



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

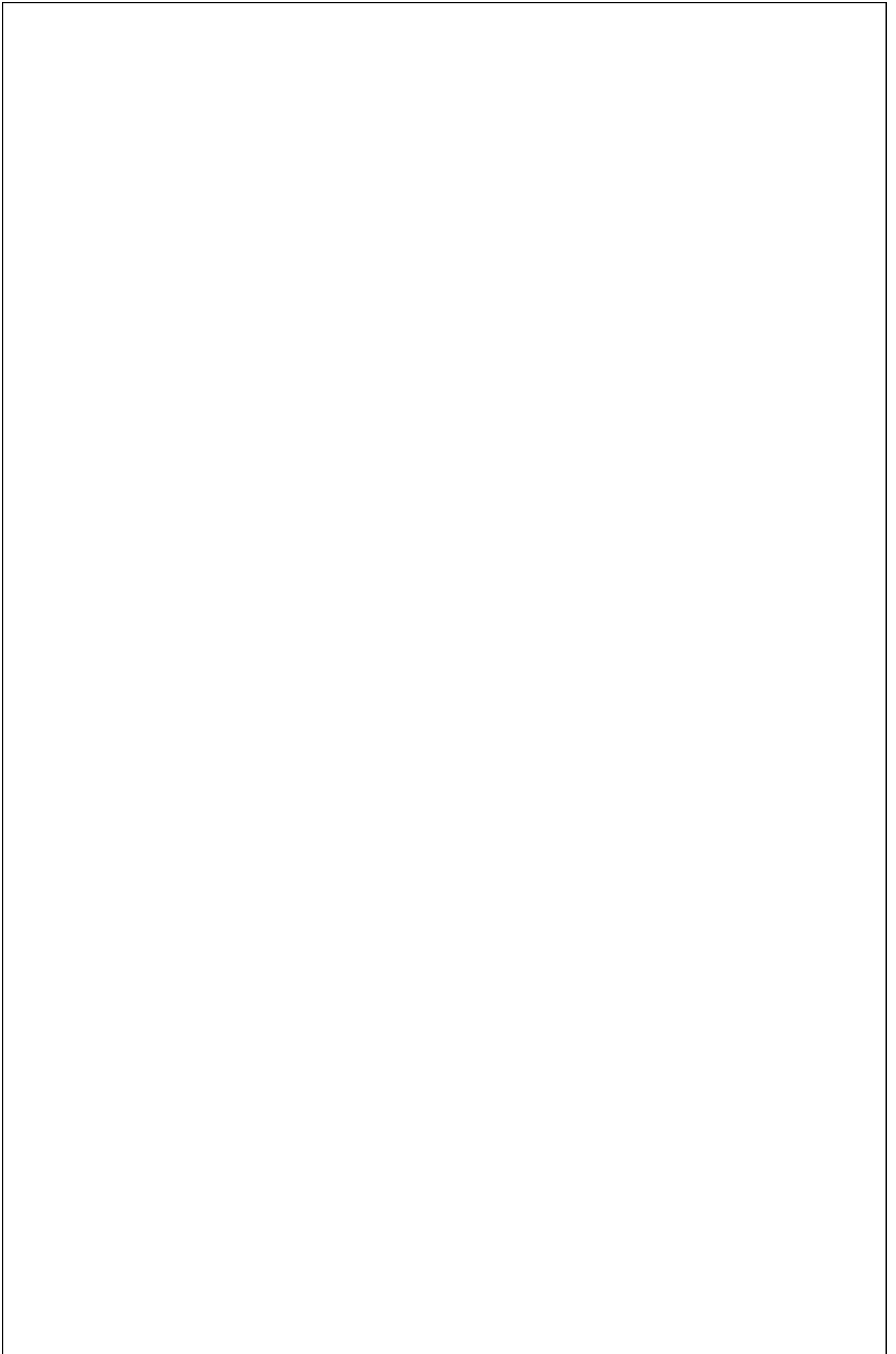
*Revisión y Actualización de la Guía Nacional de
Notificación y Gestión de Ciberincidentes*
Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Miguel Ángel Albéniz Rueda

DIRECTOR: Miguel Rodelgo Lacruz

CURSO ACADÉMICO: 2025-2026

UniversidadeVigo





Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*Revisión y Actualización de la Guía Nacional de
Notificación y Gestión de Ciberincidentes*

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

UniversidadeVigo

RESUMEN

Este trabajo analiza la necesidad de revisión y actualización de la Guía Nacional de Notificación y Gestión de Ciberincidentes (GNNGC), publicada en España tras la transposición de la Directiva (UE) 2016/1148 (NIS1) mediante el Real Decreto-ley 12/2018 y su desarrollo a través del Real Decreto 43/2021. La entrada en vigor de la Directiva (UE) 2022/2555 (NIS2), que deroga la anterior y refuerza las obligaciones de ciberseguridad y de notificación de incidentes, plantea la necesidad de adaptar la GNNGC a los nuevos requerimientos normativos europeos y nacionales.

El estudio se enmarca en un contexto de creciente dependencia de las redes y sistemas de información en sectores críticos y esenciales, así como en la consolidación de la ciberseguridad como un pilar estratégico para la resiliencia digital en Europa y España. Para ello, se realiza un análisis comparado entre la normativa vigente, las disposiciones de NIS2 y los modelos de referencia internacionales, con el objetivo de proponer una revisión de la GNNGC que facilite su alineamiento con el nuevo marco jurídico y operativo

PALABRAS CLAVE

Ciberseguridad, guía, incidentes, notificación, ciberamenazas, NIS 2.

AGRADECIMIENTOS

A mi director, Miguel Rodelgo por su inestimable ayuda y guía en este trabajo.

A mis jefes y amigos, especialmente a Alberto y Leandro por su apoyo y consejo.

A mis compañeros de la promoción de este Máster, por su compañerismo y amistad.

A mis padres por haberme dado todo para llegar hasta aquí y a mi hermana por ser un ejemplo de constancia y capacidad.

Y, por supuesto, a mi pareja Noelia por su paciencia y amor, apoyándome en cada reto y acompañándome allá donde vaya.

CONTENIDO

Contenido	2
Índice de Figuras	4
Índice de Tablas.....	6
Tabla de Acrónimos	8
1 Introducción.....	12
1.1 Motivación de este trabajo de fin de máster	12
1.2 Objetivos	13
1.3 Metodología de investigación	14
1.4 Estructura del trabajo	14
2 Conceptos esenciales de Ciberseguridad.....	16
2.1 Definiciones y conceptos relativos a la Ciberseguridad	16
3 Estado del Arte del sistema de la ciberseguridad (Unión Europea y España)	20
3.1 Panorama estratégico	20
3.2 Marco normativo.....	21
3.3 Estructura organizativa y operativa.....	22
4 Evolución del marco regulatorio europeo	28
4.1 Estrategia de ciberseguridad de la Unión Europea (2020).....	28
4.2 Directiva NIS 1 Directiva (UE) 2016/1148	29
4.3 Directiva NIS 2. Directiva (UE) 2022/2555	29
4.4 Reglamento DORA. Reglamento (UE) 2022/2554.....	30
4.5 Directiva CER. Directiva (UE) 2022/2557	31
5 Derecho comparado.....	34
5.1 Comparativa entre la Directiva NIS 1 y la Directiva NIS 2.....	34
5.2 Análisis del Anteproyecto de Ley de Coordinación y Gobernanza de Ciberseguridad.....	42
5.3 Comparación del Anteproyecto de Ley de Coordinación y Gobernanza y el RDL.....	46
6 Marcos de notificación de incidentes	54
6.1 Guía Nacional de Notificación y Gestión de Ciberincidentes	54
6.2 Framework de Notificación Belga	60
6.3 Directrices de ENISA sobre el reporte de incidentes (ENISA)	65
6.4 Reglamento de Ejecución de la Comisión (UE) 2024/2690	66
6.5 Esquema Nacional de Seguridad (ENS)	69
7 Propuestas de Actualización de la Guía Nacional de Notificación y Gestión de Ciberincidentes	72
7.1 Objetivos y Alcance	72

7.2	Gobernanza Nacional de Ciberseguridad.....	73
7.3	Notificación de Ciberincidentes.....	75
7.4	Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.....	78
7.5	Taxonomía y Clasificación de Incidentes	78
7.6	Creación de un Anexo Técnico de Métricas para Entidades Pertinentes.....	79
7.7	Inclusión de un Procedimiento para la Gestión de Incidentes Recurrentes	80
7.8	Notificación de Ciberamenazas Significativas	81
7.9	Incorporación de Medidas de Gobernanza y Supervisión	82
7.10	Mecanismos de Revisión y Adaptabilidad.....	83
8	Conclusiones	84
8.1	Gobernanza Centralizada como Eje Vertebrador.....	84
8.2	Cambio de Paradigma: De la "Peligrosidad" a la "Significatividad"	84
8.3	Exigencia Operativa: Inmediatez y Continuidad.	85
8.4	ENS como marco de Ciberseguridad Nacional.....	85
8.5	Taxonomía Simplificada.	85
8.6	Gestión de la Recurrencia y Amenazas Proactivas	85
	ANEXO 1 PLANTILLAS DE NOTIFICACIÓN	86
A.	PLANTILLA DE ALERTA TEMPRANA.....	86
B.	PLANTILLA DE NOTIFICACIÓN DE INCIDENTE SIGNIFICATIVO	87
C.	PLANTILLA DE NOTIFICACIÓN DE INFORME FINAL.....	89
9	Bibliografía.....	94

ÍNDICE DE FIGURAS

Figura 1 Gobernanza de la ciberseguridad UE. Fuente: TCE. Dictamen 02/2023.....	22
Figura 2 Modelo de gobernanza. Elaboración propia	24
Figura 3 Sectores de Alta criticidad y Críticos. Elaboración propia.	36
Figura 4 Modelo Nacional de Gobernanza. Elaboración propia	43
Figura 5 Flujograma de la Ventanilla Única de Notificación. Fuente: GNNGC	58
Figura 6 Portal web principal de la PNNSC. Fuente web: PNNSC	59
Figura 7 Página de notificación incidentes del sector público. Fuente: PNNSC	59
Figura 8 Flujograma de notificación de incidentes según el CCB. [37]	62
Figura 9 Formulario de notificación del CCB. Fuente: CCB.....	63
Figura 10 Comparación de datos del formulario de notificación. Fuente: CCB	64
Figura 11 Esquema de aplicación NIS 2. Elaboración propia.....	73
Figura 12 Plantilla de comunicación a usuarios. Elaboración con IA (Gemini)	82

ÍNDICE DE TABLAS

Tabla 1 Acrónimos 10

Tabla 2 Umbrales de notificación de la GNNGC. Elaboración propia 57

Tabla 3 Plazos de cierre de incidentes. Elaboración propia 57

Tabla 4 Tipos de notificación y sus plazos. Elaboración propia 62

Tabla 5 Obligatoriedad de notificar.....77

Tabla 6 Notificaciones obligatorias y umbrales temporales 77

Tabla 7 Tabla de umbrales de notificación automática. Elaboración propia 80

Tabla 8 Ejemplo de Relación de Controles entre el ENS y el Reglamento 2024/2690 83

TABLA DE ACRÓNIMOS

Acrónimo	Significado
AC / ACo	Autoridad Competente / Autoridad de Control,
AEPD	Agencia Española de Protección de Datos
APL	Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad
APT	<i>Advanced Persistent Threat</i> (Amenaza Avanzada Persistente)
CCB	<i>Centre for Cybersecurity Belgium</i> (Centro de Ciberseguridad Belga)
CCN	Centro Criptológico Nacional
CCN-CERT	Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional
CDN	<i>Content Delivery Network</i> (Red de Distribución de Contenidos)
CER	<i>Critical Entities Resilience</i> (Directiva sobre la resiliencia de las entidades críticas)
CERT	<i>Computer Emergency Response Team</i> (Equipo de Respuesta ante Emergencias Informáticas)
CERT-EU	<i>Computer Emergency Response Team for the EU Institutions</i>
CNAE	Clasificación Nacional de Actividades Económicas
CNC	Consejo Nacional de Ciberseguridad
CNCíber	Centro Nacional de Ciberseguridad
CNI	Centro Nacional de Inteligencia
CNPIC	Centro Nacional de Protección de Infraestructuras y Ciberseguridad
CSIRT	<i>Computer Security Incident Response Team</i> (Equipo de Respuesta a Incidentes de Seguridad Informática)
CSN	Consejo de Seguridad Nacional
DDoS	<i>Distributed Denial of Service</i> (Denegación de Servicio Distribuida)
DNS	<i>Domain Name System</i> (Sistema de Nombres de Dominio)
DORA	<i>Digital Operational Resilience Act</i> (Reglamento de Resiliencia Operativa Digital)
DSN	Departamento de Seguridad Nacional
EC3	<i>European Cybercrime Centre</i> (Centro Europeo de Ciberdelincuencia)
ECCC	<i>European Cybersecurity Competence Centre</i> (Centro Europeo de Competencia en Ciberseguridad)
EDR	<i>Endpoint Detection and Response</i> (Detección y Respuesta en Endpoints)
EE	Entidades Esenciales
EI	Entidades Importantes

ENISA	<i>European Union Agency for Cybersecurity</i> (Agencia de la Unión Europea para la Ciberseguridad)
ENS	Esquema Nacional de Seguridad
EP	Entidades Pertinentes (en el marco del Reglamento de Ejecución 2024/2690)
ESPDEF-CERT	CSIRT del Mando Conjunto del Ciberespacio
EU-CyCLONe	<i>European Cyber Crisis Liaison Organisation Network</i>
FCSE	Fuerzas y Cuerpos de Seguridad del Estado
GNNGC	Guía Nacional de Notificación y Gestión de Ciberincidentes
INCIBE	Instituto Nacional de Ciberseguridad
INCIBE-CERT	CERT del Instituto Nacional de Ciberseguridad
IoC	<i>Indicators of Compromise</i> (Indicadores de Compromiso)
ISO/IEC	<i>International Organization for Standardization / International Electrotechnical Commission</i>
ITU / UIT	<i>International Telecommunication Union</i> (Unión Internacional de Telecomunicaciones)
KPI	<i>Key Performance Indicator</i> (Indicador Clave de Rendimiento)
MCCE	Mando Conjunto del Ciberespacio
MFA	<i>Multi-Factor Authentication</i> (Autenticación Multifactor)
MSP	<i>Managed Service Provider</i> (Proveedor de Servicios Gestionados)
MSSP	<i>Managed Security Service Provider</i> (Proveedor de Servicios de Seguridad Gestionados)
NCCN	<i>National Crisis Center</i> (Centro Nacional de Crisis de Bélgica)
NIS	<i>Network and Information Systems</i> (Seguridad de las redes y sistemas de información)
OCC	Oficina de Coordinación de Ciberseguridad
OSE	Operador de Servicios Esenciales
PCE	Perfil de Cumplimiento Específico (del ENS)
PIC	Protección de Infraestructuras Críticas
PNNSC	Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes
PoC	<i>Point of Contact</i> (Punto de Contacto)
PSC	Prestador de Servicios de Confianza
PSD	Proveedor de Servicios Digitales

RD	Real Decreto
RDL	Real Decreto-ley
RGPD	Reglamento General de Protección de Datos
RSI	Responsable de la Seguridad de la Información
SIEM	<i>Security Information and Event Management</i>
SOAR	<i>Security Orchestration, Automation and Response</i>
SOC	<i>Security Operations Center</i> (Centro de Operaciones de Seguridad)
TFM	Trabajo de Fin de Máster
TIC	Tecnologías de la Información y las Comunicaciones
TLD	<i>Top-Level Domain</i> (Dominio de Primer Nivel)
TTP	<i>Tactics, Techniques, and Procedures</i> (Tácticas, Técnicas y Procedimientos)
UE	Unión Europea
XDR	<i>Extended Detection and Response</i> (Detección y Respuesta Extendida)

Tabla 1 Acrónimos

1 INTRODUCCIÓN

1.1 Motivación de este trabajo de fin de máster

El desarrollo y uso exponencial de las Tecnologías de la Información y las Comunicaciones (TIC) ha transformado de forma irreversible la sociedad contemporánea, impulsando la digitalización de la economía, la administración pública y la vida cotidiana. Esta creciente interdependencia tecnológica ha generado no solo oportunidades de innovación y eficiencia, sino también nuevas vulnerabilidades que comprometen la continuidad operativa de los servicios esenciales y la confianza ciudadana en el ciberespacio.

La Unión Europea (UE), plenamente consciente del impacto que el ciberespacio tiene sobre la estabilidad política, económica y social de sus Estados miembros, ha consolidado una estrategia común de ciberseguridad orientada a reforzar la confianza, la cooperación y la capacidad de respuesta ante incidentes de gran escala. Este enfoque se sustenta en la armonización normativa, la coordinación institucional y el desarrollo de capacidades operativas y técnicas compartidas entre los Estados miembros. A través de instrumentos legislativos como las Directivas NIS (2016/1148 y 2022/2555), la Directiva CER (2022/2557) y el Reglamento del Cibercentro Europeo de Competencia (2021/887), la UE impulsa una gobernanza común en materia de seguridad digital, orientada a garantizar un nivel elevado de protección en toda la Unión. Esta arquitectura normativa y organizativa promueve una respuesta europea unificada frente a amenazas híbridas y cibernéticas emergentes, fortaleciendo la resiliencia digital, la protección de las infraestructuras críticas y la soberanía tecnológica como pilares fundamentales de la seguridad y la autonomía estratégica europeas.

España, en este sentido, se ha consolidado como un referente en la construcción de un modelo integral de ciberseguridad, alineado con los marcos europeos e internacionales actuales. Desde la aprobación de la Ley 8/2011 sobre protección de infraestructuras críticas, el país ha integrado la ciberseguridad como un pilar estratégico de la seguridad nacional, extendiendo su alcance más allá del ámbito tecnológico para integrarlo en la gestión de riesgos, la resiliencia y la continuidad de los servicios esenciales. Esta visión ha sido reforzada con la adopción de estrategias nacionales, la creación de organismos especializados y la participación de forma activa en las iniciativas europeas e internacionales.

Este compromiso ha sido reconocido por la Unión Internacional de Telecomunicaciones (UIT), situando a España, según a su informe de 2024 sobre el índice global de ciberseguridad [1], entre los países con mayor compromiso en ciberseguridad a nivel mundial, dentro del grupo de naciones mejor posicionadas en el índice, como modelo a seguir. Esta clasificación se basa en cinco pilares fundamentales: medidas legales, técnicas, organizativas, de desarrollo de capacidades y de cooperación.

España destaca por su marco normativo robusto, la existencia de equipos de respuesta ante incidentes (CSIRT), la formación especializada y su participación en acuerdos internacionales de ciberseguridad.

La transposición de la directiva UE 2016/1148 (NIS 1), se materializó en el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y los sistemas de la información y las comunicaciones, posteriormente desarrollado por el Real Decreto 43/2021. Este último incluía en su anexo la Instrucción de la Guía Nacional de Notificación y Gestión de Ciberincidentes (en adelante también, GNNGC), que proporcionaba los criterios y procedimientos para la notificación de incidentes. En esta se incluía una taxonomía, alineada con la de la Agencia Europea de Ciberseguridad (ENISA), así como la categorización de incidentes en los que se basa la notificación. No obstante, la inminente transposición de la directiva UE 2022/2555 (NIS 2), mediante el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, requiere, al menos, una revisión de la guía vigente para garantizar su alineación con las nuevas obligaciones jurídicas y operativas.

Asimismo, la Estrategia de Ciberseguridad de la Unión Europea (2020) y la Estrategia Nacional de Ciberseguridad de España (2019) refuerzan la idea de que la gestión de incidentes y su notificación temprana son pilares esenciales para asegurar la resiliencia de los servicios esenciales y digitales. En este sentido, actualizar la GNNGC no solo responde a un imperativo normativo, sino también a una necesidad estratégica para reforzar la cooperación público-privada, mejorar la capacidad de respuesta nacional y favorecer la interoperabilidad con otros Estados miembros.

Por tanto, este estudio se justifica en tres dimensiones principales:

1. Normativa: adecuación a la NIS 2 y su transposición en España.
2. Estratégica: necesidad de reforzar la resiliencia nacional y europea frente a incidentes críticos.
3. Operativa: actualización de los procedimientos de notificación de incidentes para mejorar la eficacia en la gestión y respuesta.

1.2 Objetivos

El objetivo general de este trabajo de fin de máster (en adelante TFM), es analizar y evaluar la adecuación de la actual Guía Nacional de Notificación y Gestión de Ciberincidentes (en adelante, GNNGC), a las exigencias, principalmente, derivadas de la Directiva UE 2022/2555 (NIS 2) y su transposición en España, con el fin de proponer medidas de actualización que garanticen su alineación normativa, estratégica y operativa.

Entre los objetivos específicos, el trabajo trata de:

- Examinar el marco teórico y regulatorio de la ciberseguridad de la Unión Europea y de España, y con especial atención a la evolución desde NIS1 hasta la NIS2.
- Comparar las disposiciones de NIS1 y NIS2 En materia de notificación de incidentes, identificando principales diferencias en plazos alcance y destinatarios.
- Analizar el contenido y alcance actual de la Guía, identificando sus puntos fuertes y debilidades frente a los nuevos requerimientos normativos.
- Contrastar modelos de guías de notificación internacionales, en particular las directrices de ENISA sobre el reporte de incidentes conforme a la NIS 2, y la Guía Nacional de Notificación de Incidentes de Bélgica, como una de las pioneras en su publicación.
- Evaluar las posibles divergencias existentes entre la Guía vigente y las exigencias de NIS2, clasificando las divergencias en aspectos jurídicos y técnicos y organizativos.
- Proponer un modelo de actualización de la Guía, que incluya recomendaciones prácticas, criterios de priorización y esquemas de notificación armonizados con el marco europeo.

1.3 Metodología de investigación

Para la elaboración de este trabajo se ha optado por un enfoque cualitativo y de carácter descriptivo-analítico, basado en la revisión de fuentes normativas, doctrinales y estratégicas de ámbito nacional e internacional. Se aplicará un análisis comparado entre los distintos marcos jurídicos y guías operativas, con el objetivo de identificar las necesidades de actualización de la Guía Nacional de Notificación y Gestión de Ciberincidentes (GNNGC).

Las etapas de la investigación han sido las siguientes:

1. Revisión documental y normativa
 - Identificación y recopilación de normas europeas y nacionales relevantes:
 - Directiva NIS 1 (UE, 2016/1148).
 - Directiva NIS 2 (UE, 2022/2555).
 - Reglamento DORA (UE, 2022/2554).
 - Directiva CER (UE, 2022/2557).
 - Reglamento (UE) 2019/881 relativo a ENISA.
 - Real Decreto-ley 12/2018 y Real Decreto 43/2021 en España.
 - Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.
2. Análisis comparado
 - Estudio de las diferencias entre NIS 1 y NIS 2, especialmente en el ámbito de la notificación de incidentes.
 - Examen de la GNNGC vigente y su correspondencia con las obligaciones derivadas de NIS 2 y el APL.
 - Revisión de marcos de referencia, como la Guía de notificación belga y el Reglamento de Ejecución 2024/2690.
 - Revisión del Reglamento de Ejecución UE 2024/2690 donde se establecen los criterios para determinar un incidente significativo.
3. Propuesta de actualización
 - Formulación de recomendaciones para adaptar la GNNGC a NIS 2.
 - Diseño de un esquema operativo alineado con las directrices de ENISA y el Reglamento de Ejecución UE 2024/2690, con los plazos y requisitos de notificación.

1.4 Estructura del trabajo

Este Trabajo de Fin de Máster está organizado en ocho capítulos y un anexo con una progresión lógica que abarca desde el marco normativo y conceptual hasta una propuesta de actualización de la Guía Nacional de Notificación y Gestión de Ciberincidentes.

El Capítulo 1, Introducción, presenta la síntesis del trabajo, su justificación y motivación, definidos el objetivo general y los específicos, así como la metodología empleada. A continuación, el Capítulo 2 establece los conceptos esenciales de ciberseguridad, definiendo los términos fundamentales para facilitar la comprensión del ensayo.

Posteriormente, el Capítulo 3 expone el estado del arte, analizando la situación actual de la ciberseguridad tanto a nivel europeo como nacional desde una perspectiva estratégica, normativa y

organizacional. En el Capítulo 4 se examina la evolución del marco regulatorio europeo, con foco en las directivas que tienen repercusión directa sobre la seguridad de las redes y sistemas de información.

El análisis continúa en el Capítulo 5 mediante un ejercicio de derecho comparado, donde se contrastan los diferentes marcos normativos europeos y nacionales para identificar sus divergencias. El Capítulo 6 se centra en los marcos de notificación de incidentes, describiendo la actual Guía Nacional de Notificación y Gestión de Ciberincidentes, las directrices de ENISA alineadas con la directiva NIS 2 y la Guía Nacional de Bélgica. Finalmente, el Capítulo 7 concluye con la revisión de la propuesta de actualización de la Guía Nacional de Notificación y Gestión de Ciberincidentes y el 8 con las Conclusiones del trabajo.

En el Anexo I se incluyen plantillas de notificación generales para las diferentes notificaciones obligatorias y las voluntarias, que faciliten a las entidades qué reportar.

2 CONCEPTOS ESENCIALES DE CIBERSEGURIDAD

2.1 Definiciones y conceptos relativos a la Ciberseguridad

Tras haber presentado la temática y los objetivos del trabajo, resulta conveniente precisar ciertos conceptos fundamentales que permitirán entender mejor su desarrollo. Para ello, se recurrirá a definiciones recogidas en documentos de referencia elaborados por organismos oficiales de reconocido prestigio, como la Agencia Europea de Ciberseguridad (ENISA), así como en normas y estándares tanto nacionales como internacionales.

2.1.1 *Redes y sistemas de información*

El Real Decreto Ley 12/2018 (en adelante también, RDL), define las redes y sistemas de información como:

1. “Las redes de comunicaciones electrónicas, tal y como vienen definidas en el número 31 del anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones;
2. Cualquier dispositivo o grupo de dispositivos interconectados que realicen un tratamiento automático de datos digitales.
3. Los datos digitales almacenados, tratados, recuperados o transmitidos por los elementos antes mencionados para su funcionamiento, utilización, protección y mantenimiento”. [2]

La Directiva (UE) 2022/2555 (NIS 2), además, llevó esta definición más allá, reforzando la función crítica que tienen los sistemas de información, no solo en los servicios esenciales (salud, transporte, energía, etc.), sino también en operadores de importancia crítica, proveedores de servicios digitales y gestión pública [3]

Respecto a la seguridad de los sistemas de redes y de información según la define la Directiva NIS 2, se define como: “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”. [4]

2.1.2 *Ciberseguridad: Definiciones y Alcance*

La Unión Internacional de Telecomunicaciones (ITU), define la ciberseguridad como: “El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de

gestión de riesgos, acciones formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios del ciberentorno [...]”. [5]

ENISA, por otro lado, 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 y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (en adelante Reglamento de Ciberseguridad), define este concepto como el conjunto de mecanismos necesarios para proteger las redes, sistemas, así como a los usuarios frente a ciberamenazas, garantizando la confidencialidad, integridad y disponibilidad de la información. Esta definición, también es recogida por el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad de España, que transpone la Directiva (UE) 2022/2555. [6]

2.1.3 Ciberamenazas, Vulnerabilidades e Incidentes de Seguridad

Parece necesario definir qué son las ciberamenazas, vulnerabilidades y qué se entiende por incidentes de seguridad para entender el contexto y la relevancia de la ciberseguridad. Además, los tres están íntimamente relacionados de tal manera que una ciberamenaza intenta aprovechar una vulnerabilidad, y de lograr explotar esa falla, se desataría un incidente de seguridad, en mayor o menor grado. Por lo tanto, a continuación, se definen los tres términos de acuerdo con diferentes normas u organizaciones:

- Ciberamenaza, según ENISA es aquella circunstancia, evento o acción potencialmente dañina que explota una vulnerabilidad para comprometer o perturbar la seguridad de sistemas o personas. [7]
- Vulnerabilidad, de acuerdo con la definición de la Organización Internacional de Estandarización y su norma 27000, se trata de la debilidad de un sistema que puede ser explotada por una amenaza, originando un incidente de seguridad. [8]
- Incidente, puede entenderse como cualquier suceso que tenga un impacto adverso significativo sobre alguna de las dimensiones de la seguridad como la disponibilidad, la autenticidad, la integridad o la confidencialidad de los datos, en la provisión de servicios esenciales o digitales, conforme a lo que explica la directiva NIS2. [4]

ENISA en su informe *Threat Landscape 2024* [9], identifica como ciberamenazas en tendencia: los ataques tipo *ransomware*², cuyo objetivo suele ser lucrativo mediante la doble extorsión, por un lado, para la recuperación de los datos cifrados (secuestrados), y por otro para la no publicación de estos en foros u otros medios de difusión *online*. Seguido de los anteriores, los ataques de denegación de servicio distribuido³ (DDoS, por sus siglas en inglés), cuyo auge es motivado por campañas contra organismos públicos principalmente por parte de grupos hacktivistas con objetivos reivindicativos o desestabilizadores relativas a conflictos o ideas de políticas contrarias a su ideología. Además de los anteriores, también aumentaron los ataques a la cadena de suministro, amenazas a infraestructuras críticas y explotación de vulnerabilidades de día cero, o *Zero-day*.

2.1.4 Gestión de incidentes de ciberseguridad

La gestión de incidentes constituye un proceso estructurado y continuo para identificar, analizar, contener, erradicar y recuperar los servicios afectados por un incidente de ciberseguridad. No existe un método concreto, ni un modelo universal, sin embargo, a nivel internacional sí que existen guías de referencia como las del NIST o las guías ISO de la familia 27000 entre las más reconocidas.

²1 *Ransomware* constituye una modalidad de ataque en la que los delincuentes bloquean o cifran la información de una organización y posteriormente solicitan un rescate económico a cambio de restituir el acceso a dichos datos. [49]

³ DDoS (*Distributed Denial of Service*): ataques buscan interrumpir el acceso legítimo a un sistema o servicio al sobrecargarlo con tráfico malicioso proveniente de múltiples fuentes comprometidas. La naturaleza distribuida de estos ataques dificulta su mitigación y detección, ya que el tráfico malicioso se origina desde diversos puntos de la red [49]

A nivel europeo, ENISA han desarrollado guías y buenas prácticas en materia de equipos de respuesta ante incidentes informáticos, o CSIRT (por sus siglas en inglés, *Computer Security Incident Response Team*) y protocolos de notificación [10]. Por su parte, en España el Centro Criptológico Nacional (CCN), entre sus guías STIC, publica la guía CCN-STIC-817 de Gestión de Ciberincidentes⁴, como marco de referencia nacional.

En España, el CCN-CERT y el INCIBE-CERT son los equipos de respuesta ante emergencias informáticas⁵ de referencia a nivel nacional en la gestión de incidentes, bajo el marco establecido por el RDL y el RD 43/2021. Sin embargo, existen diversos CSIRT, tanto privados, como públicos como los CSIRT autonómicos, véase el CSIRT-CV de Valencia o el CERT vasco, entre otros, que dan soporte técnico a las empresas y administraciones de la comunidad autónoma a la que pertenecen, o como por ejemplo, organizaciones como CSIRT.es, formado por empresas y administraciones públicas para el intercambio de información relativa a ciberseguridad, buenas prácticas y otras iniciativas para fomentar la colaboración público-privada.

En el ámbito de los operadores de servicios esenciales (OSE), como sujetos obligados dentro del RDL y el RD 43/2021 que desarrolla el anterior, la Guía Nacional de Notificación y Gestión de Ciberincidentes, se erige como un marco común de referencia a seguir para el cumplimiento de tales normas.

⁴ <https://www.ccn-cert.cni.es/es/guias.html>

⁵ CERT (*Computer Emergency Response Team*), es el nombre registrado por la universidad Canergie Melon de Estados Unidos, mientras que el acrónimo CSIRT, se refiere al término general de Computer Security Incident Response Team (Equipo de Respuesta de Incidentes de Seguridad Informáticos)

3 ESTADO DEL ARTE DEL SISTEMA DE LA CIBERSEGURIDAD (UNIÓN EUROPEA Y ESPAÑA)

La política de ciberseguridad europea ha evolucionado desde un enfoque dividido y sectorial hacia un ecosistema normativo y organizativo integrado y cohesionado, a la vez que exigente. En este capítulo se describirán las diversas directivas y reglamentos relativos a la ciberseguridad, así como a los entes y actores que se encargan de la misma y que configuran el marco europeo en esta materia.

Por otro lado, España ha desarrollado asimismo estructuras nacionales especializadas y con un gran nivel de madurez y está en proceso de adaptar su marco jurídico con un Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad por el que, adicionalmente se crea un Centro Nacional de Ciberseguridad y se refuerza la gobernanza y la supervisión.

3.1 Panorama estratégico

3.1.1 Estrategia de la Unión Europea

La Estrategia de Ciberseguridad de la UE para la Década Digital (“*Cybersecurity Strategy for the Digital Decade*”) marca las prioridades: prevención, resiliencia y respuesta colectiva, impulso a capacidades industriales y tecnológicas, certificación y cooperación operativa. La estrategia impulsa inversiones, el desarrollo industrial (cadena de suministros) y políticas de habilidades y concienciación. Para implementar dicha estrategia, la UE ha creado mecanismos de financiación e innovación orientados a fortalecer capacidades y mercado.

La estrategia busca alcanzar un doble propósito, por un lado, aumentar la resiliencia de la Unión frente a las ciberamenazas y, por otro, garantizar la fiabilidad de las tecnologías de la información a los ciudadanos y empresas. Para ello, la Unión pretende ser tecnológicamente soberana e impulsar estándares de ciberseguridad para servicios esenciales e infraestructuras críticas, además de impulsar el desarrollo y la aplicación de nuevas tecnologías.

El documento hace un llamamiento a la seguridad en áreas críticas, exigiendo una responsabilidad compartida entre los Estados miembros, sus gobiernos, empresas y ciudadanos para garantizar una transformación digital segura. [12]

3.1.2 Estrategia de ciberseguridad de España

La Estrategia Nacional de Ciberseguridad (2019) continúa siendo el marco estratégico nacional con ejes sobre gobernanza, prevención, respuesta y cultura de seguridad; sin embargo, la coyuntura normativa europea obliga a actualizarla y a reforzar la coordinación interinstitucional. [13]

El objetivo fundamental se centra en garantizar la seguridad y promover el progreso. De una parte, se propone garantizar el uso seguro y fiable del ciberespacio a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques. Además, pone el foco en la protección de los datos personales, la privacidad, la libertad de expresión y el acceso a la información veraz y de calidad. Por último, pretende promover el apoyo y el impulso de la industria española en materia de ciberseguridad, la investigación, el desarrollo y la innovación, así como la gestión del talento tecnológico.

Los principios rectores de la Estrategia se sustentan en los siguientes cuatro pilares:

- 1) Unidad de acción: para asegurar una respuesta coherente, coordinada, rápida y eficaz ante incidentes, mediante una gestión de crisis centralizada, implicando a los actores nacionales con competencia en la materia.
- 2) Anticipación: priorizando la prevención a través de mecanismos como la compartición de información de manera casi inmediata.
- 3) Eficiencia: gestionando los recursos disponibles de manera óptima y eficiente.
- 4) Resiliencia: como característica fundamental para asegurar la disponibilidad de los sistemas e infraestructuras críticas ante ciberamenazas o usos ilícitos del ciberespacio.

3.2 Marco normativo

En línea con el sistema regulatorio actualmente vigente y las normas que se encuentran en desarrollo o en ciernes de ser publicadas, se expone a continuación de manera abreviada el panorama actual, si bien más adelante se profundizará en algunas de las más significativas para este ensayo.

3.2.1 Marco regulatorio de ciberseguridad europeo

- Reglamento ENISA (Reglamento (UE) 2019/881) y Cybersecurity Act: refuerzan la agencia europea de ciberseguridad (ENISA), el marco de certificación y el apoyo técnico a Estados miembros.
- NIS 2 (Directiva (UE) 2022/2555): amplía el alcance (más sectores y entidades), endurece obligaciones sobre gestión de riesgos, notificación de incidentes, gobernanza y sanciones; crea obligaciones de cooperación operativa (Cooperation Group, CSIRTs Network, EU-CyCLONe).
- DORA (Reglamento (UE) 2022/2554, *Digital Operational Resilience Act*, por sus siglas en inglés): resiliencia operativa digital en el sector financiero mediante controles de TIC, pruebas, gestión de terceros y notificación de incidentes graves.
- CER (Directiva (UE) 2022/2557, *Critical Entities Resilience*, por sus siglas en inglés): resiliencia de entidades críticas (gestión de riesgos y notificación), complemento sectorial para infraestructuras clave. [14]

3.2.2 Marco regulatorio de ciberseguridad de España

- Transposición NIS 1: RD-ley 12/2018 de seguridad de las redes y los sistemas de la información, desarrollo por RD 43/2021. En 2024 se transpuso la directiva NIS 2 en el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, que deroga a los anteriores y en el que, como novedad respecto a la directiva en sí, se establece la creación de un Centro Nacional de Ciberseguridad para reforzar la gobernanza y supervisión a nivel nacional.
- Transposición de la directiva CER materializada a fecha de la redacción de este trabajo, en el anteproyecto de ley de Protección y Resiliencia de Entidades Críticas. Este viene a derogar y actualizar a la Ley 8/2011 de Protección de Infraestructuras Críticas. [15]

3.3.1.3 CSIRTs Network

La red de equipos de respuesta ante incidentes informáticos formada por miembros de CSIRT nacionales y del CERT-EU para coordinar la respuesta técnica a incidentes transfronterizos. [20]

3.3.1.4 Grupo de trabajo NIS

Este grupo, dependiente de la Comisión europea, constituye un órgano de apoyo técnico creado con motivo de los trabajos de desarrollo de la directiva NIS. Su función principal es la de apoyar y coadyuvar la cooperación estratégica y el intercambio de información en materia de seguridad de las redes y los sistemas de información entre los Estados miembros. [21]

3.3.1.5 ECCC

El Centro Europeo de Competencia en Ciberseguridad (*European Cybersecurity Competence Centre*, por sus siglas en inglés), depende de la Comisión europea y tiene como misión coordinar los proyectos e inversiones europeos en materia ciber, al objeto de aumentar la autonomía estratégica digital en la Unión. [22]

3.3.1.6 EUROPOL-EC3

El Centro Europeo de Ciberdelincuencia, incardinado en el seno de la Oficina Europea de Policía (Europol), constituye la unidad especializada en la UE en materia de cibercrimen, análisis forense digital y cooperación operativa internacional. [23]

3.3.1.7 EU-CyCLONe

European Cyber Crisis Liaison Organisation Network, como se denomina en inglés, constituye la red para la coordinación operativa de crisis a alto nivel (articulada por NIS2, bajo la secretaría ENISA). Su objetivo es colaborar y desarrollar el intercambio de información ante ataques y crisis cibernéticas a gran escala y con impacto transfronterizo. Además, ENISA apoya la organización de ejercicios para los miembros de EU-CyCLONe, como CySOPex (para representantes de las autoridades de gestión de crisis cibernéticas de los Estados Miembros) y BlueOLEx (para alta dirección) [24]

3.3.2 Modelo institucional en España

España, por su parte ha configurado un modelo institucional de gobernanza que queda representado de la siguiente manera y que será descrito a continuación.

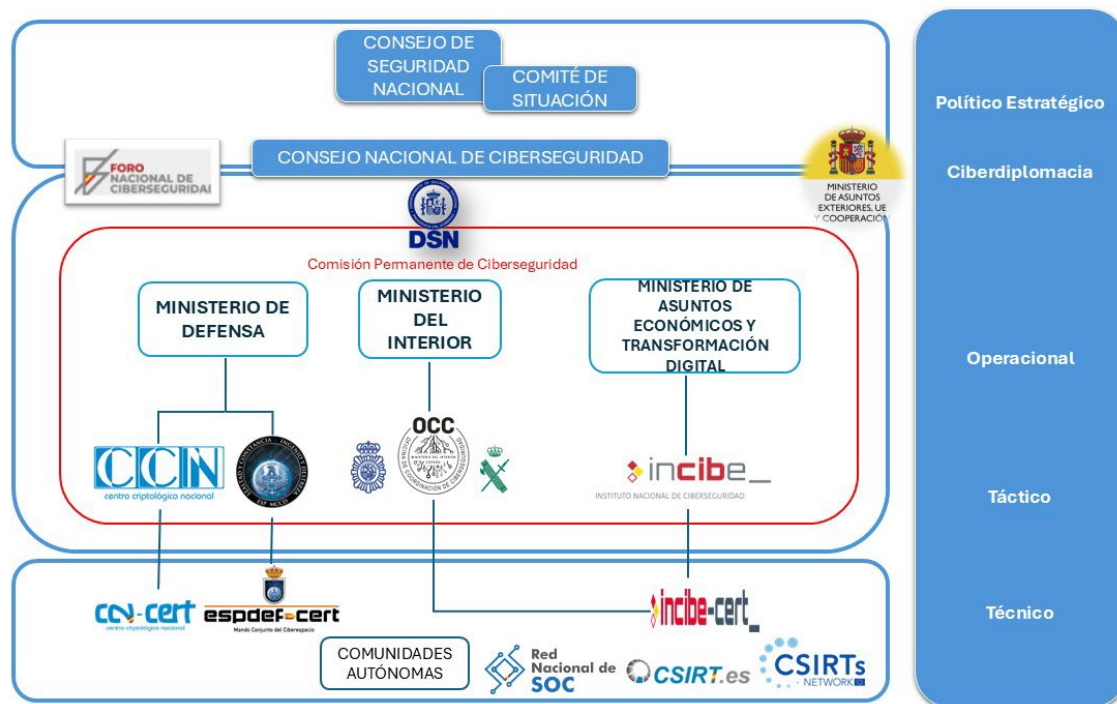


Figura 2 Modelo de gobernanza. Elaboración propia

3.3.2.1 Consejo de Seguridad Nacional (CSN)

Se trata del órgano superior de apoyo al Gobierno en materia de seguridad nacional y se sitúa en el nivel más alto de la estructura de gobernanza. Presidido por el presidente del Gobierno, se encarga de dirigir y coordinar la política de seguridad nacional, siendo un órgano de decisión a nivel político-estratégico. [25]

3.3.2.2 Comité de Situación

Este Comité dependiente del anterior, es el órgano de apoyo operativo del Consejo de Seguridad Nacional, responsable de la gestión de crisis de seguridad nacional, incluyendo aquellas derivadas de incidentes de ciberseguridad de gran impacto. Este se activa a instancia del presidente del Gobierno o del CSN cuando la gestión de un incidente o amenaza supere las capacidades de los órganos competentes en este ámbito. [26]

3.3.2.3 Consejo Nacional de Ciberseguridad

El Consejo Nacional de Ciberseguridad (CNC) se compone de representantes de ministerios, organismos y agencias con competencias en ciberseguridad, pudiendo incorporar expertos y actores del sector privado cuando se requiera. Entre sus funciones, están las de asesorar y apoyar al Consejo de Seguridad Nacional en materia de ciberseguridad, coordinando la cooperación interministerial y público-privada para prevenir, detectar y responder ante ciberamenazas. Además, supervisa la ejecución y revisión de la Estrategia de Ciberseguridad Nacional, analiza riesgos y capacidades, propone medidas, planes y normativa en la materia, y actúa como órgano de coordinación operativa entre las autoridades competentes hasta la eventual activación del Comité de Situación.

3.3.2.4 Ministerio de Asuntos Exteriores y de Cooperación

Este Ministerio juega un papel esencial en la ciberdiplomacia⁷, o diplomacia digital, al ser el responsable de la proyección internacional de la política española, actuando como elemento clave para proteger los intereses de España, reforzar alianzas internacionales y consolidar el papel del país como socio fiable y activo en la seguridad digital global. [27]

3.3.2.5 Nivel operacional y táctico

A nivel táctico y operativo del modelo de gobernanza, intervienen diferentes ministerios con responsabilidades concretas, que llevan a cabo y coordinan las acciones técnicas y operativas para salvaguardar el ciberespacio nacional, de acuerdo con la Ley 40/2015 del Régimen Jurídico del Sector Público, que establece la cooperación entre administraciones y la coordinación entre entidades estatales. Estos son los ministerios y sus correspondientes órganos implicados:

- Ministerio de Defensa: a través del Centro Criptológico Nacional y Mando Conjunto del Ciberespacio. El CCN, adscrito al Centro Nacional de Inteligencia (CNI), es la autoridad nacional en materia de seguridad de las Tecnologías de la Información y las Comunicaciones (TIC) del ámbito de la ley 40/2015. Entre sus funciones está la de garantizar la protección de la información clasificada, la ciberdefensa de los sistemas públicos y la aplicación de la normativa nacional de seguridad. [28] Por otro lado, el MCCE dispone de las capacidades de ciberdefensa de las Fuerzas Armadas, asegurando la protección, detección, respuesta y recuperación frente a ciberataques que afecten a la seguridad nacional. [29]
- Ministerio del Interior: a través de la Oficina de Coordinación de Ciberseguridad (OCC), dependiente de la Secretaría de Estado de Seguridad (SES), es el punto de contacto nacional conforme a la Directiva 2013/40/UE, para el intercambio de información sobre ataques a sistemas de la información. Además, ejerce como autoridad en el ámbito la NIS (RDL). Adicionalmente, la OCC ejerce la coordinación entre las Fuerzas y Cuerpos de Seguridad del Estado todo lo relativo a ciberdelitos dentro de su ámbito competencial.
- Ministerio de Asuntos Económicos y Transformación Digital: por medio del Instituto Nacional de Ciberseguridad (INCIBE), es responsable de garantizar la seguridad de los sistemas de la información y la comunicación para ciudadanos, empresas y operadores de servicios digitales.

3.3.2.6 Nivel técnico

Esta capa es donde se enmarcan los organismos con capacidades técnicas para dar soporte al sistema de gobernanza en materia de seguridad pública y defensa nacional por medio de los equipos de respuesta ante incidentes de ciberseguridad.

- CCN-CERT: es el equipo de respuesta a incidentes de ciberseguridad de las administraciones públicas y otras entidades que trabajan con datos clasificados o sensibles. Asimismo, ofrece soporte técnico, elabora guías y emite alertas e instrucciones sobre buenas prácticas. Asimismo, se encarga del diseño del Esquema Nacional de Seguridad (ENS) y coopera con los CSIRT sectoriales y otros actores europeos y nacionales por medio de la red CSIRTs Network de la UE. [30]
- ESPDEF CERT: es el CSIRT del Mando Conjunto del Ciberespacio (MCCE) encargado de proteger las redes, sistemas y operaciones militares frente a ciberamenazas, tanto en tiempos de

⁷ El término "ciberdiplomacia" se refiere al establecimiento de pactos multilaterales entre los responsables de los Estados y actores no estatales en el ámbito cibernético y de gobernanza con el fin de fomentar los intereses de los Estados, negociar convenios y resolver conflictos en el contexto de las relaciones internacionales. Su objetivo es establecer un ciberespacio abierto, libre, seguro y estable, basado en el derecho internacional a través de acuerdos entre naciones afines, organizaciones, la sociedad civil, el sector privado y expertos. [48]

paz como en situaciones de crisis o conflicto. Su actividad incluye la detección, análisis y respuesta ante ciberincidentes que afecten a los sistemas de defensa, la colaboración con aliados de la OTAN y la UE, y el apoyo técnico al MCCE en el desarrollo de capacidades avanzadas de ciberdefensa. [29]

- INCIBE-CERT: que ejerce de CSIRT de referencia para individuos, empresas y proveedores de servicios digitales. Su objetivo es proteger el tejido económico y social frente a ciberamenazas, proporcionando servicios de gestión de incidentes, análisis forense, concienciación, desarrollo de capacidades y cooperación público-privada. Además, el CERT, dentro del ámbito de los operadores críticos, es cooperado con la Oficina de Coordinación de Ciberseguridad (OCC), en el marco de un convenio interministerial. [31]
- Otros organismos: en este nivel técnico se incluyen otros actores como los CSIRT autonómicos, la Red Nacional de SOC (Centros de Operaciones de Seguridad) o la Red europea de CSIRT.

4 EVOLUCIÓN DEL MARCO REGULATORIO EUROPEO

Las estrategias y políticas europeas sobre ciberseguridad han dado como resultado diferentes normas que han evolucionado significativamente en la última década, pasando de un enfoque sectorial y fragmentado hacia un marco más armonizado y exigente, que engloba la protección de redes, sistemas, servicios esenciales y proveedores digitales. Esta evolución se articula principalmente a través de las Directivas NIS1 y NIS2, complementadas por el reglamento DORA y la directiva CER, como normas especiales, y el marco regulatorio de ENISA.

4.1 Estrategia de ciberseguridad de la Unión Europea (2020)

El desarrollo de las diferentes Estrategias de Ciberseguridad de la Unión Europea (UE) ha demostrado un avance gradual en términos políticos, técnicos y geoestratégicos de la Unión ante el aumento de los peligros digitales y la dependencia tecnológica en ascenso. En la última década, la Unión Europea ha evolucionado desde una perspectiva sectorial y defensiva a un enfoque integral que abarca la soberanía digital, la resiliencia y la seguridad. Esta evolución de las estrategias de ciberseguridad de la UE ha impulsado de forma directa el desarrollo de su marco normativo, consolidando una política europea coherente y progresivamente más exigente.

La primera estrategia de ciberseguridad europea publicada en 2013, titulada “Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, seguro y protegido”, representó el punto de partida de la política europea de ciberseguridad, concebida como un instrumento estratégico transversal que integraba la seguridad nacional, la defensa, la economía digital y la diplomacia. Pretendía convertir el espacio de la Unión en un entorno digital seguro y de confianza para los ciudadanos, las empresas y las instituciones. Fue, además, la base conceptual sobre la que se construyeron las estrategias posteriores de 2017 y 2020, así como la Directiva NIS 1.

La vigente estrategia, publicada en 2020 y denominada: “Estrategia de Ciberseguridad de la Unión Europea para la Década Digital 2020”, sienta las bases para una Europa digital soberana, resiliente y segura. Su objetivo principal es conseguir que todos los dispositivos y componentes conectados (incluidos los de uso industrial y de consumo) así como y la cadena de suministro sean seguros desde el diseño y resistentes a Ciberincidentes. La consecución de estos objetivos pretenden alcanzar mediante la propuesta de legislación horizontal sobre requisitos de ciberseguridad. La Estrategia exige que la ciberseguridad se integre en la digitalización y sea coherente e interoperable entre todos los sectores, a la vez que impulsa el desarrollo de una infraestructura de conectividad ultra segura, incluyendo un sistema basado en el espacio con encriptación cuántica. [32]

4.2 Directiva NIS 1 Directiva (UE) 2016/1148

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 (en adelante NIS 1, por sus siglas en inglés de *Network and Information Systems*), representó la primera iniciativa legislativa europea para garantizar un nivel común de seguridad de las redes y sistemas de información en la Unión Europea. Constituyó un punto de inflexión en el ámbito de la seguridad de las redes y los sistemas de la información de los servicios esenciales y proveedores de servicios digitales en el espacio de la Unión Europea. Como marco armonizador para todos los miembros de la Unión, se definían requisitos mínimos de seguridad comunes en materia de desarrollo de capacidades, planificación, intercambio de información a los sujetos obligados.

Entre los objetivos principales de la NIS 1, el primero era establecer obligaciones de seguridad para operadores de servicios esenciales (OSE) y proveedores de servicios digitales (PSD), debiendo tomar medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de sus sistemas y garantizar la continuidad de sus servicios esenciales. Otro aspecto era garantizar la notificación de incidentes significativos a las autoridades competentes y a los Equipos de Respuesta ante Incidentes Informáticos. Además, para la cooperación transfronteriza se constituye el Grupo de Cooperación NIS y paralelamente, se crea la Red de CSIRT para promover una cooperación operativa rápida y eficaz, permitiendo el intercambio de información sensible no comercial sobre incidentes, la respuesta coordinada a incidentes transfronterizos y la asistencia mutua voluntaria. [33]

Sin embargo, en cuanto a la armonización de la norma entre los Estados miembros, ésta no ha resultado como se esperaba. Cada miembro ha interpretado y transpuesto la norma de forma que las diferencias entre ellos han sido notables, no consiguiendo el objetivo de acercar criterios.

4.3 Directiva NIS 2. Directiva (UE) 2022/2555

A pesar de los logros obtenidos con la NIS 1, como el desarrollo de las capacidades nacionales de los Estados miembros, su aplicación por parte estos, con el tiempo dejó patente algunas deficiencias. Lo más llamativo fueron las diferencias sobre su ámbito de aplicación (sectores), las obligaciones de seguridad y la notificación, así como los métodos de supervisión y cumplimiento. Esto planteaba la necesidad de un cambio para abordar eficazmente los retos comunes en esta materia y generar un nivel homogéneo de ciberresiliencia.. [34]

La NIS 2 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, que deroga a la NIS 1, trata de superar las deficiencias detectadas en esta con las transposiciones por los Estados miembros de la Unión. Además, en los escasos seis años de diferencia entre la primera directiva y esta, la transformación digital, la sofisticación de las amenazas y los, cada vez más, riesgos emergentes, han obligado a las autoridades a tomar más medidas y actualizar las normas y los medios para prevenirlas y combatirlas desde un punto de vista nacional, como internacional a través de políticas, estrategias, normas y mecanismos de cooperación y colaboración. [6]

El objetivo principal de esta nueva directiva es el de alcanzar un alto nivel de ciberseguridad común para toda la Unión Europea. Para lograr esto, establece unos criterios más estrictos y uniformes, como dividir las entidades en dos grupos: Entidades Importantes y Esenciales, por lo general en función de su tamaño (empresas medianas y grandes) y la criticidad de su sector, suprimiendo la vieja clasificación entre Proveedores de Servicios Digitales y Operadores de Servicios Esenciales. También requiere que los Estados miembros implementen Estrategias Nacionales de Ciberseguridad que aborden políticas sobre la ciberseguridad en la cadena de suministro, el manejo de vulnerabilidades y la promoción de una ciberprotección activa.

Además, las entidades están obligadas a cumplir con las responsabilidades de gobernanza y gestión de riesgos, que son un elemento esencial del NIS 2. Las entidades que son esenciales e importantes, tienen que implementar medidas técnicas, operativas y organizacionales apropiadas y proporcionadas para gestionar los riesgos y asegurar la continuidad de sus servicios. Deben ser incluidas medidas como el análisis de riesgos, la administración de incidentes, la continuidad de las actividades (recuperación y copias de seguridad), y, lo más importante, la protección de la cadena de suministro. Estas medidas están fundamentadas en una perspectiva que abarca "todos los peligros", es decir, la seguridad del entorno físico y de los sistemas informáticos y de redes.

NIS 2 también armoniza y endurece las obligaciones de notificación y la cooperación a nivel de la Unión. La notificación de incidentes significativos se vuelve obligatoria "sin dilación indebida", con un proceso de múltiples etapas: una alerta temprana en el plazo de veinticuatro (24) horas desde que se tiene conocimiento del incidente, una notificación del incidente en setenta y dos (72) horas, y un informe final en el plazo de un mes.

La cooperación transfronteriza se refuerza a través del mantenimiento del Grupo de Cooperación (para el intercambio estratégico de información) y la Red de CSIRT (para la cooperación operativa rápida). Asimismo, se crea la Red Europea de Organizaciones de Enlace para las Crisis de Ciberseguridad (EU-CyCLONe) para coordinar la respuesta a incidentes y crisis de ciberseguridad a gran escala.

Finalmente, para garantizar el cumplimiento, la Directiva establece un régimen de supervisión y aplicación y prevé un régimen sancionador con multas más onerosas.

4.4 Reglamento DORA. Reglamento (UE) 2022/2554

El Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero (DORA), tiene como objetivo alcanzar un elevado nivel común de resiliencia operativa digital para el sector financiero de la Unión. Su propósito es reforzar la resiliencia de las entidades financieras, para que puedan hacer frente a las interrupciones operativas; proteger la estabilidad financiera, contribuyendo a mantener la estabilidad e integridad de los mercados financieros; y armonizar requisitos, eliminando las incoherencias y lagunas existentes en el código normativo único sobre los riesgos relacionados con las TIC. Se aplica a las entidades financieras y a los proveedores de servicios TIC que les prestan servicios.

DORA establece una serie de obligaciones a las entidades sujetas a su cumplimiento. Entre las obligaciones principales destacan:

- Las entidades deben disponer de un marco de gestión del riesgo relacionado con las TIC, en el que se incluya al menos las estrategias, políticas y procedimientos necesarios para proteger los activos de información y TIC. Asimismo, se debe establecer un modelo de gobernanza en el que el órgano de dirección asuma la responsabilidad última de gestionar el riesgo relacionado con las TIC. Éste, debe aprobar el marco, la estrategia de resiliencia digital, la política de continuidad de actividad, y asegurar un presupuesto adecuado para la resiliencia operativa. Además, deben implementar políticas que limiten el acceso físico y lógico, utilizar autenticación fuerte, proteger las claves criptográficas, y contar con políticas documentadas para la gestión de cambios y actualizaciones (parches)
- Se establece un régimen armonizado y centralizado de notificación de incidentes graves relacionados con las TIC, diseñado para eliminar diferencias y evitar la duplicación de requisitos, especialmente para las entidades que también estaban sujetas a la Directiva (UE) 2015/2366 (sobre servicios de pago). Los incidentes se clasifican según criterios como el número de clientes o contrapartes afectadas, la duración del incidente, la extensión geográfica, la pérdida de datos y el carácter esencial de los servicios afectados. Además, se establece la obligación de notificar a la autoridad nacional competente los incidentes considerados graves.

- Es obligatorio realizar pruebas de resiliencia para detectar vulnerabilidades y garantizar la continuidad de la actividad. Por ello se deben establecer ejercicios que incluyan pruebas de penetración basadas en amenazas, que deben llevarse a cabo al menos cada tres años.
- En cuanto a la gestión del riesgo relacionado con las TIC derivado de terceros (cadena de suministro), se imponen requisitos rigurosos. En el Reglamento se determina que la responsabilidad plena y final recae sobre la entidad financiera responsable de las obligaciones de cumplimiento.

Finalmente, este Reglamento considerado *lex specialis* (ley especial) respecto a la Directiva NIS 2, excluye a las entidades financieras de las disposiciones de la NIS 2, en cuanto a la gestión de riesgos de ciberseguridad, notificación y supervisión. [35]

4.5 Directiva CER. Directiva (UE) 2022/2557

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 (CER, *Critical Entities Resilience*, por sus siglas en inglés) constituye el marco legislativo de la Unión Europea diseñado para reforzar la resiliencia física y operativa de las entidades que prestan servicios esenciales en el mercado interior. Fue adoptada para derogar y sustituir la Directiva 2008/114/CE, la cual, tras tantos años en vigor, ha demostrado que un enfoque centrado solo en activos individuales (infraestructuras críticas), resulta insuficiente para mitigar el impacto resultante de la interconexión de las operaciones.

El objetivo central de CER es establecer normas mínimas armonizadas para garantizar la prestación sin obstrucciones de servicios esenciales para el mantenimiento de funciones sociales o actividades económicas vitales, independientemente de la causa de la perturbación. A diferencia de NIS 2, su enfoque es de "todos los peligros" (*all-hazards*), comprendiendo riesgos naturales (catástrofes naturales, cambio climático), así como riesgos de origen humano, ya sean accidentales o intencionales (como accidentes, emergencias de salud pública, amenazas híbridas, terrorismo e infiltración delictiva).

Las entidades objetivo (Entidades Críticas o EC) son identificadas por los Estados miembros en función de si una interrupción tuviera un efecto perturbador significativo en la prestación de servicios esenciales, basándose en criterios como el número de usuarios, la duración de la perturbación y la dependencia de otros sectores.

La Directiva CER como *lex specialis*, igual que el Reglamento DORA, excluye expresamente materias reguladas por otros actos legales para evitar duplicidades y cargas administrativas innecesarias, como:

- Ciberseguridad (NIS 2): Las materias reguladas por la Directiva (UE) 2022/2555 (NIS 2) quedan excluidas del ámbito de aplicación de la Directiva CER. Esto se debe a que NIS 2 impone requisitos exhaustivos para garantizar la ciberseguridad, aplicando un enfoque más amplio ("todos los riesgos posibles"), a los sistemas de redes y de información, incluidos sus componentes físicos.
- Sector Financiero (DORA): Las entidades de los sectores de Banca e Infraestructuras de los mercados financieros, si bien son identificadas como entidades críticas, están exentas de los capítulos de obligaciones de resiliencia, supervisión y ejecución de CER. Esto se debe a que su resiliencia está ampliamente cubierta por el Reglamento (UE) 2022/2554 (DORA), que regula los riesgos de las TIC y la protección de las infraestructuras físicas de las TIC.
- Infraestructura Digital: Las entidades del sector de infraestructura digital, también están exentas de las obligaciones de resiliencia, supervisión y ejecución de CER porque los requisitos de NIS 2 son considerados, al menos, equivalentes a las obligaciones correspondientes de CER.

Por lo tanto, la Directiva CER (UE) 2022/2557 no se aplicará a las materias reguladas por la Directiva (UE) 2022/2555 (NIS 2) o DORA, sino que están diseñadas para aplicarse de manera

coordinada. Por ejemplo, la NIS 2 impone requisitos exhaustivos para garantizar la ciberseguridad a un amplio número de entidades, aplicando el mismo enfoque que la CER (*all-hazards*) a los sistemas de redes y de información, incluidos sus componentes físicos. Sin embargo, la CER se centra en la resiliencia física y operativa de las entidades críticas con respecto a todos los peligros físicos, como catástrofes naturales, accidentes, emergencias de salud pública y amenazas híbridas. [36]

5 DERECHO COMPARADO

Una vez analizadas las directivas UE 1148/2016 (NIS 1) y UE 2555/2022 (NIS 2), relativas al marco europeo de ciberseguridad que pretende armonizar el nivel de seguridad de los sistemas y las redes de información entre los Estados miembros y reforzar su resiliencia, se van a comparar a continuación ambas normas para conocer sus diferencias.

5.1 Comparativa entre la Directiva NIS 1 y la Directiva NIS 2

La Directiva (UE) 2016/1148, conocida como NIS 1, ha sido derogada y reemplazada por la Directiva (UE) 2022/2555, denominada NIS 2. Este examen comparativo entre ambas normas pone de manifiesto la evolución del marco europeo de ciberseguridad, orientada a corregir las limitaciones identificadas en NIS 1 y a reforzar la capacidad de respuesta ante los desafíos de ciberseguridad actuales y futuros.

5.1.1 *Objetivos y nivel de armonización*

Mientras que el objetivo de la directiva NIS 1 era establecer ciertas medidas que garantizaran un nivel alto de seguridad dentro de la Unión y mejorar así el funcionamiento del mercado interior, mediante el desarrollo de capacidades de ciberseguridad y la reducción de las amenazas a los sistemas utilizados para prestar servicios esenciales, la directiva NIS 2 tiene como propósito armonizar el nivel de ciberseguridad en todo el espacio de la UE. Tras varios años bajo la NIS 1 y sus respectivas transposiciones, se han podido observar divergencias y deficiencias entre los Estados miembros que han motivado la revisión de aquella y el desarrollo de la nueva para eliminar esas diferencias y acercar a todos los miembros hacia un nivel de ciberseguridad común y elevado.

5.1.2 *Ámbito de aplicación y clasificación de entidades*

Como se ha mencionado anteriormente, con la Directiva NIS 2 se pretende superar las deficiencias de la anterior que le impedían abordar eficazmente los retos de ciberseguridad. La revisión de la NIS 1 había puesto de manifiesto la existencia de grandes diferencias en su aplicación por parte de los Estados miembros, particularmente en lo que respecta a su ámbito de aplicación, cuya delimitación se dejó en gran medida a su discreción.

5.1.2.1 *Clasificación de entidades y criterios de aplicación (NIS 1)*

La Directiva (UE) 2016/1148 se centraba en dos categorías de entidades: Operadores de Servicios Esenciales (OSE) y Proveedores de Servicios Digitales (PSD).

Asimismo, cada Estado miembro era responsable de determinar qué entidades cumplían los criterios para ser consideradas OSE. Para ello, los miembros debían valorar, como mínimo, si la entidad desarrollaba su actividad en los sectores y subsectores que figuraban en su Anexo II, y si cumplía los siguientes tres criterios de identificación:

1. La entidad presta un servicio esencial para el mantenimiento de actividades sociales o económicas.
2. La prestación de dicho servicio depende de las redes y sistemas de información.
3. Un incidente tendría efectos perturbadores significativos en la prestación de dicho servicio.

Los Estados miembros debían revisar y actualizar esta lista de OSE periódicamente, al menos cada dos años.

Proveedores de Servicios Digitales (PSD): Los PSD se definían como personas jurídicas que prestan un servicio digital de los tipos que figuraban en el Anexo III, incluyendo mercados en línea, motores de búsqueda en línea o servicios de computación en nube. La NIS 1 consideraba que, debido a su carácter transfronterizo, los PSD debían estar contemplados en la norma para conseguir una armonización a nivel de la Unión. Además, la Directiva no se aplicaba a las microempresas ni a las pequeñas empresas que fueran PSD.

NIS 1 reconocía que la distinción entre OSE (sujetos a requisitos más exigentes y supervisión a cargo de los Estados miembros) y PSD (sujetos a un tipo de supervisión menos rigurosa, reactiva y a posteriori) se debía a las diferencias fundamentales entre ambos, especialmente por la vinculación de los OSE con infraestructuras críticas y el carácter transfronterizo de los PSD.

5.1.2.2 Reestructuración y ampliación del ámbito de aplicación (NIS 2)

La NIS 2 tiene como objetivo eliminar las deficiencias de su antecesora respecto a la clasificación de los sectores y servicios para las actividades sociales y económicas en el conjunto de la Unión. Para ello, introduce un criterio común sobre el tamaño para determinar a los sujetos obligados, aplicando, incluso, a entidades consideradas medianas empresas, o que superan los límites máximos para las medianas empresas, y que operan en los sectores listados en el Anexo I (Sectores de Alta Criticidad) o el Anexo II (Otros Sectores Críticos).

Las entidades incluidas se clasifican en dos categorías, basándose en su criticidad y tamaño:

- A. **Entidades Esenciales (EE):** Incluyen entidades del Anexo I que superan los límites de medianas empresas, o ciertos proveedores de servicios digitales (como prestadores cualificados de servicios de confianza, registros de nombres de dominio de primer nivel y proveedores de servicios de DNS, independientemente de su tamaño), así como las entidades identificadas como críticas con arreglo a la Directiva (UE) 2022/2557 (directiva CER). También se consideran EE las entidades que, independientemente de su tamaño, cumplen otros criterios específicos que demuestran su papel clave para la sociedad, o las entidades de la Administración Pública Central.
- B. **Entidades Importantes (EI):** Son todas las entidades de los Anexos I o II que no se consideran Entidades Esenciales.

En cuanto a la ampliación del ámbito sectorial, NIS 2, se extiende para una parte más vasta de la economía en aras de alcanzar una cobertura más completa de los servicios de vital importancia. En el texto de la norma se incluyen dos anexos con las categorías que se muestran en la figura 3.

Directiva (UE) 2022/2555: Clasificación de Entidades (NIS2)



Figura 3 Sectores de Alta criticidad y Críticos. Elaboración propia.

Aunque NIS 2 no incluye de forma general a las microempresas y pequeñas empresas (basado en el criterio de tamaño), sí que se aplica a aquellas que, independientemente de su tamaño:

- Prestan servicios como proveedores de redes públicas de comunicaciones electrónicas, servicios de comunicaciones electrónicas disponibles para el público, prestadores de servicios de confianza, registros de nombres de dominio de primer nivel, o proveedores de servicios de DNS.
- La entidad es el único proveedor de un servicio esencial en un Estado miembro.
- La perturbación del servicio pudiera tener repercusiones significativas en la seguridad pública, el orden público, la salud pública, o riesgos sistémicos significativos.

Por último, en cuanto a la clasificación en Entidades Esenciales (EE) y Entidades Importantes (EI) establece diferentes regímenes de supervisión y cumplimiento para equilibrar los requisitos según el riesgo y la carga administrativa:

- Las Entidades Esenciales están sujetas a un régimen de supervisión completo (a priori y a posteriori).
- Las Entidades Importantes están sujetas a un régimen de supervisión menos estricto, exclusivamente a posteriori. La supervisión a posteriori para las EI se inicia cuando las autoridades competentes tienen evidencias, indicios o información que sugieren un posible incumplimiento de la Directiva.

5.1.3 Requisitos de seguridad y gestión de riesgos

Ambas directivas exigen la adopción de medidas técnicas y organizativas adecuadas y proporcionadas para gestionar los riesgos. Sin embargo, la NIS 2 detalla y amplía estos requisitos.

- Enfoque de riesgos:** NIS 2 establece un enfoque basado en todos los peligros (“*all-hazards approach*”) que tiene como objetivo proteger los sistemas de redes y de información y el entorno físico de dichos sistemas frente a cualquier tipo de suceso (natural, malintencionado, etc.).
- Contenido mínimo:** NIS 2 establece una lista detallada de elementos obligatorios que deben incluir las medidas de gestión de riesgos, incluyendo:

- Análisis de riesgos y políticas de seguridad.
- Gestión de incidentes y continuidad de las actividades (incluida la gestión de crisis).
- Seguridad de la cadena de suministro, teniendo en cuenta los riesgos provenientes de los proveedores y los resultados de las evaluaciones coordinadas de riesgos de seguridad.
- Seguridad en la adquisición, desarrollo y mantenimiento de sistemas, incluyendo la gestión y divulgación de vulnerabilidades.
- Prácticas básicas de ciberhigiene y formación en ciberseguridad.
- Uso de criptografía y cifrado (obligatorio si es necesario para salvaguardar la seguridad y la privacidad).
- Uso de soluciones de autenticación multifactorial (MFA), o autenticación continua.

5.1.4 Notificación de incidentes

Puesto que la notificación de incidentes constituye un pilar fundamental en el modelo europeo de ciberseguridad, cuyo objetivo es promover una cultura de gestión de riesgos y permitir la cooperación y la respuesta coordinada a nivel de la Unión, en este apartado se va a dedicar un análisis algo más detallado.

5.1.4.1 Obligación de notificar: Alcance y Disparidades

Uno de los principales motivos que han llevado a derogar y actualizar estas directivas ha sido la diferencia de criterio en cuanto a la definición de los sujetos obligados por cada Estado miembro. Esto ha supuesto una brecha en cuanto a la disparidad en el número y tipo de entidades sometidas a la norma.

Por un lado, la NIS 1, no aplicaba de forma automática, ya que requería que cada Estado miembro realizara un proceso de identificación individualizado. Para que cada entidad fuera regulada como OSE, debía cumplir a la vez tres requisitos: que su servicio fuera esencial para la sociedad, que la prestación de ese servicio dependiese de las redes y los sistemas de la información y que, en caso de incidente, este tuviera efectos perturbadores en la prestación del servicio. La norma imponía a los OSE y a los PSD requisitos de notificación de incidentes, cuyo requisito general era que los incidentes que tuvieran “efectos significativos” en la continuidad de los servicios esenciales o digitales debían ser reportados.

La NIS 2, sin embargo extiende esa obligación a las Entidades Esenciales (EE) y las Entidades Importantes (EI). Además, las entidades que ofrecen servicios de registro de nombres de dominio también están obligadas a notificar.

5.1.4.2 Definición de “incidente significativo”

Ambas directivas vinculan la obligación de notificar al grado del impacto del incidente (NIS 1, también a la peligrosidad), aunque NIS 2 amplía los criterios de evaluación.

- NIS 1: Para determinar la importancia de los efectos de un incidente, se tenían en cuenta varios parámetros:
 - El número de usuarios afectados por la interrupción del servicio esencial o del servicio digital.
 - La duración del incidente.
 - La extensión geográfica de la zona afectada.

En el caso de los PSD, también se consideraba el grado de perturbación del funcionamiento del servicio y el alcance del impacto sobre las actividades económicas y sociales.

- NIS 2: Un incidente se considera significativo si:
 - Ha causado, o tiene potencial de causar, graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada.

- Ha afectado, o tiene potencial de afectar, a otras personas físicas o jurídicas, causándoles perjuicios materiales o inmateriales considerables.

5.1.4.3 El Proceso de notificación

La NIS 1 exigía una notificación diligente, sin demora injustificada, a la autoridad competente o al CSIRT correspondiente. Sin embargo, NIS 2 plantea el proceso en tres fases obligatorias, de modo que exista un equilibrio entre la celeridad y la exhaustividad de la información. Alerta Temprana. Plazo máximo de 24 horas para la notificación desde su conocimiento. Principalmente, se debe indicar si se sospecha de un origen ilícito o malintencionado y si puede tener impacto transfronterizo.

1. Notificación del incidente. El plazo máximo es de 72 horas desde que se tenga conocimiento, y se debe proporcionar una evaluación inicial de la gravedad o el impacto, y actualizar la información, a medida que se conozcan más datos (indicadores de compromiso, tácticas, técnicas y procedimientos, etc.).
2. Informe final. En el que se detallen todos los datos del incidente, como el impacto, medidas de mitigación, etc. Este informe debe ser entregado en el plazo de un mes desde la notificación. En caso de no haberse resuelto por completo el incidente, se presentarán informes de situación en el mismo plazo.

Con la anterior directiva, los sujetos obligados disponían de una ventana temporal relativamente más holgada, mientras que, con la nueva, ese arco se reduce con la alerta temprana que requiere una notificación casi inmediata.

Además, existe una excepción de plazo para los prestadores de servicios de confianza deben notificar incidentes significativos en la prestación de sus servicios en un plazo más corto de 24 horas desde que se tiene constancia del incidente.

5.1.4.4 Notificación y asistencia mutua

Ambas directivas incluyen mecanismos para la gestión de incidentes transfronterizos, sin embargo, con la NIS 1, la autoridad competente, o el CSIRT, basándose en la notificación del operador, informaba a otros Estados miembros afectados si el incidente tenía carácter transfronterizo, es decir, si tenía efectos significativos en la continuidad de los servicios esenciales en ese otro Estado.

Por su parte, NIS 2 establece que, si el incidente es transfronterizo o intersectorial, el CSIRT o la autoridad competente informará “sin demora indebida” a los demás Estados miembros afectados y a la ENISA, estableciendo un requisito temporal.

Además, también establece que el CSIRT o la autoridad competente debe ofrecer una respuesta a la entidad notificante, incluyendo comentarios iniciales y, si se solicita, orientación o asesoramiento operativo sobre medidas paliativas, en un plazo de 24 horas tras recibir la alerta temprana. Si se sospecha de un origen delictivo, también deben proporcionar orientación sobre cómo denunciar el incidente a las autoridades competentes.

5.1.4.5 Notificación a destinatarios y al público

Si bien, en ambas directivas, las autoridades competentes tienen la facultad de informar al público sobre incidentes concretos, o exigir a la entidad que lo haga, siempre después de consultar a la entidad afectada. Esto se lleva a cabo cuando la difusión pública es necesaria para evitar un incidente, gestionar uno en curso, o si la divulgación redundaría en el interés público. Sin embargo, NIS 2 exige además que, cuando sea conveniente, las Entidades Esenciales e Importantes informen a los destinatarios de sus servicios afectados por una ciberamenaza significativa y sobre las medidas o soluciones que pueden aplicar en respuesta a la amenaza.

5.1.4.6 Notificación voluntaria

Tanto NIS 1, como NIS 2 prevén la posibilidad de que entidades no sujetas a las obligaciones de la norma, notifiquen incidentes de forma voluntaria. Sin embargo, la NIS 2 extiende la notificación voluntaria a:

- Entidades Esenciales e Importantes (para incidentes, ciberamenazas y cuasiincidentes).
- Otras entidades (para incidentes, ciberamenazas o cuasiincidentes significativos).

En ambos casos, la tramitación de las notificaciones voluntarias solo se realiza cuando no suponga una carga desproporcionada o indebida, y esta notificación no conlleva la imposición de obligaciones adicionales a la entidad notificante

5.1.5 Gobernanza y cooperación a nivel de la Unión

Ambas directivas establecen un Grupo de Cooperación (NIS) y una Red de CSIRT. La NIS 2, además, introduce nuevas estructuras para la gestión de crisis y reforzando las responsabilidades de gobernanza a nivel de las entidades.

5.1.5.1 Gobernanza interna de las entidades

La NIS 2 introduce requisitos explícitos sobre la gobernanza y la rendición de cuentas dentro de las entidades esenciales e importantes, como:

- Aprobación y Supervisión de la Dirección: Los Estados miembros deben garantizar que los órganos de dirección de las entidades esenciales e importantes aprueben las medidas de gestión de riesgos de ciberseguridad adoptadas. Dichos órganos también deben supervisar su puesta en práctica.
- Responsabilidad y Formación: Los órganos de dirección responden por el incumplimiento de las medidas de riesgo. Además, los miembros de estos órganos deben asistir a formaciones periódicas para adquirir conocimientos suficientes que les permitan evaluar las prácticas de gestión de riesgos.

5.1.5.2 Cooperación Estratégica: Grupo de Cooperación

El Grupo de Cooperación se constituyó bajo la Directiva NIS 1 para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros. Bajo NIS 2, tiene su propio reglamento y su estructura se mantiene y se refuerza como se detalla a continuación:

a) Composición

El Grupo está integrado por representantes de los Estados miembros, la Comisión Europea y la ENISA. La Secretaría de este órgano es asumida por la Comisión.

Con la entrada en vigor de la Directiva NIS 2, su composición se amplía con el propósito de reflejar una cooperación interinstitucional más amplia y transversal. En este sentido, el Servicio Europeo de Acción Exterior (SEAE) participa en las actividades del Grupo en calidad de observador. Asimismo, las Autoridades Europeas de Supervisión (AES) y las autoridades competentes definidas en el Reglamento DORA pueden participar en sus trabajos. Cuando se considere oportuno, también se podrá invitar al Parlamento Europeo y a representantes de las partes interesadas pertinentes a contribuir en las labores del Grupo.

b) Objetivos y programación

El objetivo principal del Grupo de Cooperación es apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros, fomentando la confianza mutua y promoviendo un nivel común elevado de ciberseguridad en la Unión.

Tanto bajo la Directiva NIS 1 como con la NIS 2, el Grupo de Cooperación desarrolla sus funciones de conformidad con programas de trabajo bienales. En el marco de NIS 1, el primer programa debía establecerse a más tardar el 9 de febrero de 2018. ,

c) Funciones comunes

Las funciones del Grupo de Cooperación han evolucionado, ampliando su alcance estratégico y operativo en NIS 2:

- Orientación y Capacidad: Proporcionar orientación estratégica a las actividades de la Red de CSIRT y asistir a los Estados miembros en el desarrollo de capacidades para garantizar la seguridad de los sistemas de redes y de información
- Intercambio de Buenas Prácticas: Intercambiar buenas prácticas en relación con el desarrollo de capacidades, la concienciación y la formación, y la investigación y el desarrollo en materia de seguridad.
- Preparación y Evaluación: Discutir sobre las capacidades y la preparación de los Estados miembros, incluyendo la evaluación voluntaria de las estrategias nacionales y la identificación de buenas prácticas. NIS 2 formaliza esto para incluir el debate y la realización de una evaluación periódica de la situación de las ciberamenazas o incidentes, como los programas de secuestro.
- Informes y Revisión: Examinar los informes resumidos sobre notificaciones de incidentes presentados por los puntos de contacto únicos. NIS 2 requiere la preparación de informes para la revisión (que evalúan la experiencia estratégica y las revisiones inter pares) y la remisión de estos informes al Parlamento Europeo y al Consejo.
- Normalización: Discutir sobre las normas y especificaciones con los representantes de los organismos europeos de normalización pertinentes.
- Cooperación Externa: Intercambiar experiencias sobre asuntos relativos a seguridad de las redes y sistemas de información con las instituciones, órganos y organismos de la Unión competentes.

d) Funciones Específicas de NIS 2

La Directiva NIS 2 introduce nuevas funciones estratégicas que refuerzan el papel del Grupo de Cooperación en el ecosistema europeo de ciberseguridad:

- Cadenas de Suministro: El Grupo de Cooperación puede llevar a cabo evaluaciones coordinadas de los riesgos de seguridad de las cadenas de suministro críticas de servicios, sistemas o productos de TIC específicos, teniendo en cuenta factores de riesgo técnicos y no técnicos.
- Gestión de Crisis: Proporcionar orientación estratégica a EU-CyCLONe (la Red Europea de Organizaciones de Enlace para las Crisis de Ciberseguridad). También debe debatir sobre las labores realizadas en relación con los ejercicios de ciberseguridad.
- Revisiones Inter pares: Establecer la metodología y los aspectos organizativos de las revisiones inter pares voluntarias entre Estados miembros, así como la metodología de autoevaluación.
- Asistencia Mutua y Supervisión: Analizar los casos de asistencia mutua, incluidas las experiencias y los resultados de las acciones transfronterizas de supervisión conjuntas, y debatir solicitudes específicas de asistencia mutua.
- Intercambio de Personal: Contribuir a las capacidades de ciberseguridad de la Unión facilitando el intercambio de funcionarios nacionales a través de un programa de

desarrollo de capacidades en el que participe el personal de las autoridades competentes o los CSIRT.

- Coordinación Sectorial: El Grupo de Cooperación debe reunirse periódicamente, al menos una vez al año, con el Grupo de resiliencia de las entidades críticas (establecido con arreglo a la Directiva (UE) 2022/2557) para facilitar la cooperación estratégica y el intercambio de información.

La Comisión está facultada para adoptar actos de ejecución que establezcan las disposiciones de procedimiento necesarias para el funcionamiento del Grupo de Cooperación, consultando y cooperando con el Grupo en el proyecto de dichos actos.

5.1.6 Supervisión y ejecución

La directiva NIS 2 implementa un marco de supervisión y ejecución considerablemente más estricto y armonizado que la NIS 1, buscando corregir las disparidades que existían en su aplicación entre los Estados miembros

5.1.6.1 Régimen de supervisión

Con la NIS 1 los Operadores de Servicios Esenciales estaban sujetos a una evaluación de cumplimiento en la que las autoridades podían exigir cierta información (como documentación sobre políticas de seguridad, y resultados de auditorías de seguridad). Sin embargo, las Entidades Esenciales, están sujetas a un régimen de supervisión completo, tanto a priori como a posteriori.

Por otro lado, tanto los PSD, con la NIS 1, como las Entidades Importantes con su sucesora, se someten a un régimen de supervisión menos estricto y a posteriori, donde la autoridad competente solo interviene cuando hay evidencias de un posible incumplimiento de los requisitos de la Directiva.

En cuanto a las facultades de supervisión y medidas de control, la nueva directiva confiere a las autoridades competentes una lista mínima de competencias de supervisión, aplicables con diferente rigor según la categoría de la entidad:

- Inspecciones y Auditorías: Bajo NIS 2, las autoridades competentes pueden someter a las EE a inspecciones in situ y supervisión a distancia (incluidos controles aleatorios) Asimismo, pueden ordenar auditorías de seguridad periódicas y específicas realizadas por un organismo independiente o por la propia autoridad. También pueden realizar auditorías *ad hoc* tras un incidente significativo o incumplimiento.
- Análisis de Seguridad: Las autoridades competentes tienen la facultad de realizar análisis de seguridad basados en criterios de evaluación de riesgo objetivos y transparentes, con la cooperación de la entidad afectada.
- Solicitud de Información y Pruebas: Para evaluar las medidas de gestión de riesgos, las autoridades pueden solicitar información necesaria y pruebas de la aplicación efectiva de las políticas de ciberseguridad, como los resultados de auditorías de seguridad

Respecto a las facultades de supervisión, la NIS 1, incluía la solicitud de información y pruebas de implementación de las políticas de seguridad (incluidos resultados de auditorías).

Finalmente, sobre en ambas directivas se establece un régimen sancionador. La NIS 2 establece cuantías máximas mínimas específicas por incumplimiento de las obligaciones de gestión de riesgos o de notificación, mientras que en su antecesora solo exigía que las sanciones fueran “efectivas, proporcionadas y disuasorias”.

5.2 Análisis del Anteproyecto de Ley de Coordinación y Gobernanza de Ciberseguridad

El anteproyecto propone una novedad respecto a la directiva, la creación de un Centro Nacional de Ciberseguridad (en adelante CNCíber), como autoridad nacional en materia de ciberseguridad, responsable de establecer las políticas de ciberseguridad nacional y ejercer la coordinación del resto de autoridades de control que se definen en él.

Este anteproyecto tiene como objeto establecer medidas para alcanzar un elevado nivel común de ciberseguridad en España, al mismo tiempo que busca contribuir a la ciberseguridad de la Unión Europea.

A continuación, se describen las claves del Anteproyecto de Ley de Coordinación y Gobernanza de Ciberseguridad para entender sus objetivos y su alcance. [6]

5.2.1 Motivación y principios rectores

La frenética evolución de las TIC y de la creciente interconexión, ha conducido a un aumento de la superficie de exposición ante las ciberamenazas. La frecuencia, complejidad y el impacto de los incidentes cibernéticos representan un riesgo considerable para la operativa de las redes y los sistemas de información.

El balance de los últimos años, respecto a la Directiva anterior NIS1, (Directiva (UE) 2016/1148) dejó patente que había carencias, como la aplicación inconsistente de medidas entre los Estados miembros, lo que afectaba tanto la ciberresiliencia como la provisión de servicios transfronterizos. Para abordar estos problemas, la nueva legislación se centra en varios objetivos principales:

1. Establecer un marco institucional regulador;
2. Fortalecer la coordinación entre las autoridades competentes;
3. Asegurar la cobertura de todos los sectores y servicios esenciales para las actividades sociales y económicas dentro del mercado único;
4. Proveer de seguridad jurídica en la gestión de riesgos de ciberseguridad y las obligaciones de notificación de incidentes.

El anteproyecto introduce criterios claros para determinar qué entidades están dentro de su ámbito de aplicación, clasificándolas en dos grupos: entidades esenciales y entidades importantes, en función del grado de criticidad de sus servicios o sectores y su tamaño.

Asimismo, se alinea con la Directiva (UE) 2022/2557 (directiva CER), que regula la resiliencia de las entidades críticas, garantizando una integración coherente entre la ciberseguridad y la seguridad física de las entidades. De este modo, las entidades consideradas críticas bajo la CER también se clasifican como esenciales a los efectos de esta normativa.

5.2.2 Esquema institucional y de gobernanza

El anteproyecto define una nueva estructura de gobernanza centralizada y coordinada, con una nueva figura que encabeza dicho modelo y que tiene como objetivo concentrar y canalizar toda la información y gestión relativa a la ciberseguridad de interés nacional.

El modelo de gobernanza quedaría configurado de la siguiente forma, describiéndose a continuación los elementos de este.



Figura 4 Modelo Nacional de Gobernanza. Elaboración propia

5.2.2.1 Centro Nacional de Ciberseguridad (CNCíber)

Como se mencionaba anteriormente, supone la principal novedad de la gobernanza en España, constituyéndose como la única autoridad nacional competente en ciberseguridad, resolviendo así la actual dispersión de competencias. El CNCíber tiene la responsabilidad de liderar, impulsar y coordinar todas las actividades establecidas en la legislación. Actuará como la Autoridad Nacional de Gestión de Crisis y Punto de Contacto Único, garantizando la cooperación tanto intersectorial como transfronteriza. [6]

- Creación y naturaleza del CNCíber

El Centro Nacional de Ciberseguridad se crea mediante la disposición adicional primera del anteproyecto y estará adscrito al Gabinete de la Presidencia del Gobierno.

En su naturaleza, el CNCíber asume un carácter híbrido, por un lado, ejerce funciones estratégicas de gobernanza, formulación de políticas, supervisión y coordinación, y por otro, se le dota de atribuciones operativas como autoridad nacional de referencia técnica y de crisis en el ámbito de redes y sistemas de información sujetos al régimen de la NIS 2. Asimismo, el anteproyecto vincula su creación a la necesidad de disponer de un sistema de ciberseguridad coherente con los estándares europeos, con responsabilidades centralizadas que permiten una respuesta ágil y articulada frente a amenazas digitales

Su objetivo principal es concentrar la actual dispersión competencial en materia de ciberseguridad en una sola autoridad nacional, que ejerza de coordinadora de las autoridades de control y se erija como punto de contacto único nacional en esta materia.

- Autoridad Nacional única

El CNCíber se establece como la autoridad nacional competente única en materia de gobernanza de la ciberseguridad. Sus funciones primordiales son la dirección, impulso y la coordinación de todas las actividades previstas en el ámbito de la ley, necesarias para garantizar un elevado nivel de ciberseguridad en España y contribuir a la ciberseguridad de la Unión Europea.

Además, ejercerá como órgano superior para la gobernanza y coordinación de las actividades en ciberseguridad previstas en la ley y su normativa de desarrollo, sin perjuicio de las competencias que

otros órganos tienen legalmente establecidas. Asumirá cualquier otra función que se le encomiende en el ámbito de la ciberseguridad nacional, sin perjuicio de las competencias legalmente reservadas a otros organismos.

- Funciones de concentración específicas

El Centro Nacional de Ciberseguridad (CNCíber) concentrará varias funciones clave, reforzando la centralización de la gobernanza. El CNCíber ejercerá de punto único de contacto para garantizar la cooperación intersectorial a nivel nacional y la cooperación transfronteriza con autoridades pertinentes de otros Estados miembros, la Comisión Europea y ENISA y actuará como autoridad nacional de gestión de crisis, como responsable de la coordinación para la gestión de incidentes y crisis de ciberseguridad a gran escala.

Entre otras tareas el Centro llevará a cabo las siguientes:

- Identificación de Entidades: Implementará los procedimientos necesarios para identificar qué entidades se encuentran recogidas en el ámbito de aplicación de la ley, con ayuda de las autoridades de control y puntos de contacto sectoriales. También elaborará y revisará regularmente (al menos cada dos años) la lista de entidades esenciales e importantes.
- Establecimiento de Medidas y Estándares: Determinará las medidas técnicas, operativas y de organización que las entidades esenciales e importantes deberán implantar para gestionar los riesgos de ciberseguridad. Podrá promover y aprobar estándares, guías, especificaciones e instrucciones técnicas en materia de seguridad de las redes y sistemas de información.
- Divulgación Coordinada de Vulnerabilidades: Designará al CSIRT nacional de referencia que actuará como organismo coordinador a efectos de la divulgación coordinada de vulnerabilidades.
- Cooperación Nacional e Internacional: Cooperará con diversos órganos y organismos públicos con competencias en Seguridad Nacional, Defensa Nacional, seguridad pública, y protección de datos, entre otros. Asumirá la representación nacional en el Grupo de Cooperación y en la Red europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLONe), facilitando la cooperación en el ámbito de la Unión Europea.
- Régimen Sancionador: Se requerirá un informe preceptivo del Centro Nacional de Ciberseguridad para la imposición de sanciones en el caso de infracciones muy graves. El CNC también podrá instar a las autoridades de control a ejercer facultades de supervisión y ejecución respecto a cualquier entidad esencial

5.2.2.2 Autoridades de control

De acuerdo con el artículo 7 del APL, las autoridades de control (AC), son las siguientes:

- Ministerio de Defensa a través del Centro Criptológico Nacional, respecto a las entidades esenciales e importantes comprendidas en el ámbito de la Ley 40/2015, siempre que no sean críticas;
- Ministerio para la Transformación Digital y de la Función Pública, a través de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y de la Secretaría de Estado de Digitalización e Inteligencia Artificial, para las entidades esenciales e importantes de los sectores de infraestructura digital y proveedores de servicios digitales;
- Ministerio del Interior mediante la Oficina de Coordinación de Ciberseguridad sobre las entidades críticas y esenciales de los sectores no incluidos en los anteriores, además de las entidades esenciales e importantes del sector de la seguridad privada.

5.2.2.3 Puntos de contacto sectoriales

Son aquellos órganos ministeriales u organismos, o entidades de derecho público vinculadas o dependientes de la Administración General del Estado, designados específicamente para cada uno de los sectores relacionados en los Anexos I y II de la ley (sectores de alta criticidad y otros sectores). Su función principal es actuar como punto de contacto especializado con el Centro Nacional de Ciberseguridad y las autoridades de control.

Se mantienen los tres equipos de respuesta a incidentes de ciberseguridad (CSIRT) de referencia: CCN-CERT (para el Sector Público), INCIBE-CERT (para ciudadanos y sector privado no incluido en la Ley 40/2015), y ESPDEF-CERT (para la Defensa Nacional), todos ellos coordinados por el CNCíber.

5.2.3 Gestión de riesgos y notificación

El anteproyecto establece obligaciones específicas sobre la gestión del riesgo en materia de ciberseguridad y fija el mecanismo para la notificación de incidentes. Entre estas medidas, destacan las que se exponen a continuación.

5.2.3.1 Responsabilidad y medidas de control

Los órganos de gobierno y dirección de las entidades clasificadas como esenciales o importantes ostentan la responsabilidad última de implantar y supervisar las medidas de gestión del riesgo. Estas contramedidas deberán ser proporcionales al riesgo identificado y, como mínimo, desarrollar políticas de seguridad formales, procedimientos de gestión de incidentes, planes de continuidad operacional, controles sobre la seguridad de la cadena de suministro TIC y mecanismos de autenticación robusta (por ejemplo, implementación de MFA⁸ para el acceso a los sistemas), entre otras salvaguardas pertinentes.

5.2.3.2 Obligaciones de notificación de incidentes

Las entidades sujetas a la norma deberán comunicar, sin retrasos injustificados, cualquier incidente que tenga un impacto significativo en la prestación de sus servicios a la autoridad de control correspondiente, canalizando la comunicación a través del CSIRT nacional de referencia. El régimen de comunicación contempla plazos escalonados: una alerta inicial de carácter precoz en el plazo de veinticuatro (24) horas y una comunicación ampliada del incidente en un plazo máximo de setenta y dos (72) horas (con un umbral más restrictivo de 24 horas para los prestadores de servicios de confianza).

5.2.3.3 Plataforma centralizada de notificación y seguimiento

Con el fin de estandarizar, automatizar y facilitar el tramitado y el seguimiento de los incidentes, se prevé la puesta en marcha de un sistema de ventanilla única: la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes. Esta plataforma estará operada por CCN-CERT bajo la dirección y coordinación del Centro Nacional de Ciberseguridad.

5.2.3.4 Actuación ante indicios de ilícito penal

Cuando existan indicios de que un incidente reviste naturaleza presuntamente delictiva, se activarán procedimientos específicos de coordinación a través de la Oficina de Coordinación de Ciberseguridad (OCC), de la Secretaría de Estado de Seguridad, el Ministerio Fiscal y las Fuerzas y Cuerpos de Seguridad del Estado, con el fin de preservar evidencias, garantizar la investigación penal y articular la respuesta interinstitucional correspondiente.

5.2.4 Estructura del Anteproyecto de Ley

Todo lo descrito anteriormente se desarrolla en un texto compuesto por 50 artículos y 7 capítulos. A continuación, se enumeran los capítulos y su contenido:

⁸ Método de seguridad basado en la autenticación multifactorial para el acceso a un sistema, requiriendo al menos por 2 factores.

- Capítulo I: Disposiciones generales (Objeto, Definiciones, Ámbito de aplicación, Entidades esenciales e importantes).
- Capítulo II: Marco estratégico e institucional (Estrategia Nacional de Ciberseguridad, Centro Nacional de Ciberseguridad, CSIRT, Cooperación).
- Capítulo III: Medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación (Gobernanza, medidas de riesgo, Plataforma Nacional de Notificación).
- Capítulo IV: Registros de entidades de naturaleza transfronteriza (Registro de proveedores de servicios e infraestructuras digitales).
- Capítulo V: Intercambio de Información (Mecanismos voluntarios de intercambio de información).
- Capítulo VI: Supervisión y Ejecución (Aspectos generales de supervisión, medidas para entidades esenciales e importantes).
- Capítulo VII: Régimen sancionador (Sujetos responsables, Infracciones y Sanciones: leves, graves y muy graves).

Con este nuevo marco legal se pretende armonizar el nivel de ciberseguridad a nivel nacional y europeo, estableciendo un sistema robusto de prevención, detección y respuesta, con un claro énfasis en la coordinación institucional y la responsabilidad de los órganos de dirección.

5.3 Comparación del Anteproyecto de Ley de Coordinación y Gobernanza y el RDL

El Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad (APL), es el resultado de la transposición de la directiva UE 2022/2555, o NIS 2. Esta última se materializó en el Real Decreto-ley 12/2018, y su desarrollo reglamentario, con el Real Decreto 43/2021. La NIS 2, como ya se ha visto anteriormente, no solo ha sido una mera actualización normativa, sino que ha supuesto un cambio sustancial en muchos de los aspectos contemplados con la primera abordando una revisión integral y una ampliación significativa respecto a lo ya establecido. En consecuencia, el APL trae consigo una reforma importante en cuanto a organización, sujetos obligados, criterios y requisitos, etc.

A continuación, para tener una perspectiva más profunda de los cambios que supone este nuevo escenario se describen las principales novedades y diferencias entre el Anteproyecto y las dos normas previas, el RDL y el RD 43/2021.

5.3.1 Cambios en el Objeto y Ámbito de Aplicación (Expansión del alcance)

El Anteproyecto tiene como fin transponer la Directiva (UE) 2022/2555 (Directiva NIS 2), resolviendo las deficiencias identificadas en la aplicación de la Directiva NIS 1, particularmente en lo relativo a la prestación transfronteriza de servicios y la disparidad de medidas entre Estados miembros.

La diferencia más notoria reside en la forma en que se identifica a los sujetos obligados. Mientras que el RDL y RD 43/2021, se aplica a Operadores de Servicios Esenciales y a Proveedores de Servicios Digitales, y la identificación de aquellos se basa en los sectores estratégicos definidos en la Ley 8/2011 de Protección de Infraestructuras Críticas; el Anteproyecto introduce una clasificación uniforme de entidades en dos categorías: Entidades Esenciales y Entidades Importantes. Esta clasificación se basa en la criticidad de sus sectores (Anexos I y II), el tipo de servicio y, fundamentalmente, el tamaño (si son medianas o grandes empresas, con umbrales específicos de trabajadores, volumen de negocios o balance de cuentas).

Esta nueva estructura asegura una cobertura completa de sectores y servicios esenciales para las actividades sociales y económicas. Además, las entidades previamente identificadas como operadores de servicios esenciales (OSE), pasan a ser consideradas Entidades Esenciales a efectos de esta nueva ley.

5.3.2 Marco institucional y gobernanza

El marco institucional y de gobernanza de la ciberseguridad ha experimentado una transformación fundamental con el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, que deroga y sustituye el modelo previamente establecido por el RDL y su desarrollo reglamentario (Real Decreto 43/2021). El cambio más significativo es el paso de un modelo de coordinación a uno de dirección centralizada, la ampliación del ámbito de los sujetos obligados y el incremento de la responsabilidad de la alta dirección.

Bajo la normativa anterior, la coordinación superior recae en el Consejo de Seguridad Nacional (CSN) a través de su comité especializado en ciberseguridad, siendo responsable de establecer los mecanismos para coordinar a las autoridades competentes. El CSN, a través del Departamento de Seguridad Nacional (DSN), también ejerce las funciones de enlace como Punto de Contacto Único para la cooperación transfronteriza. Con la transposición de la NIS 2, se crea el Centro Nacional de Ciberseguridad (CNCíber), como la autoridad nacional competente única en materia de gobernanza de la ciberseguridad, y que aspira a terminar con la dispersión competencial al asumir la dirección, impulso y coordinación de todas las actividades previstas en la ley para garantizar un elevado nivel de ciberseguridad en España. El CNCíber centraliza las funciones esenciales de gobernanza y coordinación. Específicamente, ejerce como Autoridad nacional de gestión de crisis y el Punto de Contacto Único para la cooperación intersectorial y transfronteriza, asumiendo la superior dirección y coordinación de las Autoridades de Control, los Puntos de Contacto Sectoriales y los CSIRT nacionales de referencia.

A nivel de supervisión, el APL reemplaza el concepto de Autoridades Competentes con las Autoridades de Control (ACo), que son los órganos encargados de las funciones de supervisión y ejecución, operando bajo la superior dirección del CNCíber. Además, el nuevo marco incorpora la figura de los Puntos de Contacto Sectoriales, órganos designados para cada sector (Anexos I y II) cuya función principal es colaborar con el CNCíber y las ACo en la identificación de entidades, impulsar políticas de ciberseguridad y elaborar los perfiles específicos de cumplimiento de obligaciones.

En cuanto a los sujetos obligados, la diferencia más importante estriba en la responsabilidad directa sobre la gobernanza. Mientras que en el RDL la responsabilidad legal recae sobre la entidad (OSE o PSD), y la alta dirección se limita principalmente a aprobar las políticas de seguridad, el APL establece que los órganos de dirección de las Entidades Esenciales (EE) e Importantes (EI) serán responsables de aplicar las medidas para la gestión de riesgos de ciberseguridad, supervisar su implantación efectiva y asumir la responsabilidad por su incumplimiento. Este cambio eleva la ciberseguridad a una cuestión de gobernanza ejecutiva. Para las Entidades Esenciales, la ley es más estricta al requerir que las personas físicas representantes o la autoridad con competencia para tomar decisiones supervisen el cumplimiento de la norma, asumiendo responsabilidad si incumplen este deber. De hecho, los miembros de los órganos de dirección responderán solidariamente de las infracciones que las entidades cometan. Además, el APL impone a los miembros de los órganos de dirección la obligación de recibir formación adecuada de forma periódica para detectar riesgos y evaluar las prácticas de gestión de riesgos.

Finalmente, respecto a la figura del Responsable de la Seguridad de la Información (RSI), mientras que en el RDL, el RSI es la persona, unidad u órgano colegiado encargado de actuar como punto de contacto y coordinación técnica con la Autoridad Competente y el CSIRT, en el APL esta función se mantiene. Sin embargo, se introduce una novedad institucional significativa para las Entidades Esenciales a las que se exige que el RSI, su representante físico en caso de ser un órgano colegiado, y su sustituto, sean personal acreditado por el Ministerio del Interior, sin perjuicio de los requisitos de capacidad técnica y formación. El RSI sigue siendo responsable de elaborar las políticas, supervisar su aplicación y suscribir la declaración de aplicabilidad.

5.3.3 Medidas de Seguridad y Gestión de Riesgos

De acuerdo con el RDL y el RD 43/2021, los OSE están obligados a adoptar medidas técnicas y organizativas "adecuadas y proporcionadas" para gestionar los riesgos. Estas medidas deben tomar como

referencia el Esquema Nacional de Seguridad (ENS) y la formalización se hacía mediante una Declaración de Aplicabilidad de medidas de seguridad suscrita por el RSI y aprobada por la Dirección.

El APL mantiene la necesidad de medidas técnicas, operativas y de organización adecuadas y proporcionadas, pero las detalla exhaustivamente en once puntos obligatorios (Artículo 15.2). Estas medidas se basan en el ENS y normas técnicas europeas e internacionales equivalentes, garantizando un nivel adecuado de seguridad de las redes y sistemas de información.

Las principales novedades del APL aluden a:

- La seguridad de la cadena de suministro (incluyendo aspectos de seguridad relativos a las relaciones con proveedores y el punto de contacto de seguridad principal).
- La seguridad en la adquisición, el desarrollo y el mantenimiento de redes y sistemas de información, incluyendo la gestión y divulgación de vulnerabilidades.
- Las políticas para evaluar la eficacia de las medidas de gestión de riesgos.
- El uso de soluciones de autenticación multifactorial o de autenticación continua cuando proceda.

Mientras que el RDL permite a las autoridades competentes establecer obligaciones específicas para complementar las medidas generales, atendiendo a la complejidad de los sistemas, el APL formaliza y estructura este proceso. Permite a CNCíber aprobar perfiles específicos de cumplimiento de obligaciones. Estos perfiles se diseñan de manera incremental sobre las medidas generales de gestión de riesgos y tienen en cuenta factores como el grado de exposición al riesgo, el tamaño de la entidad y la especificidad del sector. Estos perfiles específicos deben considerar la seguridad de la cadena de suministro, las vulnerabilidades específicas de los proveedores directos y los resultados de las evaluaciones coordinadas de riesgos de seguridad a nivel europeo. Los Puntos de Contacto Sectoriales tienen la función específica de colaborar en la elaboración de estos perfiles.

Conforme el RDL, la acreditación del cumplimiento podía lograrse mediante la certificación en un esquema de seguridad reconocido por la autoridad competente, previa consulta al CSIRT de referencia.

El APL establece un requisito más riguroso y diferenciado para demostrar el cumplimiento:

- Las Entidades Esenciales (EE) deben demostrar el cumplimiento de sus obligaciones mediante la obtención y mantenimiento de una certificación de conformidad acreditativa.
- Las Entidades Importantes (EI) pueden optar entre obtener la mencionada certificación o realizar una autoevaluación de la postura de seguridad.

Además, el APL prevé que el Perfil de Cumplimiento Específico del ENS para las entidades esenciales e importantes acredite automáticamente el cumplimiento de las medidas de gestión de riesgos. Las entidades sujetas al Real Decreto 311/2022 (ENS) observarán lo dispuesto en dicho Real Decreto en materia de Certificación

5.3.4 Notificación y Gestión de Incidentes

En relación con este punto, el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad establece requisitos mucho más detallados y plazos más cortos y escalonados en comparación con el Real Decreto-ley 12/2018 y el Real Decreto 43/2021. El objetivo del APL es asegurar una respuesta rápida y coordinada a los incidentes significativos, de acuerdo con la Directiva NIS 2.

5.3.4.1 Criterios de notificación

En ambas normas se mantiene el enfoque de notificación de incidentes importantes, con el matiz del RDL, que habla de incidentes que tengan “efectos perturbadores significativos”. El APL, sin embargo, adopta la definición de la directiva que transpone (NIS 2) definiendo “incidente significativo” como aquel que: “i. ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas

económicas para la entidad afectada; ii. ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables”. [3]

Las principales diferencias en las obligaciones de notificación de incidentes entre el Real Decreto-ley 12/2018, su desarrollo reglamentario Real Decreto 43/2021, y el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad (APL) radican en la definición del suceso a notificar y en el estricto marco temporal y escalonado que impone el APL.

El RDL y su desarrollo en el RD 43/2021, obligan a los Operadores de Servicios Esenciales y a los Proveedores de Servicios Digitales, a notificar a la autoridad competente a través del CSIRT de referencia aquellos incidentes cuyos efectos perturbadores pudieran interrumpir el servicio esencial que prestaban. Para ello, se establecen criterios basándose en la peligrosidad o el impacto, debiéndose notificar los incidentes cuya peligrosidad o impacto fuera alto, muy alto o crítico, conforme a la Guía Nacional de Notificación y Gestión de Ciberincidentes que establece una categorización de estos criterios según la taxonomía del incidente.

El APL también señala la obligación de notificar cualquier incidente significativo que tenga repercusión en la operativa de las Entidades Esenciales o Importantes, y se mantienen los criterios de notificación de peligrosidad e impacto de su antecesora. Además, el APL introduce la obligación de notificar a los destinatarios de sus servicios si el incidente significativo es susceptible de causarles perjuicios de relevancia. Asimismo, exige que en las notificaciones se indique si el incidente puede presentar carácter ilícito e intencional. Lo que si se mantiene es la comunicación de aquellos incidentes que revistan caracteres delictivos al Ministerio Fiscal, a través de la Oficina de Coordinación de Ciberseguridad.

5.3.4.2 Plazos

El marco anterior establecía una obligación general para los OSE y PSD de notificar incidentes que pudieran tener efectos perturbadores significativos en los servicios. Además, se requiere una notificación inicial sin demora injustificada tan pronto como el OSE disponga de información para determinar las circunstancias para la notificación, y posteriormente, notificaciones intermedias para actualizar la información, más una final tras la resolución del incidente.

Los plazos exactos de las notificaciones intermedias y finales se recogen en la Instrucción Nacional de Notificación y Gestión de Ciberincidentes (Anexo del RD 43/2021), variando según el nivel de peligrosidad o impacto (Crítico, Muy Alto o Alto). Finalmente, la notificación inicial debe incluir información que permita determinar cualquier efecto transfronterizo.

El APL establece unos tiempos más estrictos y con varias fases para la notificación de incidentes significativos, aplicando estas obligaciones tanto a las Entidades Esenciales (EE) como a las Entidades Importantes (EI), con el objetivo de obtener información crítica casi de inmediato para la coordinación nacional e internacional. La entidad debe enviar una alerta temprana sin demora indebida y, en cualquier caso, en el plazo de 24 horas. También, ha de indicar si el incidente puede responder a una acción ilícita o malintencionada, o si puede tener repercusiones transfronterizas.

La notificación, que incluye una evaluación inicial (peligrosidad e impacto) y los indicadores de compromiso disponibles, debe remitirse en un plazo máximo de 72 horas. Este plazo se reduce a 24 horas para los prestadores de servicios de confianza si el incidente afecta a la prestación de sus servicios. Por último, la entidad ha de presentar un informe final detallado en un mes como máximo.

Estas notificaciones se realizarán a través de cada CSIRT de referencia utilizando la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (PNNSC), como medio preferente, adaptada y gestionada por el CCN-CERT bajo la dirección del nuevo CNCíber.

5.3.5 Inclusión de la Seguridad en la Cadena de Suministro y Registros Transfronterizos

La inclusión de la Seguridad en la Cadena de Suministro y la obligación de mantener Registros de entidades de naturaleza transfronteriza marcan una expansión regulatoria clave en el Anteproyecto de Ley (APL) en comparación con el RDL y su desarrollo reglamentario (RD 43/2021).

Mientras que el marco anterior requería que los Operadores de Servicios Esenciales (OSE) incluyeran la gestión de riesgos de terceros o proveedores como parte de sus políticas de seguridad internas, el APL lo convierte en un requisito de gestión de riesgos explícito, obligatorio y de mayor alcance para las Entidades Esenciales (EE) e Importantes.

La nueva normativa exige la implementación de medidas específicas para la seguridad de la cadena de suministro de productos y servicios de Tecnologías de la Información y la Comunicación (TIC), incluyendo los aspectos de seguridad relativos a las relaciones con sus proveedores o prestadores de servicios directos. Además, la Estrategia Nacional de Ciberseguridad debe adoptar políticas específicas sobre la ciberseguridad en esta cadena de suministro. Por su parte, el Responsable de la Seguridad de la Información (RSI) tiene ahora la función específica de velar por el cumplimiento de los criterios de seguridad de la información por parte de empresas externas y proveedores.

El RDL, aunque reconocía el carácter transnacional de los servicios digitales, solo exigía a los Proveedores de Servicios Digitales (PSD) que comunicaran su actividad a la autoridad competente a meros efectos de conocimiento. El APL formaliza los Registros de entidades de naturaleza transfronteriza para obtener una visión completa de las entidades que operan en la Unión Europea. El CNCíber es el encargado de elaborar y mantener un registro de proveedores de servicios e infraestructuras digitales. Esta obligación recae en una lista ampliada de entidades, como proveedores de servicios de DNS, registros de nombres de dominio de primer nivel, proveedores de servicios de computación en nube, y proveedores de servicios gestionados. La información recabada debe incluir no solo datos de contacto y sector, sino también la dirección del establecimiento principal en la Unión y los Estados miembros en los que prestan servicios.

Además, CNCíber debe remitir esta información a la ENISA para su inclusión en el registro europeo de entidades. Se impone también la obligación para los registros de nombres de dominio de primer nivel de recopilar y mantener datos precisos y completos en una base de datos específica para garantizar la seguridad y resiliencia del DNS, debiendo conceder acceso a solicitantes legítimos en un plazo de setenta y dos horas.

5.3.6 Supervisión y régimen sancionador

El régimen sancionador experimenta una transformación radical en el Anteproyecto de Ley, que transpone la Directiva NIS 2, frente al marco anterior del RDL. Los cambios más relevantes se centran en la cuantía de las multas, la responsabilidad directa de los órganos de dirección y la competencia sancionadora.

A continuación, se detalla la comparativa del régimen sancionador, basado en los Capítulos VII del APL y Título VII del RDL.

5.3.6.1 Sujetos responsables y responsabilidad de la Dirección

El RDL establece que la responsabilidad de las sanciones recae sobre los OSE y los PSD (es decir, la entidad jurídica) comprendidos en su ámbito de aplicación. En el caso del APL son las entidades esenciales e importantes las responsables directas de las infracciones. Sin embargo, en este caso introduce una novedad fundamental en la gobernanza y responsabilidad, ya que los miembros de los órganos de dirección de las entidades responderán solidariamente de las infracciones que estas cometan y, además, tipifica como infracción grave el incumplimiento de la obligación, por parte de las personas físicas con facultades de representación o toma de decisiones en las EE, de supervisar el cumplimiento de la norma y asumir la responsabilidad del incumplimiento de sus obligaciones.

5.3.6.2 Clasificación de infracciones

Ambas normas tipifican las infracciones en: Leves, Graves y Muy Graves. Sin embargo, el Anteproyecto detalla infracciones mucho más específicas y vinculadas al nuevo modelo de gestión de riesgos y gobernanza:

- Muy Graves: Se centran en el incumplimiento de la implantación de medidas de gestión de riesgos determinadas por CNCíber, cuando esta falta haya motivado un incidente significativo; la reiteración del incumplimiento en la obligación de notificar incidentes significativos (a partir del segundo); la falta de adopción de medidas para resolver un incidente significativo; o el incumplimiento reiterado en el suministro de información requerida por la autoridad de control.
- Graves: Incluyen la falta o la demora injustificada en la implantación de las medidas de gestión de riesgos; el incumplimiento de la obligación de notificar incidentes significativos (no reiterado); el incumplimiento de la obligación de designar al Responsable de la Seguridad de la Información, o que este carezca de la acreditación exigida; o el incumplimiento del deber de supervisión de los órganos de dirección.
- Leves: Incluyen la remisión de información incompleta, inexacta o con dilación indebida; la falta de cumplimiento de las obligaciones de formación a empleados y órganos de dirección; o el cumplimiento de la obligación de notificar incidentes significativos sin recoger la información completa que deben reunir los informe.

5.3.6.3 Sanciones pecuniarias

El APL aumenta significativamente las cuantías máximas de las sanciones, especialmente para las infracciones muy graves cometidas por Entidades Esenciales, adoptando el criterio del volumen de negocios mundial tal como exige la Directiva NIS 2.

La diferencia más destacable en el régimen sancionador reside en la cuantía económica de las multas para las infracciones muy graves, y en la responsabilidad directa de los órganos de dirección.

En el RDL, la multa máxima por una infracción muy grave se fija en 1.000.000 euros, mientras que el APL eleva sustancialmente este límite e introduce un criterio basado en el volumen de negocio mundial:

1. Para las infracciones muy graves cometidas por Entidades Esenciales, la multa puede ascender a 10.000.000 euros o el 2% del volumen de negocios anual total mundial, eligiéndose la cuantía mayor.
2. Para las Entidades Importantes, la multa máxima es de 7.000.000 euros o el 1,4% del volumen de negocios anual total mundial.

A nivel de responsabilidad, el cambio más significativo es que el APL establece que los miembros de los órganos de dirección responderán solidariamente de las infracciones que cometan las entidades, algo que no se contempla en el RDL. Incluso, el incumplimiento de su deber de supervisión es tipificado como infracción grave.

Finalmente, en cuanto a la competencia sancionadora, el APL introduce la obligatoriedad de que la imposición de sanciones por infracciones muy graves por parte del Ministerio competente requiera el informe preceptivo del Centro Nacional de Ciberseguridad (CNCíber), lo que centraliza la decisión en el nuevo modelo de gobernanza.

Además, en el RDL, las sanciones firmes por infracciones muy graves y graves pueden llevar aparejada la sanción accesoria de publicación en el Boletín Oficial del Estado (BOE). El APL mantiene esta previsión como sanción accesoria de amonestación pública en BOE.

Finalmente, tanto el RDL como el APL establecen que las infracciones cometidas por órganos o entidades del Sector Público no serán objeto de sanción pecuniaria. En su lugar, el órgano sancionador

dictará una resolución que acuerde las medidas oportunas para que cesen y se corrijan los efectos de la infracción, y podrá proponer la iniciación de actuaciones disciplinarias si procedieran.

5.3.6.4 Competencia Sancionadora

El APL clarifica y centraliza la competencia sancionadora en el nivel superior, involucrando a CNCíber de forma preceptiva. En el RDL, la imposición de sanciones por infracciones muy graves corresponde al Ministro competente en virtud del Artículo 9 (Autoridades Competentes). Las sanciones graves y leves se impondrán por el órgano de la autoridad competente.

El APL dispone que, para las infracciones Muy Graves, la competencia corresponde al titular del Ministerio de Defensa, Transformación Digital y de la Función Pública o Interior, respecto de las entidades incluidas en el ámbito de competencia de las autoridades de control dependientes de los mismos. En este caso es necesario un informe preceptivo del Centro Nacional de Ciberseguridad. Para las infracciones Graves y Leves, la competencia recae en las Autoridades de Control designadas en el Artículo 7.1 respecto de las entidades incluidas en su respectivo ámbito de competencia.

6 MARCOS DE NOTIFICACIÓN DE INCIDENTES

6.1 Guía Nacional de Notificación y Gestión de Ciberincidentes

La GNNGC, fue publicada y aprobada por el Consejo Nacional de Ciberseguridad, el 21 de febrero de 2020. La Guía, vigente en la actualidad, sirve como referencia a nivel nacional en materia de notificación de incidentes de ciberseguridad en el marco de los operadores de servicios esenciales y proveedores de servicios digitales, conforme a lo establecido en el RDL y el RD 43/2021 en cuyo anexo se incluye. En ella se determina el qué, el cómo, a quién y cuándo se debía notificar los incidentes de ciberseguridad a la autoridad competente a través de los CSIRT de referencia conforme a una taxonomía consensuada y alineada con ENISA.

La GNNGC, basa su clasificación en la evaluación del riesgo derivado del incidente en función de una taxonomía bajo los criterios de peligrosidad (cuán grave es el ciberataque en términos técnicos y de complejidad), y el de impacto (la afectación real al servicio esencial, o a los datos). El objetivo de esta taxonomía, alineada con las directrices de la Agencia de la Unión Europea para la Ciberseguridad, es garantizar que solo los incidentes con potencial de afectar significativamente a la seguridad nacional o a la economía sean objeto de notificación obligatoria.

Como se establece en el RDL y su desarrollo reglamentario, la notificación de un Ciberincidente es obligatoria para todos aquellos sujetos a los que les sea aplicable normativa específica (como las Infraestructuras Críticas y el Sector Público) cuando el incidente se categorice con un nivel de peligrosidad o impacto de CRÍTICO, MUY ALTO o ALTO, sin perjuicio de aquellos que sin cumplir con esos parámetros se consideren relevantes. Estos sujetos obligados deben comunicar estos incidentes en tiempo y forma conforme se establece en la Guía a la autoridad competente, a través del CSIRT nacional de referencia, dentro de los plazos determinados en la propia Guía. [37]

A continuación, se detallan todos estos aspectos, que además serán objeto de análisis respecto a otros marcos, como el APL y la Guía de Notificación belga.

6.1.1 Estructura de la GNNGC

La Guía se estructura en 8 puntos o capítulos y 5 anexos. A continuación, se enumeran sus epígrafes y se abordarán algunos de ellos:

1. Introducción.
2. Objeto.
3. Alcance.

4. Ventanilla única de notificación.
5. Clasificación y taxonomía.
6. Criterios de notificación de incidentes.
7. Fases para la gestión de incidentes de ciberseguridad.
8. Métricas e indicadores.

Anexo 1: Notificación en el ámbito de Protección de Infraestructuras Críticas (PIC).

Anexo 2: Notificación en el ámbito del Sector Público.

Anexo 3: Notificación en el ámbito del Sector Privado.

Anexo 4: Marco Regulador (leyes aplicables).

Anexo 5: Glosario de Términos.

6.1.2 Sujetos Obligados y Autoridades Competentes

Esta subsección identifica con precisión a quién aplica la GNNGC y quiénes son los actores que reciben la notificación y coordinan la respuesta bajo el RDL.

- Operadores de Servicios Esenciales: Son aquellas entidades nombradas como tal, que prestan servicios críticos para la sociedad en aquellos sectores definidos (12 sectores según el RDL).
- Proveedores de Servicios Digitales: Se refiere a aquellas entidades que ofrecen servicios de computación en la nube (*cloud computing*), motores de búsqueda en línea o servicios de mercados *online*.

6.1.3 Autoridades y CSIRT de Referencia

La GNNGC establece una arquitectura de coordinación clara y definida, donde la notificación y gestión recae en los CSIRT de referencia y sus respectivas Autoridades Competentes (AC).

- Autoridades Competentes: Son aquellos organismos que deben ser informados a través de los CSIRT de referencia para su ámbito competencial:
 - CNPIC⁹ (Centro Nacional de Protección de Infraestructuras y Ciberseguridad), de la Secretaría de Estado de Seguridad, es la autoridad competente para los OSE y Operadores Críticos, a través de la Oficina de Coordinación Cibernética. Además, se encarga de coordinar información con las Fuerzas y Cuerpos de Seguridad del Estado, en caso de que un incidente constituya un delito.
 - CCN (Centro Criptológico Nacional), del Ministerio de Defensa, actúa como autoridad competente de OSE (no críticos) y PSD del Sector Público comprendido en la Ley 40/2015.
 - Secretaría de Estado de Digitalización e Inteligencia Artificial, como la autoridad competente para los Proveedores de Servicios Digitales.
- Centro Criptológico Nacional (CCN-CERT): Es el CSIRT de referencia para el sector público dando cobertura a los OSE de su ámbito de actuación.
- Instituto Nacional de Ciberseguridad (INCIBE-CERT): INCIBE es el CSIRT de referencia respecto a los OSE y PSD del sector privado.

⁹ En la actualidad, la OCC ya no se encuentra incardinada dentro del CNPIC, asumiendo la competencia en materia ciber de los operadores críticos. Asimismo, su denominación también ha cambiado pasándose a llamar: Oficina de Coordinación de Ciberseguridad (en lugar de Cibernética), así como CNPIC que cambia la C de “Ciberseguridad” por la de “Críticas”.

- Mando Conjunto de Ciberdefensa¹⁰ (ESP-DEF-CERT): u ámbito competencial son las redes y sistemas de las Fuerzas Armadas y aquellas que afecten a la Defensa Nacional. Cooperar con los otros CSIRT cuando los incidentes afectan a operadores con incidencia en la Defensa Nacional.

6.1.4 Criterios de Clasificación y Umbrales de Peligrosidad e Impacto

La GNNGC determina la obligatoriedad de la notificación de un Ciberincidente mediante la aplicación de criterios de clasificación basados en la evaluación de Peligrosidad e Impacto, alineados con las metodologías de ENISA.

6.1.4.1 Peligrosidad e impacto

La clasificación se realiza utilizando una matriz que combina dos variables clave:

1. Peligrosidad (Amenaza): Se refiere a la naturaleza del incidente y el nivel de sofisticación del atacante (ej. Ataque dirigido vs. *malware* indiscriminado).
2. Impacto (Consecuencia): Se refiere a las consecuencias directas del incidente sobre el servicio esencial o digital (ej. Duración de la interrupción, número de usuarios afectados, pérdida de datos).

Además, para cada uno de estos el documento distingue los siguientes niveles:

- Peligrosidad: Bajo, Medio, Alto, Muy Alto o Crítico;
- Impacto: Sin Impacto, Bajo, Medio, Alto, Muy Alto o Crítico.

6.1.4.2 Umbrales de Notificación Obligatoria

Un incidente debe ser notificado cuando se considere ALTO, MUY ALTO o CRÍTICO en función su peligrosidad o impacto de acuerdo con las tablas de la Guía. (Tablas 4 y 5). Estos niveles se evalúan mediante parámetros cuantitativos y cualitativos específicos para cada sector, como la duración de la interrupción, el número de usuarios afectados o el alcance geográfico de la incidencia.

Cabe significar que, en cuanto a la peligrosidad, de acuerdo con la GNNGC, solo las Amenazas Avanzadas Persistentes (APT, por sus siglas en inglés), se consideran incidentes CRÍTICOS. En estos casos se requiere una comunicación inmediata y coordinada al más alto nivel. Asimismo, la GNNGC considera incidentes de peligrosidad ALTA por ejemplo un ataque DDoS (del inglés, denegación de servicios distribuida), o un *phishing*, entre otros. Por otro lado, MUY ALTO, distribución de *malware*, sabotaje o intrusión.

En el caso del Impacto, se tienen en cuenta las consecuencias del incidente como factores sobre la afectación a la seguridad nacional o pública, a infraestructuras críticas, pérdidas financieras, extensión geográfica, tipos de clasificación de los sistemas (Secreto o Reservado), daños reputacionales, recursos empleados para mitigar el incidente o impacto económico en relación con el Producto Interior Bruto (P.I.B.), y otras que suponen una afectación al normal funcionamiento de la sociedad. Esos parámetros se contemplan en la tabla 5 del documento.

6.1.5 Procedimiento y Plazos de Notificación

Como se ha explicado en el punto anterior, la GNNGC define los incidentes a notificar de forma obligatoria, pero también determina qué, cuándo y cómo realizar estas comunicaciones.

En cuanto a qué se debe notificar, la Tabla 6 de la Guía sirve de orientación para la comunicación inicial, donde se incluyen campos como el sector afectado, las fechas y horas de conocimiento del suceso y de detección de este, si han sido en diferentes momentos. También se solicita información técnica, como recursos y activos afectados (IP, aplicaciones, etc.), los niveles de peligrosidad e impacto (si se conocen), así como la clasificación según la taxonomía de la Guía, si afecta o puede afectar a otras

¹⁰ Actualmente Mando Conjunto del Ciberespacio (MCCE).

regiones o, incluso a otros Estados miembros, si aplica a otras regulaciones (Protección de datos, PIC, ENS, etc.) y si requiere actuación de las FCSE, entre otros.

En relación con el “Cuándo”, se identifican tres hitos o fases principales, especialmente para los incidentes obligados a notificar, sin perjuicio de aquellas notificaciones que se consideren oportunas.

- Comunicación Inicial: Esta debe realizarse sin retrasos injustificados desde que se tenga conocimiento del incidente. Además, debe incluir toda la información conocida, sin que ello suponga demora alguna.
- Comunicación Intermedia: Se utiliza para actualizar la información sobre el incidente mientras este se encuentra en fase de contención o erradicación y el plazo de notificación para los incidentes categorizados como Críticos es de 24 ó 48 horas, y de 72 horas para los clasificados como MUY ALTO.
- Comunicación Final: Debe realizarse una vez que el incidente ha sido resuelto y los sistemas han sido restaurados y no más tarde de los 20 días para los CRÍTICOS y de 40 para los considerados MUY ALTO, desde la notificación inicial. Véase tabla 2 de umbrales de notificación.

	INICIAL	INTERMEDIA	FINAL
ALTO	Sin demora	-	-
MUY ALTO	Sin demora	72 horas	≤ 40 días
CRÍTICO	Sin demora	24/48 horas	≤ 20 días

Tabla 2 Umbrales de notificación de la GNNGC. Elaboración propia

En cuanto al proceso de cierre de un incidente, la Guía establece diferentes hitos para cada nivel de peligrosidad o impacto, siendo los siguientes expresados en días naturales, como se representa en la tabla 3.

BAJO.	21
MEDIO:	30
ALTO:	45
MUY ALTO:	90
CRÍTICO:	120

Tabla 3 Plazos de cierre de incidentes. Elaboración propia

6.1.6 Ventanilla Única

El RDL menciona la creación de una plataforma común para la notificación de incidentes de ciberseguridad. Por otro lado, la GNNGC, hace referencia a la Ventanilla Única de Notificación en el capítulo 4, presentando el flujograma de la metodología empleada. Véase figura 5.



Figura 5 Flujograma de la Ventanilla Única de Notificación. Fuente: GNNGC

La propia GNNGC indica que cada CSIRT registrará los incidentes comunicados a él dentro de su ámbito competencial con un identificador único. Asimismo, establece que estos equipos de respuesta podrán interactuar con el sujeto obligado por las vías que consideren oportunas durante toda la vida del incidente, sin embargo, siempre se considerará válido el correo electrónico como medio de comunicación.

La Guía especifica las siguientes autoridades competentes dentro de su ámbito de actuación.

- ESP-DEF-CERT: si tiene que ver con la Defensa Nacional;
- CNPIC: si afecta a la Ley PIC 8/2011;
- AEPD (Agencia Española de Protección de Datos): si afecta al Reglamento General de Protección de Datos;
- CCN-CERT: si afecta a las Administraciones Públicas sometidas al ENS y es obligatoria su notificación en función de los criterios de peligrosidad.

Si el evento tiene que ver con los incidentes de obligada notificación según el RDL, se hará, a través de los CSIRT de referencia a las Autoridades Nacionales competentes.

Por otro lado, el RDL propone una plataforma común para automatizar los procesos entre los CSIRT de referencia y las autoridades competentes. El RD 43/2021, además, establece el desarrollo y uso de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (PNNSC)¹¹, como mecanismo de intercambio de información entre todos los interesados, CSIRT de referencia, autoridades competentes, OSE y PSD. A día de la fecha se encuentra operativo el portal web de la PNNSC donde se establecen los medios de notificación, aunque no está operando como mecanismo de intercambio de información, ni automatiza procesos. Véase figura 6.

¹¹ <https://www.plataformanacionalciber.gob.es/index.php/incidentes?view=incidents>



Figura 6 Portal web principal de la PNNSC. Fuente web: PNNSC

La PNNSC ofrece un desplegable con varias opciones en función del sector afectado. Por un lado, para el sector público se debe seleccionar el CCN-CERT, competente en esta materia como se vio anteriormente. Una vez seleccionado, se muestra la web de notificación de incidentes. Ver figura 7.



Figura 7 Página de notificación incidentes del sector público. Fuente: PNNSC¹²

En esta sección se indican las alternativas para notificar aquellos incidentes del sector público, a saber:

- LUCIA: herramienta de gestión de incidentes del CCN-CERT, mediante instancia federada, por lo que no es accesible si no está desplegada en la entidad que desee notificar un evento.
- Correo electrónico: incidentes@ccn-cert.cni.es, describiendo lo ocurrido e indicando un punto de contacto, todo ello cifrado y firmado.

Por otro lado, si se desea notificar un incidente acaecido en el sector privado, cuyo ámbito competencial pertenece al INCIBE-CERT, la web de la PNNSC ofrece información sobre las vías de contacto para reportar un incidente, entre otros, varias cuentas de correos electrónicos en función del

¹² <https://www.plataformanacionalciber.gob.es/index.php/notificacion-de-incidentes>

sector (ciudadanos, empresas, operadores de servicios esenciales e infraestructuras críticas y proveedores de servicios digitales), y un formulario, que al hacer clic, redirige a su sitio web.¹³

Por último, al seleccionar la opción de la notificación de un incidente en el ámbito de la defensa nacional, el portal de la PNNSC, redirige a la sección del ESP-DEF-CERT, donde se muestran sus vías de contacto, su web y la clave de cifrado pública (PGP).

6.2 Framework de Notificación Belga

Bélgica, a través de su Centro de Ciberseguridad Belga (CCB), como autoridad nacional en materia de ciberseguridad, ha publicado su “Guía de Notificación NIS 2”, que en el momento de la elaboración de este trabajo se encuentra en la versión 10.2024 – 1.2. Esta guía sirve de referencia en cuanto a la notificación de Ciberincidentes conforme a la NIS 2, por lo que se encuentra alineada con el actual marco europeo. [37]

En este apartado se va a analizar la Guía de Bélgica como modelo de notificación conforme a la NIS 2, que servirá, además, para compararla con la actual GNNGC y proponer los cambios necesarios para su adaptación al nuevo marco normativo.

6.2.1 Estructura

El documento se estructura en cuatro puntos principales y tres anexos:

1. Notificaciones obligatorias
2. Notificaciones voluntarias
3. Normas de confidencialidad sobre las notificaciones
4. Qué ocurre si un incidente está relacionado también con datos personales
 - Anexo 1: Tabla resumen de incidentes significativos
 - Anexo 2: Explicación del formulario de notificación
 - Anexo 3: Resumen de las normas de la Comisión

6.2.2 Notificaciones Obligatorias y Voluntarias

Siendo este el motivo principal de la Guía, la Notificación de Ciberincidentes, la Guía belga ha diferenciado aquellas obligatorias de las voluntarias. Si bien, las comunicaciones obligatorias son para ciertos eventos y entidades de acuerdo con la NIS 2, las voluntarias son para el resto de los incidentes no significativos por parte de las entidades recogidas en la NIS 2 y las no recogidas, con la posibilidad de diferente prioridad en su tratamiento.

6.2.2.1 Qué debe notificarse

En primer lugar, se determina qué se debe notificar según la NIS 2:

- Incidentes significativos
- Ciberamenazas
- Cuasincidentes

El documento establece cómo determinar si un incidente es, o no, significativo. Esto es si, el incidente de acuerdo con la definición de incidente significativo tiene o puede tener impacto sobre las redes y sistemas de la información que soportan uno o más servicios que proveen a los sectores o

¹³ <https://www.incibe.es/incibe-cert/incidentes/notificaciones>

subsectores de los anexos. Además, el para que se considere significativo debe cumplir una serie de requisitos:

- Que afecte a la operación del servicio o servicios de los sectores de los anexos;
- Que produzca pérdidas económicas importantes a la entidad afectada (que exceda de 250.000€ o el 5% de la facturación anual, lo que sea menor);
- Que cause o pueda causar un daño considerable material, físico o moral sobre las personas, física o jurídicas.
- Que, no siendo significativos individualmente, lo puedan ser de forma conjunta respecto a las pérdidas económicas y haya ocurrido al menos dos veces en seis meses.

En cuanto a las pérdidas económicas, la Guía matiza que para determinar estas se deben tomar en cuenta todas pérdidas consecuencia del incidente, tales como los costes de sustitución del software, hardware o infraestructura. Los costes de personal empleado para la recuperación; las multas derivadas del incumplimiento de contratos u obligaciones; las compensaciones a los clientes; los asociados a la comunicación tanto interna como externa; los gastos de consultoría; los implicados en gastos de recuperación y otros. Si bien, no se toman en cuenta los de la operación de negocio habitual.

6.2.2.2 *Quién tiene que Notificar un Incidente*

Sobre quiénes están obligadas a notificar esos incidentes, la uía simplemente se ciñe a la norma y se refiere a las entidades relevantes de los sectores de los Anexos de la NIS 2.

6.2.2.3 *Cuándo es Obligatorio Notificar un Incidente*

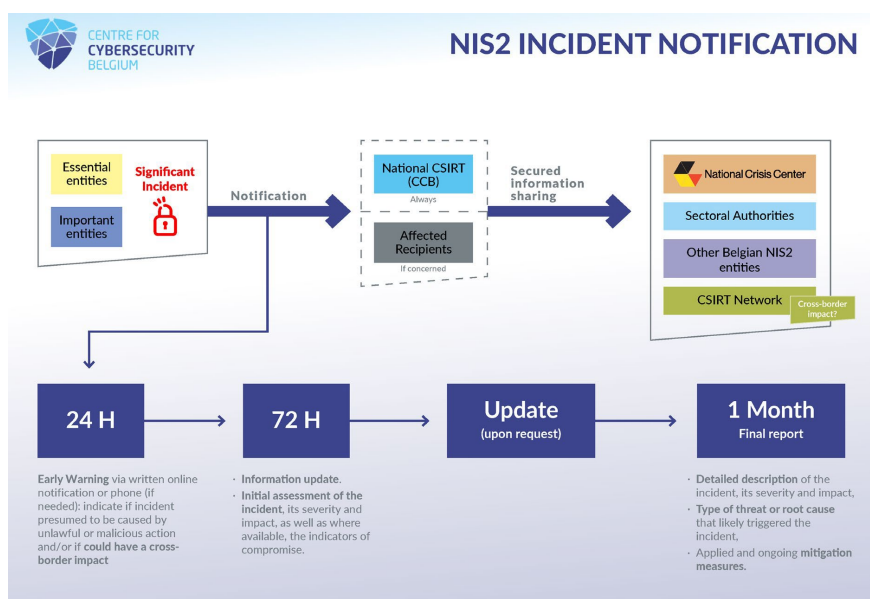
Para determinar cuándo reportar los incidentes se toma desde el conocimiento del incidente significativo. Desde el momento que se haya detectado un evento sospechoso o se tenga constancia de un potencial incidente comunicado por un tercero, la entidad debe realizar las medidas de comprobación necesarias para determinar si constituye un incidente y, de ser así, de qué tipo y su gravedad. Tan pronto como la entidad haya evaluado los aspectos anteriores y teniendo un grado razonable de certeza de que se trata de un incidente significativo, debe notificarlo a su CSIRT nacional (al CCB).

La Guía establece notificaciones obligatorias y unos umbrales asociados como se representan en la siguiente tabla.

Alerta Temprana	Sin demora indebida, dentro de las 24 horas desde el conocimiento del incidente.
Notificación del Incidente	Sin demora indebida pero dentro de las 72 horas en cualquier evento antes de llegar a ser significativo.
Informe Intermedio	En cualquier momento a petición del CSIRT nacional, o autoridad sectorial.
Informe final	Un mes después de la notificación inicial.
Informe de situación	Si después del plazo de un mes, no se ha dado por resuelto el incidente.

Tabla 4 Tipos de notificación y sus plazos. Elaboración propia

En el documento se incluye un flujograma de notificación con los plazos y tipos de reporte en cada fase del incidente (Figura 8).

**Figura 8 Flujograma de notificación de incidentes según el CCB. [37]**

La alerta temprana tiene por objeto informar al CSIRT sobre un incidente potencialmente derivado de acciones ilícitas o maliciosas o con posible impacto transfronterizo dentro de la Unión Europea. Su contenido debe limitarse a la información imprescindible para poner el incidente en conocimiento del CSIRT y, en su caso, solicitar apoyo, sin comprometer los recursos necesarios para la gestión operativa del incidente, que debe prevalecer.

La notificación del incidente permite ampliar y actualizar la información inicialmente comunicada, añadiendo una valoración preliminar de la gravedad y el impacto, así como indicadores de compromiso (IOC) cuando estén disponibles. Al igual que la alerta temprana, este proceso no debe interferir con las labores de respuesta.

El informe intermedio se limita a recoger las actualizaciones relevantes sobre la evolución del incidente.

El informe final debe ofrecer una visión completa y estructurada, incluyendo la descripción detallada del incidente, su impacto y severidad, el tipo de amenaza o causa raíz, las medidas de mitigación aplicadas o en curso, y, en su caso, los efectos transfronterizos.

Por último, el informe de progreso, cuando proceda, recogerá toda la información disponible en ese momento que deba formar parte del informe final, sin perjuicio de su posterior ampliación.

El documento aclara el sentido de “sin demora indebida”, expresión literal extraída de la directiva NIS 2, exigiendo a las entidades obligadas a notificar el incidente tan pronto como sea posible, sin agotar los plazos máximos establecidos para su comunicación.

Asimismo, en el supuesto de que un incidente significativo pueda comprometer la continuidad o calidad de los servicios incluidos en los anexos de la norma, la organización deberá notificarlo con carácter inmediato a los usuarios o clientes afectados, siempre que sea posible su identificación. Dicha obligación informativa podrá satisfacerse utilizando cualquier canal de comunicación disponible, tales como el portal corporativo, envíos masivos de correo, avisos a través de aplicaciones, o comunicaciones en soporte físico.

Del mismo modo, la entidad sujeta a NIS 2 estará obligada a informar sin demora a los destinatarios de sus servicios que puedan verse impactados por una Ciberamenaza significativa, conforme a la definición prevista en el marco voluntario aplicable. La Agencia belga se guarda el derecho de compartir la información recibida con otras autoridades.

6.2.2.4 *Cómo notificar un incidente*

La Guía remite un enlace a un formulario *web*¹⁴ para reportar la información en cualquier fase de la gestión del incidente siempre que sea posible técnicamente. No obstante, el Anexo 2 de este documento, se incluye el contenido del formulario explicado. Además, ofrece un teléfono de emergencia como contacto adicional con el CSIRT de referencia. (Ver figura 9)

NL FR DE EN

Other information and services of the government: www.belgium.be

CENTRE FOR CYBERSECURITY BELGIUM

To ensure we handle your incident in the most effective way, please provide all necessary details. If you're uncertain, kindly check with the responsible person within your organization. This will help us conduct a thorough analysis and deliver the best possible solution.

Concerning:

- Select -

- Select -

Citizen

Organisation

A supplier to the Ministry of Defence

NIS2 Entity

Figura 9 Formulario de notificación del CCB. Fuente: CCB

Dentro del recurso web, se muestra un desplegable como se puede ver en la imagen anterior, donde se selecciona el tipo de notificante, ofreciendo las opciones de: ciudadano, organización, proveedor del Ministerio de Defensa o entidad NIS 2. En función de esta selección, en el formulario se mostrarán unos campos a cumplimentar u otros, como se ve a continuación (Figura 10), entre ellos algunos son obligatorios, como se muestran en la Figura 10.

¹⁴ <https://notif.safeonweb.be/>

Figura 10 Comparación de datos del formulario de notificación. Fuente: CCB

Adicionalmente, y al objeto de facilitar estos reportes, la plataforma permite hacerlo sin tener que autenticarse. En función del comunicante se habilitan distintos campos a cumplimentar y, a su vez, dentro de cada opción se solicita información obligatoria y voluntaria.

Tras cumplimentar todos estos campos, la plataforma exige comprobar que se trata de una interacción humana y permite después imprimir, o guardar, una copia del reporte.

6.2.2.5 Notificaciones Voluntarias

Cuando se trata de incidentes no significativos, ciberamenazas y cuasiincidentes, las entidades esenciales e importantes pueden reportarlos igualmente. También aquellas entidades que no están sujetas a NIS 2 pueden notificar incidentes significativos, ciberamenazas y cuasiincidentes. Estas notificaciones se tratarán de la misma manera que las obligatorias, sin embargo, estas podrían priorizarse.

Además, las notificaciones voluntarias no implican directamente acciones de inspección sobre la entidad, ni obligaciones adicionales como sí podría ocurrir con las obligatorias.

6.2.2.6 Régimen de confidencialidad aplicable a la información notificada

La entidad sujeta a NIS 2, junto con sus proveedores, debe garantizar que el acceso a la información relacionada con incidentes (en los términos definidos por la normativa) quede limitado exclusivamente al personal que, por razón de sus funciones o responsabilidades, deba conocerla y utilizarla para el cumplimiento de sus obligaciones. Este principio es igualmente exigible al CCB en su condición de CSIRT nacional, al Centro Nacional de Crisis (NCCN) y a las autoridades sectoriales competentes.

Las notificaciones recibidas son remitidas de manera inmediata por el CSIRT nacional a las autoridades sectoriales correspondientes y, cuando procedan de entidades esenciales, también al NCCN.

La información comunicada por una entidad NIS 2 al CCB, al NCCN o a la autoridad sectorial podrá ser objeto de intercambio en formato anonimizado con autoridades de otros Estados miembros de la Unión Europea o con otras autoridades nacionales, siempre que dicho intercambio resulte necesario para la aplicación de la normativa vigente.

En todo caso, la transmisión de información se circunscribe a los datos estrictamente necesarios y proporcionados a la finalidad perseguida, respetando el Reglamento (UE) 2016/679 (RGPD), así como los requisitos de confidencialidad, seguridad y protección de los intereses comerciales de las entidades afectadas.

6.2.2.7 *Qué ocurre si un incidente implica a datos personales*

La notificación de incidentes bajo la NIS 2 no reemplaza en ningún caso la comunicación a la Autoridad de Protección de Datos, siendo ambas independientes.

Por otro lado, existe una estrecha colaboración entre la autoridad nacional de ciberseguridad y la de protección de datos. Esta colaboración podría conllevar el desarrollo de herramientas comunes.

6.2.2.8 *Anexos*

Al final del documento se incluyen 3 anexos. El Anexo 1 se trata de una tabla resumen de incidentes significativos donde se describen los tipos de eventos obligatorios a reportar y algunos ejemplos.

En el Anexo 2 se explican mediante tablas los diferentes campos del formulario y cómo cumplimentarlos. Y el Anexo 3 se trata de un resumen de las normas del Reglamento de Ejecución 2024/2690, de 17 de octubre, sobre la notificación de incidentes significativos

6.3 Directrices de ENISA sobre el reporte de incidentes (ENISA)

La Agencia de la Unión Europea para la Ciberseguridad ha desarrollado un conjunto de orientaciones técnicas y prácticas para apoyar la implementación de las directivas NIS (*guidelines related to Article 23 _summary reporting*). Estas directrices se centran en medidas de gestión de riesgos cibernéticos, detección, respuesta y notificación de incidentes, promoviendo un enfoque común para los Estados miembros. A continuación, se detalla un análisis estructurado de sus contribuciones clave, basado en publicaciones recientes como la Guía Técnica de Implementación para NIS2 (versión 1.0, 2025), que integra estándares internacionales como ISO/IEC 27001 e ISO/IEC 27035. [38]

6.3.1 *Evaluación de Riesgos como Base para la Gestión de Incidentes*

ENISA incide en la evaluación de riesgos como pilar preventivo, recomendando metodologías como ISO/IEC 27005¹⁵ para identificar amenazas, vulnerabilidades y activos críticos. Además, propone una clasificación integral que considera impactos en confidencialidad, integridad, disponibilidad y autenticidad, junto con factores ambientales y de cadena de suministro. Para actualizar guías nacionales, sugiere incorporar revisiones anuales que integren lecciones aprendidas de incidentes previos, estableciendo umbrales de tolerancia al riesgo y planes de tratamiento (evitación, mitigación, transferencia o aceptación).

6.3.2 *Detección y Monitorización de Incidentes*

Las directrices promueven el uso de herramientas automatizadas como SIEM (del inglés, Sistemas de Gestión de Eventos e Información de Seguridad), EDR (del inglés, Detección y Respuesta en *Endpoints*) y XDR (Detección y Respuesta Extendida) para la monitorización continua. Se recomienda registrar eventos específicos (tráfico de red, accesos privilegiados, anomalías) con umbrales de alarma definidos, asegurando la sincronización temporal y el cumplimiento de RGPD (Reglamento General del Protección de Datos) mediante anonimización de datos.

6.3.3 *Respuesta y Contención de Incidentes*

ENISA aboga por políticas de gestión de incidentes con fases claras como la contención (aislamiento de activos), erradicación (eliminación de causas de origen), recuperación y revisión post-incidente. Se destacan la elaboración y publicación de *playbooks*¹⁶ específicos para escenarios comunes (*ransomware*, *phishing*) y pruebas anuales mediante ejercicios de simulación (tipo *tabletop* y de ataque y defensa). La

¹⁵ Se trata de un estándar internacional para la Gestión de Riesgos de Seguridad de la Información

¹⁶ En el contexto de la ciberseguridad un *playbook* se trata de una guía operativa que establece procedimientos normalizados para la identificación, evaluación, contención, remediación y recuperación frente a un tipo concreto de incidente de seguridad. Su finalidad es asegurar una actuación ágil, homogénea y eficaz, reduciendo el impacto operativo y reforzando la capacidad defensiva global de la organización. [49]

coordinación con equipos multifuncionales y proveedores externos es clave, con énfasis en la preservación de evidencias para fines forenses.

6.3.4 Obligaciones de Notificación y Reporte

Las guías detallan criterios para clasificar incidentes por su gravedad (baja-media-alta-crítica), priorizando impactos regulatorios y en la cadena de suministro. Se promueve el uso de canales estandarizados (formularios web, correo cifrado) y plantillas que incluyan detalles como indicadores de compromiso (IoC), causas origen y lecciones aprendidas. ENISA propone revisiones trimestrales de clasificaciones y métricas de rendimiento (KPIs como tiempos de respuesta).

6.3.5 Mejores Prácticas y Armonización

ENISA integra prácticas como la adopción de estándares NIST (SP 800-61 para respuesta) y automatización con SOAR (*Security Orchestration, Automation and Response*). Se hace referencia especial a la formación en ciberhigiene y la definición de roles.

6.4 Reglamento de Ejecución de la Comisión (UE) 2024/2690

En el marco de la transposición de la Directiva NIS 2, reviste especial importancia la aprobación del Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024. A diferencia de la Directiva, que requiere transposición nacional, este Reglamento es obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro. Su objetivo es armonizar los requisitos técnicos y, fundamentalmente, detallar los casos en los que un incidente se considera “significativo” para un subconjunto específico de sujetos obligados que denomina “entidades pertinentes” (EP).

Estas EP son las que se citan en el artículo 26.1 del APL sobre proveedores de servicios e infraestructuras digitales:

- Proveedores de servicios de DNS y registros de nombres de dominio de primer nivel (TLD).
- Proveedores de servicios de computación en nube (Cloud) y centros de datos.
- Redes de distribución de contenidos (CDN).
- Proveedores de servicios gestionados (MSP) y de seguridad gestionados (MSSP).
- Mercados en línea, motores de búsqueda y redes sociales

Este tipo de entidades deberán ser registradas por el CNCíber, y se encargará de elaborar el listado y mantener el registro actualizado. Además, el Reglamento establece diferentes definiciones del concepto de “incidente significativo” respecto del resto de Entidades Esenciales e Importantes conforme a lo establecido en la NIS 2. En este caso, el Reglamento establece que, en función del tipo de proveedor, un incidente es significativo si cumple con las siguientes métricas, comunes y específicas. [39]

6.4.1 Criterios Horizontales de Significatividad

De conformidad con el Artículo 3 del Reglamento, se establecen una serie de circunstancias transversales aplicables a la totalidad de las EP. La concurrencia de cualquiera de estas circunstancias determina automáticamente la clasificación del incidente como “significativo”, activando la obligación de notificación, con independencia de los umbrales técnicos específicos de cada servicio.

Estas circunstancias comunes se categorizan en los siguientes impactos.

1. Impacto Financiero y Económico. Un incidente se considerará significativo si ha causado o tiene la capacidad de causar:
 - Pérdidas financieras directas: Cuando estas superen los 500.000 EUR o el 5% del volumen de negocios anual total de la entidad en el ejercicio financiero anterior, aplicándose la cifra que sea menor.

- Exfiltración de secretos comerciales: Se notificará cualquier incidente que implique la exfiltración de secretos comerciales, tal como se definen en el artículo 2, apartado 1, de la Directiva (UE) 2016/943¹⁷, afectando a la confidencialidad de la información crítica de la entidad.
- 2. Impacto en Personas Físicas (Seguridad y Salud). Dada la criticidad de las infraestructuras digitales, se establece un criterio de impacto humano directo. El incidente es notificable si ha causado o puede causar:
 - La muerte de una persona física.
 - Daños considerables a la salud de una persona física.
- 3. Impacto Operativo por Acceso Malicioso. Se introduce un criterio cualitativo vinculado a la naturaleza del ataque. Se considera significativo cualquier incidente en el que se haya producido un acceso presuntamente malicioso y no autorizado a los sistemas de redes y de información, siempre que dicho acceso tenga el potencial de causar graves perturbaciones operativas. Este criterio busca asegurar la notificación temprana de intrusiones exitosas, incluso si el impacto financiero o técnico inmediato no alcanza otros umbrales.
- 4. Agregación de Incidentes Recurrentes. El Reglamento introduce en su articulado un mecanismo de agregación para evitar que ataques de bajo impacto individual pasen desapercibidos. Varios incidentes que, individualmente, no se consideren significativos, se notificarán como un único incidente significativo si cumplen cumulativamente las siguientes condiciones:
 - Se han producido al menos dos veces en un plazo de seis meses.
 - Tienen la misma causa raíz aparente.
 - Colectivamente, superan el umbral de pérdidas financieras establecido (500.000 EUR o 5% del volumen de negocios).
- 5. Exclusiones. No se considerarán incidentes significativos, y por tanto no requieren notificación bajo estos criterios, las interrupciones del servicio o consecuencias derivadas de operaciones de mantenimiento programadas que hayan sido comunicadas o planificadas por la entidad pertinente

6.4.2 Criterios Sectoriales Específicos de Significatividad

Adicionalmente a los criterios horizontales, el Reglamento define circunstancias específicas para cada categoría de entidades. Estos criterios introducen parámetros técnicos objetivos (tiempos de latencia o minutos de indisponibilidad) que eliminan la discrecionalidad en la evaluación del incidente. Un incidente se considerará significativo si cumple, al menos, uno de los siguientes umbrales sectoriales:

1. Infraestructuras de Internet (DNS y TLD)

Para los proveedores de servicios del sistema de nombres de dominio (DNS) y los registros de nombres de dominio de primer nivel (TLD), la disponibilidad y la velocidad de respuesta son críticas para la estabilidad de internet. Se considerará incidente significativo si se produce cualquiera de las siguientes situaciones:

- Indisponibilidad total: El servicio de resolución deja de estar disponible por completo durante más de 30 minutos (para proveedores DNS) o durante cualquier periodo (para registros TLD);

¹⁷ “Relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas”.

- Latencia excesiva: El tiempo medio de respuesta a las solicitudes es superior a 10 segundos durante un periodo de más de una hora;
- Integridad: Se compromete la integridad, confidencialidad o autenticidad de los datos, salvo excepciones menores en proveedores DNS (menos de 1.000 dominios afectados y <1% del total).

2. Servicios de Computación en Nube y Redes de Distribución de Contenidos (CDN)

Dada la dependencia de terceros servicios sobre estas infraestructuras, se establecen umbrales basados en la duración de la caída y el volumen de usuarios afectados en la Unión:

- Indisponibilidad total: El servicio está completamente no disponible durante más de 30 minutos;
- Indisponibilidad parcial: La disponibilidad está limitada durante más de una hora, afectando a más del 5% de los usuarios en la UE o a más de un millón de usuarios;
- Compromiso de datos: Incidentes que afecten a la integridad, confidencialidad o autenticidad de los datos debido a una acción maliciosa o que impacten en los umbrales de usuarios mencionados anteriormente.

3. Centros de Datos (Data Centers)

A diferencia de los servicios en la nube, los centros de datos (proveedores de housing y facilidades físicas) tienen criterios vinculados a la infraestructura física:

- Indisponibilidad: El servicio del centro de datos está totalmente no disponible (sin umbral de tiempo mínimo especificado, lo que implica inmediatez) o su disponibilidad está limitada durante más de una hora;
- Seguridad Física: Se notificarán los incidentes en los que el acceso físico a las instalaciones se vea comprometido (intrusiones físicas).

4. Proveedores de Servicios Gestionados (MSP) y de Seguridad Gestionados (MSSP)

Estos proveedores, críticos por su acceso privilegiado a las redes de sus clientes, se rigen por umbrales idénticos a los de la nube:

- Indisponibilidad total superior a 30 minutos;
- Limitación de disponibilidad superior a una hora si afecta a más del 5% de usuarios o un millón de usuarios.

5. Plataformas en Línea (Mercados, Motores de Búsqueda y Redes Sociales)

Para estas entidades, el regulador europeo pone el foco en el impacto masivo sobre la base de usuarios de la Unión:

- Se considera significativo cualquier incidente (indisponibilidad total, parcial o compromiso de datos) que afecte a más del 5% de los usuarios de la plataforma en la UE o a más de un millón de usuarios (aplicándose el umbral que sea menor).

6. Prestadores de Servicios de Confianza (PSC)

Debido a su papel en la seguridad jurídica de las transacciones electrónicas, este sector tiene los umbrales temporales más estrictos del Reglamento:

- Indisponibilidad: El servicio está totalmente caído durante más de 20 minutos.
- Degradación: El servicio no está disponible para los usuarios durante más de una hora (acumulada en una semana natural).

- Impacto en usuarios: La degradación afecta a más del 1% de los usuarios/partes usuarias o a más de 200.000 usuarios.
- Integridad: Cualquier compromiso de integridad que afecte a más de 100 usuarios o al 0,1% de los mismos, o cualquier compromiso de la seguridad física de las zonas restringidas.

Es importante significar que, el Reglamento especifica cómo deben calcularse los "usuarios afectados", por lo que las entidades deben sumar tanto a los clientes directos con contrato como a las personas físicas y jurídicas asociadas a clientes empresariales que utilizan el servicio. Esto implica que, en el caso de un proveedor de servicios B2B (como un *cloud* que aloja una web de comercio electrónico), un incidente no solo afecta a una entidad (la empresa cliente), sino a todos los usuarios finales de esa empresa que no pueden acceder al servicio.

6.5 Esquema Nacional de Seguridad (ENS)

Para finalizar este capítulo, es requisito fundamental abordar el Esquema Nacional de Seguridad (ENS), de una forma práctica en relación con el APL y su implicación directa sobre las EE e EI. El ENS está regulado por el Real Decreto 311/2022, de 3 de mayo, como marco jurídico y técnico de referencia en España para garantizar la seguridad de los sistemas de información del sector público y las entidades privadas que colaboran con este. Su objetivo principal es crear las condiciones necesarias de confianza en el uso de los medios electrónicos, estableciendo medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos [40]

A efectos de este trabajo de revisión y actualización de la GNNGC y del nuevo marco NIS 2, el ENS es importante por tres aspectos clave:

1. **Ámbito de Aplicación y Cadena de Suministro.** El ENS no solo aplica a las Administraciones Públicas. Su alcance se extiende a las entidades del sector privado cuando, en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público. Esto convierte al ENS en un estándar de facto para gran parte de la cadena de suministro tecnológica nacional, alineándose con los objetivos de seguridad de la cadena de suministro de la Directiva NIS2. Asimismo, para este ámbito, el APL establece una equivalencia automática ya que con la acreditación del cumplimiento del PCE del ENS satisface automáticamente los requisitos de gestión de riesgos estipulados en la nueva Ley, garantizando la alineación normativa sin duplicidad de cargas administrativas.
2. A diferencia de otros estándares que son estáticos, el ENS establece un modelo de seguridad basado en el riesgo. Los sistemas de información se clasifican en tres categorías (Básica, Media y Alta) en función de la valoración del impacto que tendría un incidente sobre la información o los servicios, evaluando dimensiones como la Disponibilidad, Autenticidad, Integridad, Confidencialidad y Trazabilidad. Esta categorización determina la rigurosidad de las medidas de seguridad a aplicar (recogidas en el Anexo II del Real Decreto), lo cual es directamente relevante ya que la capacidad de detección y notificación de un incidente depende de las medidas de vigilancia implantadas según la categoría del sistema.
3. El ENS regula explícitamente la gestión de incidentes, estableciendo obligaciones que la Guía Nacional debe orquestar:
 - **Capacidad de Respuesta:** El ENS obliga a las entidades a disponer de capacidades para la prevención, detección y respuesta a incidentes, articulando dicha respuesta en torno al CCN-CERT.
 - **Notificación Obligatoria:** Se establece la obligatoriedad de notificar al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información. Esto conecta directamente con la taxonomía y los umbrales de impacto que la GNNGC debe armonizar.

- Etiquetado de Seguridad: La notificación debe permitir clasificar el incidente y determinar técnicamente el riesgo de reconexión de los sistemas afectados

El APL sitúa al ENS como referencia no solo para el sector público, que es obligatorio, sino para las entidades esenciales e importantes reguladas que pueden adoptar como base de cumplimiento de las medidas de seguridad dicho marco. El artículo 15.2 del APL establece explícitamente que para las entidades no sujetas al ENS que obtengan voluntariamente esta evaluación se dará por acreditado el cumplimiento de las obligaciones de gestión de riesgos de la ley. Esto evita tener que demostrar ante la autoridad de control, mediante auditorías *ad-hoc* complejas, que sus controles internos (basados en otros estándares internacionales) son equivalentes a lo que pide la ley [6]

Además, se introduce la figura del “Perfil de Cumplimiento Específico (PCE)”, definido como el conjunto de medidas de seguridad que resulten de aplicación a una entidad o sector concreto tras un análisis de riesgos y que debe ser habilitado por el CCN. Este PCE permite adaptar los requisitos del ENS a sectores concretos o necesidades específicas (como las de NIS 2), facilitando una certificación que acredita el cumplimiento de las obligaciones de gestión de riesgos de la nueva ley. De este modo, el ENS pasa de ser una norma administrativa para convertirse en una especie de “Piedra Rosseta” para las entidades sujetas al APL.

7 PROPUESTAS DE ACTUALIZACIÓN DE LA GUÍA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES

Como se ha explicado anteriormente, la GNNGC actual aprobada en 2020 por el Consejo Nacional de Ciberseguridad, establece un marco de referencia para la notificación y gestión de Ciberincidentes en España, alineado directamente con NIS 1 y el RDL. Sin embargo, tras el análisis del nuevo marco normativo (principalmente NIS 2 y su transposición mediante el APL), que pretende eliminar las lagunas y carencias detectadas tras la transposición y aplicación de la NIS 1 por los Estados miembros, y alcanzar un alto grado común de Ciberseguridad en la UE, se considera necesaria una revisión y actualización de la actual Guía que ha quedado obsoleta en ciertos aspectos estructurales.

En este capítulo, que da sentido y consolida el propósito del trabajo, se proponen las modificaciones necesarias para alinear este instrumento operativo con el nuevo Anteproyecto de Ley.

7.1 Objetivos y Alcance

El objetivo principal del nuevo marco normativo NIS 2, como ya se ha comentado antes es lograr que todos los miembros de la Unión logren un alto nivel de Ciberseguridad. Para alcanzar ese grado de compromiso, se establecen obligaciones y medidas comunes, siendo las principales:

- La notificación de incidentes de ciberseguridad, en tiempo y forma, que ya era objeto de las anteriores normas, como el Real Decreto Ley 12/2018 y el Real Decreto 43/2021.
- La designación de un responsable de seguridad de la información para cada entidad sujeta a la norma.
- La gestión de riesgos de ciberseguridad para las entidades reguladas.

Asimismo, en cuanto al alcance, se amplía considerablemente con la directiva NIS 2 y el APL, definiendo nuevos criterios generales. La norma se aplica a entidades públicas o privadas con residencia fiscal en España, o en otro Estado miembro pero que ofrezcan sus servicios o desarrollen su actividad a través de un establecimiento permanente en España, y que cumplan simultáneamente dos condiciones:

1. Sector: Pertenecen a los "Sectores de Alta Criticidad" (Anexo I) o a "Otros Sectores Críticos" (Anexo II).
2. Tamaño: Tienen la consideración de medianas o grandes empresas (cuentan con 50 o más trabajadores, o un volumen de negocios/balance anual superior a 10 millones de euros).

Además, independientemente del tamaño (es decir, también para pequeñas y medianas empresas), se incluyen las comprendidas en los Anexos I y II, siempre que cumplan ciertas funciones críticas:

- Infraestructura Digital y Telecomunicaciones: Proveedores de redes públicas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, prestadores de servicios de confianza, registros de nombres de dominio de primer nivel (TLD) y proveedores de servicios DNS.
- Monopolio o Criticidad: Entidades que sean el único proveedor de un servicio esencial en España o cuya perturbación tendría repercusiones significativas en la seguridad nacional, salud pública o actividad económica.
- Sector Público: Entidades de la Administración Pública definidas según la Ley 40/2015.
- Entidades Críticas: Aquellas identificadas bajo la transposición de la Directiva CER (Directiva sobre resiliencia de entidades críticas).
- Sectores Afectados (Anexos I y II)

Como propuesta a anexar al documento, se sugiere la inclusión de un flujograma o esquema que permita de forma sencilla la autoidentificación como entidad NIS 2, de acuerdo con las características de cumplimiento establecidas en el APL. Véase el siguiente ejemplo.



Figura 11 Esquema de aplicación NIS 2. Elaboración propia.

7.2 Gobernanza Nacional de Ciberseguridad

El Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad establece un nuevo y centralizado esquema de gobernanza para España. La principal novedad del APL, es la previsión de un Centro Nacional de Ciberseguridad como autoridad nacional a nivel central, coordinando y supervisando todo lo relativo a la ciberseguridad nacional.

Es necesario, por tanto, plasmar y describir este nuevo modelo, así como a las autoridades implicadas en la gestión y notificación de incidentes. (Autoridades de Control, CSIRT de referencia y el CNCíber).

A continuación, se detallan esos organismos que integran la estructura de gobernanza conforme al APL. Se propone incorporar esta descripción acompañándose de la figura 4 del modelo de gobernanza de este trabajo que representa gráficamente el esquema organizativo nacional.

1. Centro Nacional de Ciberseguridad: La Autoridad Nacional

El Centro Nacional de Ciberseguridad (cuya creación formal se contempla en una disposición adicional y que se adscribirá al Gabinete de la Presidencia del Gobierno) se erige como la pieza central y la autoridad nacional competente única en materia de gobernanza de la ciberseguridad.

Sus roles y funciones principales son:

- Dirección y Coordinación. Encargado de la dirección, impulso y coordinación de todas las actividades previstas en la ley para garantizar un elevado nivel de ciberseguridad en España.
- Punto de Contacto Único. Actúa como enlace para garantizar la cooperación intersectorial a nivel nacional y la cooperación transfronteriza con autoridades de otros Estados miembros, la Comisión Europea y la ENISA.
- Autoridad de Gestión de Crisis. Ejerce como autoridad nacional de gestión de crisis y será responsable de la coordinación de incidentes y crisis de ciberseguridad a gran escala.
- Supervisión Superior. Asume la superior dirección y coordinación de las autoridades de control, los puntos de contacto sectoriales y los CSIRT nacionales de referencia en el desarrollo de sus funciones de ejecución y supervisión.

2. Autoridades de Control (Supervisión y Ejecución)

Las autoridades de control son los órganos responsables de las funciones de supervisión y ejecución sobre las entidades esenciales e importantes, actuando bajo la superior dirección del Centro Nacional de Ciberseguridad. Se designan tres principales autoridades de control en función del ámbito de aplicación:

- Ministerio de Defensa (a través del Centro Criptológico Nacional, CCN). Para las entidades esenciales e importantes que no sean críticas, pero que estén incluidas en el ámbito subjetivo de la Ley 40/2015, de Régimen Jurídico del Sector Público.
- Ministerio para la Transformación Digital y de la Función Pública. A través de sus Secretarías de Estado, para las entidades esenciales e importantes de los sectores de Infraestructura digital y Proveedores de servicios digitales, así como para las entidades importantes de otros sectores que no sean críticas.
- Ministerio del Interior (a través de la Oficina de Coordinación de Ciberseguridad - OCC). Para las entidades críticas y las entidades esenciales de los sectores no incluidos en los puntos anteriores, además de todas las entidades esenciales e importantes del sector de seguridad privada.

3. Equipos de Respuesta a Incidentes (CSIRT) Nacionales de Referencia

Los CSIRT son los responsables de la respuesta técnica a incidentes y cooperan estrechamente con las autoridades de control. El Centro Nacional de Ciberseguridad asumirá la coordinación superior de estos equipos.

Los CSIRT nacionales de referencia son:

- CCN-CERT. Su comunidad de referencia son las entidades esenciales o importantes incluidas en el ámbito subjetivo de la Ley 40/2015 (Sector Público). El CCN-CERT también ejerce la coordinación nacional de la respuesta técnica de los CSIRT en incidentes significativos o de especial gravedad, siguiendo instrucciones del Centro Nacional de Ciberseguridad.
- INCIBE-CERT. Su comunidad de referencia son las entidades esenciales o importantes que no están incluidas en el ámbito subjetivo de la Ley 40/2015 (generalmente sector privado).
- ESPDEF-CERT. Pertenece al Mando Conjunto del Ciberespacio y coopera con el CCN-CERT e INCIBE-CERT, especialmente en incidentes que afecten a entidades con incidencia en la Defensa Nacional.

- CSIRT-MIR-PJ, de la OCC, en materia de entidades catalogadas como críticas cooperando con el CSIRT de referencia correspondiente.

4. Puntos de Contacto Sectoriales

Son órganos ministeriales u organismos públicos designados para cada sector de alta criticidad y otros sectores críticos, para impulsar las políticas de ciberseguridad en su ámbito y colaborar estrechamente con el CNCíber y las autoridades de control en la identificación de entidades esenciales e importantes y en la elaboración de perfiles específicos de cumplimiento.

7.3 Notificación de Ciberincidentes.

La GNNGC exige la notificación de aquellos Ciberincidentes categorizados como ALTO, MUY ALTO o CRÍTICO, en función de dos criterios: peligrosidad o impacto. Para ello el propio documento presenta una taxonomía, alineada con la de ENISA, con diferentes tipologías y categorías de acuerdo con esos criterios.

Un cambio clave ha sido la introducción del concepto “incidente significativo”, siendo este el elemento determinante para la notificación. Si bien, el APL sigue con la misma política de los criterios de Peligrosidad o Impacto, la NIS 2 se centra en la notificación de aquellos eventos que caen dentro de la definición de incidente significativo siendo imperativo para aquellas entidades obligadas.

Asimismo, es fundamental considerar la Disposición transitoria tercera del APL, relativa al Régimen transitorio. Esta disposición establece que, hasta que se produzca la modificación, sustitución o derogación de la actual Instrucción Nacional de Notificación y Gestión de Ciberincidentes, se seguirán considerando legalmente como incidentes significativos aquellos que puedan categorizarse con un nivel de peligrosidad o impacto Alto, Muy Alto o Crítico, conforme a lo establecido en la normativa anterior. Por consiguiente, la propuesta de actualización presentada en este trabajo está diseñada para ser el instrumento operativo que permita superar este periodo transitorio y materializar el nuevo modelo de notificación objetiva exigido por la Unión Europea.

Por tanto, la propuesta que se plantea en este trabajo es la de alinear el criterio optado por la Guía belga conforme a la NIS 2, centrándose en la notificación de aquellos incidentes significativos conforme a su definición. El resto de los incidentes que no sean de obligada notificación por no tratarse de incidentes significativos, de acuerdo con la nueva ley, igualmente podrán ser notificados de forma voluntaria.

Teniendo en cuenta lo anterior, cabe dedicar un apartado de definiciones y detallar qué notificaciones son obligatorias y cuáles son voluntarias.

7.3.1 Definiciones

Basándose en las definiciones del APL, a continuación, se exponen aquellas consideradas necesarias para el cumplimiento del deber de notificación:

- Incidente: (Artículo 2.f): "Todo hecho que comprometa la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por redes y sistemas de información o accesibles a través de ellos."
- Incidente significativo (Artículo 2.g): todo aquel incidente que,
 - i. “ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada;
 - ii. ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables."

- Cuasiincidente o incidente sin impacto: "Un hecho que habría podido comprometer la disponibilidad, autenticidad, integridad confidencialidad, o trazabilidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por redes y sistemas de información o accesibles a través de ellos, pero cuya materialización completa se previno de manera satisfactoria o que no llegó a materializarse;"¹⁸
- Ciberamenaza significativa: "Una ciberamenaza que, basándose en sus características técnicas, cabe suponer que tiene el potencial de provocar repercusiones graves en las redes y sistemas de información de una entidad o para los usuarios de los servicios de la entidad causando perjuicios materiales o inmateriales considerables;"
- Gestión de incidentes: "Conjunto de medidas y procedimientos destinados a prevenir, detectar, analizar y limitar un incidente o responder ante este y recuperarse de él."
- Riesgo: la posible pérdida o perturbación causada por un incidente expresada como una combinación de la magnitud de tal pérdida o perturbación y la probabilidad de que se produzca tal incidente;
- Vulnerabilidad: "deficiencia, susceptibilidad o fallo de productos de TIC o servicios de TIC que puede ser aprovechado por una ciberamenaza";
- Entidades esenciales: Se definen como aquellas de alta criticidad que prestan servicios esenciales para la sociedad o economía, incluyendo: a) grandes empresas en sectores del Anexo I (por ejemplo, energía, transporte, infraestructuras digitales); b) prestadores cualificados de servicios de confianza y registros de dominio TLD; c) proveedores de redes públicas de comunicaciones; d) entidades de la Administración General del Estado; e) otras identificadas por resolución motivada; f) entidades críticas según la ley CER (transposición de la directiva UE 2022/2557);
- Entidades importantes: Son aquellas entidades que pertenecen a los sectores de los Anexos I o II, pero que no llegan a considerarse esenciales.

7.3.2 Notificaciones obligatorias y umbrales temporales de notificación

Todas aquellas Entidades Esenciales e Importantes están obligadas a reportar los incidentes significativos acaecidos en su seno, o en el de proveedores externos, por parte de su Responsable de Seguridad de la Información)¹⁹ a las autoridades de control respectivas, sin "demora indebida", además de hacerlo a los destinatarios de esos servicios, a través de sus CSIRT nacional de referencia.

En primer lugar, la guía debería aclarar quién y qué se debe notificar, por lo que se plantea incorporar una tabla similar a la siguiente (Tabla 5).

	Incidentes Significativos	Otros Incidentes	Ciberamenazas	Cuasiincidentes
Entidad Esencial	Obligatorio	Voluntario	Voluntario	Voluntario
Entidad Importante	Obligatorio	Voluntario	Voluntario	Voluntario
Otras entidades	Voluntario	Voluntario	Voluntario	Voluntario

¹⁸ *Ejemplo:* Un empleado recibe un correo de *phishing* muy sofisticado (el hecho ocurre), pero el empleado estaba de vacaciones y el correo caducó o simplemente no lo abrió (no llegó a materializarse).

¹⁹ Art. 16 del APL

Tabla 5 Obligatoriedad de notificar

El proceso de notificación se compone de, al menos, 3 tipos de notificaciones estableciéndose diferentes marcos temporales y especificaciones diferentes para cada de ellas. Estos plazos constituyen otro de los cambios más relevantes respecto a la anterior Guía, siendo los nuevos más rigurosos.

Es, por tanto, crucial redefinir este aspecto dejando claras las nuevas modificaciones. Para ello se puede recurrir a un modelo de tabla como la siguiente, conforme al artículo 18 del APL:

Tipo de Notificación Obligatoria	Descripción	Plazo	PSC
Alerta temprana	Indicación inicial del incidente significativo, incluyendo si es sospechoso de acción ilícita o malintencionada, o con repercusiones transfronterizas.	Sin demora indebida, y en cualquier caso, en el plazo ≤ 24 horas desde que se haya tenido constancia del incidente significativo.	≤ 24 horas
Notificación del incidente	Evaluación inicial del incidente, actualizando la alerta temprana, incluyendo peligrosidad, impacto e indicadores de compromiso (IoCs).	En el plazo ≤ 72 horas desde que se haya tenido constancia del incidente significativo (24 horas para prestadores de servicios de confianza si afecta a la prestación de sus servicios).	≤ 24 horas (Si afecta a la prestación del servicio)
Informe intermedio de progreso	Actualizaciones sobre la situación del incidente.	A instancias del CSIRT nacional de referencia o de la autoridad de control.	
Informe final	Descripción detallada del incidente, tipo de amenaza o causa principal, medidas paliativas aplicadas, repercusiones transfronterizas e IoCs/TTPs detectados.	≤ 1 mes después de presentar la notificación del incidente. Si el incidente sigue en curso, se presenta un informe de situación en ese momento y el informe final en el plazo de 1 mes a partir de que se haya gestionado el incidente.	
Comunicación a destinatarios/usarios afectados	Notificación de incidentes significativos o ciberamenazas que puedan causarles perjuicios, incluyendo medidas o soluciones aplicables.	A la mayor brevedad posible.	

Tabla 6 Notificaciones obligatorias y umbrales temporales

Resulta imprescindible especificar que, para los Prestadores de Servicios de Confianza (PSC)²⁰, el plazo de la notificación, cuya ventana temporal es de máximo 72 horas desde la notificación de la Alerta, se reduce hasta un máximo de 24 horas para ellos, tal como se indica en la Tabla 5.

²⁰ Definidos en el Reglamento (UE) n° 910/2014 (eIDAS)

Asimismo, las entidades informarán debidamente y a la mayor brevedad a los destinatarios de sus servicios afectados. Todo ello sin perjuicio del deber de denunciar ante las autoridades competentes aquellos casos que sean constitutivos de delito público²¹.

Como establece ENISA en su guía de buenas prácticas, y el CCB en su guía de notificación, se proponen plantillas generales para la notificación de Ciberincidentes que se incluirá en el Anexo I

7.3.3 Notificaciones Voluntarias

Además de las notificaciones obligatorias, las entidades esenciales e importantes podrán reportar cualesquiera incidentes, ciberamenazas y cuasiincidentes acaecidos en su seno, que consideren oportunos. De igual forma, como indica el APL, las entidades no calificadas como esenciales o importantes que prestan servicios “vitales” podrán reportar eventos significativos sin que ello suponga obligaciones añadidas.

Como propuesta, en el Anexo II se propone una plantilla general para este tipo de notificaciones.

7.3.4 Redefinición del Umbral de Notificación: De la "Peligrosidad" a la "Significatividad"

La vigente Guía establece la obligación de notificar basándose en dos criterios fundamentales, "Nivel de Peligrosidad" y "Nivel de Impacto". Para ello se establece una categorización en base a una taxonomía alineada con la de ENISA, obligando a notificar aquellos incidentes cuyos niveles de Peligrosidad o Impacto fueran clasificados como alto, muy alto o crítico.

Además, actualmente, se utilizan criterios macroeconómicos de difícil cálculo para una entidad privada, como el impacto económico medido en porcentaje del P.I.B. nacional (Producto Interior Bruto), (entre 0,03% y 0,07% para impacto Alto).

Se propone sustituir los umbrales basados en el PIB por los criterios armonizados del Reglamento de Ejecución: pérdidas financieras directas superiores a 500.000 EUR o al 5% del volumen de negocios anual total, y la exfiltración de secretos comerciales. [41]

7.4 Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes

La PNNSC como punto neutro ya se contemplaba en la GNNGC, sin embargo, a fecha de redacción de este trabajo la plataforma se encuentra en desarrollo y, por tanto, actualmente no está operando. Este esquema de ventanilla única propone que los incidentes se reporten a la autoridad competente a través de su CSIRT nacional de referencia. Sin embargo, el procedimiento que se sigue actualmente es el reporte a través de las vías de contacto de los equipos de respuesta, que como norma general se trata de un buzón de correo electrónico, cuyas direcciones se encuentran publicadas en la web de la PNNSC.²²

Si bien la PNNSC debe ser el mecanismo de notificación único, como propuesta de actualización para la Guía, se considera práctico introducir como anexo una guía explicativa sobre el funcionamiento de la plataforma, la dirección web (URL) o cómo cumplimentar los diferentes formularios de notificación.

7.5 Taxonomía y Clasificación de Incidentes

La taxonomía de la Guía Nacional (basada en la propuesta por ENISA), se centra casi exclusivamente en la tipología técnica del ataque o el efecto observado (ej. *Código dañino, Intrusión, Disponibilidad/DDoS, Fraude*). Esta clasificación puede resultar útil para la respuesta técnica inmediata, pero resulta insuficiente para cumplir con los nuevos requisitos de notificación y estadística que exige la normativa europea y nacional.

²¹ LECrim Arts. 259-262: cualquier persona que conozca un delito público debe denunciarlo, bajo pena de multa si omite

²²<https://www.plataformanacionalciber.gob.es/index.php/notificacion-de-incidentes>

Se propone actualizar el sistema de clasificación de incidentes añadiendo una capa superior de clasificación basada en la “Causa Raíz”. Esta modificación es necesaria para dar cumplimiento al Artículo 18.6.d.ii del APL, que exige explícitamente que el informe final de un incidente significativo incluya “el tipo de amenaza o causa principal que probablemente haya desencadenado el incidente”.

Como propuesta, se sugiere estructurar la notificación en dos niveles:

- Nivel 1: Categoría de Causa Raíz. la Guía debe ofrecer al operador a seleccionar una de las siguientes 5 causas raíz para el informe final:
 - A. Fallos del Sistema: El incidente se debe a un fallo interno sin causa externa (ej. error de software, fallo de hardware, fallo en un procedimiento).
 - B. Fenómenos Naturales: El incidente es provocado por causas naturales (ej. tormentas, inundaciones, incendios forestales, terremotos).
 - C. Errores Humanos: El sistema funcionaba correctamente, pero fue utilizado de forma errónea (ej. error de tecleo, configuración equivocada por negligencia, pérdida de dispositivo).
 - D. Acciones Maliciosas: El incidente es fruto de una acción deliberada (ej. ciberataque, sabotaje físico, robo, ataque interno).
 - E. Fallos de Terceros: El incidente se debe a la interrupción de un servicio de un tercero o utilidad (ej. corte de energía, caída de internet, fallo del proveedor de nube).
- Nivel 2: Tipología del Incidente (Taxonomía Técnica). Una vez seleccionada la causa raíz, se mantendría la taxonomía técnica actual de la GNNGC (basada en la taxonomía de referencia de CSIRT de ENISA) como un subnivel o etiqueta descriptiva.

Un par de ejemplos de aplicación sería: Un ataque de *Ransomware* se clasificaría como Causa Raíz: Acciones Maliciosas -> Tipo: Código Dañino (*Ransomware*). Un corte de fibra óptica por obras se clasificaría como: Causa Raíz: Fallos de Terceros -> Tipo: Disponibilidad (Interrupción).

7.6 Creación de un Anexo Técnico de Métricas para Entidades Pertinentes

La GNNGC carece de umbrales técnicos específicos para el sector de infraestructura digital, dependiendo de matrices de impacto genéricas. Sin embargo, el nuevo marco normativo introduce un cambio sustancial estableciendo como obligación a las entidades esenciales e importantes de aplicar adecuadamente los actos de ejecución adoptados por la Comisión Europea.

En este contexto, y como se expuso en su respectivo apartado, el Reglamento de Ejecución (UE) 2024/2690 elimina la discrecionalidad en la evaluación del incidente para los proveedores de servicios e infraestructuras digitales (denominados “entidades pertinentes” en el reglamento), sustituyendo la valoración subjetiva del impacto por parámetros cuantitativos objetivos (minutos de indisponibilidad, latencia o porcentaje de usuarios afectados).

Por tanto, se propone que la actualización de la GNNGC incorpore un Anexo Técnico de obligado cumplimiento que transcriba estos umbrales para alinearlos asimismo con dicho Reglamento. Esto dotará de seguridad jurídica a los operadores, eliminando las dudas que le podrían suscitar al RSI sobre el nivel de gravedad del incidente y sustituyéndola por una instrucción basada en datos (p.e.: ¿se ha superado el umbral de tiempo? Sí o No, si es así entonces: Notifico).

Se recomienda incluir en la Guía una tabla de referencia rápida, basada en los Artículos 5 a 9 del Reglamento de Ejecución [41], que determine cuándo un incidente se considera automáticamente “significativo” por indisponibilidad del servicio con métricas objetivas. Véase el ejemplo de la tabla 7.

<i>Tipo de Entidad / Servicio</i>	Criterio de Notificación Automática (Indisponibilidad Total)	Criterio de Notificación por Degradación o Impacto	Reglamento 2024/2690)
Proveedor de Servicios DNS	El servicio de resolución (recursivo o autoritativo) no está disponible durante más de 30 minutos.	El tiempo medio de respuesta supera los 10 segundos durante más de 1 hora.	Art. 5
Servicios de Computación en Nube (Cloud)	El servicio está totalmente indisponible durante más de 30 minutos.	La disponibilidad está limitada durante más de 1 hora afectando al 5% de usuarios en la UE o >1 millón de usuarios.	Art. 7
Redes de Distribución de Contenidos (CDN)	La red está totalmente indisponible durante más de 30 minutos.	La disponibilidad está limitada durante más de 1 hora afectando al 5% de usuarios o >1 millón de usuarios.	Art. 9
Proveedores de Centros de Datos	El servicio del centro de datos está totalmente indisponible (sin umbral de tiempo mínimo especificado, implica inmediatez).	La disponibilidad del servicio está limitada durante más de 1 hora.	Art. 8

Tabla 7 Tabla de umbrales de notificación automática. Elaboración propia

7.7 Inclusión de un Procedimiento para la Gestión de Incidentes Recurrentes

La Guía vigente está diseñada bajo un paradigma de evento único, es decir, se detecta un incidente, se evalúa su peligrosidad o impacto de forma individual y se notifica si corresponde. Este enfoque deja fuera del ámbito de la norma una realidad operativa común, como lo son los ataques de bajo impacto, pero persistentes (como campañas de *phishing* continuadas o micro-interrupciones de servicio repetitivos, etc.) que, aisladamente no son críticos, pero cuya acumulación o reiteración genera un daño grave.

El Reglamento de Ejecución (UE) 2024/2690, introduce la figura de los “Incidentes Recurrentes”, que coadyuva a cerrar esta brecha. Se considera imperativo que la nueva Guía Nacional incorpore un apartado específico que ayude a los RSI a detectar, sumar y reportar estos eventos agregados.

Se propone incluir en la nueva Guía la definición normativa de “Incidente Recurrente” redactada directamente del Reglamento europeo.

Para que esta definición sea aplicable en la práctica, la Guía debe establecer un protocolo de actuación claro. Se propone el siguiente flujo de tres fases:

- A. Identificación y Correlación (Taxonomía de Causa Raíz) Para poder vincular dos incidentes distintos, la entidad debe utilizar la taxonomía de Causa Raíz propuesta en el apartado 7.6 de este trabajo.
- Instrucción: El operador no debe descartar los incidentes de bajo nivel ("Leves"). Debe registrarlos internamente y etiquetarlos con su causa raíz.
 - Mecanismo de Control: El sistema de gestión de incidentes de la entidad debe generar una alerta automática cuando se registre un segundo incidente con la misma causa raíz en una ventana de 180 días (6 meses).

- B. Evaluación de Impacto Agregado Una vez detectada la recurrencia, el RSI debe realizar una suma aritmética de los impactos.
- Ejemplo: *Un ataque de ransomware contenido rápidamente, supuso un coste de 300.000€ (no notificable por estar bajo el umbral de 500.000€). Tres meses después, un segundo ataque similar cuesta 250.000€.*
 - Resultado: *La suma (550.000€) supera el umbral del Reglamento. Se activa la obligación de notificar como "Incidente Recurrente".*
- C. Mecanismo de Notificación (Gestión del Ticket) La Guía debe resolver la duda operativa sobre cómo notificar hechos pasados. Se desaconseja la reapertura de *tickets* antiguos para no alterar las métricas de tiempos de resolución (SLA) de los CSIRT.
- Propuesta de redacción para la Guía: *"Cuando se detecte que la suma de varios incidentes menores constituye un incidente significativo recurrente, el RSI deberá:*
 - 1) *Generar una Nueva Notificación en la Plataforma Nacional (PNNSC).*
 - 2) *Marcar la tipología de incidente como "Agregado/Recurrente".*
 - 3) *Vincular los identificadores (IDs) de los incidentes previos registrados internamente o, si se notificaron voluntariamente, sus referencias de la plataforma.*
 - 4) *En el campo de "Impacto", consignar la suma total de las pérdidas o afectaciones de la serie.*
 - 5) *El plazo de notificación (24h/72h) comienza a contar desde el momento en que la entidad toma conciencia de que la suma de los eventos ha superado el umbral."*

7.8 Notificación de Ciberamenazas Significativas

A diferencia de la Guía vigente, que se centra exclusivamente en la gestión de incidentes ya materializados, el nuevo APL introduce una obligación proactiva estableciendo que las entidades esenciales e importantes deberán comunicar a los destinatarios de sus servicios "a la mayor brevedad, cualquier Ciberamenaza significativa que les pueda afectar", acompañando dicha comunicación de las "medidas o soluciones que pueden aplicar como respuesta".

Esta obligación supone un reto operativo para las entidades, ya que requiere evaluar cuándo una amenaza potencial (algo que aún no ha ocurrido) es lo suficientemente grave como para alarmar a los clientes. Por ello, es imprescindible que la actualización de la Guía incluya un protocolo que estandarice este proceso, evitando tanto la inacción como la saturación de alertas irrelevantes.

Para evitar una "sobrecarga de alertas" en los usuarios, la Guía debe instruir a las entidades para que solo notifiquen las amenazas que cumplan con la definición de "Ciberamenaza Significativa" conforme define el Artículo 2.k del APL, es decir:

1. "Características Técnicas: Existen pruebas técnicas de que la amenaza es real y activa (no meros rumores).
2. Potencial de Daño: Cabe suponer que tiene el potencial de causar repercusiones graves o perjuicios materiales/inmateriales considerables a los usuarios." [6]

Se propone incluir en la GNNGC un protocolo con el siguiente flujo de actuación para los Responsables de Seguridad de la Información.

1. Detección: Identificación de una vulnerabilidad crítica en un servicio prestado o una campaña de ataque activa dirigida al sector (ej. campaña de *phishing* suplantando a la entidad o vulnerabilidad *0-day* en sistemas proporcionados a clientes).

2. Evaluación de Impacto en el Usuario: Determinar si el usuario debe realizar una acción activa para protegerse (ej. cambiar contraseña, actualizar firmware). *Si la entidad puede mitigar la amenaza internamente sin participación del usuario, la notificación no es obligatoria, aunque sí recomendable por transparencia.*
3. Comunicación: Ejecución de la notificación utilizando una plantilla estandarizada y un lenguaje no técnico.

Además, se puede incluir un formato de plantilla de comunicación de referencia como el de la figura 12, que sea visual, claro y sencillo, al objeto de llegar a todos los públicos y no solo a personal especializado.



Figura 12 Plantilla de comunicación a usuarios. Elaboración con IA (Gemini)

7.9 Incorporación de Medidas de Gobernanza y Supervisión

A diferencia del modelo NIS 1, donde la responsabilidad recae casi exclusivamente en el departamento técnico, el APL introduce un cambio sustancial sobre la responsabilidad directa de los órganos de dirección. Estos deben aprobar las medidas de gestión de riesgos, supervisar su puesta en práctica y responder por el incumplimiento. Por tanto, la nueva GNNGC no puede ser solo un manual técnico; sino que debe proponer mecanismos de reporte ascendente hacia la dirección.

7.9.1 Integración del "Reporte de Eficacia" (Conforme al mandato del Reglamento de Ejecución)

Se sugiere incluir un cuadro de mando tipo como referencia para la dirección de la entidad con indicadores (KPI) sugeridos (basados en ENISA) como:

1. Tiempo medio de detección y respuesta a incidentes (MTTD/MTTR).
2. Porcentaje de sistemas críticos parcheados en plazo.
3. Resultados de auditorías de seguridad y pruebas de penetración.
4. Nivel de cobertura de la formación en ciberseguridad a empleados y directivos.

7.9.2 Marco de Madurez y Auditoría alineado con el ENS

Asimismo, se propone añadir un modelo de madurez que cruce los controles del Reglamento de Ejecución UE 2024/2690 con los del ENS, como ejemplo ver tabla 8.

Dominio Reg. UE 2024/2690	Requisito Específico (Resumido)	Medida ENS (RD 311/2022)
Políticas de Seguridad	Análisis de riesgos y seguridad de la información.	[op.pl.1] Análisis de riesgos [org.ps.1] Política de seguridad
Gestión de Incidentes	Detección, análisis y contención de incidentes.	[op.ges.1] Detección y gestión de incidentes [op.exp.8] Registro de actividad
Continuidad de Negocio	Gestión de copias de seguridad y recuperación ante desastres.	[op.rec.1] Continuidad del servicio [op.rec.2] Copias de seguridad
Cadena de Suministro	Seguridad en la adquisición y desarrollo.	[op.ext.3] Adquisición de productos [op.ext.9] Relación con proveedores

Tabla 8 Ejemplo de Relación de Controles entre el ENS y el Reglamento 2024/2690

7.10 Mecanismos de Revisión y Adaptabilidad

Finalmente, se sugiere establecer revisiones bienales de la GNNGC, incorporando lecciones aprendidas, retroalimentación de los representantes sectoriales y evoluciones reglamentarias. Esto asegura una alineación continua con lo dispuesto en NIS 2 y el Anteproyecto, convirtiéndola en un documento "vivo" que responda a amenazas emergentes.

8 CONCLUSIONES

La realización de este trabajo ha permitido constatar que la actual Guía Nacional de Notificación y Gestión de Ciberincidentes (GNNGC) de 2020 ha quedado superada por la realidad normativa y operativa impuesta por la Directiva (UE) 2022/2555 (NIS 2) y su transposición mediante el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad. La actualización de este instrumento no es una mera formalidad administrativa, sino un imperativo estratégico para garantizar la soberanía digital y la resiliencia de los servicios esenciales en España.

El compendio de nuevas Directivas y Reglamentos europeos que tratan de armonizar y homogeneizar el nivel de Ciberseguridad entre los miembros de la Unión, y las consiguientes transposiciones legales en España, sitúa a las empresas ante un nuevo escenario, tan cambiante y difuso, que genera incertidumbre y dudas en cuanto a sus marcos regulatorios y sus obligaciones legales. La revisión y actualización de la Guía Nacional de Notificación pretende ser un documento amable y sencillo donde aquellas entidades sometidas al amparo del ámbito NIS 2 puedan recurrir y consultar de forma ágil para lo que es el acto más relevante de la gestión de incidentes, desde el punto de vista de la seguridad pública y la gestión de crisis a nivel nacional, la “NOTIFICACIÓN”. Si bien el mecanismo de notificación debe ser, y será, un modelo de ventanilla única soportada por la PNNSC, la Guía simplemente servirá de instrumento de consulta y apoyo ante un posible evento notificable.

A continuación, se exponen las conclusiones principales derivadas del estudio, estructuradas en función de los objetivos planteados al inicio de la investigación.

8.1 Gobernanza Centralizada como Eje Vertebrador.

La revisión de la estructura institucional confirma que la creación del **Centro Nacional de Ciberseguridad** transforma modelo de gobernanza y el flujo de notificación. La nueva Guía propuesta refleja que la notificación ya no es un acto burocrático unidireccional hacia un CSIRT, sino el activador de un sistema de gestión de crisis a nivel nacional y de supervisión y control central. Se concluye que la eficacia de la nueva GNNGC dependerá de su capacidad para articular la **coordinación** entre las Autoridades de Control, los CSIRT de referencia y el CNCíber, **especialmente en la gestión de incidentes transfronterizos o de gran escala**.

8.2 Cambio de Paradigma: De la "Peligrosidad" a la "Significatividad".

El análisis comparativo ha evidenciado que el modelo actual de notificación, basado en matrices subjetivas de "Peligrosidad e Impacto", resulta ineficaz frente a los requisitos europeos. La propuesta de actualización desarrollada en este trabajo demuestra que es necesario adoptar el criterio de **“Incidentes Significativos”**, alineado con NIS 2 y el Reglamento de Ejecución (UE) 2024/2690. La incorporación

de umbrales objetivos (como la indisponibilidad superior a 30 minutos para servicios en la nube o pérdidas financieras superiores a 500.000 euros), elimina la **discrecionalidad del operador y garantiza una seguridad jurídica que la guía anterior no ofrecía**.

8.3 Exigencia Operativa: Inmediatez y Continuidad.

La drástica **reducción de los plazos de notificación** (Alerta Temprana en 24 horas y Notificación del Incidente en 72 horas) obliga a las entidades a **automatizar sus procesos de detección**. Este trabajo concluye que la mera notificación técnica es insuficiente; por ello, se han incorporado en las propuestas de **plantillas de notificación (Anexo 1)**, como mecanismo de apoyo y consulta a la hora de recopilar la información necesaria para notificar el incidente.

8.4 ENS como marco de Ciberseguridad Nacional.

En el nuevo marco del APL, el ENS deja de ser solo una norma de cumplimiento para entidades de servicio Público, para convertirse en una referencia de cumplimiento de Ciberseguridad. El ENS convierte las obligaciones legales abstractas de la Directiva NIS 2 (el "qué") en controles técnicos precisos y auditables (el "cómo"). La propuesta de integrar los Perfiles de Cumplimiento Específicos (PCE), que nombra el APL, en la gestión de incidentes facilita la armonización entre el sector público y el privado haciendo que "hablen el mismo idioma", y permitiendo que la certificación en el ENS acredite automáticamente el cumplimiento de las medidas de gestión de riesgos exigidas por la ley.

8.5 Taxonomía Simplificada.

Se ha propuesto un **sistema en dos niveles**. Primero, identificar la Causa Raíz y luego la clasificación técnica, permite descartar el fallo natural, la intencionalidad maliciosa, error humano o de terceros y además reconocer incidentes recurrentes. Se trata de pasar de un **modelo de notificación** puramente técnico-reactivo a uno que **aporte inteligencia sobre las amenazas**.

8.6 Gestión de la Recurrencia y Amenazas Proactivas

Finalmente, se ha identificado una carencia crítica en el modelo vigente respecto a los ataques de bajo impacto, pero continuados. La inclusión de un **procedimiento para la gestión de "Incidentes Recurrentes"** (ventana de 6 meses) y la obligación de **notificar Ciberamenazas Significativas** a los usuarios, suponen un avance cualitativo. Esto permite **pasar de un modelo puramente reactivo a uno preventivo** y de defensa activa, donde la información compartida sirve **para proteger a la cadena de suministro** antes de que el incidente se materialice completamente.

La propuesta de actualización de la GNNGC presentada en este TFM constituye una necesidad estratégica inaplazable para adaptar el nivel de Ciberseguridad de España a la nueva realidad normativa europea y garantizar la soberanía de sus servicios esenciales. Ante la incertidumbre que genera este cambio legislativo, se propone un modelo de referencia claro y accesible que transforma la naturaleza de la notificación, dejando de ser un mero trámite administrativo para convertirse en el mecanismo fundamental de activación y respuesta ante crisis nacionales. Asimismo, se evidencia la necesidad de abandonar valoraciones subjetivas en favor de criterios objetivos que aporten seguridad jurídica a las empresas. En definitiva, se plantea una evolución desde un modelo reactivo hacia uno preventivo y de inteligencia compartida, capaz de anticiparse a las amenazas y proteger el tejido productivo mediante una coordinación centralizada y eficaz.

ANEXO 1 PLANTILLAS DE NOTIFICACIÓN

A. PLANTILLA DE ALERTA TEMPRANA

NOTIFICACIÓN DE ALERTA TEMPRANA	
Por favor, cumplimente este formulario con el mayor rigor y detalle posible.	
PREGUNTAS	DATOS
Fecha y hora de notificación	DD/MM/AAAA – hh:mm (UTC, formato 24 horas)
Información de contacto del Punto de Contacto	Información de contacto PoC (Al menos, nombre completo, correo electrónico y/o teléfono)
Denominación legal completa de la entidad afectada y código CNAE	Nombre de la entidad afectada y código CNAE ²³
Posible impacto transfronterizo	En caso de afectar a dos o más Estados miembros, indicar cuáles
Código de referencia	Código o número de incidente que identifica de forma única el evento reportado
Denuncia ante FCSE u otras autoridades	El hecho ha sido denunciado ante las FCSE u otra autoridad (Sí/No)
Tipo del incidente	Tipo de evento: Incidente significativo (Taxonomía)
Información sobre el impacto del incidente	Impacto en los sectores afectados
Estado del incidente	Información si el incidente está en curso al momento del informe
¿Es un incidente recurrente?	Información si el incidente es recurrente (≥2 veces en 6 meses)
¿El incidente se originó en un proveedor?	Indicar si el incidente proviene de un proveedor externo
Resumen de los hechos	Descripción cronológica de los hechos
Fecha y hora de conocimiento del evento	DD/MM/AAAA – hh:mm (UTC, formato 24 horas)
¿Qué medidas se planifican o se toman para recuperarse?	Acciones/medidas temporales tomadas o planificadas para recuperarse del incidente.
¿Cómo se reportó/descubrió el incidente?	Indicación de la fuente/canal inicial (por ejemplo, si el incidente fue reportado por el operador/proveedor o no)

¿Qué tipo de áreas funcionales y procesos de negocio se vieron afectados?	Indicación de las áreas funcionales y procesos empresariales afectados por el incidente, incluyendo productos y servicios.
¿Cuáles son los factores que hacen que el incidente sea significativo (por favor, elige todos los que se apliquen)	Información sobre cuál de los factores hace que el incidente sea significativo (si el incidente ha causado o es capaz de causar tales consecuencias)
Comunicación con otras autoridades	Si es así, indicar a cuáles. (FCSE, AEPD, etc)
¿Requiere soporte de su CSIRT de referencia o de las autoridades nacionales?	Indicar si requiere apoyo de autoridades nacionales o CSIRT de referencia

B. PLANTILLA DE NOTIFICACIÓN DE INCIDENTE SIGNIFICATIVO

NOTIFICACIÓN DE INCIDENTE SIGNIFICATIVO	
Por favor, cumplimente este formulario con el mayor rigor y detalle posible.	
PREGUNTAS	DATOS
Fecha de Notificación	Fecha de presentación DD/MM/AAAA
Información de contacto del Punto de Contacto	Información de punto de contacto PoC (Nombre completo, correo electrónico y/o teléfono).
Denominación legal completa de la entidad afectada y código CNAE	Nombre de la entidad afectada y código CNAE ²⁴
Posible impacto transfronterizo	En caso de afectar a dos o más Estados miembros, indicar cuáles
Código de referencia	Código o número de incidente que identifica de forma única el evento reportado
Tipología:	Tipo de incidente (según la taxonomía de la GNNGC)
Impacto del incidente	Impacto en los sectores afectados
Número estimado de usuarios afectados	Número de usuarios afectados, y si es posible, número por sector
Porcentaje de usuarios afectados	Porcentaje de afectados en relación con el número total de usuarios que utilizan el servicio afectado

por el incidente significativo	
Impacto reputacional	Información sobre el posible impacto reputacional a consecuencia del incidente
¿Afecta a la cadena de suministro?	Indicar si afecta a la cadena de suministro
¿El incidente procede de un proveedor de servicios?	Indicar si el incidente proviene de un proveedor externo
Fecha y hora en que la entidad ha tenido conocimiento del incidente significativo.	Fecha (DD/MM/AAAA) y hora (hh:mm, UTC formato 24 h) de la detección del incidente
Estado actual del incidente	○ Abierto: en fase de contención, de mitigación o recuperación. ○ Cerrado.
Resumen del incidente	Breve reseña del incidente y sus consecuencias
¿Es un incidente recurrente?	¿Se ha producido ≥ 2 veces en 6 meses, el mismo hecho o de la misma naturaleza?
¿Está relacionado con otro/s incidente/s?	De ser afirmativo, indicar cuáles (Indicar fechas, notificaciones y números asignados)
Indica cómo se reportó/descubrió el incidente	Fuente/canal inicial (por ejemplo, si el incidente fue reportado por el operador/proveedor o no)
Cronología del incidente	Establecer una cronología del incidente, desde que fue detectado, hasta que la fecha de este reporte.
Qué medidas se planifican o se han tomado para recuperarse	Acciones/medidas temporales tomadas o planificadas para recuperarse del incidente (incluida la activación de los planes de continuidad de negocio)
¿Qué servicios se han visto afectados?	Indicar las áreas funcionales y procesos operativos afectados por el incidente, incluyendo productos y servicios.
Vector de entrada	Si se conoce, indicar la/s vulnerabilidad/es explotadas
Indicadores de compromiso (IoC)	Indicar los IoC recopilados durante el incidente (IPs, dominios, hashes, TTP, etc.
Incidente tipo Ransomware	En caso de un incidente tipo <i>ransomware</i> , aportar información relevante sobre el tipo, si se contactó con los atacantes, si se realizó algún pago de rescate, si se obtuvo la “vacuna”, cualquier otra comunicación por parte de los actores, como chantajes o extorsiones sobre publicación de datos, etc.

¿Qué tipo de activos tecnológicos se vieron afectados?	Referenciar los activos tecnológicos afectados.
¿Cuáles son los factores que hacen que el incidente sea significativo?	Indicar cuál de los factores hace que el incidente sea significativo (si el incidente ha causado o es capaz de causar tales consecuencias)
Comunicación con otras autoridades	Si es así, indicar a cuáles. (FCSE, AEPD, etc)
¿Requiere soporte de su CSIRT de referencia o de las autoridades nacionales?	Indicar si se requiere apoyo de las autoridades nacionales o CSIRT de referencia

C. PLANTILLA DE NOTIFICACIÓN DE INFORME FINAL

NOTIFICACIÓN FINAL DE INCIDENTE SIGNIFICATIVO	
Por favor, cumplimente este formulario con el mayor rigor y detalle posible.	
PREGUNTAS	DATOS
Fecha de la notificación	Indicar la fecha de la primera notificación: DD/MM/AAAA
Datos de contacto	Datos del punto de contacto (al menos Nombre completo, correo electrónico y/o teléfono)
Tipo de Entidad	☐ Esencial ☐ Importante ☐ Otra
Denominación legal completa de la entidad afectada	Denominación legal y CNAE
Impacto transfronterizo	Indicar si ha tenido afectación en dos o más Estados Miembros de la UE
Número de referencia	Indicar el número identificador del incidente
Tipo de Incidente	Tipología conforme a la taxonomía de la GNNGC
Impacto en otros sectores	Indicar si ha tenido afectación en otros sectores
Número estimado de usuarios afectados	Número estimado de usuarios afectados
Porcentaje de usuarios afectados	Porcentaje de afectados sobre el total

Tiempo de indisponibilidad del servicio	Tiempo de indisponibilidad del servicio en minutos
Impacto reputacional	Indicar si ha habido daños reputacionales
Implicación en otros marcos regulatorios	Indicar si el incidente tiene implicación en otros marcos regulatorios (RGPD, DORA, CER, etc)
¿Es un incidente recurrente?	Señalar si este u otro de igual naturaleza se ha repetido dos o más veces en 6 meses
¿Está relacionado con otro/s incidente/s?	Indicar si existe relación con otros hechos, si es así señalar cuáles, fechas, notificaciones, números de referencia, o cualquier otro dato que pueda identificarlos
Aportar otra información relevante	Otra información relevante
¿Ha sido provocado por acciones maliciosas?	Indicar si se trata de actos deliberados y malintencionados
¿Las causas fueron por fallos en el proceso?	Indicar si se trata de un incidente por algún fallo o error
¿Hubo un incidente causado por un fallo o fallo del sistema (por favor, elige todos los que se aplican)	Fallo/fallo del sistema
¿Fue causado por errores humanos?	Si es así, describa cuáles
¿Fue un incidente causado por un evento externo?	Si es así, descríbalos
¿Tuvo origen en otra entidad?	Si es así, en cuál y cómo tuvo afectación en su entidad
Otra información relevante	Indique cualquier otra información que pudiera ser relevante
Resumen cronológico	Resuma cronológicamente todas las fases del incidente tras su análisis
Fecha y hora en que la entidad ha tenido conocimiento del incidente significativo.	DD/MM/AAAA; hh:mm (Horario UTC y formato 24 horas)
¿Cuándo se detectó el incidente (si es diferente al anterior), comenzó y cuándo verificó la información sobre el incidente?	Cronología (incluyendo el momento de descubrimiento del incidente y el tiempo de verificación del impacto reportado)

Información sobre la fecha y hora de la restauración de los servicios, actividades y/o operaciones afectadas por el incidente significativo	Fecha (DD/MM/AAAA) y hora (hh:mm, UTC) en que se han restaurado los servicios, actividades y/o operaciones
Qué medidas se planifican o se toman para recuperarse	Acciones/medidas temporales tomadas o planificadas para recuperarse del incidente (incluida la activación los planes de continuidad de negocio)
¿Hubo alguna acción de seguimiento	Acciones de seguimiento/medidas de recuperación
Describe las lecciones aprendidas, si las hay	Lecciones aprendidas
Indica cómo se reportó/descubrió el incidente	Indicar la fuente/canal inicial (por ejemplo, si el incidente fue reportado por el operador/proveedor o no)
Qué tipo de áreas funcionales y procesos de negocio se vieron afectados	Indicar de las áreas funcionales y procesos empresariales afectados por el incidente, incluyendo productos y servicios.
Vector de entrada	Si se conoce, indicar la/s vulnerabilidad/es explotadas
Indicadores de compromiso (IoC)	Indicar los IoC recopilados durante el incidente (IPs, dominios, hashes, TTP, etc.
Incidente tipo Ransomware	En caso de un incidente tipo <i>ransomware</i> , aportar información relevante sobre el tipo, si se contactó con los atacantes, si se realizó algún pago de rescate, si se obtuvo la “vacuna”, cualquier otra comunicación por parte de los actores, como chantajes o extorsiones sobre publicación de datos, etc.
¿Qué tipo de activos tecnológicos se vieron afectados?	Referenciar los activos tecnológicos afectados.
¿Cuáles son los factores que hacen que el incidente sea significativo	Indicar cuál de los factores hace que el incidente sea significativo (si el incidente ha causado o es capaz de causar tales consecuencias)
Si se explotó una vulnerabilidad conocida	Información sobre vulnerabilidades explotadas:
Pérdidas de datos	Tipo de pérdidas de datos que conlleva el incidente significativo en relación con la disponibilidad, autenticidad, integridad y confidencialidad de los datos.
Descripción de las pérdidas de datos	Descripción del impacto del incidente en la disponibilidad, autenticidad, integridad y confidencialidad de los datos críticos.

Magnitud del impacto en la sociedad, evaluando el impacto global en España	Valore la magnitud del impacto del incidente
Indica si el incidente fue reportado a otras autoridades	Si es así, indicar a cuáles. (FCSE, AEPD, etc)
¿Requiere soporte de su CSIRT de referencia o de las autoridades nacionales?	Indicar si se requiere apoyo de las autoridades nacionales o CSIRT de referencia

9 BIBLIOGRAFÍA

- [1] Unión Internacional de Telecomunicaciones (UIT), «Global Cybersecurity Index,» Ginebra, Suiza, 2024.
- [2] Jefatura del Estado, «Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información,» Boletín Oficial del Estado, 2018.
- [3] Parlamento Europeo y del Consejo, «Directiva (UE) 2022/2555, relativa a medidas para un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS 2),» Diario Oficial de la Unión Europea, 2022.
- [4] Parlamento Europeo y Consejo de la Unión Europea, «Directiva (UE) 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS 2),» Diario Oficial de la Unión Europea, 2022.
- [5] Unión Internacional de Telecomunicaciones (UIT), «X.1205: Aspectos generales de la ciberseguridad,» UIT-T, 2008.
- [6] Ministerio del Interior, «Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad,» Madrid, España, 2025.
- [7] Parlamento Europeo y Consejo de la Unión Europea, «Reglamento (UE) 2019/881 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad,» Diario Oficial de la Unión Europea, 2019.
- [8] ISO/IEC, «ISO/IEC 27000:2018 Information technology; Security techniques; Information security management systems; Overview and vocabulary,» ISO/IEC, 2018.
- [9] Agencia de la Unión Europea para la Ciberseguridad (ENISA), «ENISA Threat Landscape 2024,» Atenas, Grecia, 2024.
- [10] Agencia de la Unión Europea para la Ciberseguridad (ENISA), «Technical Guideline on Incident Reporting under the EEC,» Atenas, Grecia, 2021.
- [11] Comisión europea, «European Cybersecurity Competence Centre (ECCC),» [En línea]. Available: https://cybersecurity-centre.europa.eu/index_en?. [Último acceso: 14 noviembre 2025].
- [12] Comisión europea, «ec.europa.eu,» 16 diciembre 2020. [En línea]. Available: <https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-strategy>.
- [13] Consejo de Seguridad Nacional, «Estrategia Nacional de Ciberseguridad 2019,» 2019.
- [14] Departamento de Seguridad Nacional, «dsn.gob.es,» 12 abril 2019. [En línea]. Available: <https://www.dsn.gob.es/sites/default/files/documents/Estrategia%20Nacional%20de%20Ciberseguridad%202019.pdf?>.
- [15] Ministerio del Interior, «Anteproyecto de Ley de Protección y Resiliencia de Entidades Críticas,» Madrid, España, 2025.
- [16] Jefatura de Estado, «Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad,» Boletín Oficial del Estado, 2022.

- [17] Jefatura del Estado, «Ley 11/2022, de 28 de junio, General de Telecomunicaciones,» Boletín Oficial del Estado., 2022.
- [18] Agencia de la Unión Europea para la Ciberseguridad (ENISA), «About ENISA - What we do,» 2025. [En línea]. Available: <https://www.enisa.europa.eu/about-enisa/what-we-do>. [Último acceso: noviembre 2025].
- [19] CERT-EU, «About us - Computer Emergency Response Team for the EU Institutions,» 2025. [En línea]. Available: <https://cert.europa.eu/about-us>. [Último acceso: noviembre 2025].
- [20] CSIRTs Networks, «CSIRTs Network platform,» 2016. [En línea]. Available: <https://csirtsnetwork.eu/>. [Último acceso: noviembre 2025].
- [21] Comisión Europea, «NIS Cooperation Group,» 1 agosto 2025. [En línea]. Available: <https://digital-strategy.ec.europa.eu/es/policies/nis-cooperation-group>. [Último acceso: noviembre 2025].
- [22] European Cybersecurity Competence Centre (ECCC), «Home Page,» [En línea]. Available: https://cybersecurity-centre.europa.eu/index_en?prefLang=es. [Último acceso: noviembre 2025].
- [23] Europol, «European Cybercrime Centre (EC3),» 2025. [En línea]. Available: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>. [Último acceso: noviembre 2025].
- [24] Agencia de la Unión Europea para la Ciberseguridad (ENISA), «EU-CyCLONe (European Cyber Crisis Liaison Organisation Network),» 16 enero 2023. [En línea]. Available: <https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone>. [Último acceso: noviembre 2025].
- [25] Departamento de Seguridad Nacional (DSN), «El Consejo de Seguridad Nacional,» 2024. [En línea]. Available: <https://www.dsn.gob.es/es/estructuras-de-seguridad-nacional/el-consejo-de-seguridad-nacional>. [Último acceso: noviembre 2025].
- [26] Departamento de Seguridad Nacional (DSN), «El Consejo de Seguridad Nacional,» 2024. [En línea]. Available: <https://www.dsn.gob.es/es/estructuras-de-seguridad-nacional/comites-especializados/comite-de-situacion>. [Último acceso: noviembre 2025].
- [27] Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, «Diplomacia Pública Digital,» s.f. [En línea]. Available: <https://www.exteriores.gob.es/es/PoliticaExterior/Paginas/DiplomaciaPublicaDigital.aspx>. [Último acceso: noviembre 2025].
- [28] Centro Criptológico Nacional (CCN), «Quiénes somos / Funciones,» [En línea]. Available: <https://www.ccn.cni.es/index.php/es/menu-ccn-es>. [Último acceso: noviembre 2025].
- [29] Estado Mayor de la Defensa, «Mando Conjunto del Ciberespacio (MCCE),» [En línea]. Available: <https://emad.defensa.gob.es/unidades/mcce/>. [Último acceso: noviembre 2025].
- [30] CCN-CERT, «Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional,» 2025. [En línea]. Available: <https://www.ccn-cert.cni.es/>. [Último acceso: noviembre 2025].
- [31] INCIBE-CERT, «Centro de Respuesta a Incidentes de Seguridad del INCIBE,» [En línea]. Available: <https://www.incibe.es/incibe-cert>. [Último acceso: noviembre 2025].
- [32] Parlamento Europeo, Estrategia de Ciberseguridad de la UE para la Década Digital, 2020.

- [33] Parlamento Europeo y Consejo de la Unión Europea, «Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión,» Diario Oficial de la Unión Europea, 2016.
- [34] Unión Europea, «NIS2,» DOUE, 2022.
- [35] Parlamento Europeo y Consejo, REGLAMENTO (UE) 2022/2554, DOUE, 2022.
- [36] Parlamento Europeo y Consejo de la Unión Europea, «Directiva (UE) 2022/2557 relativa a la resiliencia de las entidades críticas (Directiva CER),» Diario Oficial de la Unión Europea, 2022.
- [37] Consejo Nacional de Ciberseguridad, «Guía Nacional de Notificación y Gestión de Ciberincidentes,» Madrid, 2020.
- [38] Centre for Cybersecurity Belgium (CCB), «NIS2 Notification guide Belgium,» Bruselas, Bélgica, 2024.
- [39] Agencia de la Unión Europea para la Ciberseguridad (ENISA), «NIS2 Technical Implementation Guidance,» Atenas, Grecia, 2025.
- [40] Comisión Europea, «Reglamento de Ejecución (UE) 2024/2690 de la Comisión de 17 de octubre de 2024 por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gest,» Diario Oficial de la Unión Europea, 2024.
- [41] Jefatura del Estado, Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, Boletín Oficial del Estado, núm. 106, 2022.
- [42] Comisión Europea, «Reglamento de Ejecución (UE) 2024/2690 de la Comisión,» 2024.
- [43] Jefatura del Estado, «Ley 9/2014, de 9 de mayo, General de Telecomunicaciones,» Boletín Oficial del Estado, núm. 114, 2014.
- [44] National Institute of Standards and Technology (NIST), «Ransomware Protection and Response,» 27 septiembre 2021. [En línea]. Available: <https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware>. [Último acceso: septiembre 2025].
- [45] Agencia de la Unión Europea para la Ciberseguridad (ENISA), «Distributed Denial of Service,» ENISA Threat Landscape, 2019.
- [46] Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (PNNSC), «Formulario de reporte de incidentes,» 2025. [En línea]. Available: <https://www.plataformanacionalciber.gob.es/index.php/incidentes?view=incidents>. [Último acceso: diciembre 2025].
- [47] E. García, «Qué es un Playbook en Ciberseguridad,» 2 julio 2025. [En línea]. Available: <https://es.linkedin.com/pulse/qu%C3%A9-es-un-playbook-en-ciberseguridad-edward-garcia-k0qje>. [Último acceso: octubre 2025].
- [48] Tribunal de Cuentas Europeo, «Dictamen 02/2023 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen medidas para reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para e,» 2023.

- [49] Parlamento Europeo, «Understanding the EU's approach to cyber diplomacy and cyberdefence,» 2020.