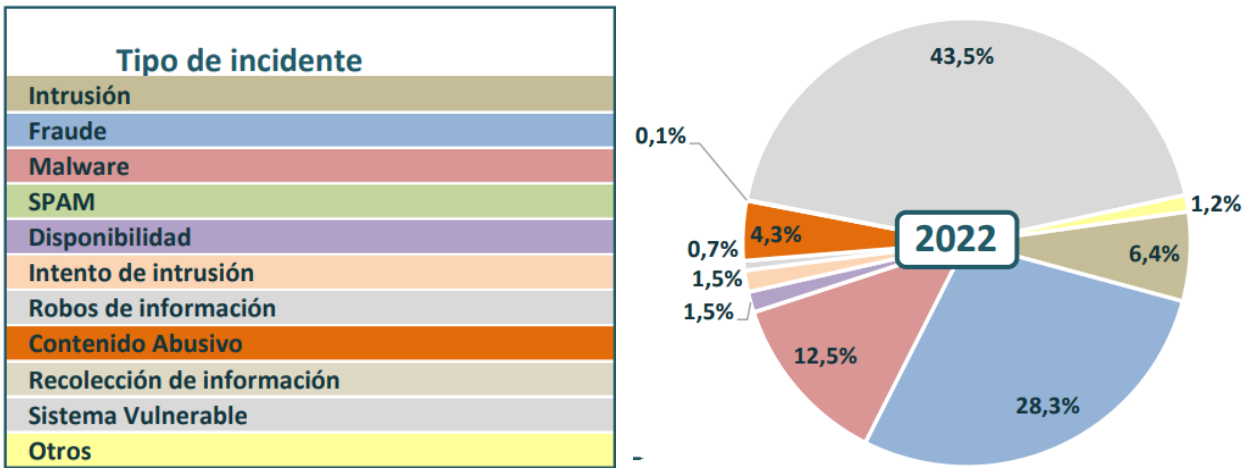

Figura 4 Incidentes nacionales de proveedores de servicios digitales en 2022[6]

[5] Fuente: https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7188-ccn-cert-ia-35-23-ciberamenazas-y-tendencias-edicion-2023/file.html

[6] Fuente:https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2022_126200212.pdf

El INCIBE-CERT muestra en este gráfico que el robo de datos supone el 43,5% de los incidentes padecidos por los proveedores de servicios digitales. Siendo el segundo tipo de incidencia más relevante el fraude, con un 28,3%.

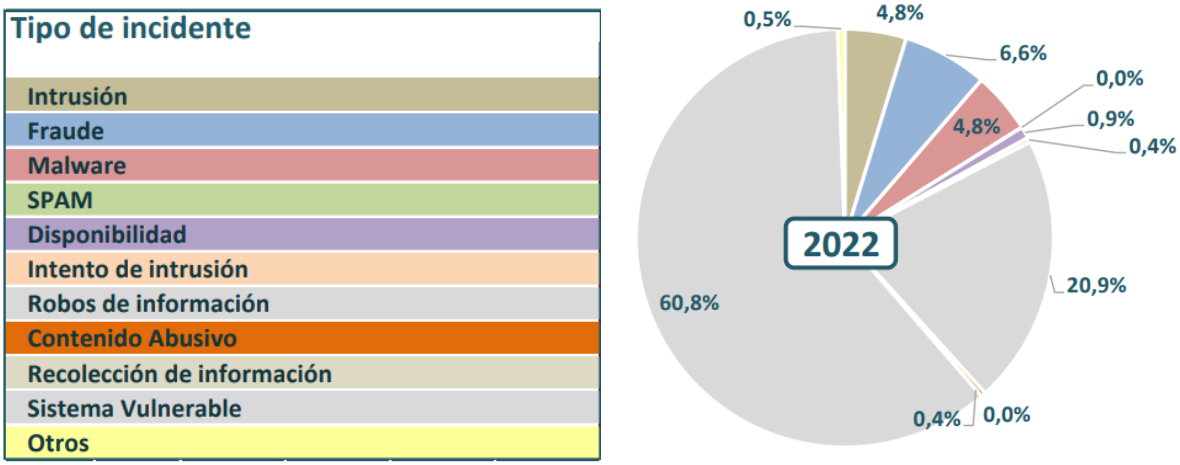

Figura 5 Incidentes nacionales de operadores de servicios esenciales críticos en 2022[7]

En cuando los operadores de servicios esenciales designados críticos, con un nivel de ciberseguridad mucho más maduro que los proveedores de servicios digitales, los ciberdelincuentes se centran más aún en el robo de datos con 60,8% de incidentes y la explotación de vulnerabilidades suponen casi un 21% de los incidentes, lo que indica que un aspecto a reforzar.

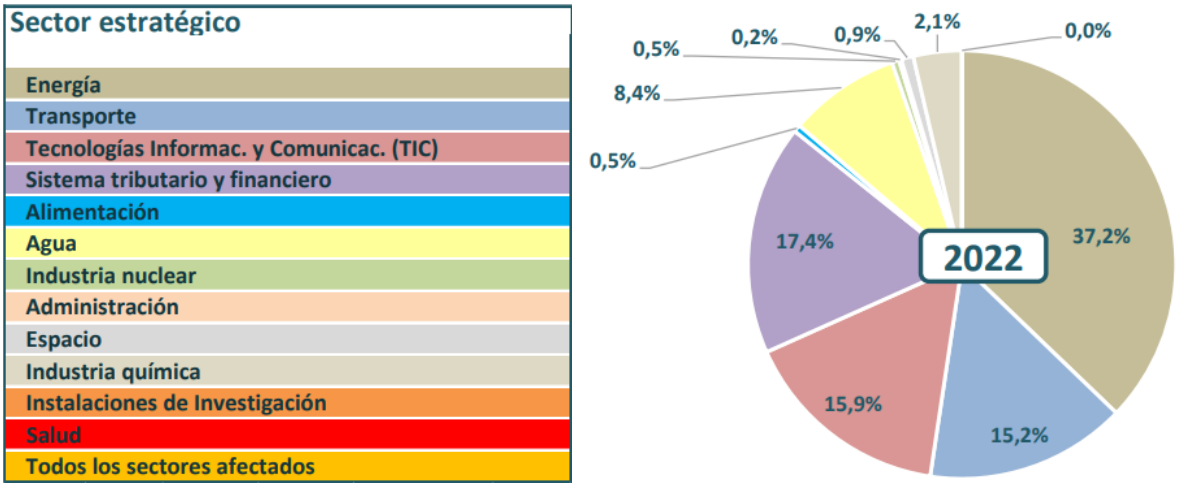

Figura 6 Incidentes de operadores de servicios esenciales críticos por sectores estratégicos en 2022[8]

De los doce sectores estratégicos recogidos en el Real Decreto-ley 12/2018 es el energético el que más incidentes sufre con un 37,2% siendo seguido por el sector financiero y tributario, el de las tecnologías de la información y la comunicación y el de transportes.

[7]Fuente:https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2022_126200212.pdf

[8]Fuente:https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2022_126200212.pdf

HECHOS CONOCIDOS	2018	2019	2020	2021	2022
ACCESO E INTERCEPTACIÓN ILÍCITA	3.384	4.004	4.653	5.342	5.578
AMENAZAS Y COACCIONES	12.800	12.782	14.066	17.319	15.982
CONTRA EL HONOR	1.448	1.422	1.550	1.426	1.191
CONTRA PROPIEDAD INDUST./INTELEC.	232	197	125	137	114
DELITOS SEXUALES(*)	1.581	1.774	1.783	1.628	1.646
FALSIFICACIÓN INFORMÁTICA	3.436	4.275	6.289	10.476	12.569
FRAUDE INFORMÁTICO	136.656	192.375	257.907	267.011	335.995
INTERFERENCIA DATOS Y EN SISTEMA	1.192	1.473	1.590	2.138	1.662
Total HECHOS CONOCIDOS	**160.729**	**218.302**	**287.963**	**305.477**	**374.737**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración

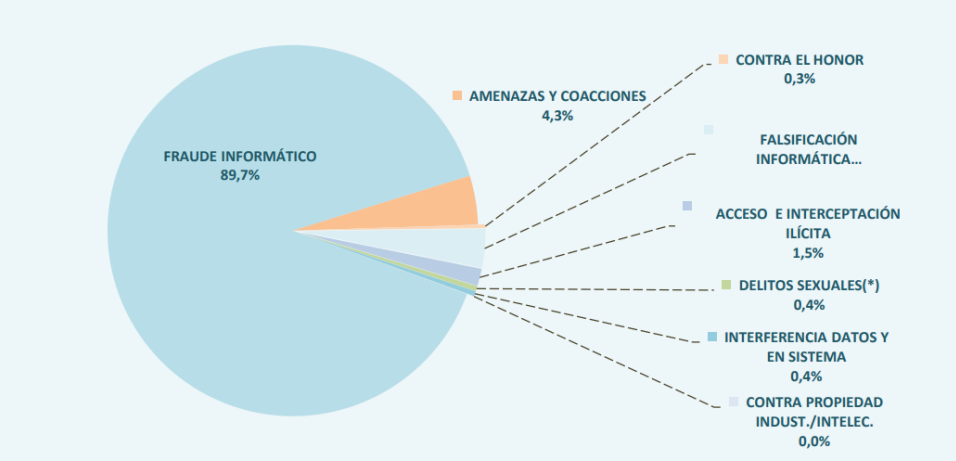

Figura 7 Ciberdelitos denunciados en España desglosados por tipologías de 2016 a 2022[9]

El Sistema Estadístico de Criminalidad del Ministerio del Interior muestra en esta imagen la enorme preponderancia del fraude informático (estafas en el ámbito "cíber") en relación con el resto de ciber delitos y como de 2018 a 2022 estos fraudes se han incrementado un 65%, lo que supone en términos de criminalidad un aumento poco menos que alarmante.

[9]Fuente:https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2022_126200212.pdf

2 NORMAS SOBRE CIBERSEGURIDAD

En este capítulo se van a exponer las múltiples normas sobre ciberseguridad que están en vigor en nuestro ordenamiento jurídico. Algunas son transversales a diferentes ámbitos mientras que otras son mucho más específicas, sectoriales o de naturaleza más técnica. No obstante, para realizar una exposición con un orden sistemático y jerárquico normativamente primero se relacionan las de ámbito internacional, para seguir con las de la Unión Europea y finalmente las nacionales.

2.1 Normas internacionales

En este apartado, es bastante significativo, que mientras sí que hay estrategias y certificaciones a nivel global sobre ciberseguridad, en el rango puramente normativo únicamente hay por el momento dos, y en la vertiente más especializada de la lucha contra la cibercriminalidad, además una de ellas solo se encuentra en estado de desarrollo y negociación.

Esta carencia es una evidencia de las dificultades ya suscritas en la introducción del presente, que se hacen más acuciantes cuanto más amplio es el entorno geográfico y los actores involucrados.

2.1.1 Borrador de las Naciones Unidas de la Convención Internacional amplia contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos

A pesar de ser una norma que aún se encuentra en negociación, por la repercusión que tendrá una vez sea ratificada por todos los estados miembros de las Naciones Unidas, presumiblemente tras su aprobación durante el año 2024, no podíamos dejar al menos de mencionarla.

Este borrador[10], que en muchos aspectos es relativamente similar al Convenio sobre la Ciberdelincuencia de Budapest, del que se hablará en el siguiente apartado, pretende respecto a este último:

- Ampliar el número de estados suscriptores.

- Al abarcar más estados, que en algunos casos pueden considerarse menos garantistas, este borrador está más orientado al respeto de los derechos humanos en la lucha contra el cibercrimen.

- Un mecanismo de revisión más eficaz para adaptarse a los nuevos desafíos y amenazas que plantean las tecnologías de la información y las comunicaciones sin llegar a la complejidad y que requieren los protocolos adicionales.

El borrador define un ámbito de aplicación y unas provisiones generales en su capítulo I con el objetivo de facilitar la investigación y el enjuiciamiento de los delitos cibernéticos internacionalmente, pero sin olvidar el respeto a los derechos humanos.

Por su parte, el capítulo II lista y define un catálogo delitos cibernéticos, tales como como la intrusión en sistemas informáticos, el fraude informático, la pornografía infantil en internet, el ciberacoso, el ciberterrorismo, etc.

El tercer capítulo III recoge, entre otras medidas procesales, medidas para la preservación de las evidencias, su validez probatoria y mecanismos de coordinación y colaboración internacionales.

[10] https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fourth_session/main.html

2.1.2 Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001

El comúnmente conocido como Convenio de Budapest fue elaborado por el Consejo de Europa en 2001. Sin embargo, ha sido suscrito por un número sustancialmente importante de países que no son miembros del Consejo de Europa, siendo en este momento ratificado por sesenta y seis estados[11], entre ellos España, que lo publicó en el BOE el 20 de mayo de 2010, para lo que se vio comprometida a modificar el Código Penal, por medio de la Ley Orgánica 5/2010, de 22 de junio.

El Convenio de Budapest presenta la siguiente estructura:

Capítulo I, definiciones y objetivos. Proporciona una definición clara de ciberdelincuencia y se delinean los objetivos fundamentales destinados a salvaguardar a la sociedad de los delitos perpetrados mediante sistemas informáticos. Asimismo, se marcan los principios para la implementación del convenio.

El capítulo II sobre medidas sustantivas, recoge las medidas los estados firmantes deben asumir para la prevención y persecución de la ciberdelincuencia. Estas medidas comprenden, entre otras, la definición de numerosos delitos informáticos, la adopción de salvaguardas para la protección de datos y la privacidad, y la promoción de la cooperación internacional en la investigación y el enjuiciamiento de los delitos cibernéticos.

Los procedimientos y la cooperación internacional se regulan en el capítulo III. Pudiendo destacar la obtención y traslado de pruebas electrónicas, colaboración a nivel global en la investigación, la extradición de los acusados por los delitos referidos en el capítulo II o la creación de un mecanismo que se ha demostrado muy útil, la Red de puntos de contacto 24/7 para el auxilio en investigaciones y procedimientos penales relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito.

Por último, el capítulo IV contempla las indispensables disposiciones finales para la ratificación del convenio y los procedimientos de revisión y enmienda.

Como se expone en varias ocasiones en el presente, los tiempos manejados por el legislador difieren de los tiempos de evolución de las tecnologías de la información y la comunicación. Siendo conscientes de esta disparidad y la inexcusable necesidad de adaptación de este convenio, se hizo uso de lo previsto en su capítulo V para actualizarlo mediante, por el momento, estos dos protocolos adicionales:

- Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, hecho en Estrasburgo el 28 de enero de 2003.

Este Protocolo adicional fue la respuesta jurídica a la propaganda de índole racista y xenófoba difundida por un mal uso de los sistemas informáticos.

Para ello se elaboró una lista de nuevos tipos penales sobre actos de índole racista y xenófoba cometidos a través de las tecnologías de la información y la comunicación para que tuvieran una correspondencia en todos los países firmantes de este protocolo adicional. Uno de ellos España que modificó de este modo su Código Penal, por medio de la Ley Orgánica 1/2015, de 30 de marzo.

- Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas.

La motivación de este segundo protocolo adicional, aplicable tanto al convenio original como al protocolo anterior, surge de constatar que la obtención y el traslado de evidencias electrónicas (aquellas

[11] https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

necesariamente vinculadas a los delitos con una bis digital) entre los países firmantes era a todas luces ineficaz.

Por ello se reglaron unas medidas de cooperación reforzada para la solicitud de información sobre el registro de nombres de dominio, sobre los abonados de los proveedores de servicio, para la revelación rápida de datos informáticos almacenados en caso de emergencia, así como estandarizar el uso procesal de las videoconferencias y la constitución de equipos conjuntos de investigación e investigaciones conjuntas.

2.2 Normas de la Unión Europea

La Unión Europea es el principal promotor de políticas y estrategias de ciberseguridad para nuestro país, siendo un correcto uso y desarrollo de las tecnologías de la información y la comunicación una de sus mayores inquietudes. De este modo, la Estrategia de ciberseguridad de la UE para la Década Digital, que se trata en el presente TFM, está marcando las pautas para las iniciativas legislativas a llevar a cabo en los próximos años, varias de las cuales ya se han llevado a efecto.

Estas normas dimanantes de la Unión Europea tienen un gran impacto en España debido a su aplicación directa, reglamentos, o por su obligada trasposición a nuestro ordenamiento jurídico, directivas.

Seguidamente se van a exponer los reglamentos y directivas de la UE. Se puede afirmar que estas normas son la parte fundamental de este TFM, ya que por su alcance, relevancia, grado técnico de desarrollo, interrelaciones, organismos que regulan, etc., son la piedra de toque para las normas de ciberseguridad de todos los estados miembros.

Como reflejo de la diversidad de la ciberseguridad expuesta en la introducción, estas normas vienen a regular múltiples aspectos de esta en mayor o menor medida. Asimismo, hay que mencionar que la Directiva NIS 2 supone el núcleo indiscutible de todas esas normas tal y como se verá.

Igualmente es destacable la profusión de recientes reglamentos y directivas y aquellos próximos a aprobarse que es un ejemplo del esfuerzo de la UE en regular adecuadamente las tecnologías de la información y la comunicación y la ciberseguridad en particular.

2.2.1 Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo

Esta directiva aborda la dimensión de la ciberseguridad dedicada a la lucha con la cibercriminalidad. El objeto de la Directiva 2013/40 es aproximar las normas de derecho penal en la UE respecto a los ataques contra los sistemas de información. Para ello, primero, define infracciones penales y sanciones aplicables, y segundo, pretende mejorar la cooperación entre autoridades, incluida la policía y los demás servicios especializados para la aplicación de la ley, así como Eurojust, Europol y la ENISA.

La primera premisa de las definiciones ya se realizó sin mayor incidencia por medio del Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Sin embargo, en lo relacionado con la mejora de la cooperación, que se recoge específicamente en su artículo 13 (intercambio de información), aunque esta norma fue pionera en la Unión Europea, con el tiempo se ha puesto en evidencia que debido a su grado de indefinición, la red de puntos de contacto 24x7 no se está empleando con la operatividad para la que fue planteada, por lo que hay un debate abierto en estos momentos sobre cómo debería coordinarse esta red con otros mecanismos y organismos que comparten el ámbito de actuación similar, como pueden ser la previstas en la reciente Directiva NIS 2 (Red europea de organizaciones de enlace para las crisis de ciberseguridad −EU-CyCLONe− o la Red de CSIRT), la Unidad Cibernética Conjunta, el Centro Europeo de Cibercrimen de Europol (EC3) o la

propia red de puntos de contacto establecida por el Convenio de Budapest sobre la Ciberdelincuencia del Consejo de Europa, al que están suscritos todos los estados miembros.

2.2.2 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Este reglamento vino a derogar la anterior directiva dado que en esos más veinte años el exponencial incremento de los datos introducidos, procesados y difundidos a través de las redes y sistemas, sin olvidar las nuevas circunstancias derivadas de la globalización y los flujos transfronterizos de datos, tratando con ello de reforzar la seguridad jurídica y la transparencia del tratamiento de los datos. Cuya confidencialidad no solo supone una de las dimensiones de la ciberseguridad, sino que está específicamente protegido como derecho fundamental en el artículo 18.4 de la Constitución española como más adelante se relata.

El Reglamento tiene como objeto principal proteger a las personas físicas en lo que respecta al tratamiento de sus datos personales, pero sin obviar otros derechos fundamentales, como la libertad de expresión o de información. Todo ello regulando los aspectos de acceso, tratamiento, rectificación y supresión, estableciendo unas obligaciones para el responsable y encargado del tratamiento de los datos, las funciones de las autoridades de supervisión independientes, etc.

Igualmente mantiene unas garantías para asegurar los tratamientos de datos personales que puedan ser necesarios para fines legítimos, tales como la prevención del fraude.

Uno de los aspectos a reseñar por su relación con otras vertientes más propias de la ciberseguridad son las medidas de seguridad en las redes y sistemas, que impone a los responsables en el tratamiento, en la sección II sobre seguridad de datos personales del capítulo IV.

Otro elemento a tener en cuenta es la promoción a nivel de europeo de mecanismos de certificación en materia de protección de datos, los cuáles han de ser coherentes con otras certificaciones más específicas sobre ciberseguridad que también se están planteando en estos momentos, sobre todo por el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y conforme a lo propuesto por la Directiva NIS 2.

Como se explicará en su apartado correspondiente, el Reglamento general de protección de datos ha sido a su vez complementado a mayores en nuestro ordenamiento por medio de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

En este reglamento se dota de la competencia a la Comisión Europea para adoptar actos delegados, lo que le permite modificar varias disposiciones de esta norma, para que no quede obsoleta y sin que sea necesario iniciar el largo y complejo procedimiento legislativo de la Unión Europea. Esta técnica jurídica es ciertamente adecuada para la regulación de materias relacionadas con las tecnologías de la información y comunicación a tenor de su constante evolución, por lo que por este y otros motivos se aplica en otras normas de la Unión Europea vistas en este TFM, como el Reglamento DORA, la Directiva NIS 2 o el proyecto del Reglamento de la UE de inteligencia artificial.

2.2.3 Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013 (Reglamento sobre la Ciberseguridad)

Esta norma es conocida como el Reglamento sobre la Ciberseguridad, y así consta como tal en el Diario Oficial de la Unión Europea (DOUE) y en nuestro Boletín Oficial del Estado (BOE). Esto da una clara idea de su relevancia para todo el ecosistema de ciberseguridad de la Unión Europea.

Entre otras materias, el Reglamento sobre la Ciberseguridad, aborda dos con más detalle. Por un lado, las funciones, estructura y aspectos organizativos de ENISA, y por otro, establecer el marco necesario para la elaboración de esquemas europeos de certificación de la ciberseguridad. Pero ambos ámbitos comparten el objetivo de garantizar un nivel adecuado de ciberseguridad en la Unión Europea, algo que también recoge en su articulado otra de las normas capitales para la ciberseguridad, la Directiva NIS 2, tan comentada a lo largo del presente.

ENISA lleva a cabo sus cometidos con la sustancial colaboración de los estados miembros, así como del resto de las instituciones, órganos y organismos de la Unión vinculados a la ciberseguridad en mayor o menor medida.

Entre sus muchas tareas, se pueden señalar las de contribuir a la promoción, elaboración y aplicación de políticas y normas de la Unión Europea en el ámbito de la ciberseguridad, destacando especialmente lo relativo a la Directiva NIS 2. Así como asistir a los estados miembros, las instituciones, órganos y organismos de la Unión Europea en sus propias políticas de ciberseguridad (entendiendo estas en su acepción técnica, definida en la ISO/IEC 27001 como "un documento formal que establece los objetivos y principios de la seguridad de la información de una organización").

Engarzando con la otra materia que trata este reglamento, ENISA apoya y promueve el desarrollo y la aplicación de certificaciones de ciberseguridad en toda la Unión Europea. Esta actividad de ENISA respecto a las certificaciones va encaminada a labor crucial para los operadores y usuarios de servicios digitales de evitar la fragmentación actual en la Unión Europea, debida a los múltiples esquemas de certificación de la ciberseguridad para los mismos aspectos en los diferentes estados miembros. Tratando así de conseguir una mayor armonización y coadyuvando a la creación de un mercado único que englobe los productos, servicios y procesos de las tecnologías de la información y la comunicación.

Este marco europeo de certificación de la ciberseguridad, como denomina el propio reglamento establece un procedimiento para la implementación de esquemas europeos comunes de certificación de la ciberseguridad, además de verificar que los productos, servicios y procesos de las tecnologías de la información y la comunicación por esos esquemas cumplen las medidas para proteger la disponibilidad, autenticidad, integridad o confidencialidad de los datos durante todo su ciclo de vida.

Esto último está directamente relacionado con otra norma europea que se espera que sea aprobada en 2024, sobre la que se hace necesario realizar aquí un inciso, la propuesta de Reglamento sobre los requisitos de ciberseguridad de los productos con elementos digitales[12], ya en este estado germinal conocida como la Ley de Ciberresiliencia.

Este borrador de la Ley de Ciberresiliencia tiene como objeto garantizar la ciberseguridad de los productos con cualquier elemento digital (ya sean *software* o *hardware*) por medio de requisitos de diseño, obligando a los fabricantes a aplicar uno de los principios matrices de la ciberseguridad, considerar la seguridad desde el comienzo (*security by design*), determinar procesos de gestión de vulnerabilidades, etc.

[12] https://eur-lex.europa.eu/legal-content/ES/TXT/DOC/?uri=CELEX:52022PC0454

Volviendo al marco europeo de certificación de la ciberseguridad del Reglamento sobre la ciberseguridad, ENISA está facultada para elaborar una propuesta de esquema de certificación o revisar uno ya existente adaptándolo a las consideraciones de la Unión Europea. No obstante, para las certificaciones en sí, esa tarea se adjudica a autoridades nacionales de certificación de la ciberseguridad.

2.2.4 Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales)

Este reglamento viene a paliar en cierto modo la desprotección de los usuarios y a reforzar las capacidades de las fuerzas y cuerpos de seguridad, en el marco de investigaciones judicializadas, y autoridades administrativas ante los grandes proveedores de servicios gestores de las redes sociales y plataformas, que ofertan una multitud de servicios, a los que esta norma define como prestadores de servicios intermediarios y prestadores de plataformas en línea.

Para lograr estas metas este reglamento impone de manera armonizada unas medidas de control, comunicación y colaboración para todos los servicios prestados en la Unión Europea, independientemente de la localización de sus establecimientos físicos o sede social.

Uno de los aspectos más sustanciales es la responsabilidad sobre los contenidos ilícitos que alojan y trasmiten. Entendiendo estos contenidos, conforme a su artículo 3, letra h) como: "toda información que, por sí sola o en relación con una actividad, incluida la venta de productos o la prestación de servicios, incumpla el Derecho de la Unión o el Derecho de cualquier Estado miembro que cumpla el Derecho de la Unión, sea cual sea el objeto o carácter concreto de ese Derecho".

Esta responsabilidad evidentemente no es ilimitada, ya que a estos proveedores no se les puede exigir, ni técnicamente, un conocimiento inmediato de los datos que sus usuarios poseen o comparten a través de sus servicios, ni legalmente, por respeto al derecho fundamental a la intimidad y el secreto de las comunicaciones, una eventual monitorización de datos sin autorización judicial.

Respecto a ese contenido ilícito se fijan mecanismos para su notificación, denuncia, preservación como ulterior medio de prueba, retirada al público y trasmisión en el marco de un procedimiento judicial u ordenado por una autoridad administrativa facultada. España ya disponía en nuestro ordenamiento de esas herramientas, pero los requerimientos adolecían de ser ejecutados con la celeridad y eficacia requerida, algo que esta norma pretende cambiar.

Sin embargo, no hay que olvidar que este Reglamento 2022/2065 está enfocado principalmente hacia la ciberseguridad de los usuarios. Por lo que el legislador europeo consciente, como se ha puesto de relieve al explicar la Estrategia de ciberseguridad de la UE para la Década Digital, de los grandes retos que supone el lograr un elevado nivel común de ciberseguridad en toda la Unión, también cuenta con normas sectoriales que cubren el mismo espectro, y complementan a este reglamento pero desde la vertiente de la lucha contra la cibercriminalidad, las cuales solo paso a mencionar por ser de un carácter eminentemente procesal penal que nos desviaría de la materia objeto en este trabajo:

- Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales.

- Directiva 2011/99/UE, de 13 de diciembre de 2011, del Parlamento Europeo y del Consejo, sobre la orden europea de protección. Traspuesta en nuestro ordenamiento por la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea.

- Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal. Traspuesta por la Ley 3/2018, de 11 de junio, por la que se

modifica la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, para regular la Orden Europea de Investigación.

Volviendo al contenido material del Reglamento 2022/2065, también resulta significativo que este modula sus medidas de aplicación a los prestadores atendiendo a su diferente tamaño llegando a distinguir entre microempresas, pequeñas empresas, plataformas en línea de muy gran tamaño y motores de búsqueda en línea de muy gran tamaño.

Además de lo anterior, los ciudadanos pasan a beneficiarse de una mayor transparencia por parte de los prestadores de plataformas en línea que utilicen sistemas de recomendación que han de informar en sus condiciones generales, de forma clara y comprensible, de los parámetros empleados utilizados en sus sistemas de recomendación y posibilitar a los usuarios a modificar esos parámetros.

Por su parte, los prestadores de plataformas en línea de muy gran tamaño o de motores de búsqueda en línea de muy gran tamaño que muestren publicidad han de mostrar en un repositorio toda la información en relación al contenido del anuncio, la persona física o jurídica que se publicita, el número total de destinatarios del servicio alcanzados, etc.

Para todo lo anterior, y sin perjuicio de lo ya comentado de la jurisdicción procesal, esta norma establece que haya autoridades nacionales competentes para la supervisión de su ejecución y en el caso de detectar infracciones, incoar procedimientos sancionadores.

2.2.5 Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011 (Reglamento DORA)

Como viene siendo ya algo habitual con otras normas de la Unión Europea este reglamento es más conocido por el acrónimo de sus términos en ingles más relevantes, en este caso se suele referir a él como Reglamento DORA (*Digital Operational Resilience Act*).

Un elemento fundamental para comprender esta norma y su alcance, y por eso se recoge al principio de su articulado es que es un acto jurídico sectorial respecto a la Directiva NIS 2. Esto supone que se aplica siguiendo el principio básico del Derecho Continental de *lex specialis derogat legi generali*. Por tanto, el Reglamento DORA se aplicará en defecto de la Directiva NIS 2 en los aspectos que regulen ambas normas conjuntamente. No obstante, en aras de la eficiencia y evitar duplicidades, la cooperación recíproca con las estructuras y autoridades establecidas por la Directiva NIS 2 también viene explicitada en ambas normas.

El Reglamento DORA responde a la especial compleja y extendida implementación de la digitalización en el sector financiero, que lo hace más susceptible a los riesgos de ciberseguridad que otros sectores recogidos en la Directiva NIS 2, y por tanto mucho más necesitado de un nivel de resiliencia adecuada.

Esta norma determina requisitos uniformes relativos a la seguridad de las redes y los sistemas de información que articulan todo el funcionamiento de las entidades financieras, pero lo hace siguiendo un principio de proporcionalidad teniendo en cuenta su tamaño. Esta adaptación de las medidas impuestas a las distintas características de los sujetos obligados ya se recoge en otras normas de la Unión Europea, como el Reglamento de Servicios Digitales o la Directiva NIS 2, de forma que la ciberseguridad, aun siendo totalmente necesaria, no suponga una carga excesiva para los operadores y merme el mercado único.

Esos requisitos a cumplir por las entidades financieras se aglutinan en estos capítulos.

- Gestión del riesgo relacionado con las tecnologías de la información y la comunicación:

En él se establece un marco de gestión del riesgo relacionado con las tecnologías de la información y la comunicación, determinando que las entidades cuenten al menos con estrategias de resiliencia operativa digital, políticas, procedimientos, protocolos y herramientas de las tecnologías de la información y la comunicación para la protección de todos sus activos.

Este marco se orienta a las diferentes fases de la ciberseguridad, partiendo lógicamente la identificación de los activos y sus riesgos y amenazas inherentes, para seguidamente, establecer las medidas para su protección, prevención de riesgos, la detección de las amenazas, respuesta ante los incidentes y finalmente la recuperación hasta el restablecimiento total de las redes y sistemas que se hubieran vistos afectados por esos eventuales incidentes.

Además, como un concepto capital de la resiliencia, las entidades han de recopilar información sobre vulnerabilidades, ciberamenazas y ciberincidentes para su proceso constante de mejora continua.

Asimismo, contarán con planes de comunicación de crisis, sin perjuicio de las imperativas notificaciones a las autoridades, para la divulgación responsable de determinado tipo de incidentes o vulnerabilidades a clientes, contrapartes y al público en general.

- Gestión, clasificación y notificación de incidentes relacionados con las tecnologías de la información y la comunicación:

Mientras que el capítulo anterior está fundamentalmente orientado a la prevención, este establece de qué forma las entidades financieras afectadas han de clasificar el ciberincidente padecido; contemplando como parámetros el número de clientes afectados, la duración del incidente, la pérdida de datos, carácter esencial de los servicios afectados, etc. Así como, los plazos y procedimientos en la notificación de esos incidentes a las autoridades competentes, de forma que estas puedan llevar a efecto sus labores de supervisión, que incluyen el asesoramiento, medidas correctoras y el seguimiento posterior.

La obligación de notificar incidentes resulta de capital importancia, pues se ha constatado como históricamente las entidades que han sufrido ciberincidentes, en gran medida no comunicaban ni a las autoridades ni a sus clientes estos hechos para evitar los perjuicios aparejados al daño reputacional por fallar sus sistemas de seguridad. Esto se ha solventado al añadir, esta y otras normas como la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo 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, de aquí en adelante Directiva NIS, y por supuesto más aún la NIS 2, estas obligaciones, que en el caso de no cumplirse pueden suponer una sanción.

- Pruebas de resiliencia operativa digital:

Con la misma finalidad, pero distinto objeto, que las pruebas de resiliencia puramente financieras se diseñan los programas de estas pruebas de resiliencia operativa digital, para que las autoridades competentes puedan valorar el grado de preparación para gestionar ciberincidentes, detectar debilidades y en caso de ser necesario, aplicar medidas correctoras.

- Gestión del riesgo relacionado con las tecnologías de la información y la comunicación derivado de terceros:

Esta gestión de riesgos es más amplia que otra, que ha adquirido mucha visibilidad tras la crisis del Covid 19, la de los riesgos inherentes a la cadena de suministro de tecnologías de la información y la comunicación. Para esta gestión de riesgos con terceros, el Reglamento DORA impone unas cláusulas contractuales fundamentales a suscribir entre las entidades financieras y esos terceros.

El adecuado cumplimiento de todos los preceptos definidos en estos capítulos no puede dejarse al albur de la voluntad de las entidades, a sabiendas de que esas medidas de ciberseguridad suponen un coste nada desdeñable y que su fallo conlleva el ya comentado daño reputacional. Por este motivo las autoridades competentes supervisoras de cada estado miembro para este reglamento poseen las facultades de inspección, dictar instrucciones y medidas correctoras, dirigir las pruebas, etc. Y en el caso

de detectarse las infracciones previstas para el incumplimiento del reglamento, imponer sanciones administrativas, sin perjuicio de la posible responsabilidad penal.

2.2.6 Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). Conocida como Directiva NIS 2

La Directiva NIS 2 es considerada la norma más importante aplicable en Europa en relación a la ciberseguridad por su visión y alcance, lo cual no es poco teniendo en cuenta el cuantioso número de normas analizadas en todo este trabajo.

Esta directiva ha supuesto un salto cualitativo y cuantitativo en relación a su antecesora y a la que ha derogado, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, 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, mucho más conocida como Directiva NIS (por sus siglas en inglés, *Network Information Systems*).

Por tanto, para poder comprender la relevancia de la Directiva NIS 2 primero hay que explicar someramente el contenido de la Directiva NIS y las conclusiones que se obtuvieron tras su trasposición por los estados miembros.

La Directiva NIS tenía el más que ambicioso y complicado objetivo de garantizar un elevado nivel común de seguridad de las redes y sistemas de información en toda la Unión Europea. Con esto en mente, el legislador europeo estableció un marco basado en estos pilares:

- Operadores de servicios esenciales y proveedores de servicios digitales:

Para poder manejar a todo el ámbito de aplicación, esta norma define y determina que todos los sujetos obligados, por tener una parte sustancial de su actividad relacionada con las tecnologías de la información y la comunicación, se identifican y diferencian en dos categorías. La de operadores de servicios esenciales y la de proveedores de servicios digitales.

Como las definiciones para estos dos términos eran intencionadamente abiertas para facilitar su dispar trasposición por los estados miembros, recurrimos aquí a las efectuadas por la trasposición española, de la que se habla en su apartado correspondiente, por medio del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información:

- Servicio esencial: servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de redes y sistemas de información.

- Servicio digital: servicio de la sociedad de la información entendido en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico[13].

[13] a) "Servicios de la sociedad de la información" o "servicios": todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

Siendo ambas definiciones complementadas en cuantos sus operadores por estas otras dos del mismo RD-ley 12/2018:

- Operador de servicios esenciales: entidad pública o privada que se identifique considerando los factores establecidos en el artículo 6 de este real decreto-ley, que preste dichos servicios en alguno de los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril.
- Proveedor de servicios digitales: persona jurídica que presta un servicio digital.

Esta diferenciación tiene como finalidad modular con más facilidad los requisitos de ciberseguridad y notificación de incidentes exigibles a las dos categorías. Además, los servicios esenciales se dividen en sectores y subsectores, de tal modo que las autoridades nacionales puedan ejercer de forma eficaz sus funciones de supervisión sobre estos servicios de mayor importancia para los estados miembros.

Sectores Directiva NIS
1. Energía
2. Transporte
3. Banca
4. Infraestructuras de los mercados financieros
5. Sector sanitario
6. Suministro y distribución de agua potable
7. Infraestructura digital

Tabla 1 Sectores de la Directiva NIS 2016/1148

- Requisitos en materia de seguridad y notificación de incidentes:

Como ya se ha mencionado más arriba estos requisitos son de diferente rigurosidad en función de que sean servicios esenciales o servicios digitales.

La responsabilidad de implementar las medidas técnicas y de organización para gestionar los riesgos son de los operadores, pero con una supervisión, asesoramiento y directrices por parte de las autoridades, que pueden realizar auditorías, inspecciones y en su caso, sancionar ante incumplimientos reflejados como infracciones en las trasposiciones nacionales.

- Autoridades nacionales competentes y Equipos de respuesta a incidentes de seguridad informática (CSIRT):

Ambos se complementan y coordinan para dar cumplimiento en lo establecido en la directiva, pero las autoridades con un carácter más estratégico, con potestades de control y sanción, mientras que los CSIRT tienen como función la gestión de incidentes y riesgos de los operadores de servicios esenciales y proveedores de servicios digitales.

1.º La contratación de bienes o servicios por vía electrónica.
2.º La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
3.º La gestión de compras en la red por grupos de personas.
4.º El envío de comunicaciones comerciales.
5.º El suministro de información por vía telemática.
No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes: (…)

Además, entre las autoridades nacionales designa un punto de contacto único que garantice algo tan importante para la ciberseguridad como es la cooperación internacional, en este caso entre las autoridades de otros estados miembros y el Grupo de cooperación NIS.

- Estrategia nacional de seguridad de las redes y sistemas de información:

Como ya se refirió en el apartado sobre la Estrategia Nacional de Ciberseguridad 2019, la promoción de la realización de esa estrategia partió de la directiva NIS, que fija como elementos comunes para todo los estados miembros que se ha de contar un marco de gobernanza para asegurar el cumplimiento de los objetivos y las prioridades de la estrategia, programas de educación y concienciación para toda la sociedad, identificar las medidas para sobre preparación, respuesta y recuperación, planes de evaluación de riesgos, etc.

- Grupo de Cooperación NIS y Red de CSIRT:

A mayor abundamiento de las funciones del punto de contacto único por cada país, para darle la esencial perspectiva internacional, la cooperación, homogeneización de criterios, puestas en común de problemas, análisis e iniciativas, así como la asistencia técnica extranjera se produce por medio del Grupo de Cooperación NIS (compuesto por representantes de los estados miembros, la Comisión y la ENISA y por la Red de CSIRT, que está a su vez formada por representantes de los CSIRT de los Estados miembros).

Una vez pasados unos pocos años de la entrada en vigor de la Directiva NIS, y menos aún de las normas nacionales que la traspusieron, el estudio de situación por parte de la Comisión Europea, a través del Grupo de Cooperación NIS, ENISA y otros actores, puso de relieve estas circunstancias:

- La ya consabida vertiginosa evolución de la tecnología que da soporte a las redes y sistemas va de la mano a la aparición de vulnerabilidades que no dejan de ser aprovechadas por los atacantes. Además de evidenciarse que otros desafíos novedosos no habían podido ser contemplados en ese momento por su escaso desarrollo, como la inteligencia artificial o las redes 5G.

Este anacronismo provocaba un inadecuado nivel de ciberresiliencia en las empresas y organismos públicos de la Unión Europea.

- La Directiva NIS dejó un margen amplio a los estados miembros en la identificación de sus sujetos obligados (operadores de servicios esenciales y los proveedores de servicios digitales) y en obligaciones sobre los requisitos en materia de seguridad y notificación de incidentes que debían cumplir.

Como consecuencia, se dio una gran disparidad entre las trasposiciones, en las que algunos países solo tenían poco más de una decena de operadores de servicios esenciales y otros varios centenares. Lo que añadido a los diferentes niveles de exigencia sobre sus medidas de seguridad provocó la fragmentación del mercado interior de la Unión Europea y una ciberresiliencia conjunta deficiente.

- También se puso de relieve, y más aún a raíz de las consecuencias de la pandemia del Covid 19, que los siete sectores identificados inicialmente eran a todas luces insuficientes.

- Otra de las lagunas que se detectó fue la ausencia de mecanismos de respuesta conjuntos y coordinados en caso de crisis de ciberseguridad que trascendieran a la jurisdicción territorial de un estado miembro.

Por estos y otros motivos, se actualiza la Directiva NIS por la NIS 2 en “solo” seis años, lo que en tiempos tradicionales legislativos es un logro, pero que para los tiempos “cíber” son décadas.

Para aportar una simple una idea de la envergadura de los cambios operados, solo hay que reparar en que el articulado pasa de 27 a 46 artículos.

Seguidamente pasamos a analizar cómo la Directiva NIS 2 ha dado repuesta a esas carencias de la Directiva NIS resaltadas más arriba y otros aspectos novedosos que ha incluido *ex novo*:

- Los sectores de aplicación pasan de siete a dieciocho, pero catalogados como de alta criticidad, en el anexo I, y otros sectores críticos, en el anexo II.

Sectores de alta criticidad. Anexo I NIS 2	Otros sectores críticos. Anexo II NIS 2
Energía	Servicios postales y de mensajería
Transporte	Gestión de residuos
Banca	Fabricación, producción y distribución de sustancias y mezclas químicas
Infraestructuras de los mercados financieros	Producción, transformación y distribución de alimentos
Sector sanitario	Fabricación
Agua potable	Proveedores de servicios digitales
Aguas residuales	Investigación
Infraestructura digital	
Gestión de servicios de tecnologías de la información y la comunicación (de empresa a empresa)	
Administración	
Espacio	

Tabla 2 Sectores de la Directiva NIS 2

- La Directiva NIS 2 establece un criterio básico mínimo (hay que recordar que rige el principio de armonización mínima en la trasposición) para todos los estados miembros para la identificación de las entidades que son objeto de aplicación de la norma.

Se aplica a las entidades públicas o privadas consideradas medianas empresas conforme al artículo 2[14] del anexo de la Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas[15] (Recomendación 2003/361/CE), que estén a su vez comprendidas en los anexos I o II.

Por otro lado, también es de aplicación independientemente de su tamaño para las entidades en los sectores del anexo I y II si:

- Los servicios son prestados por proveedores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles para el público,

[14] Artículo 2:

"Los efectivos y límites financieros que definen las categorías de empresas

1. La categoría de microempresas, pequeñas y medianas empresas (PYME) está constituida por las empresas que ocupan a menos de 250 personas y cuyo volumen de negocios anual no excede de 50 millones de euros o cuyo balance general anual no excede de 43 millones de euros.

2. En la categoría de las PYME, se define a una pequeña empresa como una empresa que ocupa a menos de 50 personas y cuyo volumen de negocios anual o cuyo balance general anual no supera los 10 millones de euros.

3. En la categoría de las PYME, se define a una microempresa como una empresa que ocupa a menos de 10 personas y cuyo volumen de negocios anual o cuyo balance general anual no supera los 2 millones de euros".

[15] https://www.boe.es/buscar/doc.php?id=DOUE-L-2003-80730

prestadores de servicios de confianza o registros de nombres de dominio de primer nivel y proveedores de servicios de sistema de nombres de dominio.

- La entidad sea el único proveedor en un Estado miembro de un servicio esencial para el mantenimiento de actividades sociales o económicas críticas.
- Una perturbación del servicio prestado por la entidad pudiera tener repercusiones significativas sobre la seguridad pública, el orden público o la salud pública.
- Una perturbación del servicio prestado por la entidad pudiera inducir riesgos sistémicos significativos, en particular para los sectores en los que tal perturbación podría tener repercusiones de carácter transfronterizo.
- La entidad sea crítica a la luz de su importancia específica a nivel nacional o regional para el sector o tipo de servicio en concreto o para otros sectores interdependientes en el Estado miembro.
- La entidad sea una entidad de la administración pública central, o regional si presta servicios cuya perturbación podría tener un impacto significativo en actividades sociales o económicas críticas.
- Entidades que se identifiquen como entidades críticas con arreglo a la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo.
- Entidades que presten servicios de registro de nombres de dominio.

- A su vez, los tipos de entidades, que pasan de denominarse operadores de servicios esenciales y los proveedores de servicios digitales a entidades esenciales e importantes, respectivamente, se categorizan conforme a estos criterios bastante reglados:

Entidades esenciales:

- De los sectores del anexo I superiores a las medianas empresas[16].
- Prestadores cualificados de servicios de confianza y registros de nombres de dominio de primer nivel y proveedores de servicios de DNS, independientemente de su tamaño.
- Proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles para el público consideradas medianas empresas[17].
- Entidades de la Administración pública central.
- Otras comprendidas en los anexos I o II que el estado identifique como esencial según el artículo 2, 2, letras b) a e)[18].
- Identificadas como entidades críticas con arreglo a la Directiva (UE) 2022/2557.
- Si lo dispone el estado, las entidades identificadas antes del 16 de enero de 2023 como operadores de servicios esenciales.

[16] Artículo 2 del anexo de la Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas

[17] Artículo 2 del anexo de la Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas

[18] *"b) la entidad sea el único proveedor en un Estado miembro de un servicio esencial para el mantenimiento de actividades sociales o económicas críticas;*

c) una perturbación del servicio prestado por la entidad pudiera tener repercusiones significativas sobre la seguridad pública, el orden público o la salud pública;

d) una perturbación del servicio prestado por la entidad pudiera inducir riesgos sistémicos significativos, en particular para los sectores en los que tal perturbación podría tener repercusiones de carácter transfronterizo;

e) la entidad sea crítica a la luz de su importancia específica a nivel nacional o regional para el sector o tipo de servicio en concreto o para otros sectores interdependientes en el Estado miembro".

Entidades importantes: de los sectores de los anexos I o II no consideradas esenciales y las que el estado miembro identifique como entidades importantes según el artículo 2, 2, letras b) a e).

- La Directiva NIS 2 incrementa notablemente los objetivos, funciones de las estrategias nacionales de ciberseguridad de las autoridades competentes y de los CSIRT. Lo que supone de facto aumentar las capacidades de estos organismos.

De forma paralela también aumentan considerablemente las obligaciones para establecer y mantener unas adecuadas medidas para la gestión de riesgos de ciberseguridad por parte de las entidades esenciales e importantes.

- La gestión de las crisis de ciberseguridad, tanto nacionales o que afecten a varios miembros, adquieren una importancia sustancia.

A nivel nacional determinando que se haya unos marcos de gestión de crisis de ciberseguridad con planes nacionales de respuesta a incidentes y crisis de ciberseguridad a gran escala.

Cuando estas crisis trasciendan el ámbito nacional, y dando cumplimiento a la Recomendación (UE) 2017/1584 de la Comisión, de 13 de septiembre de 2017, sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala[19] es para lo que se crea la Red europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLONe).

El EU-CyCLONe tiene entre otros cometidos, establecidos en el artículo 16.1, el de: "respaldar la gestión coordinada de los incidentes y las crisis de ciberseguridad a gran escala en el ámbito operativo y de garantizar el intercambio regular de información relevante entre los estados miembros y las instituciones, los órganos y los organismos de la Unión".

- Otra de las disfunciones que la Directiva NIS 2 trata de paliar son los riesgos de las cadenas de suministro de las entidades esenciales e importantes. Estos riesgos van desde las dependencias críticas, puntos únicos de fallo, vulnerabilidades hasta las posibles influencias indebida de terceros países.

Como contramedida, se fija la protección de estas cadenas de suministro como una prioridad para las estrategias nacionales de ciberseguridad, que incluyan planes de mitigación y de mejores prácticas. Además de como una parte fundamental en las medidas para la gestión de riesgos de ciberseguridad, que las entidades han de implementar y las autoridades supervisar.

- El impacto que tiene para la ciberseguridad de las redes y sistemas la explotación maliciosa de las vulnerabilidades era otra de las cuestiones que ha sido revisada. Para disminuir su afectación se determina que la divulgación coordinada vulnerabilidades sea otro de los objetivos a realizar por las estrategias nacionales de ciberseguridad, y que se realice esta tarea por medio de los CSIRT.

Asimismo, para alcanzar la utilidad demandada estas divulgaciones se coordinarán a nivel europeo por la Red de CSIRT y con el apoyo del Grupo de Cooperación NIS para confeccionar una base de datos europea de vulnerabilidades.

- En el afán de mejora continua para alcanzar el elevado nivel común de ciberseguridad tan preconizado por la Unión Europea, la Directiva NIS 2 propone un mecanismo voluntario de revisión interpares.

La finalidad es que mediante la revisión por expertos de otros estados miembros de aspectos de nacionales de ciberseguridad se coadyuve a obtener experiencias compartidas, reforzar la confianza mutua y mejorar las capacidades y políticas de ciberseguridad.

- Por último, cabría destacar que la Directiva NIS 2, con su carácter transversal está obligada a cumplirse, a través de sus trasposiciones nacionales, de forma coordinada con otras normas europeas con objetos de aplicación solapados, como son los datos personales, la protección de las infraestructuras críticas o la ciberseguridad del sector financiero.

[19] https://www.boe.es/buscar/doc.php?id=DOUE-L-2017-81864

Con esta finalidad de asegurar la ausencia de lagunas legales, evitar duplicidades y cargas excesivas (tanto para los sujetos obligados como para las autoridades, CSIRT, etc.), la propia Directiva NIS 2 deja claro a lo largo de todo el articulado de qué forma ha de coordinarse con:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo.
- Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011.

2.2.7 Reglamento (UE) 2023/588 del Parlamento Europeo y del Consejo de 15 de marzo de 2023 por el que se establece el Programa de Conectividad Segura de la Unión para el período 2023-2027

Este programa está dirigido a garantizar a los usuarios autorizados de la Administración el acceso a escala mundial de comunicación por satélite seguros, fiables y rentables, y, al mismo tiempo, evitando la dependencia de soluciones ajenas a la UE, en especial para las infraestructuras críticas y el acceso al espacio.

Asimismo, entre los objetivos específicos del programa se encuentran estos, con especial relevancia para ciberseguridad:

- Mejorar la resiliencia y seguridad de los servicios de comunicación de la UE y de los estados miembros.

- Seguir desarrollando e integrando la Infraestructura Europea de Comunicación Cuántica (EuroQCI) en el sistema de conectividad segura.

EuroQCI se está desarrollando como canal de comunicación cuántico seguro de extremo a extremo para transmitir y almacenar información y datos por toda la Unión.

- Aumentar la ciberresiliencia de la UE por medio de la redundancia, la ciberseguridad y otras medidas contra amenazas electromagnéticas.

Ante los eventuales riesgos para la UE y sus estados miembros en la ejecución del programa, la seguridad de los sistemas y servicios implantados se ha de llevar a cabo una acreditación de seguridad por el Consejo de Acreditación de Seguridad establecido en la Agencia de la Unión Europea para el Programa Espacial.

2.2.8 Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión

Este proyecto de reglamento europeo pretende adelantarse a un fenómeno que en el último año ha adquirido unas dimensiones, por su uso generalizado y por su vertiginoso desarrollo, ciertamente inquietantes. Ello con el complicado equilibrio de regular los sistemas de inteligencia artificial para garantizar los derechos de las personas, pero sin penalizar su desarrollo, por otra parte, crucial para el avance tecnológico, comercial y del conocimiento para los ciudadanos y organizaciones de la Unión Europea.

De esta forma este borrador nace con estos objetivos:

- Garantizar que los sistemas de inteligencia artificial usados en la Unión Europea sean seguros y respeten los derechos fundamentales.

- Garantizar una seguridad jurídica que facilite la inversión e innovación en inteligencia artificial y evitar la fragmentación del mercado.

- Mejorar la aplicación efectiva de los requisitos de seguridad a los sistemas de inteligencia artificial.

Es en la regulación de ese uso seguro y respetuoso con los derechos humanos de la inteligencia artificial, en la que nos centraremos al analizar este proyecto por ser su relación con la ciberseguridad.

El reglamento se aplicará a los proveedores y usuarios de sistemas inteligencia artificial en la Unión o si la información generada se utilice en la Unión, pero con la salvaguarda de para utilizados exclusivamente con fines militares.

De todas las definiciones aportadas en el artículo 3 del borrador resulta de especial interés para el objeto de este TFM la de "componente de seguridad de un producto o sistema", aquel que "cumple una función de seguridad para dicho producto o sistema, o cuyo fallo o defecto de funcionamiento pone en peligro la salud y la seguridad de las personas o los bienes".

Como se ha mencionado más arriba para acometer la regulación de los sistemas de inteligencia sin perjudicar su desarrollo, el borrador clasifica los sistemas como de riesgo inaceptable (prohibidos), de riesgo alto y de riesgo bajo o mínimo artificial, de esta forma puede modular los requisitos a cumplir por los sujetos obligados, las medidas de supervisión por las autoridades, así como los sanciones.

Los sistemas directamente prohibidos son:

- Los que empleen técnicas subliminales que trasciendan la conciencia de una persona para alterar su comportamiento.

- Aprovechen las vulnerabilidades de un grupo de personas para alterar su comportamiento.

- Los susceptibles de ser operados por autoridades para evaluar o clasificar la fiabilidad de personas y provoque un trato perjudicial o desfavorable.

- Los que permitan la identificación biométrica remota en espacios públicos para la aplicación de la ley, salvo búsqueda de víctimas, prevención de una amenaza específica o enjuiciamiento por penas graves.

Por su parte, los sistemas de alto riesgo están listados en el anexo II de este borrador y requieren: - Un sistema específico de gestión de riesgos.

- Que su entrenamiento y prueba cumplan con unos criterios de calidad.

- Preparar antes de su puesta en servicio documentación técnica a disposición de las autoridades, así como acceso directo a sus datos.

- Contarán con archivos de registro que aseguren la trazabilidad del funcionamiento del sistema.

- Informar a sus usuarios con suficiente y adecuada transparencia sobre el funcionamiento del sistema y para que puedan usar correctamente la información generada, y especialmente en estos casos:

  - Informarán a las personas que están interactuando con un sistema de inteligencia artificial.
  - Informar si el sistema reconoce emociones o categoriza biométricamente.
  - Harán constar específicamente si crea o manipula imagen, sonido o vídeo.

- Poder ser vigilados de manera efectiva por personas.
- Han de diseñarse con un nivel adecuado de ciberseguridad. Concretamente, han de ser resistentes a fallos que pueden surgir de los propios sistemas y a los intentos de terceros de alterar su uso y acorde a los riesgos cambiantes que puedan darse.

Además, para solventar sus vulnerabilidades, los sistemas de inteligencia artificial de alto riesgo contarán con medidas para prevenir y mitigar ataques que traten de manipular su entrenamiento o los datos de entrada.

- Han de inscribirse en la base de datos de la Unión Europea para sistemas de IA de alto riesgo.

- En cuanto a los usuarios, estos utilizarán los sistemas de alto riesgo conforme a las instrucciones de uso.

Para los sistemas de inteligencia artificial considerados de riesgo bajo el proyecto plantea su adhesión voluntaria a códigos de conducta basados en los requisitos exigidos a los sistemas de alto riesgo.

El cumplimiento de las disposiciones de la norma se efectuará con el modelo similar a otros vistos en otras normas emanadas de la Unión Europea, autoridades nacionales, denominadas "notificantes" y otra a nivel europeo, el Comité Europeo de Inteligencia Artificial, compuesto por representantes de los estados miembros y la Comisión Europea.

Además de la supervisión de las obligaciones arriba listadas, estas autoridades han de ser notificadas por los responsables de los sistemas, en cuanto estos tengan conocimiento de incidentes graves y fallos de funcionamiento, de forma que se puedan iniciar los procedimientos previstos en la Directiva NIS 2, Reglamento DORA o en el Reglamento general de protección de datos si fuera preciso.

Por último, cabe reseñar la facultad que se le concede a la Comisión Europea, a semejanza de otras normas vistas en el presente para adoptar actos delegados, que cobra, si cabe, más importancia en una materia tan cambiante como es la inteligencia artificial.

2.2.9 Propuesta del Parlamento Europeo y del Consejo por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos

Las Conclusiones del Consejo de octubre de 2021 y la Estrategia de Ciberseguridad de la UE para la Década Digital destacaron que el aumento constante en el uso de las tecnologías de la información y la comunicación incrementa la exposición a incidentes de ciberseguridad y sus posibles repercusiones en toda la Unión Europea. Por lo que resulta urgente mejorar las capacidades colectivas y aumentar los intercambios de información para detectar ciberamenazas y ciberincidentes.

Como respuesta a esta situación se ha elaborado este borrador de reglamento europeo, que tiene en cuenta los procedimientos y mecanismos ya contemplados en otras normas estudiadas en el presente: el Reglamento sobre la Ciberseguridad, la Directiva NIS 2 y la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información; de forma que se aprovechen esas capacidades y se eviten duplicidades. El proyecto de reglamento se centra en estas iniciativas:

Creación del Ciberescudo Europeo

El Ciberescudo Europeo es una infraestructura interconectada de los centros de operaciones de seguridad (COS) de los estados miembros y los transfronterizos para detectar, analizar y tratar datos sobre ciberamenazas y ciberincidentes mediante "el intercambio de herramientas de vanguardia y el desarrollo conjunto de capacidades de detección, análisis y prevención cibernéticos y de prevención y protección en un entorno de confianza", tal y como se establece en su artículo 3.1.

Entre la información compartida en el Ciberescudo se encuentran las ciberamenazas, cuasiincidentes, vulnerabilidades, tácticas, técnicas y procedimientos (TTP´s), indicadores de compromiso, alertas, recomendaciones de configuración, etc.

Para su correcta coordinación con los organismos establecidos en la Directiva NIS 2, los centros de operaciones de seguridad transfronterizos comunicarán sin demora la información sobre un incidente de ciberseguridad a gran escala a EU-CyCLONe, a la red de CSIRT y a la Comisión.

Asimismo, el Ciberescudo mantendrá todas las medidas pertinentes para garantizar la propia seguridad de sus sistemas y la de los datos que comparte.

Creación del Mecanismo de Ciberemergencia

Este mecanismo tiene como objetivo mejorar la resiliencia ante las principales ciberamenazas de la Unión Europea y para afrontar y mitigar los efectos de los ciberincidentes significativos y a gran escala. El Mecanismo apoya estas acciones:

- Preparación, incluidas las pruebas de preparación de las entidades en sectores muy críticos.

- Respuesta a ciberincidentes significativos y a gran escala y la recuperación inmediata.

- Asistencia mutua entre las autoridades nacionales de diferentes estados miembros, según lo dispuesto en la Directiva NIS 2.

Para ayudar a responder y recuperarse ante ciberincidentes de ciberseguridad significativos o a gran escala se creará una Reserva de Ciberseguridad de la UE.

Entre los usuarios de los servicios de esa reserva se encuentran las autoridades de gestión de crisis de ciberseguridad de los estados miembros y los CSIRT referidos a tal efecto en la Directiva NIS 2, así como las instituciones, órganos y organismos de la Unión Europea.

Mecanismo de Revisión de Incidentes de Ciberseguridad

ENISA a solicitud de la Comisión Europea (a través del Grupo de Cooperación NIS), el EU-CyCLONe o la red de CSIRT revisará y evaluará las ciberamenazas, vulnerabilidades y medidas de mitigación respecto a un ciberincidente específico significativo o a gran escala.

ENISA presentará el resultado en un informe a esos organismos con el fin de ayudarles a realizar las funciones que tienen encomentadas en ese sentido en la Directiva NIS 2.

2.3 Normas nacionales

Tras haber expuesto las normas internacionales y comunitarias es el momento de explicar la legislación estrictamente nacional. Como ya se ha dejado constancia, las normas nacionales de los estados miembros, España entre ellos, tienen una influencia directa de la Unión Europea, y más si cabe en una materia de tanta importancia para ella como es la ciberseguridad.

Asimismo, de semejante manera como ocurre en la UE con la Directiva NIS 2, la trasposición de esta directiva por medio del Real Decreto-ley 12/2018 hace de esta real decreto-ley la norma sobre la que van a pivotar los elementos esenciales de la ciberseguridad nacional.

Sin embargo, no hay que restar mérito al legislador español, que ha sido proactivo regulando varias facetas sin necesidad de los imperativos legales o acicates estratégicos comunitarios e incluso ha sido pionero regulando la firma electrónica con el documento nacional de identidad.

2.3.1 Constitución Española

Nuestra carta magna regula en su artículo 18 el derecho fundamental del honor, la intimidad personal y familiar y la propia imagen. Especificando el 18.4 que “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

De este modo, ya en 1978 se contempló con notable previsión la afectación de ese derecho fundamental de la informática, a pesar de que en ese momento su influencia en nuestra vida cotidiana distaba muchísimo de la actual.

2.3.2 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Esta Ley Orgánica 3/2018 viene a desarrollar el Reglamento UE 2016/679 (Reglamento general de protección de datos), no obstante, al ser este último de aplicación directa en nuestro ordenamiento jurídico nacional la Ley Orgánica 3/2018 solo regula aquellos aspectos que el propio Reglamento le faculta expresamente.

Por otro lado, en relación a la ciberseguridad, no realiza mayor aportación relevante más allá de volver a incidir, como hace el Reglamento, en entender la protección de datos desde la perspectiva de su integridad y confidencialidad de los datos, mediante el concepto de "violación de la seguridad de los datos".

2.3.3 Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales

Incluimos aquí una mención a esta norma por evitar cierta incoherencia que produciría su omisión, ya que junto a la Ley Orgánica 3/2018 y al Reglamento UE 2016/679 completa el corpus legislativo específico para la protección de datos personales en nuestro país.

La particularidad que presenta esta norma es que atiende a un especial y fundamentado derecho de acceso y tratamiento de los datos de carácter personal menos restrictivo para las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial en ciertos supuestos.

2.3.4 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

Esta norma que fue pionera ya muestra claros indicios de estar siendo superada por la realidad "cíber" tras sus más de veinte años de vigencia. En lo que respecta a la ciberseguridad, se pueden destacar tres de sus preceptos:

- La retirada del contenido ilícito. El artículo 8 faculta a autoridades y judiciales a la interrupción o retirada de contenido que atente contra el orden público, la investigación penal, la seguridad pública, la defensa nacional, la salud pública, la dignidad de la persona, el principio de no discriminación, la juventud, la infancia y la propiedad intelectual.

Todo ello viene a intentar evitar los efectos perniciosos e ilegales de un uso inadecuado de las tecnologías de la información y la comunicación.

- Obligaciones de información sobre seguridad. Este artículo 12 bis fue introducido por la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

Los prestadores de servicios de acceso a Internet han de informar a sus clientes sobre los diferentes medios técnicos que puedan aumentar los niveles de ciberseguridad, entre otros, frente a virus informáticos y programas espía.

- Gestión de incidentes de ciberseguridad que afecten a la red de Internet. Se determina que los prestadores de servicios, los registros de nombres de dominio y los agentes registradores que estén establecidos en España han de colaborar con el CSIRT que competa para la resolución de incidentes de ciberseguridad que afecten a Internet y actuar conforme a las recomendaciones de seguridad establecidas en los códigos de conducta.

Además, se incide en que los CSIRT gestionados por el sector público tienen el deber aportar las evidencias técnicas necesarias para la persecución de los delitos derivados de esos incidentes. Lo que vuelve a poner de manifiesto la relación entre la ciberseguridad y la persecución de la cibercriminalidad.

2.3.5 Ley 36/2015, de 28 de septiembre, de Seguridad Nacional

Esta ley de Seguridad Nacional tuvo su germen en la Estrategia de Seguridad Nacional de 2013, y vino a dar cuerpo legal a lo ya establecido en ella, destacando para este caso de estudio el Sistema de Seguridad Nacional, citado aquí en diversos apartados.

Como órgano principal de ese sistema se halla el Consejo de Seguridad Nacional, una comisión delegada del Gobierno que asiste al Presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional.

Uno de los ámbitos de especial interés para la Seguridad Nacional que cita la propia ley es la ciberseguridad y para poder realizar esa labor de asistencia es por lo que la ley 36/2015 facultó para la creación de comités especializados de apoyo al Consejo de Seguridad Nacional, siendo uno de ellos el Consejo Nacional de Ciberseguridad.

Lo dispuesto en este real decreto, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

2.3.6 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

La Ley 39/2015, junto a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, articuló múltiples novedades en el ámbito del Derecho Administrativo, debiendo centrarnos en su relación con la ciberseguridad a través de la derogación que efectuó de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Ya que vino a integrar, con las debidas modificaciones, sus preceptos en el procedimiento administrativo común, del mismo modo que fue plenamente coherente con el entonces reciente Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica.

Esta Ley 39/2015 dio un paso adelante importante en la digitalización de la Administración Pública y en su relación con los ciudadanos. Abordó o reformuló la representación mediante comparecencia electrónica, identificación de los interesados mediante certificados electrónicos cualificados de firma electrónica y de sello electrónico, el derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas, la creación y mantenimiento de un registro electrónico general por cada Administración y sus organismos dependientes que será accesible a través de una sede electrónica, la digitalización de los documentos y de los expedientes, los efectos de las notificaciones electrónicas, etc.

Todo lo anterior aumentaba considerablemente la superficie de exposición ante cualquier ciberincidente o ciberataque, por lo que resultaba esencial garantizar, al menos, la integridad, autenticidad, confidencialidad de los datos. Para lo que la norma hace remisiones expresas al cumplimiento del Esquema Nacional de Seguridad (actualmente regulado en Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad), del que más adelante se hablará.

Asimismo, es de destacar por su actualidad, que la disposición adicional sexta desautorizaba los sistemas de identificación y de firma basados en tecnologías de registro distribuido (lo que se conoce como *blockchain*) hasta que no fueran regulados. Resultando que la Resolución de 6 de julio de 2023, de la Secretaría de Estado de Digitalización e Inteligencia Artificial; por la que se publica el Acuerdo del Consejo de Ministros de 27 de junio de 2023, por el que se determinan los supuestos de validez de sistemas de identificación y firma electrónica en la Administración del Estado cuya verificación se lleve a cabo por medio de un sistema de tecnología de registro distribuido, ha venido a validar “un sistema de

identificación y firma de los interesados por medio de una credencial incorporada a la Cartera digital cuya verificación se lleve a cabo por medio de un sistema de tecnología de registro distribuido basado en la Infraestructura Europea de Servicios de *Blockchain* (EBSI, por sus siglas en inglés) en el contexto de los proyectos europeos vinculados a la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea (futuro Reglamento eIDAS 2)". Ello siempre que las credenciales se adecúen a lo preceptuado por Esquema Nacional de Seguridad.

2.3.7 Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público

La otra ley estrechamente relacionada con la 39/2015, por la preeminencia de ambas para el Derecho Administrativo, y del mismo modo que ocurre con ella respecto a la digitalización y la inherente necesidad de dotarse de medidas adecuadas de ciberseguridad, igual acontece en esta.

La Ley 40/2015 establece en el marco con el que se configuran los órganos administrativos, sus funciones, las relaciones que establecen entre ellos, etc. Para lo que en aras de la eficiencia y eficacia del funcionamiento de la Administración es indispensable valerse de medios digitales.

Por tanto, en cuanto a elaboración de actas, el archivo de documentación, el intercambio de información, el acceso a las sedes electrónicas, etc., tal y como refleja expresamente esta ley, hay que garantizar en todos sus procedimientos la integridad, confidencialidad, disponibilidad y autenticidad de todos esos datos. Valiéndose para ello de nuevo en el Esquema Nacional de Seguridad, reseñado específicamente junto al Esquema Nacional de Interoperabilidad en el artículo 156.

Además, esta ley hace constar a la ciberseguridad como uno de sus principios generales cuando reza en su artículo 3.2 que: "las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados".

2.3.8 Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza

El rápido, y en ocasiones vertiginoso, desarrollo de las tecnologías de la información y la comunicación tan comentado a lo largo del presente, es una vez más el motivo de la necesidad de una modificación legal, en el caso de esta Ley 6/2020 que supuso la derogación de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

La Ley 6/2020 regula elementos tan sustanciales para la ciberseguridad como la autenticidad e integridad de los datos y complementa al Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

Los prestadores de servicios electrónicos de confianza emiten certificados electrónicos destinados a que personas físicas o jurídicas puedan acreditar su identidad mediante la firma electrónica, sello o autenticación de sitio web.

Como medidas para tratar de garantizar la ciberseguridad de esos certificados tanto los prestadores cualificados y no cualificados de servicios electrónicos de confianza han de notificar al Ministerio de Asuntos Económicos y Transformación Digital[20] las violaciones de seguridad o pérdidas de la integridad, sin perjuicio de su notificación a la Agencia Española de Protección de Datos, a otros

[20] Actualmente el Ministerio para la Transformación Digital y de la Función Pública.

organismos relevantes o a las personas afectadas. Además, están obligados a adoptar las medidas pertinentes para resolver esos ciberincidentes.

2.3.9 Ley 11/2022, de 28 de junio, General de Telecomunicaciones

Esta ley regula las telecomunicaciones en nuestro país, abarcando la instalación y explotación de las redes de comunicaciones electrónicas, así como la prestación de los servicios de comunicaciones electrónicas, los equipos terminales de telecomunicación, etc. De nuevo supone una rauda modificación legislativa pues derogó la relativamente reciente Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Haciendo alusión a las repercusiones que una afectación de la normal prestación de los servicios de comunicaciones electrónicas puede tener para los intereses generales, esta ley, con coherencia con el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que traspuso la Directiva NIS, establece las pautas básicas para la ciberseguridad de una entidad.

Para ello, provee en el punto 67 de su anexo II de esta definición para la seguridad de las redes y servicios de comunicaciones electrónica: "capacidad de las redes y servicios de comunicaciones electrónicas de resistir, con un determinado nivel de confianza, cualquier acción que comprometa la disponibilidad, autenticidad, integridad y confidencialidad de dichas redes y servicios, de los datos almacenados, procesados o transmitidos y la seguridad de los servicios conexos que dichas redes y servicios de comunicaciones electrónicas ofrecen o hacen accesibles".

Seguidamente su artículo 63 desglosa esas pautas en un marco claro y estructurado del parecido modo al que se refleja en el Real Decreto-ley 12/2018:

- Esos proveedores de redes y servicios han de conocer todos sus activos para poder conocer sus riesgos y aplicar medidas organizativas y técnicas adecuadas a los mismos.

- Por la naturaleza esencial del servicio prestado han de garantizar su mayor disponibilidad.

- En el caso de que se produzcan ciberincidentes con impacto significativo hay que comunicarlo a la autoridad ministerial competente.

- Para valorar ese impacto, hay que evaluar estos parámetros:

    - El número de usuarios afectados.
    - La duración del incidente.
    - Área geográfica afectada.
    - Cómo ha visto afectado al funcionamiento de la red o servicio.
    - El alcance del impacto en la economía y la sociedad.

- Ante una amenaza particular y significativa de incidente el proveedor informará a sus usuarios.

- Para verificar todo lo anterior la autoridad competente supervisará estas medidas solicitando información a esos proveedores y podrá realizar auditorías y en caso de infracción, sancionar.

2.3.10 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

Como norma nacional de trasposición de la Directiva NIS, comentada más arriba a colación de la Directiva NIS 2, este real-decreto ley, complementado por el Real Decreto 43/2021 del que más adelante se hablará, procedió a adaptar a nuestra realidad e idiosincrasia nacionales a los preceptos de esa directiva. Pero haciendo un empleo adecuado del principio de armonización mínima fue más ambiciosa que lo acordado en ella, lo cual ha redundado en términos generales en un mayor nivel de ciberseguridad nacional y ha colocado a nuestro país en una posición más ventajosa de cara a la trasposición de la Directiva NIS 2, que ya ha comenzado.

Sin ánimo de reiterar lo ya mencionado sobre la Directiva NIS, exponemos aquí las particularidades concretas en su adaptación nacional por este Real-Decreto Ley y los organismos que desempeñan las funciones descritas en esa directiva.

Operadores de servicios esenciales y proveedores de servicios digitales

La Directiva NIS estableció al menos siete sectores estratégicos, pero el RD-ley 12/2018 aumentó hasta doce el número de sectores estableciendo un paralelismo a los establecidos en el Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, al realizar una remisión expresa a los sectores estratégicos citados en esa ley.

Ese paralelismo, permite también adelantar la tan repetida coordinación entre la protección del ámbito físico y digital en las Directivas NIS 2 y en la Directiva 2022/2557.

Es necesario recordar aquí que estos sectores del RD-ley se aplican a los servicios esenciales, mientras que los proveedores de servicios digitales son los prestadores de servicios digitales independientemente de esos sectores.

Sectores Directiva NIS	Sectores RD-ley 12/2018
1. Energía	1. Administración
2. Transporte	2. Espacio
3. Banca	3. Industria nuclear
4. Infraestructuras de los mercados financieros	4. Industria química
5. Sector sanitario	5. Instalaciones de investigación
6. Suministro y distribución de agua potable	6. Agua
7. Infraestructura digital	7. Energía
	8. Salud
	9. Tecnologías de la información y la comunicación
	10. Transporte
	11. Alimentación
	12. Sistema financiero y tributario

Tabla 3 Comparación de los sectores regulados por la Directiva NIS y por el RD-ley 12/2018

Autoridades nacionales competentes

- Para los operadores de servicios esenciales designados como operadores críticos conforme a la Ley 8/2011, la Secretaría de Estado de Seguridad del Ministerio del Interior, a través de la Oficina de Coordinación de Ciberseguridad[21].
- Para los operadores de servicios esenciales designados no considerados críticos y que estén comprendidos en el ámbito de aplicación de la Ley 40/2015, el Ministerio de Defensa, a través del Centro Criptológico Nacional (CCN).

[21] En la norma consta Centro Nacional de Protección de Infraestructuras y Ciberseguridad, pero eso órgano fue suprimido por el Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, y las funciones que desempeñaba en el RD-ley las realiza ahora la Oficina de Coordinación de Ciberseguridad (OCC).

- Para los operadores de servicios esenciales designados no considerados críticos ni comprendidos en el ámbito de aplicación de la Ley 40/2015, establece las siguientes autoridades para estos sectores:

a) Transporte: el Ministerio de Transportes, Movilidad y Agenda Urbana, a través de la Secretaría de Estado de Transportes, Movilidad y Agenda Urbana.

b) Energía: el Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Energía.

c) Tecnologías de la información y las telecomunicaciones: el Ministerio de Asuntos Económicos y Transformación Digital[22], a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

d) Sistema financiero:

1.º El Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Economía y Apoyo a la Empresa, en el ámbito de los seguros y fondos de pensiones.

2.º El Banco de España, para las entidades de crédito.

3.º La Comisión Nacional del Mercado de Valores, para las entidades que prestan servicios de inversión y las sociedades gestoras de instituciones de inversión colectiva.

e) Espacio: el Ministerio de Defensa, a través de la Secretaría de Estado de Defensa.

f) Industria química: el Ministerio de Interior, a través de la Secretaría de Estado de Seguridad.

g) Investigación: el Ministerio de Ciencia e Innovación, a través de la Secretaría General de Investigación.

h) Salud: el Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad.

i) Agua: el Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Medio Ambiente.

j) Alimentación:

1.º El Ministerio de Agricultura, Pesca y Alimentación, a través de la Secretaría General de Agricultura y Alimentación.

2.º El Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad.

3.º El Ministerio de Industria, Comercio y Turismo, a través de la Secretaría de Estado de Comercio.

4.º El Ministerio de Consumo, a través de la Agencia Española de Seguridad Alimentaria y Nutrición (AESAN).

k) Industria nuclear:

1.º El Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Energía.

2.º El Consejo de Seguridad Nuclear.

- Para los proveedores de servicios digitales comprendidos en el ámbito de aplicación de la Ley 40/2015, el Ministerio de Defensa, a través del Centro Criptológico Nacional.
- Para los proveedores de servicios digitales no comprendidos en el ámbito de aplicación de la Ley 40/2015, la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital[23].

Es necesario reseñar, que del mismo modo que como se ha apuntado más arriba, con la Oficina de Coordinación de Ciberseguridad y el ya suprimido Centro Nacional de Protección de Infraestructuras y Ciberseguridad, igual ocurre con otros de los órganos designados nominalmente como autoridades, que han cambiado de denominación o incluso de adscripción ministerial, pero no por ello sus competencias se han dejado de ejercer, sino desempeñadas por sus órganos sustitutos funcionalmente.

[22] Actualmente el Ministerio para la Transformación Digital y de la Función Pública.

[23] Actualmente el Ministerio para la Transformación Digital y de la Función Pública.

AUTORIDAD COMPETENTE			
Tipo de operador	**Subtipo**	**Características**	**Organismo competente**
Operador de servicios esenciales	Operador Crítico	-	CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD (CNPIC)
	No operador crítico	Comprendido en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público	CENTRO CRIPTOLÓGICO NACIONAL (CCN)
		Resto	AUTORIDAD SECTORIAL
Proveedor de Servicios Digitales	Sector privado	-	SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
	Sector público	Comprendido en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público	CENTRO CRIPTOLÓGICO NACIONAL (CCN)

Tabla 4 Autoridades nacionales competentes[24]

Equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia

- INCIBE-CERT:
  - Para los operadores de servicios esenciales identificados como críticos, siendo en este caso operado conjuntamente por el INCIBE[25]y la OCC[26].
  - Para los operadores de servicios esenciales no críticos ni comprendidos en el ámbito de aplicación de la Ley 40/2015.
  - Para los proveedores de servicios digitales no comprendidos en el ámbito de aplicación de la Ley 40/2015.

- CCN-CERT:
  - Para los operadores de servicios esenciales no críticos comprendidos en el ámbito de aplicación de la Ley 40/2015.
  - Para los proveedores de servicios digitales comprendidos en el ámbito de aplicación de la Ley 40/2015.

[24]Fuente:https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

[25] Sociedad dependiente del Ministerio de Transformación Digital y de Función Pública, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

[26] Como en la referencia en la nota al pie 20, la función es encomendada ahora a la Oficina de Coordinación de Ciberseguridad.

- ESPDEF-CERT:
    - Para los operadores de servicios esenciales con incidencia en la Defensa Nacional, cooperando con el CCN-CERT y el INCIBE-CERT.

EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) DE REFERENCIA		
Tipo de operador	**Características**	Organismo competente
Operador de servicios esenciales	Sector Público (entidades incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015)	**CCN-CERT**
	Sector Privado (entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015)	**INCIBE-CERT**
Proveedor de Servicios Digitales	Sector Público (entidades incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015)	**CCN-CERT**
	Sector Privado (entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015)	**INCIBE-CERT**

Tabla 5 CSIRT nacionales competentes[27]

Punto de contacto único

Como punto de contacto se designa al Consejo de Seguridad Nacional, a través del Departamento de Seguridad Nacional. Sus funciones son la cooperación transfronteriza entre las autoridades competentes con las de otros estados miembros, con el grupo de cooperación NIS y la red de CSIRT.

Estrategia nacional de seguridad de las redes y sistemas de información:

Se concreta el mandato acordando un Estrategia de Ciberseguridad Nacional, enmarcada y alineada con la Estrategia de Seguridad Nacional, cuyo mandato se cumplió al materializarse la Estrategia Nacional de Ciberseguridad 2019, la cual es objeto de estudio en un apartado específico.

Plataforma común para la notificación de incidentes

Este RD-ley también resultó innovador al prever una plataforma la notificación de incidentes, lo que, por un lado, facilita sobremanera las comunicaciones por parte de los operadores, cuya omisión, retraso o carencia de información es motivo de sanción, y por otro las labores de gestión y supervisión de los incidentes de los CSIRT y las autoridades competentes.

[27]Fuente:https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

2.3.11 Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación

Las redes de quinta generación, más conocidas como 5G, son las redes y sistemas de transmisión que conectan los dispositivos móviles de comunicación con características técnicas muy avanzadas que permiten mucha más velocidad y capacidad que las anteriores generaciones, de tal modo que alteran el paradigma actual de las tecnologías de la información y la comunicación y ello supone a su vez un incremento directamente proporcional de sus riesgos de seguridad.

El legislador ha sido consciente de esta situación y de la necesidad de promulgar una norma específica que responda a este reto, además de contar con otras normas como es el Real Decreto-ley 12/2018 ya visto más arriba. Por ello, este real decreto-ley hace constar en su artículo 2 letra a) que el que su objetivo primordial es "impulsar una seguridad integral del ecosistema generado por la tecnología 5G".

Primero se acota el ámbito de aplicación a los operadores, suministradores y usuarios corporativos 5G (estos últimos son aquellos con derechos de uso del dominio público radioeléctrico respecto a la explotación de redes o servicios 5G) y que devienen en los sujetos obligados de todas las imposiciones previstas en la norma.

A mayores, en atención a las técnicas de funcionamiento y la operatividad de sus equipos, productos y servicios, además de su grado de exposición a injerencias de sociedades o estados extranjeros, los suministradores también pueden catalogarse como suministradores 5G de riesgo alto o riesgo medio, elevando las medidas a adoptar respecto al resto de sujetos obligados.

Siguiendo las pautas tradicionales en la gestión de la ciberseguridad, esta norma aborda para el 5G el enfoque de seguridad integral, contemplando no solo las redes y sistemas, sino infraestructuras físicas, suministradores, etc.

Los sujetos obligados han de comenzar realizando un análisis de los riesgos amenazas y vulnerabilidades tras identificar todos sus activos. Tras ello, el siguiente paso en el ciclo de la ciberseguridad obliga a esos sujetos a adoptar la gestión de riesgos con el objetivo de eliminarlos o al menos mitigarlos, para lo que habrán de hacer uso de las técnicas y medidas necesarias y adecuadas.

Para dotar a esta gestión de la seguridad integral 5G de una mayor coherencia y homogeneidad, este real decreto-ley prevé la creación de un Esquema Nacional de Seguridad de redes y servicios 5G, que regulará de forma más concreta y actualizada todos los aspectos anteriormente mencionados.

Asimismo, acorde a la dimensión transnacional de la ciberseguridad, este Real Decreto-ley 7/2022 hace constar expresamente que el Esquema Nacional de Seguridad de redes y servicios 5G puede supeditar la utilización de un equipo, programa o servicio a la obtención previa de una certificación establecida en virtud del Reglamento (UE) 2019/881 sobre la ciberseguridad.

Como acontece en todas las normas que establecen imposiciones a sujetos, si no hay una autoridad que supervise su correcto cumplimiento y un catálogo de infracciones que la faculte a sancionar la conculcación de los preceptos, esta norma correría el riesgo de devenir ineficaz, puesto que la aplicación de medidas de seguridad y su mantenimiento en el tiempo tiene aparejado un coste económico sustancial para estos sujetos.

En este caso las potestades de supervisión, inspección y sanción recaen en el Ministerio de Asuntos Económicos y Transformación Digital[28], que además es el encargado de aplicar y hacer cumplir el Esquema Nacional de Seguridad de redes y servicios 5G.

[28] Actualmente el Ministerio para la Transformación Digital y de la Función Pública.

2.3.12 Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica

En el ámbito europeo y mundial España fue uno de los países pioneros en la implantación de un documento nacional de identidad que permitiese a su titular acreditar su identidad con los mismos efectos que mostrando el soporte físico y además permitir la firma digital de documentos con plenos efectos legales.

La relevancia de la mención de este real decreto en este estudio reside, entre otras cosas, en que regula para todos de los españoles dos de las dimensiones de la ciberseguridad, la autenticidad y la integridad.

La autenticidad, al constatar mediante documento público oficial que el titular de los certificados electrónicos alojados en la propia tarjeta física es quién dice ser. Y la integridad, puesto que la firma electrónica efectuada con esos certificados permite comprobar al receptor del documento que este ha sido firmado electrónicamente por el titular del DNI y que no ha sido alterado de ninguna forma desde el momento de la firma.

Para garantizar la seguridad del documento nacional de identidad electrónico el organismo competente es el Ministerio del Interior a través de la Dirección General de la Policía, que, asimismo, es responsable de la custodia de los archivos y ficheros, lo que comprende por tanto su disponibilidad, integridad y confidencialidad.

Como medidas preventivas para la ciberseguridad general del documento nacional de identidad electrónico se adoptan estas acciones adicionales:

- En el acto de emisión y entrega del documento nacional de identidad se informa claramente a su titular sobre todo lo relevante del funcionamiento y seguridad de los certificados que permite la identificación y la firma digital y, por su parte, el Ministerio del Interior realiza genéricamente una Declaración de Prácticas y Políticas de Certificación. Lo que ya desde 2005 supone un precedente claro de la actualmente tan en boga "cultura de ciberseguridad".

- La activación del certificado de firma electrónica es voluntario y para su empleo se requiere una clave personal secreta.

- El certificado electrónico solo tiene una validez de cinco años, independientemente de que el soporte físico tenga una validez de diez años o permanente.

Este real decreto se sustanciaba en ciertos aspectos en la Ley 59/2003 de firma electrónica que, como ya hemos comentado, fue sustituida en su totalidad por la Ley 6/2020 reguladora de determinados aspectos de los servicios electrónicos de confianza. Este cambio legal ha venido a apuntalar y actualizar esos aspectos, pero sin afectar en mayor medida a este real decreto.

2.3.13 Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

En el proceso de digitalización de las diferentes Administraciones Públicas resulta fundamental la interoperabilidad entre sus redes, sistemas de información y sus procedimientos para lograr un adecuado intercambio de información. Todo lo cual tiene, como es lógico, grandes implicaciones en la seguridad de los datos compartidos y los posibles riesgos añadidos ante accesos ilegítimos en esas redes y sistemas.

En relación a la ciberseguridad, este real decreto no entra a regular esa materia sino que determina que para de garantizar la "integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación física y lógica de los documentos electrónicos, sus soportes y medios" se deberán adoptar los principios básicos y las medidas de seguridad contempladas en el Esquema Nacional de Seguridad (en ese momento en su versión del Real Decreto 3/2010, pero tras su derogación, actualmente por el Real Decreto 311/2022, de 3 de mayo).

2.3.14 Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

Como se adelantó más arriba, este reglamento desarrolla el Real Decreto-ley 12/2018, que a su vez ya había traspuesto la Directiva NIS, en aquellos aspectos que debido a su grado técnico de detalle no habían sido regulados en su totalidad en ese Real Decreto-ley 12/2018 y que destacamos a continuación.

Requisitos en materia de seguridad

Los operadores de servicios esenciales y los proveedores de servicios digitales han de adoptar medidas técnicas y organizativas para gestionar los riesgos que afecten a sus redes y sistemas y para el caso de las políticas de seguridad de los operadores de servicios esenciales estas han de comprender al menos estos aspectos:

a) Análisis y gestión de riesgos.

b) Gestión de riesgos de terceros o proveedores.

c) Catálogo de medidas de seguridad, organizativas, tecnológicas y físicas.

d) Gestión del personal y profesionalidad.

e) Adquisición de productos o servicios de seguridad.

f) Detección y gestión de incidentes.

g) Planes de recuperación y aseguramiento de la continuidad de las operaciones.

h) Mejora continua.

i) Interconexión de sistemas.

j) Registro de la actividad de los usuarios

Las medidas de seguridad concretas para la gestión de riesgos se recogen en una declaración de aplicabilidad y toman como referencia las recogidas en el Esquema Nacional de Seguridad.

Responsable de la seguridad de la información.

Los operadores de servicios esenciales han de designar una persona o unidad de naturaleza administrativa como responsable de la seguridad de la información con la tarea de ser el punto de contacto y coordinación técnica con la autoridad y CSIRT de referencia de la entidad.

Además, el responsable de la seguridad de la información supervisa la aplicación de las políticas de seguridad, elabora el documento de declaración de aplicabilidad de medidas de seguridad y comunica a la autoridad competente, a través del CSIRT de referencia las notificaciones de incidentes que perturben significativamente la prestación de los servicios de su entidad.

Instrucción nacional de notificación y gestión de ciberincidentes

En el anexo del Real Decreto 43/2021 se recoge esta guía que rige las pautas para la notificación y gestión de ciberincidentes.

Esta Instrucción considera que son incidentes con perturbación significativa (aquellos cuya notificación es obligatoria) de los servicios esenciales, los que se identifiquen con un nivel crítico, muy alto o alto conforme a su peligrosidad[29] e impacto[30].

[29] Nivel crítico:
– APT.
Nivel muy alto:
– Distribución de malware.
– Configuración de malware.
– Robo.
– Sabotaje.
– Interrupciones.
Nivel alto:
– Pornografía infantil, contenido sexual o violento inadecuado.
– Sistema infectado.
– Servidor C&C (Mando y Control).
– Compromiso de aplicaciones.
– Compromiso de cuentas con privilegios.
– Ataque desconocido.
– DoS (Denegación de servicio).
– DDoS (Denegación distribuida de servicio).
– Acceso no autorizado a información.
– Modificación no autorizada de información.
– Pérdida de datos.
– *Phishing*.
Nivel medio:
– Discurso de odio.
– Ingeniería social.
– Explotación de vulnerabilidades conocidas.
– Intento de acceso con vulneración de credenciales.
– Compromiso de cuentas sin privilegios.
– Desconfiguración.
– Uso no autorizado de recursos.
– Derechos de autor.
– Suplantación.
– Criptografía débil.
– Amplificador DDoS.
– Servicios con acceso potencial no deseado.
– Revelación de información.
– Sistema vulnerable.
Nivel bajo:
– *Spam.*
– Escaneo de redes (*scanning*).
– Análisis de paquetes (*sniffing*).
– Otros.

[30] Nivel crítico:
– Afecta apreciablemente a la Seguridad Nacional.
– Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.
– Afecta a una infraestructura crítica.
– Afecta a sistemas clasificados SECRETO.
– Afecta a más del 90 % de los sistemas de la organización.
– Interrupción en la prestación del servicio superior a 24 horas y superior al 50 % de los usuarios.
– El ciberincidente precisa para resolverse más de 100 Jornadas-Persona.
– Impacto económico superior al 0,1 % del Producto Interior Bruto (PIB) actual.
– Extensión geográfica supranacional.
– Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.
Nivel muy alto:
– Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.

Alineada con la taxonomía de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) esta Instrucción facilita una clasificación y taxonomía de los ciberincidentes, junto a su descripción y ejemplos aclaratorios.

Clasificación	Tipo de incidente	Descripción y ejemplos prácticos
Contenido abusivo.	*Spam.*	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
	Delitos de odio, contra la libertad o el honor.	Contenido difamatorio o discriminatorio. Ej.: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
	Pornografía infantil, contenido sexual o violento inadecuado.	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido dañino.	Sistema infectado.	Sistema infectado con malware. Ej.: sistema, computadora o teléfono móvil infectado con un *rootkit*.
	Servidor C&C (Mando y Control).	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.

– Afecta apreciablemente a actividades oficiales o misiones en el extranjero.
– Afecta a un servicio esencial.
– Afecta a sistemas clasificados RESERVADO.
– Afecta a más del 75 % de los sistemas de la organización.
– Interrupción en la prestación del servicio superior a 8 horas y superior al 35 % de los usuarios.
– El ciberincidente precisa para resolverse entre 30 y 100 Jornadas-Persona.
– Impacto económico entre el 0,07 % y el 0,1 % del PIB actual.
– Extensión geográfica superior a 4 Comunidades Autónomas (CC.AA.) o un territorio de Interés Singular (TIS, se considera como tal a las ciudades de Ceuta y Melilla y a cada una de las islas que forman los archipiélagos de las islas Baleares y las islas Canarias).
– Daños reputacionales a la imagen del país (marca España).
– Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.

Nivel alto:
– Afecta a más del 50 % de los sistemas de la organización.
– Interrupción en la prestación del servicio superior a 1 hora y superior al 10 % de usuarios.
– El ciberincidente precisa para resolverse entre 5 y 30 Jornadas-Persona.
– Impacto económico entre el 0,03 % y el 0,07 % del PIB actual.
– Extensión geográfica superior a 3 CC.AA.
– Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.

Nivel medio:
– Afecta a más del 20 % de los sistemas de la organización.
– Interrupción en la presentación del servicio superior al 5 % de usuarios.
– El ciberincidente precisa para resolverse entre 1 y 5 Jornadas-Persona.
– Impacto económico entre el 0,001 % y el 0,03 % del PIB actual.
– Extensión geográfica superior a 2 CC.AA.
– Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).

Nivel bajo:
– Afecta a los sistemas de la organización.
– Interrupción de la prestación de un servicio.
– El ciberincidente precisa para resolverse menos de 1 Jornada-Persona.
– Impacto económico entre el 0,0001 % y el 0,001 % del PIB actual.
– Extensión geográfica superior a 1 CC.AA.
– Daños reputacionales puntuales, sin eco mediático.

Sin impacto:
– No hay ningún impacto apreciable.

Clasificación	Tipo de incidente	Descripción y ejemplos prácticos
	Distribución de malware.	Recurso usado para distribución de malware. Ej.: recurso de una organización empleado para distribuir malware.
	Configuración de malware.	Recurso que aloje ficheros de configuración de malware Ej.: ataque de *webinjects* para troyano.
Obtención de información.	Escaneo de redes (*scanning*).	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej.: peticiones DNS, ICMP, SMTP, escaneo de puertos.
	Análisis de paquetes (*sniffing*).	Observación y grabación del tráfico de redes.
	Ingeniería social.	Recopilación de información personal sin el uso de la tecnología. Ej.: mentiras, trucos, sobornos, amenazas.
Intento de intrusión.	Explotación de vulnerabilidades conocidas.	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej.: desbordamiento de *buffer*, puertas traseras, *cross site scripting* (XSS).
	Intento de acceso con vulneración de credenciales.	Múltiples intentos de vulnerar credenciales. Ej.: intentos de ruptura de contraseñas, ataque por fuerza bruta.
	Ataque desconocido.	Ataque empleando *exploit* desconocido.
Intrusión.	Compromiso de cuenta con privilegios.	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Compromiso de cuenta sin privilegios.	Compromiso de un sistema empleando cuentas sin privilegios.
	Compromiso de aplicaciones.	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej.: inyección SQL.
	Robo.	Intrusión física. Ej.: acceso no autorizado a Centro de Proceso de Datos.
Disponibilidad.	DoS (Denegación de servicio).	Ataque de denegación de servicio. Ej.: envío de peticiones a una aplicación *web* que provoca la interrupción o ralentización en la prestación del servicio.
	DDoS (Denegación distribuida de servicio).	Ataque de denegación distribuida de servicio. Ej.: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	Mala configuración.	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej.: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
	Sabotaje.	Sabotaje físico. Ej.: cortes de cableados de equipos o incendios provocados.
	Interrupciones.	Interrupciones por causas ajenas. Ej.: desastre natural.
Compromiso de la información.	Acceso no autorizado a información.	Acceso no autorizado a información. Ej.: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación no autorizada de información.	Modificación no autorizada de información. Ej.: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante *ransomware*.
	Pérdida de datos.	Pérdida de información Ej.: pérdida por fallo de disco duro o robo físico.

Clasificación	Tipo de incidente	Descripción y ejemplos prácticos
Fraude.	Uso no autorizado de recursos.	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej.: uso de correo electrónico para participar en estafas piramidales.
	Derechos de autor.	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej.: Warez.
	Suplantación.	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
	Phishing.	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
Vulnerabilidad.	Criptografía débil.	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej.: servidores web susceptibles de ataques POODLE/FREAK.
	Amplificador DDoS.	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej.: DNS *open-resolvers* o Servidores NTP con monitorización *monlist*.
	Servicios con acceso potencial no deseado.	Ej.: Telnet, RDP o VNC.
	Revelación de información.	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej.: SNMP o Redis.
	Sistema vulnerable.	Sistema vulnerable. Ej.: mala configuración de *proxy* en cliente (WPAD), versiones desfasadas de sistema.
Otros.	Otros.	Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
	APT.	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

Tabla 6 Clasificación/Taxonomía de los ciberincidentes[31]

Igualmente, la Instrucción también deja tasados los plazos de notificación de esos ciberincidentes. por los operadores de servicios esenciales a su autoridad competente a través de su CSIRT de referencia y por medio de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

Nivel de peligrosidad o impacto	Notificación inicial	Notificación intermedia	Notificación final
CRÍTICO.	Inmediata.	24/48 horas.	20 días.
MUY ALTO.	Inmediata.	72 horas.	40 días.
ALTO.	Inmediata.	–	–
MEDIO.	–	–	–
BAJO.	–	–	–

Tabla 7 Ventana temporal de reporte[32]

[31] Anexo del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

[32] Anexo del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

2.3.15 Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos

Ya se vio en los apartados dedicados a la Ley 39/2015 y a la Ley 40/2015 la importancia que otorgan estas dos leyes a la actuación y el funcionamiento electrónico del sector público, siendo sus aspectos más técnicos tratados con este real decreto de desarrollo.

Entre sus diversos principios rectores, la ciberseguridad de los trámites y actuaciones electrónicas ya aparece incardinada en el principio de proporcionalidad. De forma más concreta sale a colación a lo largo de toda la norma la sujeción de las Administraciones Públicas al Esquema Nacional de Seguridad, al menos en cuanto a esta al cumplimiento de las medidas de seguridad para proteger:

- Portales de internet de las Administraciones Públicas.

- Sistemas de identificación y firma electrónica del personal al servicio de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.

- Intercambio electrónico de datos en entornos cerrados de comunicación.

- Sistemas de clave concertada y otros sistemas de identificación de las personas interesadas.

- Conservación de documentos electrónicos.

- Archivo electrónico único.

Todo en aras de tratar de garantizar la autenticidad, conservación, integridad, confidencialidad, disponibilidad y cadena de custodia de los expedientes y documentos intercambiados y almacenados por las Administraciones en el ejercicio de sus competencias.

También aprovecha esta norma para actualizar las medidas de seguridad respecto a las políticas de firma electrónica y de certificados en el ámbito estatal adecuándolas a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Asimismo, regula con más especificidad la verificación de certificados electrónicos y de otros sistemas de identificación mediante una Plataforma de la Administración General del Estado, así como el sistema de firma basado en un código seguro de verificación que permite garantizar la autenticidad e integridad de los documentos firmados electrónicamente.

3 ESTRATEGIAS SOBRE CIBERSEGURIDAD

Como ya se ha apuntado más arriba, una de las respuestas que se ha manifestado como más eficaz frente a las consecuencias del desarrollo de las tecnologías de la información y la comunicación, y por ende, de la ciberseguridad, son los planes estratégicos. La planificación estratégica, del mismo modo que las certificaciones, se ha extendido a múltiples disciplinas, no obstante, tuvo origen en la iniciativa privada, en este caso, la empresarial, pudiendo citar como sus autores germinales más influyentes a Ansoff[33] [1], Chandler[34] [2], o Drucker[35][3].

Antes de exponer cuáles son las virtudes y ventajas de estas estrategias, para una más fácil comprensión, es necesario realizar una explicación muy somera sobre en qué consiste un plan estratégico:

- Los planes estratégicos se plantean desde dos puntos de vista; para el desarrollo y mejora continua de las organizaciones conforme a su visión, misión o valores; o para reaccionar ante cambios de situaciones de cualquier índole (social, económica, técnica, etc.), que suscitan interés o inquietud.

- La primera fase de la estrategia supone analizar, en su caso, desde una de las dos perspectivas anteriores, el estado de la propia organización y su medio ambiente o, por otro lado, aclarar de forma objetiva el estado de situación de las circunstancias a las que se quiere responder. Ese análisis situacional da lugar a establecer los retos que afronta esa estrategia.

- Con esos retos fijados, ya sean amenazas o no, se decide un objetivo general, que se desglosa en varios objetivos específicos, cuyo logro se va a examinar más adelante mediante la consecución de unos indicadores. A su vez, se determinan líneas de acción que respondan adecuadamente a esos objetivos.

- Seguidamente, se desciende de la abstracción de alto nivel a la concreción de bajo nivel. Esto se realiza a través de distintos planes operativos, que adaptan esa estrategia y concretamente sus líneas de acción al ámbito geográfico, funcional o competencial concreto.

- El proceso finaliza al contrastar periódicamente la ejecución por los planes operativos de las líneas de acción, valorándolo con los indicadores que se marcaron con los objetivos específicos.

Esta valoración permite adaptar esos elementos que componen la estrategia para llevar a cabo un proceso de mejora continua[36] (planificar, hacer, verificar y actuar) [4].

Una vez ya puestos en perspectiva, es más sencillo entender cómo las estrategias, a pesar de una cierta complejidad, resultan una herramienta eficaz para responder a los retos de las tecnologías de la información y la comunicación.

La principal ventaja que suponen los planes estratégicos respecto a la regulación legal de organizaciones o realidades sociales es que son mucho más flexibles material, espacial, y temporalmente, pues más allá de la estructura mostrada más arriba, no se ven sujetos a plazos, informes preceptivos, restricciones competenciales, etc., como sí ocurre en la elaboración de las normas.

Además de ello, la ejecución de las estrategias se lleva a efecto de una forma muy ágil, por medio de planes operativos, que como se ha descrito adaptan la consecución de los objetivos generales de la estrategia a circunstancias concretas.

Sin embargo, *a sensu contrario*, la principal desventaja de llevar a cabo medidas sobre las tecnologías de la información y la comunicación, respecto a la regulación normativa tradicional, reside en la incapacidad de hacer efectivas esas medidas obligatoriamente frente a terceras personas físicas o jurídicas no pertenecientes a las organizaciones que las han dictado, ni aún el en el supuesto de que

[33] Ansoff, I. (1980). La estrategia de la empresa. Madrid: Pirámide
[34] Chandler, A. (1962). Estrategia y estructura: capítulos de la historia industrial de Estados Unidos. Barcelona: Ariel
[35] Drucker, Peter. (2008). La práctica del management. Barcelona: Ediciones Deusto
[36] Deming, W. E. (1989). Calidad, productividad y competitividad: la salida de la crisis. Madrid: Díaz de Santos

emanasen de organismos públicos, salvo que posteriormente reciban un respaldo legal, y más aún si nos circunscribimos a la ciberseguridad, cuyo grueso de medidas supone la imposición de obligaciones a sujetos "obligados". Esto deviene del principio del principio de legalidad[37] [38]que supone que las disposiciones administrativas o reglamentos no pueden imponer obligaciones o sanciones si no hay una habilitación previa por una norma con rango de ley.

Y teniendo en cuenta esta última salvedad, surge otra de las virtudes de las estrategias. Sirven de acicate y fundamento para llevar a cabo iniciativas legislativas una vez ya se ha constatado las utilidades de esas estrategias en su ámbito de aplicación. En definitiva, sin estos informes de análisis de situación ni las estrategias, no puede comprenderse la normativa sobre ciberseguridad ni el resto del ecosistema.

3.1 Estrategias internacionales

Al realizar de labor de búsqueda y recopilación de estrategias de organizaciones y agencias internacionales que traten sobre la ciberseguridad, llama la atención que estas no abundan y en muchos casos en los que han sido adoptadas, tratan la ciberseguridad de forma sectorial o tangencial dentro de estrategias más amplias dedicadas a las tecnologías de la información o la comunicación, la ciberdefensa o sobre la seguridad en su concepto más tradicional.

En este apartado se van a referir las más significativas, ya sea por su capacidad de influencia o el número de miembros de las organizaciones y agencias que las han elaborado, entre los que se encuentra España u organizaciones nacionales.

3.1.1 Organización de Naciones Unidas (ONU)

Un ejemplo de lo anterior supone la estrategia de la ONU de ciberseguridad[39], pero que está incardinada dentro de una dedicada contra el terrorismo. En la Resolución A/RES/72/284[40], aprobada por la Asamblea General el 26 de junio de 2018, se llevó a cabo el examen de la Estrategia Global de las Naciones Unidas contra el Terrorismo, donde su punto 35 reza: "*Expresa preocupación* (la Asamblea General) *ante el creciente uso, en una sociedad globalizada, por los terroristas y quienes les prestan apoyo, de las tecnologías de la información y las comunicaciones, en particular Internet y otros medios, y ante el uso de esas tecnologías para cometer actos terroristas y en actividades de incitación, reclutamiento, financiación o planificación para actos de terrorismo, hace notar la importancia de la cooperación entre las partes interesadas en la aplicación de la Estrategia, en particular entre los Estados Miembros, las organizaciones internacionales, regionales y subregionales, el sector privado y la sociedad civil, para afrontar esta cuestión, respetando los derechos humanos y las libertades fundamentales y ajustándose al derecho internacional y los propósitos y principios de la Carta, y reitera que este tipo de tecnologías pueden ser medios sumamente útiles para contrarrestar la propagación del terrorismo, entre otras cosas si se utilizan para promover la tolerancia y el diálogo entre los pueblos y la paz".*

[37] Artículo 103.1 de la Constitución Española: *"la Administración Pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la ley y al Derecho".*

[38] Artículo 47.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas: *"también serán nulas de pleno derecho las disposiciones administrativas que vulneren la Constitución, las leyes u otras disposiciones administrativas de rango superior, las que regulen materias reservadas a la Ley, y las que establezcan la retroactividad de disposiciones sancionadoras no favorables o restrictivas de derechos individuales."*

[39] https://www.un.org/counterterrorism/es/cct/programme-projects/cybersecurity

[40]https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F72%2F284&Language=E&DeviceType=Desktop&LangRequested=False

Ya se explicó al inicio de este capítulo que los planes estratégicos se elaboraban desde dos perspectivas, responder a situaciones y reconfigurar y mejorar organizaciones. Esta segunda perspectiva es la que se aborda por el Informe de 2021 de la Unidad de Inspección Conjunta sobre la Ciberseguridad en el sistema de organismos de las Naciones Unidas[41].

Al constatar que en los últimos años habían aumentado los ciberataques contra las Naciones Unidas se evaluó la eficacia de su ciberseguridad centrándose en:

- La gestión de riesgos.

- Concienciación sobre la ciberseguridad.

- La seguridad de las redes y sistemas.

- La respuesta a los incidentes.

Como resultado de lo anterior, se determinó que esos aspectos de la ciberseguridad de los organismos de las Naciones Unidas no eran del todo eficaces, por lo que el informe estableció que se debían realizar acciones que cumplieran con estos objetivos específicos para mejorar la ciberresiliencia:

- Obtener un compromiso adecuado de los órganos de gobierno con la ciberseguridad.
- Integrar la ciberseguridad en la gestión de riesgos de la organización.
- Aprovechar la convergencia entre seguridad física y ciberseguridad.
- Reconfigurar las estructuras organizativas para el cumplimiento normativo por los responsables.
- Aprovechar la contribución de los mecanismos de supervisión.
- Inculcar una cultura de ciberseguridad desde la dirección.
- Aplicar un enfoque de ciberseguridad a toda la organización.
- Establecer el personal como primera línea de ciberseguridad.
- Optimizar la asignación de recursos financieros para la ciberseguridad.
- Invertir en recursos humanos dedicados y especializados.
- Reflexionar e informar sobre los esfuerzos de toda la organización para mejorar la ciberresiliencia.

3.1.2 Foro Económico Mundial

El Foro Económico Mundial[42] es una fundación dedicada a la promoción, como organización internacional, de la cooperación público-privada desde la perspectiva empresarial. Y es precisamente con esa visión trasversal, pero enfocada al ámbito organizativo empresarial particular, desde la que realiza distintas iniciativas, siendo especialmente relevante para el caso que nos ocupa su informe Global Cybersecurity Outlook 2023[43].

Este informe de naturaleza estratégica del Foro Económico Mundial primero proporciona un análisis de las principales tendencias y desafíos en materia de ciberseguridad para las corporaciones a nivel mundial, destacando, entre ellos, que los atacantes tienen una ventaja estructural en ciberseguridad ya que solo necesitan encontrar un punto débil en una organización y puede adaptarse más rápido que las organizaciones para defenderse. Además de que ejecutar el ataque no tiene porqué requerir muchos medios, mientras que, para la defensa, los costes siempre son considerablemente mayores. Esto es lo que se viene a conocer comúnmente como la "asimetría en la ciberseguridad".

[41] https://www.unjiu.org/news/cybersecurity-united-nations-system-organizations-jiurep20213-0
[42] https://es.weforum.org/about/world-economic-forum.
[43] https://www.weforum.org/reports/global-cybersecurity-outlook-2023/.

Asimismo, el número de grupos de ciberdelincuentes profesionalizados, en ocasiones promovidos por potencias extranjeras, siguen creciendo, aumentando su especialización y creando nuevos tipos de ataques.

Paralelamente, el impacto de un solo ataque ya tiene consecuencias en terceras organizaciones debido a la cada vez más extendida interconexión e interoperabilidad de los sistemas y redes.

El informe también identifica como uno de los puntos clave, una de las premisas ya explicadas al inicio de este TFM: que la normativa sobre ciberseguridad se elabora de forma centralizada y requiere bastante tiempo, generalmente años desde su conceptualización hasta su entrada en vigor, mientras que los ciberataques se ejecutan y producen sus efectos con ubicuidad y en pocas horas.

Motivado en todo lo anterior el informe propone estas medidas para intentar conseguir organizaciones ciberresilientes:

- Proteger la cadena de suministro de los sistemas y redes de las organizaciones, algo que ya recoge, como ya se ha visto, la Directiva NIS 2.

- Contratar ciberseguros como medida de mitigación ante el impacto de un incidente.

- Alineamiento de los objetivos estratégicos de los máximos responsables de la organización, de forma que el responsable de la seguridad de la información[44] (RSI, o CISO por sus siglas en inglés) no se entienda como un responsable ajeno y/o opuesto al consejero delegado (CEO por sus siglas en inglés).

- Captar y retener personal especializado en ciberseguridad, no solamente en la operación en los sistemas y redes de la organización.

- Convencer a los máximos responsables de la organización que la inversión en ciberseguridad resulta rentable ante la probabilidad y las consecuencias para sus activos de sufrir un incidente.

- Crear una cultura de ciberseguridad y concienciación que impregne a todos los empleados de la organización.

3.1.3 Organización para la Seguridad y la Cooperación en Europa (OSCE)

La OSCE es la organización de seguridad regional más grande del mundo con 57 países miembros en América del Norte, Europa y Asia. Tiene como misión[45] "alcanzar y mantener estabilidad, paz y democracia de más de mil millones de personas, a través del diálogo político y proyectos sobre el terreno".

Entre las diversas acciones e iniciativas que realiza la OSCE, como no puede ser de otro modo en una organización dedicada a la seguridad, se presta especial atención a las tecnologías de la información y la comunicación, y por tanto a la ciberseguridad, abarcando no solo las ciberamenazas, sino la ciberdelincuencia y el ciberterrorismo. Tras determinar estos y otros retos, la OSCE ha desarrollado desde 2013 dieciséis medidas de fomento de la confianza[46] (MFC) entre sus miembros para reducir los riesgos inherentes a las tecnologías de la información y la comunicación.

En este sentido resulta de interés para su análisis en este TFM el informe de 2023 de la OSCE sobre *Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States*[47].

[44] Cuyas funciones son definidas en el artículo 7 del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

[45] https://www.osce.org/es/who-we-are.

[46] https://www.osce.org/secretariat/cyber-ict-security.

[47] https://www.osce.org/secretariat/539108.

Este informe destaca la aplicación de la ciberseguridad dentro de la medida de fomento de la confianza número catorce de la OSCE, que viene a promover la colaboración público-privada y el desarrollo de mecanismos para intercambiar las mejores prácticas de respuesta a los retos comunes de seguridad derivados del uso de las tecnologías de la información y la comunicación.

La colaboración público-privada, muy en boga estos años, ha venido a demostrar más si cabe su utilidad para lograr que la ciberseguridad alcance sus objetivos de una forma que si se realizase solo desde la perspectiva pública o la privada distaría de lograr esos grados de consecución.

Como viene a ser norma habitual en estos informes estratégicos, este, como más abajo se explica, parte de un análisis del estado de situación del que salen a relucir los desafíos para seguidamente proponer medidas de actuación para responder a esos desafíos de forma efectiva.

El informe expone que las sociedades actuales dependen en gran medida de las tecnologías digitales, por lo que la ciberseguridad resulta crítica para el bienestar económico, social y nacional. Sin embargo, los gobiernos pueden tener dificultades para comprender y responder a las amenazas cibernéticas. Por esta razón, los gobiernos dependen cada vez más de la colaboración público-privada para responder a esas las amenazas, al compartir información, cooperar en la respuesta, colaborar en la investigación, fomentar el incremento de capacidades, etc.

Además, la colaboración público-privada supone el engarce ideal entre el cumplimiento de medidas de ciberseguridad legal obligatorio y el voluntario. Pero siempre que esta colaboración se base en principios clave como la transparencia y la rendición de cuentas, ya que de otra forma podrían darse efectos perniciosos como tratar de influir en el sector público de maneras indebidas.

Los diferentes modelos de colaboración, formales o informales, dependen de los sistemas políticos, económicos y sociales de cada país.

Teniendo todo lo anterior en cuenta, este informe presenta una serie de recomendaciones aglutinadas en los epígrafes de propósito, políticas, proceso y personas. En todas esas recomendaciones se destaca que la colaboración público-privada relacionada con la ciberseguridad y otros acuerdos de esos tipos deben tener un objetivo claramente definido, para lo que se necesita llevar a cabo unas acciones.

Propósito general:

- Obtener una clara comprensión del ecosistema nacional de ciberseguridad.

- Conocer los puntos fuertes y débiles de las entidades y privadas pertinentes del país en relación con los retos de ciberseguridad y resiliencia que deben abordarse.

- Identificar las áreas en las que la colaboración público-privada podría abordar los retos identificados.

- Identificar cómo incentivar el compromiso del sector privado y otros actores relevantes.

- Determinar si es necesario un cargo gubernamental específico para facilitar o coordinar las relaciones entre los sectores público y privado.

Políticas:

- Reconocer la importancia de los acuerdos de colaboración público-privada en las políticas y estrategias nacionales de ciberseguridad, incluso concretando como esta contribuirá a alcanzar sus objetivos.

- Consultar con las entidades privadas pertinentes sobre las decisiones políticas, legislativas y reglamentarias que les afecten.

- El compromiso de establecer mecanismos de transparencia y supervisión de los acuerdos enmarcados en esa colaboración público-privada.

Proceso:

- Pactar previamente entre los actores públicos y privados los objetivos específicos del acuerdo y los problemas concretos que pretende resolver.

- Consensuar con ambas partes las actividades para alcanzar los objetivos acordados.

- Duración y fuentes de financiación.

- Los requisitos y protocolos de seguridad o confidencialidad que deben establecerse y las prácticas de ciberhigiene que deben promoverse entre los participantes.

- Mecanismos de seguimiento y supervisión de las actividades emprendidas.

- Mecanismos para revisar y actualizar las modalidades de aplicación de la colaboración público-privada

- Estrategia de comunicación y divulgación.

Personas:

- Designar claramente las partes interesadas implicadas, sus funciones y responsabilidades.

- Establecer si ese acuerdo de colaboración público-privada está abierto a todas las partes interesadas o restringido a un grupo específico.

- Determinar de qué forma los implicados contribuirán a la consecución de los objetivos de la colaboración público-privada.

- Aclarar los conocimientos y funciones específicas para facilitar las relaciones entre los agentes de los sectores público y privado implicados.

3.2 Estrategias de la Unión Europea

La Unión Europea tiene una visión estratégica muy acusada que le permite desarrollar sus políticas, normas y acciones con la suficiente antelación, más allá de las acciones reactivas y contingentes, y para lograr una mayor coherencia y homogeneidad con todas sus instituciones, organismos y agencias, así como con sus estados miembros y otras organizaciones internacionales aliadas.

Por la profusión de informes de situación, como por las competencias que ostenta la Unión Europea sobre España, estas estrategias resultan fundamentales para el desarrollo de las propias a nivel nacional, como para la actividad legislativa en la que derivan.

Como piedra angular de esa visión se encuentra la Nueva agenda estratégica para la Unión Europea 2019-2024[48], que se centra en cuatro prioridades. La primera de esas prioridades es "proteger a los ciudadanos y las libertades" y esta, a su vez, comprende siete objetivos, siendo uno de ellos el de "proteger a nuestras sociedades de ciberactividades maliciosas, amenazas híbridas y desinformación". Esto da una idea clara de la importancia que le concede la Unión Europea a la ciberseguridad[49].

Con estas premisas en mente pasamos a exponer la estrategia de mayor interés para la ciberseguridad de la UE, la Estrategia de ciberseguridad de la UE para la Década Digital y el IOCTA, que es el informe que realiza anualmente Europol.

3.2.1 Estrategia de ciberseguridad de la UE para la Década Digital

De las diferentes estrategias que la Unión Europea había acometido en el ámbito de la ciberseguridad, la Estrategia de ciberseguridad de la UE para la Década Digital[50] por su ambición y plazo es sin duda la más relevante, ya que abarca desde 2020 hasta 2030. Además de encontrarse, como no puede ser de otra forma, coordinada plenamente con la seguridad física, ya planteada en la Estrategia de la UE para una Unión de la Seguridad[51].

[48] https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/.
[49] https://www.consilium.europa.eu/es/policies/cybersecurity/.
[50] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.
[51] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0605

El objetivo general de esta estrategia es fortalecer la resiliencia de Europa ante las ciberamenazas y garantizar que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios y herramientas digitales seguros y fiables. Para ello incluye propuestas concretas para la implementación de instrumentos normativos, de actuación y de inversión.

En su parte introductoria se destacan reflexiones sobre las amenazas para la ciberseguridad de la Unión Europea:

- El transporte, la energía y la salud, las telecomunicaciones, las finanzas, la seguridad, los procesos democráticos, el espacio y la defensa dependen en gran medida de las redes y sistemas información, que están cada vez más interconectados.

- El panorama de las amenazas se ve agravado por las tensiones geopolíticas sobre un internet global y abierto y sobre el control de las tecnologías en toda la cadena de suministro.

- El ataque malicioso a infraestructuras críticas es un riesgo global importante.

- La preocupación por la seguridad es un importante desincentivo para el uso de los servicios en línea.

- La investigación de casi todos los tipos de delitos tiene un componente digital.

- Los servicios digitales y el sector financiero figuran entre los objetivos más frecuentes de los ciberataques, junto con el sector público y el de la producción, pero, a pesar de ello, la preparación y la concienciación sobre ciberseguridad entre las empresas y las personas siguen siendo escasas.

- La UE carece de una conciencia colectiva de la situación de las ciberamenazas.

Teniendo en cuenta esas amenazas y los logros conseguidos con estrategias anteriores, esta estrategia contiene propuestas concretas para desplegar tres instrumentos principales -reguladores, de inversión y políticos- para abordar los siguientes tres ámbitos de actuación de la Unión Europea.

Resiliencia, soberanía tecnológica y liderazgo

Este ámbito tiene como objetivos proteger las infraestructuras críticas y los servicios esenciales de la Unión Europea y de liderar el desarrollo de tecnologías seguras en toda la cadena de suministro. Para ello, se centra aspectos más concretos, como son:

- Infraestructuras y servicios críticos resilientes.

- Creación de un escudo cibernético europeo.

- Una infraestructura de comunicaciones ultrasegura.

- Asegurar la próxima generación de redes móviles de banda ancha.

- Una internet de las cosas segura (IoT).

- Mayor seguridad global de internet.

- Una presencia reforzada en la cadena de suministro tecnológico.

- Una mano de obra de la UE cibercualificada.

Del examen de todos los anteriores se obtienen unas conclusiones que vendrían a ser las líneas de acción para abordar esos retos, destacando que varias de ellas, como se incide más arriba, suponen actuaciones legislativas (un ejemplo más de la promoción de actividad regulatoria por medio de los informes y estrategias).

De esta forma, se concluye que se han de realizar estas acciones:

- Inversión en ciberseguridad (especialmente a través del Programa Europa Digital, Horizonte Europa y el mecanismo de recuperación).

- Una red de la UE de centros de operaciones de seguridad (SOC, por sus siglas en inglés) basados en la inteligencia artificial y una infraestructura de comunicación ultrasegura que aproveche las tecnologías cuánticas.

- Adopción generalizada de tecnologías de ciberseguridad mediante el apoyo específico a las PYME.

- Desarrollo de un servicio de resolución de sistema de nombres de dominio (DNS, por sus siglas en inglés) de la UE como alternativa segura y abierta para que los ciudadanos, las empresas y la administración pública de la UE accedan a Internet. Aquí hay que reseñar también que la Directiva NIS 2 ha regulado varios aspectos de los DNS.

- Finalización de la aplicación de la "5G Toolbox", los mecanismos para afianzar la seguridad de las redes 5G. La última revisión de la aplicación de instrumentos de la UE para la seguridad de las redes 5G[52] se ha efectuado por la Comisión Europea en junio de 2023.

Desarrollo de la capacidad operativa para prevenir, disuadir y contrarrestar

Los ciberincidentes, ya sean accidentales o deliberados, pueden causar enormes daños. Su escala y complejidad provocan que esas amenazas sean muy difíciles de contrarrestar sin un intercambio de información sistemático y exhaustivo y sin la cooperación en una respuesta común.

Con esto en consideración, la Unión Europea pretende; mediante instrumentos normativos, la movilización, la cooperación y la coordinación de redes de contacto, instituciones, organismos y agencias de la UE, así como por autoridades de los Estados miembros y sus CSIRT; conseguir prevenir, disuadir, disuadir y responder a estos ciberincidentes. De forma específica propone estas medidas:

- Crear una Unidad Cibernética Conjunta.
- Lucha contra la ciberdelincuencia.
- Herramientas de ciberdiplomacia de la UE.
- Refuerzo de las capacidades de ciberdefensa.
- Iniciativas estratégicas.

Del mismo modo que el anterior ámbito el análisis de estas medidas culmina con estas iniciativas:

- Completar el marco europeo de gestión de crisis de ciberseguridad y determinar el proceso, los hitos y el calendario para establecer la Unidad Cibernética Conjunta[53]. La Unión Europea todavía está trabajando en esta plataforma, que tiene como fin reforzar la cooperación entre las instituciones, agencias, organismos y autoridades de los Estados miembros de la UE para aprovechar todo su potencial.
- Continuar la aplicación de la agenda sobre ciberdelincuencia en el marco de la Estrategia de la Unión de la Seguridad. De esta forma, confluyen aquí, como se ha repetido anteriormente, la ciberseguridad y la ciberdelincuencia. En esta ocasión por la ligazón entre la Estrategia de ciberseguridad de la UE para la Década Digital y la Estrategia de la UE para una Unión de la Seguridad de 2020[54], al reconocer esta última a la ciberdelincuencia como una de las principales amenazas para la seguridad de la Unión Europea.
- Fomentar y facilitar la creación de un grupo de trabajo de ciberinteligencia de los estados miembros que resida en el INTCEN[55] (Centro de inteligencia y situación de la Unión Europea).

[52]https://digital-strategy.ec.europa.eu/es/library/communication-commission-implementation-5g-cybersecurity-toolbox
[53] https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit
[54] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0605
[55] https://op.europa.eu/es/web/who-is-who/organization/-/organization/EEAS_INTCEN/EEAS_INTCEN

- Avanzar en la postura de ciberdisuasión de la UE para prevenir, desalentar, disuadir y responder a las ciberactividades maliciosas.
- Revisar el Marco político de ciberdefensa[56].
- Facilitar el desarrollo de una "Visión y estrategia militar de la UE sobre el ciberespacio como dominio de operaciones" para las misiones y operaciones militares.
- Apoyar las sinergias entre las industrias civil, de defensa y espacial[57].
- Reforzar la ciberseguridad de las infraestructuras espaciales críticas en el marco del Programa Espacial.

Fomentar un ciberespacio mundial y abierto

La UE debe promover un modelo internacional del ciberespacio basado en el estado de Derecho, los derechos humanos, las libertades fundamentales y los valores democráticos, para lo que resulta esencial la cooperación internacional. Este fin se articula con tres propuestas:

- Liderazgo de la UE en materia de estándares, normas y marcos en el ciberespacio.

- Cooperación con los socios y la comunidad de múltiples partes interesadas.

- Refuerzo de las capacidades mundiales para aumentar la resistencia mundial.

Para la consecución de estas propuestas se establecen estas líneas de actuación, algunas de las cuales ya se han llevado a efecto:

- Definir objetivos en los procesos de normalización internacionales y promoverlos.
- Fomentar la seguridad y la estabilidad internacional en el ciberespacio. Enfocando los esfuerzos de la UE y sus Estados miembros en un Programa de acción para avanzar en la actuación responsable de los Estados en el ciberespacio en las Naciones Unidas.
- Realizar una guía sobre la aplicación de los derechos humanos y las libertades fundamentales en el ciberespacio.
- Incidir en la protección de la infancia contra el abuso sexual y su explotación de menores y la Estrategia sobre los Derechos de la Infancia.
- Fortalecer y promover el Convenio de Budapest sobre la Ciberdelincuencia. Algo que ya se ha hecho tras la elaboración y ratificación de su Segundo Protocolo adicional al Convenio de Budapest.
- Ampliar el diálogo cibernético, no solo en relación a la ciberseguridad, de la UE con terceros países, organizaciones regionales e internacionales y empleando también para ello la Red de Ciberdiplomacia informal de la UE.
- Reforzar los intercambios con múltiples partes interesadas, con el intercambio periódico y organizado con el sector privado, la academia[58] y el resto de la sociedad civil. Esta acción no deja de ser la colaboración público-privada de la que ya se ha venido hablando a lo largo del presente.
- Desarrollar una agenda para el desarrollo de la capacidad cibernética exterior de la UE y un consejo para lograrlo.

En lo tocante a la ciberseguridad de las propias instituciones, órganos y organismos de la UE se proponen estas actuaciones para disminuir el impacto de las crecientes amenazas a sus redes y sistemas de información:

[56] http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/es/pdf

[57] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12611-Industrias-civil-de-defensa-y-espacial-plan-de-accion-sobre-sinergias_es

[58] Entendido aquí en el entorno estratégico como los representantes de centros de investigación o de enseñanza superior.

- Proteger más eficazmente la confidencialidad de la información clasificada y la confidencial no clasificada.
- Armonizar y dotar de mayor coherencia las normas de ciberseguridad para todas instituciones, órganos y organismos de la UE.
- Implantar un Programa de concienciación cibernética para el personal de todas las instituciones, órganos y organismos de la UE sobre la ciberhigiene y la cultura común de ciberseguridad en general.
- Reforzar el CERT-EU[59], que es el CSIRT específico para esas instituciones, órganos y organismos, dotándole de una financiación acorde a sus necesidades.

Estas actuaciones se pretenden realizar mediante estos proyectos normativos que las fundamenten y sustenten:

- Reglamento sobre la Seguridad de la Información en los organismos y agencias de las instituciones de la UE.
- Reglamento relativo a las normas de ciberseguridad comunes para las instituciones, organismos y agencias de la UE.
- Un nuevo fundamento legal para que el CERT-UE refuerce su mandato y su financiación.

No obstante, hasta que estos proyectos lleguen a poder articularse, la Directiva NIS 2 ya contempla en su capítulo III para la cooperación a nivel de la Unión e internacional parte de esas propuestas.

Finalmente, esta Estrategia de ciberseguridad de la UE para la Década Digital en sus conclusiones establece que la UE ha de impulsar estándares y normas con el objetivo de alcanzar soluciones de ciberseguridad a nivel internacional. Esta premisa viene confirmar lo referido al principio de este capítulo: que los planes estratégicos suponen uno de los principales motivos para la creación de normas y la aplicación de certificaciones, aquí referidos como estándares.

3.2.2 IOCTA 2023

Europol[60] es la agencia de la Unión Europea que tiene la misión de asistir a los Estados miembros en la prevención y la lucha contra toda forma grave y organizada de delincuencia, ciberdelincuencia y terrorismo a escala internacional.

Entre sus cometidos se encuentra el de elaborar informes estratégicos periódicos sobre criminalidad organizada (SOCTA), terrorismo (TESAT) y ciberdelincuencia (IOCTA), siendo el último de estos por su estrecha vinculación con la ciberseguridad el de mayor interés para este TFM.

El informe estratégico de Evaluación de la Amenaza de la Delincuencia Organizada en Internet (IOCTA por sus siglas en inglés) se elabora con una frecuencia anual. Estando en este momento ya disponible el IOCTA 2023[61].

Al ser meramente un informe estratégico y no una estrategia completa, la parte de la misma encargada de plasmar las líneas a ejecutar se lleva a cabo de forma separada a través de la Plataforma Multidisciplinar Europea contra las Amenazas Delictivas (EMPACT por sus siglas en inglés) que tiene en cuenta los riesgos y amenazas detectados en el IOCTA y fija unas líneas de acción para prevenirlos y facilitar la persecución de esos ciberdelitos por medio de planes operativos concretos.

El informe IOCTA 2023 destaca la creciente amenaza de la ciberdelincuencia en la UE, enfocándose en ciberataques, explotación sexual infantil en línea y fraudes en línea, representando una seria amenaza para personas, organizaciones y la economía de la UE.

[59] https://cert.europa.eu/

[60] https://www.europol.europa.eu/about-europol:es

[61]https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023#downloads

También refleja como los ciberdelincuentes, no solo están altamente especializados, sino que, además entre los que no conforman organizaciones criminales, se da el caso de que pueden recurrir, a través de los foros de la web oscura, a organizaciones delictivas que les proveen de las herramientas informáticas necesarias o incluso delegar la comisión, lo que se conoce como "crimen como servicio".

Respecto a las técnicas comunes más habituales para iniciar el delito (los ciberdelitos requieren de diversas fases en su *iter criminis*) tiene mayor predicamento el "*phising*", que por medio de técnicas de ingeniería social permite el acceso ilegítimo a las redes y sistemas tras conseguir engañar a la víctima.

Dentro de los delitos mencionados al comienzo, el robo de datos es el bien que resulta el más provechoso para los cibercriminales, ya sea para revenderlos en la web oscura o para aprovecharlos para suplantar identidades (con la ulterior estafa), amenazas condicionales, etc.

La web oscura resulta fundamental para los cibercriminales por los motivos expuestos más arriba, pero además facilita un lugar para acoger a comunidades dedicadas a formar y reclutar ciberdelincuentes.

Como se aprecia, excepto los delitos de índole sexual y algunos otros, la principal motivación de los cibercriminales es el lucro económico, ya sea logrando el enriquecimiento injusto directamente o siendo retribuidos por sus servicios por terceros. Para el blanqueo de sus ganancias recurren al intercambio de criptomonedas, apuestas en línea y el uso de "mulas" o "pitufos" (en argot policial son las terceras personas físicas que retiran el dinero físico y lo transportan).

Para combatir todo lo anterior, además de los EMPACT ya referidos, Europol ha establecido unidades especializadas como el Centro Europeo de Ciberdelincuencia (EC3) y el Grupo Operativo Conjunto de Acción contra la Ciberdelincuencia (J-CAT) para combatir este tipo de delitos. Asimismo, cuenta con herramientas y servicios de apoyo para las fuerzas y cuerpos de seguridad, como son el Sistema de Información de Europol (EIS), la Plataforma de Expertos de Europol (EPE) y el Sistema de Análisis de Europol (EAS).

3.3 Estrategias nacionales

Una vez más hay que sacar a colación que una de las incontables consecuencias relevantes de la integración de España en la Unión Europea es su sujeción estratégica en múltiples ámbitos. De tal forma que España, ya sea por un imperativo legal, como puede ser la obligación establecida en el artículo 7 de la Directiva NIS 2 de adoptar una Estrategia nacional de ciberseguridad, o inspirada por la visión estratégica de la UE, desarrolla planes estratégicos plenamente coherentes y alineados con las políticas y directrices de la UE. Esto no deja de ser otra dimensión de la integración, en el mismo sentido que lo son las trasposiciones nacionales de las directivas comunitarias en el ámbito puramente normativo.

Sin embargo, esa alineación con esas estrategias supranacionales no impide que España sea proactiva a la hora de elaborar estrategias por su propia iniciativa, como es el ejemplo del Plan Estratégico contra la Cibercriminalidad del Ministerio del Interior, que será comentado más abajo tras explicar seguidamente las estrategias nacionales de ciberseguridad por su orden de prevalencia.

3.3.1 Estrategia de Seguridad Nacional 2021

Como ya se ha mencionado más arriba, la UE cuenta desde 2020 con la Estrategia de la UE para una Unión de la Seguridad, y precisamente esta, como no puede ser de otra forma, sirve como uno de los fundamentos para nuestra Estrategia de Seguridad Nacional 2021.

Y es en esta estrategia nacional, sobre la que vamos a hablar seguidamente, donde se da una convergencia entre el ámbito estratégico y el normativo, ya que fue aprobada por medio del Real Decreto 1150/2021, de 28 de diciembre.

Esta estrategia refleja en sus tres primeros capítulos el estado actual de situación para la seguridad nacional, posteriormente marca unos objetivos y líneas de acción acordes a lo constatado con antelación y finalmente explica de forma somera en qué consiste el Sistema de Seguridad Nacional y el

funcionamiento de la gestión de crisis. Como se va a referir seguidamente, en todo el texto de la estrategia se confiere un rol prominente a la ciberseguridad.

El primer capítulo aborda diferentes cuestiones sobre el contexto internacional de seguridad y las dinámicas de transformación. En el apartado específico al contexto geopolítico se destacan las tecnologías 5G[62], la inteligencia artificial, los ciberataques y la desinformación. Además, llama la atención en relación a la transformación digital el gran reto que supone conjugar, por un lado, su notable y creciente implantación, con la suficiente seguridad en la virtualización de redes o el internet de las cosas.

El capítulo tercero de la estrategia expone los riesgos y amenazas para la seguridad nacional resaltando el protagonismo de las estrategias híbridas, en la que una de sus facetas se ejecuta por medio de las tecnologías de la información y la comunicación. Del mismo modo que deja claro que además de los tradicionales dominios de defensa, terrestre, naval y aéreo, ahora es inexcusable prestar atención al ciberespacio.

De forma más concreta, este capítulo explica el riesgo que suponen para el ciberespacio, en general, y para las infraestructuras críticas, en particular, la explotación de las vulnerabilidades de la digitalización, las tecnologías 5G, el uso de la inteligencia artificial y el *big data*, así como las campañas de desinformación, llevadas a cabo por la criminalidad organizada, la delincuencia grave, el ciberterrorismo o terceros países hostiles, que, a su vez, además pueden realizar labores de ciberespionaje.

Como es norma habitual en los planes estratégicos, conforme se ha explicado con anterioridad, tras el análisis de la situación, enumerando los activos y bienes jurídicos a proteger respecto a los riesgos y amenazas, se marcan unos objetivos, con unos ejes estratégicos y líneas de acción que los desarrollan. De esta manera, el capítulo cuarto de la Estrategia de Seguridad Nacional de 2021 tiene estos tres objetivos:

- El primer objetivo es avanzar en el modelo de gestión de crisis.

- El segundo objetivo es favorecer la dimensión de seguridad de las capacidades tecnológicas y de los sectores estratégicos.

- El tercer objetivo es desarrollar la capacidad de prevención, disuasión, detección y respuesta de España frente a estrategias híbridas, en un contexto de seguridad en el que las amenazas convencionales se alternan con el uso combinado de vectores económicos, tecnológicos, diplomáticos y de información, entre otros, como elementos de presión y desestabilización.

En virtud de estos objetivos se establecen los siguientes tres ejes estratégicos para darles respuesta, que, a su vez, se desglosan en apartados específicos y sus correspondientes líneas de acción que se implementarán en planes operativos. En relación con los diversos aspectos de la ciberseguridad se contemplan aquí los siguientes:

En el primer eje, sobre una España que protege la vida de las personas y sus derechos y libertades, así como el orden constitucional, la ciberseguridad sale a colación en su parte referente a la actuación frente a situaciones de crisis, la contrainteligencia y en la lucha contra las campañas de desinformación y acción frente a las injerencias del exterior.

En relación a esas campañas de desinformación, cabe destacar que ya se ha publicó el 27 de septiembre de 2022 por el Departamento de Seguridad Nacional el documento Lucha contra las

[62] Un nuevo ejemplo de cómo una estrategia es un acicate para la actividad legislativa es el posterior Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación y que viene a dar una respuesta complementaria legal a la operativa prevista en esta Estrategia de Seguridad Nacional de 2021.

campañas de desinformación en el ámbito de la seguridad nacional: propuestas de la sociedad civil[63]. Se elaboró en alineado con la estrategia de la Unión Europea para hacer frente a las campañas de desinformación, recogida en su Plan de Acción contra la desinformación, de diciembre de 2018, y en el Plan de Acción para la Democracia Europea, de diciembre de 2020.

En el segundo eje, respecto a una España que promueve la prosperidad y el bienestar de los ciudadanos, se destaca especialmente como un ámbito de actuación, dentro de la seguridad de los espacios comunes globales, el ciberespacio.

Finalmente, reseñar el tercer eje referido a una España que participa en la preservación de la paz y seguridad internacional y defiende sus intereses estratégicos.

El capítulo quinto, es donde se recogen las premisas principales en esta estrategia del Sistema de Seguridad Nacional, que emana de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, y en el que se recalca que el Consejo de Seguridad Nacional es el organismo vertebrador del Sistema. Y esto es aquí especialmente interesante porque sirve de engarce para otros mecanismos subyacentes de ciberseguridad, como es el Consejo Nacional de Ciberseguridad.

3.3.2 Estrategia Nacional de Ciberseguridad 2019

Por sus propósitos, alineamiento con otras de ámbito supranacional y alcance esta estrategia supone sin duda la de mayor relevancia para la ciberseguridad nacional. El mandato original para la elaboración de esta estrategia proviene de la Directiva NIS.

La Estrategia Nacional de Ciberseguridad de 2019 viene a desarrollar todo lo mencionado sobre ciberseguridad en la Estrategia de Seguridad Nacional de 2017 y fue publicada en la Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.

Aquí es importante evidenciar que, aunque esta Estrategia Nacional de Ciberseguridad se refiere a la Estrategia de Seguridad Nacional de 2017 en lugar de a la posterior de 2021, la implementación final de la estrategia por medio del Plan Nacional de Ciberseguridad de 2022, (que es el que adjudica las medidas operativas de la estrategia a diferentes órganos y unidades y con una dotación presupuestaria concreta) permite una adaptación a las realidades más recientes.

La Estrategia Nacional de Ciberseguridad plasma primero el estado de situación para seguidamente marcar las actuaciones para afrontarla y finalmente circunscribe la ciberseguridad en el Sistema de Seguridad Nacional.

En el capítulo 1: el ciberespacio como espacio común global, la estrategia llama la atención sobre varias cuestiones.

Oportunidades y desafíos: el ciberespacio “territorialmente” destaca por la carencia de una verdadera soberanía y jurisdicción que haga cumplir eficazmente, por otro lado, el desarrollo de las tecnologías de la información y la comunicación resulta vertiginoso. Todo ello alentado por el aumento de la digitalización desde el entorno físico al virtual, la inteligencia artificial, la robótica, el *big data*, el *blockchain* y el internet de las cosas (IoT).

Estos factores acrecientan las vulnerabilidades de los servicios esenciales y, por ende, de las infraestructuras críticas y sus cadenas de suministro. Para paliar estos riesgos y tratar de poner cierta coherencia en las medidas de seguridad y las diferentes certificaciones entre la miríada de sistemas esenciales e importantes en los Estados miembros, es precisamente para lo que se ha llevado a cabo la publicación de la Directiva NIS 2.

[63]https://www.dsn.gob.es/es/documento/lucha-contra-campa%C3%B1as-desinformaci%C3%B3n-%C3%A1mbito-seguridad-nacional-propuestas-sociedad-civil

España, consciente de estos desafíos está integrada en organismos supranacionales que coadyuvan en sus esfuerzos e iniciativas para reforzar la ciberseguridad global, mencionando expresamente a la Unión Europea, la OTAN y las Naciones Unidas.

Igualmente, se concibe una concepción novedosa del ciberespacio con un enfoque no solo internacional, como el ya citado, sino multidisciplinar, que supere el ámbito más técnico y que facilite la participación del sector privado, en lo que se conoce como colaboración público-privada.

Ese enfoque también se dirige a reorientar el modelo de ciberseguridad de carácter preventivo y defensivo hacia uno que resulte disuasorio a través de las capacidades adquiridas.

Otra de las ideas fuerza es potenciar la ciberinteligencia que no solo ayuda a la prevención al reconocer las tácticas, técnicas y procedimientos (TTP´s) de los atacantes, sino que facilita la posterior atribución de los hechos a los responsables.

Finalmente, este capítulo resalta la importancia de promover en toda la sociedad la cultura de ciberseguridad, para que los ciudadanos tomen conciencia de los riesgos, amenazas y medidas para paliarlos como corresponsables de la ciberseguridad.

El capítulo 2: las amenazas y desafíos en el ciberespacio, tomando como punto de partida la Estrategia de Seguridad Nacional de 2017, diferencia entre las amenazas sufridas, por un lado, por las propias redes, sistemas y dispositivos digitales, y por otro, las amenazas para cualquier bien jurídico llevadas a cabo a través de las tecnologías de la información y la comunicación (siendo esta también una división ya tradicional en cuanto a las dos vertientes de la cibercriminalidad).

En el primer supuesto cobran importancia por su relativa novedad las acciones de ciberespionaje, cuyas acciones se han visto multiplicadas, sobre su vis física tradicional, pues como ocurre en gran medida con la cibercriminalidad, la comisión se lleva a efecto con más garantías de anonimato y permite asimismo tratar de obtener información de forma colectiva.

Otra de las amenazas que salen a colación en este apartado son las híbridas, que esta estrategia define al principio de ese capítulo 2 como “acciones coordinadas y sincronizadas dirigidas a atacar de manera deliberada las vulnerabilidades sistémicas de los estados democráticos y las instituciones, a través de una amplia gama de medios, tales como acciones militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica”.

Actores estatales y no estatales, bien de forma directa o a través de intermediarios, explotan las facilidades que ofrece Internet para la desinformación y propaganda y un interés generalizado en la obtención y desarrollo de capacidades militares para operar en el ciberespacio, incluyendo en muchos casos capacidades ofensivas.

En relación a la cibercriminalidad, como más adelante se expondrá cuando se explique el Plan estratégico contra la cibercriminalidad del Ministerio del Interior, hay destacar aquí no solo un importante incremento de los delitos con una componente de las tecnologías de la información y la comunicación, sino la disminución de los de los delitos tradicionales físicos respecto a los digitales.

Entre esos delitos, por su relevancia, hay que mencionar el ciberterrorismo, cuyos tipos penales ya fueron adecuados en el Código Penal a las nuevas manifestaciones de comisión por medio de la Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo.

Tampoco hay que olvidar el fenómeno de contratar servicios de cibercriminales expertos, como un paso más en la concepción tradicional penal del cooperador necesario, para la comisión de gran número de tipos penales.

Como elemento común, amén de muchos otros, a los dos tipos amenazas mencionados al inicio del capítulo 2, se encuentran los datos personales. Ya que como fin o como medio tienen una importancia crucial en la ciberseguridad y en la cibercriminalidad. Prueba de ello es la protección no solo penal de

forma tangencial, sino directa por otros órdenes jurisdiccionales, a través del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE; la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Ese capítulo 2 concluye exponiendo la amenaza cada vez con más impacto de las campañas de desinformación para las organizaciones internacionales, los estados, los procesos electorales, etc. y sobre las que ya se ha citado más arriba el documento sobre Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional: propuestas de la sociedad civil.

El capítulo 3 refleja el propósito, principios y objetivos de esta estrategia. De nuevo a colación de la Estrategia de Seguridad Nacional de 2017, el propósito, según se establece al comienzo del capítulo, es "garantizar un uso seguro y responsable de las redes y los sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para un contribuir a la promoción de un ciberespacio seguro y fiable".

Este propósito se ve complementado por estos cuatro principios rectores que han de impregnar a todas las medidas que la vayan a ejecutar: unidad de acción, anticipación, eficiencia y resiliencia:



Figura 8 Principios rectores de la Estrategia Nacional de Ciberseguridad 2019[64]

[64] Fuente: Estrategia Nacional de Ciberseguridad 2019.

Tras ello, la estrategia establece su objetivo general de "garantizar el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico", que, a su vez, se ve desglosado en estos otros cinco objetivos específicos:

- Objetivo I: Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.

Determina la necesidad de consolidar un marco nacional para la ciberseguridad de la información gestionada por el sector público y por los servicios esenciales. Concretando que para ello hay que establecer medidas de seguridad dirigidas a la prevención, detección y respuesta ante incidentes, sin dejar de contemplar la correspondiente adaptación del ordenamiento jurídico.

Sin perjuicio, de la concreta ejecución en diversas medidas, se puede adelantar aquí, que precisamente la Directiva NIS 2, con su trasposición que se está llevando a cabo en estos momentos, aborda directamente esas cuestiones.

- Objetivo II: Uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso.

Para la consecución de este objetivo se ha de lograr una adecuada persecución de los ciberdelitos en estos tres ámbitos:

- El ciberespacio como objetivo directo del delito o la amenaza.
- El ciberespacio como medio para la comisión del delito.
- El ciberespacio como medio u objeto directo de investigación.

Y para ello se ha de contar con unas normas penales y procesales apropiadas pero también resulta fundamental fortalecer la cooperación judicial y policial, tanto nacional como internacional. Sin olvidar la indispensable formación específica de todos esos funcionarios ni el fomento de la colaboración y participación ciudadana con las Fuerzas y Cuerpos de Seguridad y con el Poder Judicial, del mismo modo que se realiza en el ámbito físico.

- Objetivo III: Protección del ecosistema empresarial y social y de los ciudadanos.

Como ya se ha afirmado más arriba, hacer un uso seguro del ciberespacio es un derecho indiscutible de los ciudadanos y las organizaciones, públicas y privadas, pero, dada la magnitud de la implantación de las tecnologías de la información y la comunicación y el incesante proceso de transformación digital, resulta esencial que estos actores asuman su responsabilidad implementando no solo medidas de autoprotección, sino también medidas de ciberdefensa activa.

- Objetivo IV: Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológica.

España ha de poseer recursos técnicos y humanos para contar con una autonomía tecnológica que refuerce su ciberseguridad. Siendo este objetivo corroborado con las situaciones que la reciente pandemia del Covid 19 ha puesto de relieve.

Y esto se puede especificar promoviendo la capacitación de profesionales con formación especializada en ciberseguridad, fomentado el I+D+i en ciberseguridad y el empleo de productos y servicios certificados (esto último se pretende conseguir mediante el proyecto de Reglamento de Europeo de Ciberresiliencia ya comentado en este TFM).

Este objetivo no desatiende la protección del patrimonio tecnológico y de la propiedad industrial e intelectual. Para lo que, entre otras medidas, ya se cuenta con la Ley 19/2003, de 4 de julio, sobre régimen jurídico de los movimientos de capitales y de las transacciones económicas con el exterior y sobre determinadas medidas de prevención del blanqueo de capitales.

- Objetivo V: Seguridad del ciberespacio en el ámbito internacional.

España promoverá un ciberespacio seguro tanto en sus relaciones bilaterales como en las organizaciones multilaterales, así como en los foros en los que participe y proceda. De este modo,

continuará participando en las políticas e iniciativas en ese sentido como estado miembro de las Naciones Unidas, la OTAN, la Unión Europea, la Organización para la Seguridad y la Cooperación en Europa (OSCE), en la Organización de Estados Americanos (OEA), etc. Además, se ha de reforzar la cooperación bilateral sobre ciberseguridad con terceros estados.

Tras haber reflejado todos los objetivos, la Estrategia Nacional de Ciberseguridad 2019 dedica su capítulo 4 a asignar las siete líneas de acción que responderán a esos objetivos desarrollando sesenta y cinco medidas. Estas, a su vez se adjudicarán a distintos órganos de los departamentos ministeriales, por medio del Plan Nacional de Ciberseguridad, este sí, clasificado de difusión limitada.

- Línea de Acción 1. Reforzar las capacidades ante las amenazas provenientes del ciberespacio. Esta línea de acción responde al Objetivo I de la Estrategia y se compone de 12 medidas.

Siendo una de ellas la encaminada a "desarrollar y mantener actualizadas las normas, procedimientos e instrucciones de respuesta frente a incidentes de ciberseguridad, asegurando su integración en el Sistema de Seguridad Nacional". Un ejemplo más del impulso normativo promovido por las estrategias

- Línea de Acción 2. Garantizar la seguridad y resiliencia de los activos estratégicos para España. Esta línea de acción responde al Objetivo I de la Estrategia y se compone de 12 medidas.

Se destacan aquí dos medidas que también fomentan la creación o modificación de normas y certificaciones para adaptar la ciberseguridad al estado de situación:

- "Potenciar el desarrollo de la normativa sobre protección de infraestructuras críticas, reforzando la seguridad de las redes y sistemas de información que las soportan".
- "Asegurar la plena implantación del Esquema Nacional de Seguridad, del Sistema de Protección de las Infraestructuras Críticas, y el cumplimiento y armonización de la normativa sobre protección de infraestructuras críticas y servicios esenciales, con un enfoque prioritario basado en el riesgo".

- Línea de Acción 3. Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio. Esta línea de acción responde al Objetivo II de la Estrategia y se compone de 9 medidas.

- Línea de Acción 4. Impulsar la ciberseguridad de ciudadanos y empresas. Esta línea de acción responde al Objetivo III de la Estrategia y se compone de 9 medidas.

Su medida 7 tiene por objeto "impulsar en el sector empresarial la implantación de estándares reconocidos de ciberseguridad. Estimular, junto con las entidades de normalización nacional e internacional, la creación, difusión y aplicación de mejores prácticas sectoriales en materia de ciberseguridad, incluidos diferentes esquemas de certificación". De esta forma reconoce la estrategia importancia de las certificaciones para la ciberseguridad.

- Línea de Acción 5. Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital. Esta línea de acción responde al Objetivo IV de la Estrategia y se compone de 9 medidas.

- Línea de Acción 6. Contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales. Esta línea de acción responde al Objetivo V de la Estrategia y se compone de 9 medidas.

- Línea de Acción 7. Desarrollar una cultura de ciberseguridad. Esta línea de acción responde al Objetivo IV de la Estrategia y se compone de 8 medidas. Pero, además contribuye al Plan de Cultura de Seguridad Nacional, que ha sido publicado en la Orden PCM/575/2021, de 8 de junio, por la que se publica el Acuerdo del Consejo de Ministros de 25 de mayo de 2021.

Finalmente, el capítulo 5 de la Estrategia Nacional de Ciberseguridad 2019 explica la integración de la ciberseguridad en el Sistema de Seguridad Nacional a través de estos organismos:

- El Consejo de Seguridad Nacional: órgano emanado de la Ley 36//2015 de Seguridad Nacional con la función, conforme a su artículo 17, de "asistir al Presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional".

- El Comité de Situación: bajo las directrices del Consejo de Seguridad Nacional, gestiona las crisis que desborden los mecanismos de respuesta habituales.

- El Consejo Nacional de Ciberseguridad: apoya al Consejo Nacional de Ciberseguridad en el ámbito de la ciberseguridad y fomenta la coordinación, colaboración y cooperación público-privada. Sus funciones son detalladas por medio de la Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad.

- La Comisión Permanente de Ciberseguridad: asiste al Consejo Nacional de Ciberseguridad en cuestiones más operativas y técnicas en relación a los riesgos y las ciberamenazas.

- Foro Nacional de Ciberseguridad: tiene por objeto fomentar sinergias para aprovechar oportunidades y afrontar amenazas del ciberespacio. Está compuesto por representantes expertos de asociaciones, la academia (docentes e investigadores de la Universidad), otros sectores privados y representantes del sector público.

- Autoridades públicas competentes y los CSIRT de referencia nacionales: Estas son a día de hoy las reflejadas en el Real Decreto-ley 12/2018 y en el Real Decreto 43/2021 y con las funciones comentadas en esos apartados del presente.

3.3.3 Estrategia España Digital 2026

Esta estrategia de España Digital 2026[65] resulta fundamental para la implementación de las tecnologías de la información y la comunicación en España, impulsando los procesos de transformación digital en nuestro país.

España Digital actúa en tres dimensiones (infraestructuras y tecnología, empresas y personas), en las que se distribuyen doce ejes estratégicos, que, a su vez, contemplan múltiples medidas.

En cuanto a la ciberseguridad, nuestro objeto de estudio, la estrategia le dedica su eje número tres, constando de esta forma en ese eje: "El reto para 2026 es incrementar las capacidades de ciberseguridad en España, fomentar el desarrollo del ecosistema empresarial en este sector (industria, I+D+i y talento), y potenciar el liderazgo internacional del país en materia de ciberseguridad".

La estrategia, como no puede ser de otra forma, considera la ciberseguridad como un "eje crítico" para el proceso de transformación digital y destaca acciones que ya se han llevado a cabo, están en estado germinal, procedentes de la anterior Estrategia España Digital 2025, como son el Plan de Choque de Ciberseguridad, para el fortalecimiento de capacidades de ciberseguridad de la ciudadanía, pymes y profesionales, el Centro de Operaciones de Ciberseguridad de la Administración General del Estado, la aprobación del Plan Nacional de Ciberseguridad (mencionado en el apartado anterior) o la aprobación del Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, del que ya se ha hablado en el presente.

Asimismo, se aprovecha para sacar a colación un dato que no resulta baladí: España es el segundo país a nivel mundial con más equipos de respuesta a incidentes (CERT/ CSIRT), solo tras Estados Unidos.

Como medidas específicas de ciberseguridad este eje refleja estas cuatro:

[65] https://portal.mineco.gob.es/es-es/ministerio/estrategias/Paginas/00_Espana_Digital.aspx

- Fortalecimiento de la ciberseguridad de la ciudadanía, pymes y profesionales. Para ello se aumenta el capital para fortalecer la concienciación respecto a los riesgos asociados a la digitalización y para la formación específica en competencias digitales de ciberseguridad.

- Impulso del ecosistema empresarial del sector ciberseguridad. Esta medida se focaliza en fomentar la I+D+i e identificar y desarrollar el talento de profesionales en ciberseguridad.

- Impulso de España como nodo internacional en el ámbito de la ciberseguridad. Con el objetivo de cumplir con esta meta se ha proyectado el Centro Nacional de Competencias en Ciberseguridad (NCC-ES).

- Despliegue y operación de centros de operaciones de ciberseguridad. Como ya se ha apuntado más arriba, se sigue avanzando en la materialización del Centro de Operaciones de Ciberseguridad, que tendrá como misión reforzar la prevención, monitorización, vigilancia y respuesta a ciberincidentes de los sistemas de la Administración General del Estado y de sus organismos dependientes.

3.3.4 Plan Estratégico contra la Cibercriminalidad del Ministerio del Interior

Como se puso de relieve en la introducción del presente y en varias de las estrategias ya analizadas, la cibercriminalidad o ciberdelincuencia es una dimensión esencial en el concepto integral de ciberseguridad.

De este modo, el Ministerio del Interior tomó como punto de partida lo preceptuado, entre otras, en la Estrategia de ciberseguridad de la UE para el Década Digital, el IOCTA de 2020[66], la Estrategia Nacional de Ciberseguridad 2019, la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave[67] y la Estrategia Nacional contra el Terrorismo 2019[68], para concebir en 2021 este Plan Estratégico contra la Cibercriminalidad.

Más allá de tener en consideración esas y otras estrategias, el resultado de los análisis sobre la cibercriminalidad determinaba la acuciante necesidad de abordar un tipo de delincuencia que en esos momentos arrojaban unas preocupantes cifras, que plasmamos aquí para contextualizar debidamente el estado de situación:

- El perjuicio económico causado por la ciberdelincuencia a escala mundial en el año 2020 fue de unos 5,5 billones de euros, no siendo superado por otras modalidades delictivas.

- En el ámbito nacional, en el año 2015, la cibercriminalidad suponía el 4.1% de toda la criminalidad, mientras que en el año 2020 llegaba al 9,9% del total de las infracciones penales conocidas, lo que ponía de manifiesto un fuerte y progresivo incremento anual.

Igualmente, este plan estratégico se hace eco de las tendencias observadas en la cibercriminalidad, analizando aquellas más pujantes y que se adecúan a los tipos penales, así como, por otra parte, de los retos a afrontar, siendo muchos de ellos referidos a lo largo del presente por afectar eminentemente a la ciberseguridad:

- Cultura sobre ciberseguridad.

- Las tecnologías de la información y la comunicación como elemento facilitador para la comisión de delitos.

- Redes sociales y seguridad ciudadana.

---

[66] https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020

[67] Orden PCI/161/2019, de 21 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave.

[68] Orden PCI/179/2019, de 22 de febrero, por la que se publica la Estrategia Nacional contra el Terrorismo 2019, aprobado por el Consejo de Seguridad Nacional.

- Cifrado de la información y de las comunicaciones.

- Servicios en la nube.

- Redes *Darknet.*

- Crimen como servicio (*CaaS*).

- La dificultad de atribución de acciones delictivas.

- Criptovalores.

- Tecnología 5G.

- El *blockchain.*

- La inteligencia artificial.

- Dispositivos electrónicos y terminales telefónicos.

- Identidad digital.

Con estos antecedentes y situación, el Ministerio del Interior afronta la estrategia desde los vectores comunes en la ciberseguridad: la detección, prevención, protección, respuesta y persecución, y añadiendo la necesaria atención a las víctimas.

Seguidamente, con la estructura estratégica ya vista en otras estrategias explicadas en el presente, el plan se concibe primero refiriendo sus principios rectores:

- Focalización en la prevención.

- Cooperación entre las diferentes fuerzas y cuerpos de seguridad y colaboración estrecha con los operadores jurídicos, en el ámbito nacional e internacional.

- Disponibilidad de capacidades suficientes y adecuadas para articular respuestas adaptadas a las diferentes modalidades delictivas.

- Colaboración con la industria y con todos los operadores relevantes en materia de ciberseguridad en el sector público y privado, tanto en el ámbito nacional como internacional.

- Respeto escrupuloso a la libertad, a la privacidad y demás derechos fundamentales.

Tras haber reflejado todo lo anterior, consta en su apartado específico el objetivo principal del Plan: "potenciar las capacidades del Ministerio del Interior para detectar, prevenir, proteger, responder y perseguir la cibercriminalidad, de modo que permita la convergencia entre los ámbitos cibernético y físico, generando un impulso operativo y técnico eficaz que garantice la protección de los derechos y libertades y la seguridad ciudadana".

Este objetivo principal, para una consecución más eficaz, se fracciona en estos objetivos específicos:

- Objetivo I: promover la cultura de prevención de la cibercriminalidad entre la ciudadanía y la empresa.

- Objetivo II: impulsar la formación y la especialización de los miembros de la Policía Nacional y la Guardia Civil en materia de ciberseguridad y cibercriminalidad.

- Objetivo III: proteger los sistemas de información y telecomunicaciones utilizados por el Ministerio del Interior.

- Objetivo IV: incrementar y mejorar el uso y disposición de las herramientas tecnológicas e implementar I+D+i.

- Objetivo V: gestionar adecuadamente la información disponible en el ciberespacio.

- Objetivo VI: promover un marco legal e institucional que dé solución a los desafíos que surjan relacionados con la ciberseguridad y la cibercriminalidad.

- Objetivo VII: impulsar la coordinación a nivel nacional e internacional y favorecer la colaboración entre el sector público y privado.

Una vez ya determinados, para el logro de esos objetivos, se marcan estos seis ejes estratégicos que, a su vez, se desglosan en cuarenta y nueve líneas de acción:

- Eje I: cultura de prevención de la cibercriminalidad, que responde al Objetivo I.

- Eje II: potenciación de capacidades, que responde a los Objetivos II, III y IV.

- Eje III: generación de ciberinteligencia, que responde al Objetivo V.

- Eje IV: coordinación nacional y cooperación internacional, que responde al Objetivo VII.

- Eje V: contribuir a la disponibilidad de un marco normativo adecuado, que responde al Objetivo VI.

- Eje VI: colaboración público-privada, que responde al Objetivo VII.

De entre todos los objetivos y ejes, con el ánimo de no ser excesivamente prolijos, solo vamos a destacar para su interés para este trabajo el objetivo VI y el eje V que le da respuesta. En ambos queda manifiestamente claro el mandato dado, que se especifica en "impulsar la actualización de la legislación, mediante el traslado de las oportunas propuestas que favorezcan la adaptación o creación de instrumentos jurídicos, administrativos, penales y procesales, en función de la demanda que se origine en la lucha contra la cibercriminalidad".

Finalmente, los organismos dependientes del Ministerio del Interior, como son la Policía Nacional, la Guardia Civil, la Oficina de Coordinación de Ciberseguridad, etc., son los que elaboran planes operativos que ejecutan las cuarenta y nueve líneas de acción, de las que once de ellas se dedican a lograr ese impulso normativo ya destacado.

4 CERTIFICACIONES DE CIBERSEGURIDAD

A lo largo de todo este TFM se ha dejado constancia de la capital importancia para la ciberseguridad de las certificaciones de ciberseguridad. Esto se debe a que estas son capaces de descender hasta el nivel técnico requerido para que las numerosísimas medidas de seguridad tan complejas y cambiantes sean aplicadas tal y como las normas y estrategias establecen, pero que no son capaces de alcanzar con ese grado de eficacia, adecuación y rapidez.

De entre todo el catálogo de certificaciones dos sobresalen de forma manifiesta por su grado de implantación a nivel nacional, el Esquema Nacional de Seguridad y la serie ISO/IEC-27000, la primera por ser de obligado cumplimiento para las entidades del sector público y la segunda por ser el estándar más aceptado y extendido a nivel nacional e internacional.

4.1 Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad

Este estándar de certificación posee la particularidad de ser aprobado por medio una norma, el Real Decreto 311/2022 y proviene a su vez de lo previsto en el artículo 156.2 de la ley 40/2015.

El Esquema Nacional de Seguridad (ENS) tiene como objeto tratar de garantizar la ciberseguridad de las redes y sistemas de todo el sector público, conforme a la Ley 40/2015, pero además a las entidades privadas que presten servicios a este sector e incluso a terceros prestadores de esas entidades, abarcando de esta forma toda la ciberseguridad propia del sector público y de la cadena de suministro, siendo de obligado cumplimiento.

Para el cumplimiento de su objeto, el ENS establece los siguientes principios básicos, que son ampliamente aceptados por la mayoría de normas, estrategias, estándares de certificación (como se verá más adelante en la ISO 27001), así como por los expertos en ciberseguridad.

- Seguridad como proceso integral.
- Gestión de la seguridad basada en los riesgos.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua.
- Reevaluación periódica.
- Diferenciación de responsabilidades.

En sintonía con lo anterior, el ENS, además de seguir los principios de ciberseguridad arriba plasmados, también recurre a un concepto común a otras certificaciones, como es la política de seguridad, que el mismo ENS define en su artículo 12.1 como “el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta”.

Las políticas de seguridad han de ser elaboradas, y cumplidas, por cada administración pública, aunque existe la posibilidad de que una parte o todos los sujetos de un sector público institucional puedan adscribirse a la política de seguridad de la Administración de la que dependan.

El contenido de estas políticas de seguridad es abierto, pero forzosamente han de incluir estos conceptos, sobre los que hay que volver a referir que son empleados por la generalidad de normas, estrategias, estándares de ciberseguridad.

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.

- Profesionalidad.

- Autorización y control de los accesos.

- Protección de las instalaciones.

- Adquisición de productos de seguridad y contratación de servicios de seguridad.

- Mínimo privilegio.

- Integridad y actualización del sistema.

- Protección de la información almacenada y en tránsito.

- Prevención ante otros sistemas de información interconectados.

- Registro de la actividad y detección de código dañino.

- Incidentes de seguridad.

- Continuidad de la actividad.

- Mejora continua del proceso de seguridad.

Para poder cumplir con esos requisitos básicos de la política de seguridad la organización ha de tener en cuenta:

- Los activos de la organización, definidos en el anexo IV como: "componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización".

- La categoría del sistema: que permite ponderar entre la importancia de su información y el servicio prestado y el esfuerzo de seguridad necesario para protegerlo de los riesgos. De esta forma, aplicando los criterios específicos en el Anexo I del ENS los sistemas se catalogarán en categoría baja, media y alta.

- Las decisiones para la gestión de riesgos detectados.

Una vez hecho esto, la organización ha de adoptar las medidas de seguridad comprendidas en el Anexo II. Se trata de 73 medidas que se distribuyen de esta forma:

- Marco organizativo: medidas sobre la organización global de la seguridad.

- Marco operacional: medidas para proteger la operación de los sistemas.

- Medidas de protección: destinadas a la protección de activos concretos.

En atención al principio de proporcionalidad y en aras de una idónea aplicación del ENS, determinados sectores o entidades pueden implementar perfiles de cumplimiento específicos y aplicar esquemas de acreditación para productos suministrados por terceros.

El Centro Criptológico Nacional (CCN) valida y publica esos perfiles y esquemas específicos, del mismo modo que elabora las guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC) que complementan los aspectos técnicos del ENS y que son de obligado cumplimiento.

En lo referente a la certificación el ENS, hay que seguir el procedimiento registrado en la resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, en el que se determinan dos formas en función de las categorías del sistema mencionadas en el Anexo I:

- Certificación de Conformidad, para todas las categorías del sistema, mediante auditoría por entidades de certificación acreditadas por ENAC.

- Declaración de Conformidad, solo para los sistemas de categoría básica, por medio de una autoevaluación de la propia organización.

En cuanto a la protección de datos, como un aspecto específico de la ciberseguridad, el Reglamento general de protección de datos, la Ley Orgánica 3/2018 y la Ley Orgánica 7/2021 serán de aplicación en atención a su consideración de leyes especiales, pero en todo caso, a la hora de determinar las medidas de seguridad para la protección de los datos personales, se aplicarán las medidas de seguridad más rigurosas que resulten del análisis de riesgos, ya sean de aplicación de esas normas o de este ENS.

4.2 ISO/IEC-27001

La familia ISO/IEC 27000 es un conjunto de estándares internacionales publicados por la Organización Internacional de Normalización (ISO por sus siglas en inglés) y la Comisión Electrotécnica Internacional (IEC por sus siglas en inglés) cuyo objetivo es lograr la seguridad de la información en redes y sistemas o en otras palabras la ciberseguridad. Estos estándares se componen de varios documentos, aunque solo la ISO/IEC 27001 es susceptible de ser objeto de certificación.

La ISO 27001 es un estándar internacional certificable consistente en un código de buenas prácticas para implantar un sistema de gestión de la seguridad de la información. En estos momentos la versión vigente es la de 2022.

Se basa en un ciclo de mejora continua, ya descrito en el capítulo dedicado a los planes estratégicos, lo que le proporciona una mayor robustez y madurez. Para su desarrollo es necesario documentar todos los planes, procedimientos, medidas, etc. y registrar cada cambio efectuado en ellos.

La certificación, en caso de obtenerse, es válida durante 3 años y al ser compatibles con a otros sistemas de gestión ISO es integrable en ellos lo que aporta mucha versatilidad y grado de coherencia a esta certificación.

El proceso de certificación consta de dos grandes etapas: la consultoría y la auditoría:

- Consultoría: consultores con experiencia en la ISO 27001 ayudan a la organización a acometer cambios para cumplir con los requisitos de certificación, a la vez que eliminan otras posibles causas de no conformidad.

- Auditoría: un organismo acreditado externo (en España es AENOR), revisa los planes, procesos y procedimientos exigidos por la ISO 27001 y la aplicación de los controles y medidas de gestión de riesgos.

Este estándar se compone de estas siete fases cíclicas:

- Fase 1, política de seguridad de la información: como inicio del sistema de gestión de la seguridad de la información se ha de concebir la política de seguridad, publicando un documento de alto nivel que compromete a la dirección para el impulso y apoyo a este sistema de gestión y delimitando las responsabilidades para las diversas actuaciones organizativas y técnicas requeridas. Entre los variados aspectos tratados por estas políticas se encuentran la gestión de riesgos de los activos de la organización y la gestión de incidentes.

Es esencial que la política de seguridad esté alineada con la visión, misión y objetivos estratégicos de la organización.

- Fase 2, el alcance del sistema de gestión de la seguridad de la información: es otro documento, más técnico que registra cuál va a ser el ámbito de actuación y los sistemas implicados. La ISO 27001 solo se aplicará aquellos procedimientos, sistemas y redes contemplados en ese documento.

- Fase 3, análisis de riesgos: Por un lado, se identifican y catalogan los activos de la organización y, por otro, las amenazas y vulnerabilidades (los riesgos) que les corresponden. Por último, se relacionan con las contramedidas ya implantadas.

Su importancia radica en que permite comprender a la organización su nivel real y actualizado de ciberseguridad de la información e identificar las áreas que necesitan mejoras.

- Fase 4, gestión del riesgo: los riesgos identificados de los activos en la fase anterior se evalúan conforme a la probabilidad de materialización y el impacto que tienen en la organización si se producen.

Teniendo eso en cuenta los riesgos son tratados para intentar evitarse, mitigarse, transferirse o asumirse.

- Fase 5, controles y medidas de seguridad: en el anexo A de la ISO 27001 se encuentran 93 controles, agrupados en los cuatro dominios más abajo referidos. La organización selecciona aquellos controles que considera apropiados para la gestión de los riesgos.

  - Controles organizacionales: políticas de seguridad, funciones y responsabilidades, contacto con autoridades, inteligencia sobre amenazas, seguridad en la gestión de proyectos, etc.
  - Controles orientados a las personas: gestión de recursos humanos, concienciación, educación, capacitación en seguridad, gestión de ciberincidentes, continuidad del negocio y cadena de suministro.
  - Controles físicos: perímetro de seguridad, controles de acceso, seguridad de instalaciones y gestión de equipos.
  - Controles tecnológicos: seguridad de la red y de los sistemas (incluyendo su desarrollo y mantenimiento) y seguridad de las aplicaciones.

- Fase 6, declaración de aplicabilidad (SoA, por sus siglas en inglés): es el documento en que la organización refleja cuáles de los 93 controles arriba ha elegido para acometer la gestión de riesgos. Asimismo, hay que justificar cuál es el motivo por el que no se aplica alguno de los controles.

Es uno de los documentos fundamentales del sistema de gestión de la seguridad de la información para que el auditor realice su labor.

- Fase 7, revisión del sistema: al estar la ISO 27001 fundamentada en la mejora continua, uno de sus pilares es la revisión de todas sus fases para detectar fallos, procedimientos ineficaces y actualizar el sistema de gestión de la seguridad de la información a los nuevos activos y los constantes riesgos novedosos.

Para esto se realiza una evaluación periódica de todo lo anterior y se llevan a cabo medidas correctivas correspondientes.



Figura 9 Fases de la ISO/IEC 27001[69]

[69] https://www.normas-iso.com/wp-content/uploads/2012/02/SGSI.png

5 CONCLUSIONES

Además de haber proporcionado un estudio de las normas, estrategias y certificaciones fundamentales para la ciberseguridad, la lectura y análisis de los capítulos precedentes de este TFM permite llegar a una serie de conclusiones.

La innegable complejidad de la ciberseguridad respecto a las tecnologías de la información y la comunicación tiene su correspondencia en una multitud de normas, estrategias y estándares. Pero resulta indiscutible que son las normas la piedra angular de ese ecosistema. No solo porque son de obligado cumplimiento, sino porque, respecto a las estrategias, son las que concretan y regulan algunos de los objetivos, algunas veces demasiado ambiciosos, de los planes estratégicos. Y sin dejar de destacar que en ocasiones son las propias normas las que determinan la obligación de elaborar esas estrategias, como ocurre con la Directiva NIS 2 y las estrategias nacionales de ciberseguridad.

A su vez, en cuanto a la relación entre las normas y los estándares de certificación, estos desarrollan aquellos elementos eminentemente técnicos en los que las normas no suelen entrar a detallar para no resultar en exceso complejas o dilatar en demasía los plazos para su elaboración.

Sin embargo, como resulta patente, el mero hecho de legislar, aunque sea con profusión, no consigue responder satisfactoriamente a las problemáticas consustanciales a la ciberseguridad, como son el origen internacional de las ciberamenazas o la ya tan mentada vertiginosa evolución de las tecnologías de la información y la comunicación.

Todo ello ha provocado una regulación de las tecnologías de la información y la comunicación y, por ende, de la ciberseguridad, que ha tenido que adaptarse a estos condicionamientos para resultar eficaz.

La transversalidad y afectación de las tecnologías de la información y la comunicación a prácticamente todos los aspectos de la sociedad conlleva que un enfoque tradicional no sea el adecuado.

De este modo, cada vez más se llevan a cabo planes estratégicos con un objeto de estudio muy amplio, que tras su elaboración permite acometer, con la flexibilidad que les caracteriza, diferentes soluciones a los retos identificados. Siendo en varias de las ocasiones, como en este TFM se ha dejado constancia, una de las soluciones un llamamiento al legislador para que regule una faceta concreta de esos retos.

En cuanto a la dimensión internacional de la ciberseguridad, que viene dada, por mencionar solo algunos factores, por las relaciones entre las redes y sistemas de las organizaciones, los proveedores de servicios radicados en el extranjero (un ejemplo paradigmático son los servicios que se prestan en la nube) o los ataques de los ciberdelincuentes que aprovechan las lagunas del auxilio penal internacional para cometer sus delitos desde otros países, es crucial contar con una armonización internacional.

Y en esta promoción de normas comunes se ha avanzado mucho, sin duda dentro de la Unión Europea, pero también a nivel global con los convenios como el de Budapest, que en un periodo razonablemente corto de tiempo ya ha sido ampliado con dos protocolos adicionales y cuyo notable éxito ha propiciado el proyecto de la convención de las Naciones Unidas amplia contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos que se está negociando en estos momentos.

Asimismo, en el plano más técnico es donde los estándares internaciones de certificación han puesto de relieve su utilidad, pues plantean un marco común donde las organizaciones internacionales que se someten al proceso de certificación en un país conforme a un estándar pueden hacer valer esa certificación en otro.

Lo que, sin llegar a suponer una seguridad jurídica propiamente dicha, facilita la confianza entre los actores, a la vez que evita trabas al desarrollo e implantación de esas organizaciones, ya sean públicas o privadas.

En relación a la dimensión temporal de la regulación de la ciberseguridad dos herramientas se han mostrado particularmente útiles a la hora de superar la obsolescencia.

Por un lado, la Unión Europea cada vez recurre más a los actos delegados de la Comisión, lo que agiliza sobremanera la actualización de reglamentos y directivas, que de seguir el cauce convencional de modificación por el Parlamento y el Consejo resultarían desfasados antes de poder llevarse a cabo esa necesaria actualización.

Por otra parte, concluimos resaltando nuevamente la utilidad de los estándares de certificación a las que las normas pueden recurrir para regular aspectos no solo técnicos, sino que pueden adaptarse con mucha más agilidad y rapidez a una realidad cambiante que el proceso necesario para modificar una ley o incluso un reglamento.

Por este motivo, se aboga desde aquí, a la luz de la materia estudiada, en emplear en mayor medida estos estándares de certificación y culminar ese proceso de armonización internacional y europea que está siendo ya promovido entre otras normas, por la Directiva NIS 2.

6 ÍNDICE DE ABREVIATURAS

BOE: Boletín Oficial del Estado.

CCN: Centro Criptológico Nacional.

CERT: equipo de respuesta a incidentes de seguridad informática, por sus siglas en inglés.

CSIRT: equipo de respuesta a incidentes de seguridad informática.

Directiva NIS: Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo 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.

Directiva NIS 2: Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148.

DNS: sistema de nombres de dominio, por sus siglas en inglés.

DOUE: Diario Oficial de la Unión Europea.

EMPACT: Plataforma Multidisciplinar Europea contra las Amenazas Delictivas, por sus siglas en inglés.

ENAC: Entidad Nacional de Acreditación.

ENISA: Agencia de la Unión Europea para la Ciberseguridad.

ENS: Esquema Nacional de Seguridad.

ESPDEF-CERT: Equipo de Respuesta ante Emergencias Informáticas del Ministerio de Defensa.

Eurojust: Agencia de la Unión Europea para la Cooperación Judicial Penal.

Europol: Agencia de la Unión Europea para la Cooperación Policial.

EuroQCI: Infraestructura Europea de Comunicación Cuántica.

EU-CyCLONe: Red europea de organizaciones de enlace para las crisis de ciberseguridad.

INCIBE: Instituto Nacional de Ciberseguridad de España.

IOCTA: Evaluación de la Amenaza de la Delincuencia Organizada en Internet, por sus siglas en inglés.

IoT: internet de las cosas.

ISO/IEC: Organización Internacional de Normalización/Comisión Electrotécnica Internacional.

NIS: redes y sistemas de información, por sus siglas en inglés.

OSCE: Organización para la Seguridad y la Cooperación en Europa.

PYME: pequeña y mediana empresa.

Reglamento DORA: Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011.

Reglamento general de protección de datos: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta

al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga l Directiva 95/46/CE.

Reglamento sobre la Ciberseguridad: Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación por el que se deroga el Reglamento (UE) 526/2013.

SoA: Declaración de aplicabilidad, por sus siglas en inglés.

TFM: trabajo de fin de máster.

TIC: tecnologías de la información y la comunicación.

TTP´s: tácticas, técnicas y procedimientos.

UE: Unión Europea.

7 BIBLIOGRAFÍA

[1] Ansoff, I. (1980). La estrategia de la empresa. Madrid: Pirámide

[2] Chandler, A. (1962). Estrategia y estructura: capítulos de la historia industrial de Estados Unidos. Barcelona: Ariel

[4] Deming, W. E. (1989). Calidad, productividad y competitividad: la salida de la crisis. Madrid: Díaz de Santos

[3] Drucker, Peter. (2008). La práctica del management. Barcelona: Ediciones Deusto