Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

guía sobre la notificación de incidentes de ciberseguridad

índice

El informe *Guía sobre la notificación de incidentes de Ciberseguridad* ha sido elaborado por la empresa EY para el Observatorio Nacional de Tecnología y Sociedad. La información contenida en la presente publicación es responsabilidad exclusiva de sus autores. El Ontsi no garantiza la exactitud de los datos incluidos en este estudio y, por tanto, no podrá ser considerado responsable del uso que pueda hacerse de la información aquí recogida. La normativa a la que hace referencia este informe es la vigente a marzo de 2026.

Guía sobre la noti icación de incidentes de Ciberseguridad. Observatorio Nacional de Tecnología y Sociedad. Red.es. Secretaría de Estado de Digitalización e Inteligencia Arti icial. Ministerio para la Transformación Digital y de la Función Pública.

Reservados todos los derechos. Se permite su copia y distribución por cualquier medio siempre que se mantenga el reconocimiento de sus autores, no se haga uso comercial de las obras y no se realice ninguna modi icación de las obras.

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

red.es · ontsi · observa ciber.es · incibe_ · Plan de Recuperación, Transformación y Resiliencia

01

Resumen ejecutivo

El Ontsi publica la *Guía sobre la notificación de incidentes de Ciberseguridad*. Se trata de ofrecer un marco integral que ayude a las organizaciones y ciudadanía en España a gestionar de manera efectiva los incidentes de ciberseguridad. Es un tema que ha cobrado una importancia crítica en el contexto actual, donde la digitalización y la interconexión de sistemas han aumentado la exposición a riesgos de ciberseguridad.

En el año 2023, España registra más de 83.000 incidentes de ciberseguridad, lo que representa un aumento del 24% en comparación con el año anterior. Este incremento no solo pone de manifiesto la creciente frecuencia de los incidentes de ciberseguridad, sino que también subraya la necesidad urgente de establecer un sistema de informes que permita a las organizaciones abordar de manera sistemática las amenazas y vulnerabilidades que enfrentan.

La guía enfatiza que la respuesta rápida y la gestión adecuada de las crisis son fundamentales para mitigar los efectos de los incidentes de ciberseguridad, que comúnmente incluyen técnicas como el *phishing* (suplantación de identidad mediante correos o mensajes fraudulentos para obtener información sensible), el ransomware (secuestro de datos) y los ataques de denegación de servicio *DDoS*, por sus siglas en inglés, *Distributed Denial of Service*.

Estos tipos de ataques no solo pueden causar pérdidas financieras significativas, sino que también pueden dañar la reputación de las organizaciones y afectar la confianza de los clientes y socios.

Uno de los temas clave que trata la guía es la legislación vigente, en particular la Directiva NIS2, que establece un marco legal que obliga a las entidades responsables de infraestructuras críticas a reportar incidentes de ciberseguridad. Como parte de la estrategia de ciberseguridad de la UE, su objetivo es fortalecer la resiliencia de estas infraestructuras y garantizar un alto nivel de protección en todos los Estados miembros.

Además, se destaca el Anteproyecto de ley en desarrollo para adaptar la Directiva NIS2 al marco normativo nacional.

La guía también aborda la identificación y clasificación de incidentes, así como los procedimientos para su notificación tanto interna como externa. Se subraya la importancia de una comunicación efectiva con las autoridades y las partes involucradas, asegurando el cumplimiento de normativas como la NIS2, que regula la notificación de incidentes en infraestructuras críticas.

Además, se trata el concepto de ventanilla única, un sistema diseñado para unificar el proceso de notificación de incidentes. Este enfoque busca mejorar la comunicación y la coordinación entre las diferentes entidades involucradas en la gestión de incidentes de ciberseguridad, lo que es esencial para garantizar una respuesta rápida y efectiva.

La ventanilla única permite a las organizaciones notificar incidentes de manera centralizada, lo que facilita la recopilación de información y la colaboración entre las distintas partes interesadas, incluyendo organismos gubernamentales, agencias de seguridad y empresas privadas.

Asimismo, se muestran procedimientos de notificación específicos que las organizaciones españolas deben seguir, lo que facilita una respuesta más efectiva ante situaciones de crisis. Estos incluyen la identificación de los incidentes, la evaluación de su impacto y la comunicación de la información relevante a las

partes interesadas. La claridad en estos procedimientos es fundamental para asegurar que las organizaciones puedan actuar de manera rápida y eficiente en caso de un incidente de ciberseguridad.

Finalmente, la guía refleja el interés que tiene la UE por mejorar la cooperación entre miembros. La colaboración, a través de legislaciones comunes y simulacros de crisis, es esencial para fortalecer las infraestructuras de ciberseguridad en toda la región. Esta guía resalta el interés de que se adopte un enfoque proactivo en la gestión de los incidentes de ciberseguridad.

En resumen, este documento busca unificar las distintas normativas, tanto de España como de la Unión Europea, a la hora de notificar los incidentes de ciberseguridad.

02

Introducción y contexto

Este informe tiene como propósito explicar y detallar, de manera clara y accesible, cómo deben gestionarse y cuál es el proceso para reportar los incidentes de ciberseguridad, con la vista puesta tanto las normativas nacionales como internacionales.
Los reportes de incidentes de ciberseguridad son documentos esenciales que ofrecen información detallada sobre amenazas, vulnerabilidades y ataques que pueden impactar tanto a organizaciones, personas, infraestructuras críticas o servicios esenciales.

La gestión de estos incidentes sigue un plan estructurado mediante el cual, a través de una serie de pasos definidos, se identifican, responden, analizan y mitigan los efectos de cada uno de ellos, asegurando así una respuesta eficiente y eficaz.

Contexto

En 2023 España experimenta un notable incremento en incidentes de ciberseguridad, especialmente en sectores como el bancario y el público, con amenazas como el *phishing* y los ataques *DDoS*[III]. Cabe destacar que los datos utilizados en este informe provienen de varios documentos tanto nacionales como internacionales. Los informes nacionales son de carácter anual, publicados en 2024, que recogen los datos de enero a diciembre del 2023.

Los informes internacionales, en cambio, recogen normalmente los datos comprendidos entre julio de 2023 a junio de 2024.

A nivel europeo, los ataques de *ransomware*[IV] a sectores críticos como la energía y la salud han sido más comunes. Este panorama resalta la urgencia de fortalecer las defensas de ciberseguridad y mejorar la coordinación regional para hacer frente a las amenazas crecientes y garantizar la seguridad digital.

Situación actual de incidentes de ciberseguridad en España

Incremento de incidentes de ciberseguridad en 2023

La ciberseguridad en España se enfrenta a un desafío creciente, con un aumento significativo en el número de incidentes gestionados. El Instituto Nacional de Ciberseguridad (INCIBE) reporta la gestión de 83.517 incidentes en 2023, lo que representa un incremento del 24% respecto al año anterior. Este crecimiento prueba la intensificación de las amenazas de ciberseguridad y subraya la necesidad de fortalecer las defensas en todos los sectores[1].

En 2024 reportó 97.348 incidentes de seguridad, un 16,6% más que en 2023 y en 2025 reportó 122.223 incidentes de ciberseguridad, un 26% más que el año anterior.

Impacto en ciudadanos y empresas

En 2023, España enfrentó un panorama muy preocupante en materia de ciberseguridad, con un número significativo de incidentes que afectaron tanto a ciudadanos como a empresas. Más de 58.000 incidentes de ciberseguridad impactaron a individuos, exponiéndolos a amenazas como suplantación de identidad, ciberacoso y fraudes en línea, situación que se agravó en 2024 al aumentar los individuos afectados hasta 65.808, lo que supone un 12,1% más. En el ámbito empresarial, se registraron más

de 22.000 incidentes en 2023 y hasta 31.540 en 2024, que comprometieron a pymes, micropymes y autónomos, poniendo en peligro la continuidad de sus operaciones.[1]

Asimismo, en 2023 se identificaron 183.077 sistemas vulnerables en todo el país, cifra que se mantuvo prácticamente estable en 2024 con 183.851 sistemas, pero que aumentó de forma significativa en 2025 hasta alcanzar los 237.028 sistemas vulnerables, lo que evidencia la necesidad de adoptar medidas proactivas para proteger las infraestructuras críticas.

Estos datos subrayan la urgencia e importancia de fortalecer las defensas de ciberseguridad y fomentar la concienciación en todos los niveles de la sociedad.[2]

Por otro lado, al analizar los incidentes reportados en función de su tipo, según los últimos datos disponibles de Eurostat (2019) se observa que el 3% de población en España sufre un uso fraudulento de sus tarjetas de crédito o débito.
Y resulta por ello el sexto país más afectado de Europa. Además, el 1% fue víctima de robo de identidad al realizar compras en línea, ocupando el séptimo lugar en Europa en cuanto a este tipo de incidentes.

El 19% de la ciudadanía recibe mensajes de *phishing*, lo que coloca a España como el decimotercer país más afectado de Europa. Finalmente, el 17% sufre ataques de *pharming*[VI], donde fueron redirigidos a páginas web falsas diseñadas para robar información personal; fue el tercer país europeo más afectado por este tipo de ataque[3].

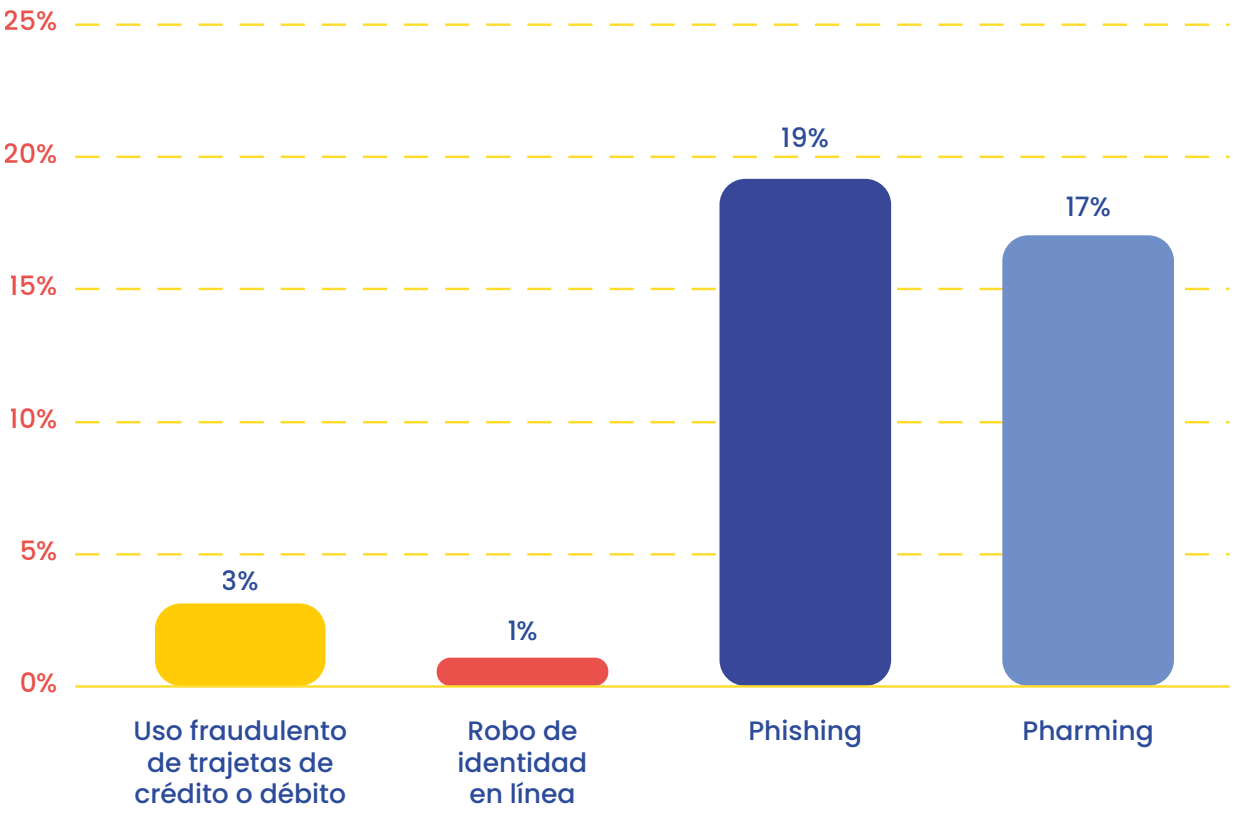


Figura 1
Porcentaje de individuos que han sufrido incidentes de ciberseguridad en el año 2019[3]

[1] INCIBE_Infografía_Balance de ciberseguridad 2023.
[2] Balance de Ciberseguridad relativo al año 2023 de INCIBE.
[3] Base de Datos Eurostat *Security related problems experienced when using the Internet*.

Por otro lado, según otra estadística de Eurostat de 2024, alrededor del 15% de las empresas españolas ha sufrido algún tipo de ataque, lo que coloca a España en el puesto 21 de Europa y el 17 de la Unión Europea.[4]

Además, según datos de la encuesta del INE sobre *Seguridad TIC*, donde se muestran los datos de las pymes españolas del primer trimestre de 2022, el 5,2% de las pymes en España se enfrentó a algún tipo de incidente. Dentro de la misma estadística, se detalla que un 25% de esas empresas vio interrumpidos sus servicios TIC debido a ataques externos. Asimismo, se podría destacar que el 23% de las empresas afectadas sufrió una destrucción o corrupción de datos como consecuencia de un ataque. Por otro lado, un 11% reportó que un tercero divulgó información confidencial, mientras que un 8% señaló que la filtración provino de sus propios empleados.

En comparación, los datos del primer trimestre de 2024 muestran que el 4,57% de las pymes declaró haber sufrido algún incidente de seguridad TIC, siendo el 18,85% de estos debido a ataques externos, mientras que se observa un aumento en los incidentes relacionados con la destrucción o corrupción de datos (28,79%), así como en los casos de divulgación de información por terceros (8,94%), manteniéndose estable el porcentaje de incidentes causados por empleados internos (5,12%).

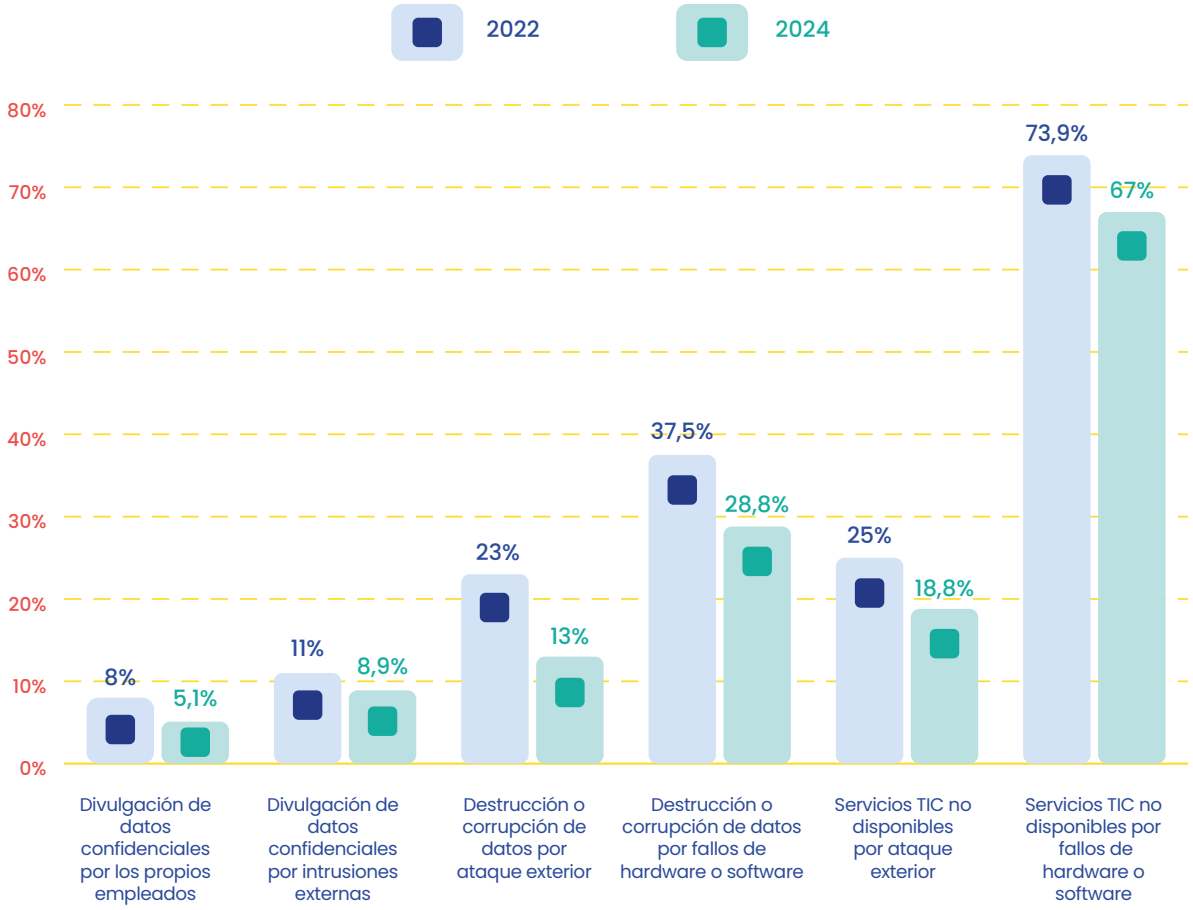


Figura 2
Distribución porcentual de los incidentes sufridos por pymes españolas en el primer trimestre de 2022 y 2024[5]

[4] Base de Datos Eurostat *Security incidents and consequences by size class of enterprise.*
[5] Base de Datos INE *Seguridad TIC* (2022 y 2024).

Principales amenazas detectadas[6]

En 2023, surgieron amenazas de ciberseguridad que afectan tanto a la ciudadanía como a empresas y organismos gubernamentales. Entre las principales se encuentran los ataques de *ransomware*, que causaron interrupciones operativas graves y pérdidas económicas significativas. Los rescates exigidos por los y las atacantes variaron desde miles hasta millones de euros, y afectaron a la capacidad de las organizaciones para recuperarse rápidamente.

Los ataques *DDoS* también fueron destacables. Por ejemplo, en octubre de 2022, Ziyaettin lanza ataques *DDoS* contra sitios de alta relevancia, como el Banco de España y La Moncloa, a través de servicios *botnet*[VIII] avanzados. Además, el grupo *hacktivista*[IX] prorruso NoName057(16) atacó al Ministerio de Defensa en represalia por decisiones políticas relacionadas con el conflicto en Ucrania.

Otro hecho destacable sería el compromiso de las infraestructuras críticas[X]. Por ejemplo, en diciembre de 2022, la red interna del Punto Neutro Judicial (PNJ) fue comprometida, y expuso bases de datos sensibles[XI] y permitió actividades de blanqueo de capitales. Por suerte, este incidente llevó a la detención de un presunto responsable en marzo de 2023.

Las campañas de *phishing* y suplantación bancaria también han sido frecuentes. Durante 2023, se registran múltiples campañas dirigidas al sector financiero, siendo los bancos más suplantados el Santander, BBVA y Sabadell. Este tipo de campañas se usan para recopilar información sensible de las personas usuarias.

Hay que destacar que Telegram se consolida como una herramienta clave para actividades ilícitas, donde se facilita la venta de datos, el alquiler de servicios de ataque y el fraude bancario. Su anonimato y accesibilidad lo convierten en una plataforma perfecta para ciberdelincuentes[XII].

A su vez, en 2023, múltiples entidades y organizaciones españolas sufrieron fugas de información[XIII], principalmente filtraciones de bases de datos con información confidencial tanto de clientes como de trabajadores. Los sectores más afectados fueron el gubernamental y el educativo.

El *hacktivismo* (activismo *hacker*) también tuvo un impacto notable. El grupo NoName057(16) fue el que más atacó a España durante 2023; dirigió sus ataques a empresas públicas y privadas de transportes y logística terrestre, marítimo y aéreo, organismos gubernamentales, entidades bancarias y financieras, y compañías de telecomunicaciones.

Impacto en Sectores Críticos

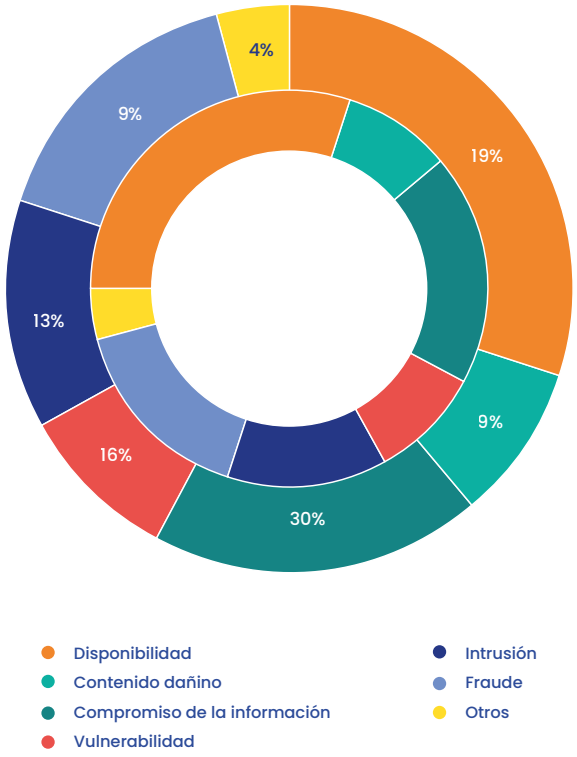
En el año 2023, los sectores esenciales en España estuvieron bajo una gran presión debido al aumento de incidentes de ciberseguridad.

Se registraron 237 ataques dirigidos a empresas de servicios críticos, lo que deja a relucir la vulnerabilidad de estas infraestructuras clave. De los cuales se han gestionado un total de noventa (90) incidentes7 con niveles de peligrosidad e impacto alto, muy alto o crítico en base a lo definido en el Real Decreto 43/2021, del 26 de enero. Esto implica un aumento del 23% con respecto al año anterior.

Analizando la tipología de incidentes más común, este fue del tipo Disponibilidad, siendo un 30% sobre el total de incidentes seguido de los incidentes del tipo Compromiso de la Información con un 19%.[7]

[6] CCN-CERT-IA-04-24_Ciberamenazas_y_Tendencias_2024
[7] Informe sobre la Cibercriminalidad en España 2023. Ministerio del Interior – Secretaría de Estado de Seguridad.

Figura 3
Tipos de incidentes gestionados para Operadores Críticos[7]



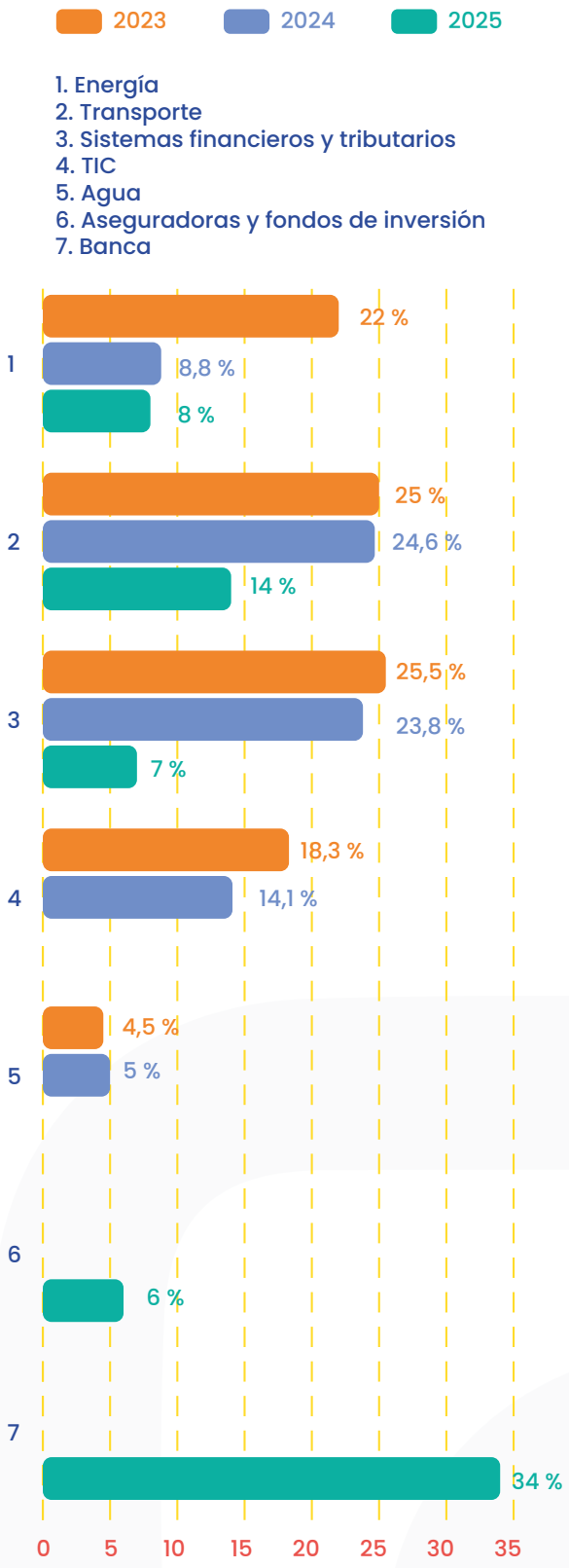
En 2023, entre los sectores más afectados por incidentes de ciberseguridad destacaron el transporte, que concentró el 25% de los casos, seguido de los sistemas financieros y tributarios con un 25,42%, el sector energético con un 22,08%, las tecnologías de la información y las comunicaciones (TIC) con un 18,33%, y el sector del agua, que supuso el 4,58% de los incidentes; en 2024, el transporte siguió siendo el sector más afectado (24,6%), seguido de los sistemas financieros y tributarios (23,8%), las TIC (14,1%), el sector energético (8,8%) y el sector del agua (5,0%); mientras que en 2025 se observa un cambio en la distribución, con la mayor incidencia en el sector bancario (34%), seguido del transporte (14%), la energía (8%), la infraestructura de los mercados financieros (7%) y el sector de aseguradoras y fondos de pensiones (6%).[8]

La interrupción de servicios en estos sectores puede tener consecuencias serias, afectando aspectos tan fundamentales como el suministro de energía y agua, la movilidad o incluso la estabilidad financiera del país.

Estos datos resaltan la necesidad de fortalecer la ciberseguridad en las infraestructuras críticas, para protegerlas y garantizar su capacidad de resistir futuras amenazas.

[8] Balance de INCIBE 2023, 2024 y 2025.

Figura 4
Sectores más afectados por incidentes de ciberseguridad[8]



[8] Balance de INCIBE 2023, 2024 y 2025.

Consultas ciudadanas y formación en ciberseguridad

En 2023, el servicio público *Tu Ayuda en Ciberseguridad*[XIV] atendió 80.920 consultas, lo que representa un aumento del 17% respecto al año anterior, de las cuales el 56% tuvieron un carácter preventivo y el resto estuvieron orientadas a la resolución de incidentes ya ocurridos, tendencia que aumentó en 2024, con 98.546 consultas (+21,8%), y especialmente en 2025, cuando se alcanzaron las 142.767 consultas, lo que representa un incremento del 45%, reflejando un aumento sostenido tanto de la concienciación como de la demanda de asistencia en materia de ciberseguridad.

En 2023, los problemas más comunes que reportaron los ciudadanos fueron el *phishing*, que representó aproximadamente 3 de cada 10 consultas, seguido de la suplantación de identidad (12%), el ciberacoso (11%) y las compras fraudulentas, que necesitaron más de 5.300 consultas de asesoramiento. En el año 2024, esta distribución se mantuvo con un 33% de consultas relacionadas con *phishing*, un 14% con suplantación de identidad, un 5,9% con ciberacoso y un 8% con compras fraudulentas y, por último, en 2025 se observó una reducción del *phishing* (28%), estabilidad en la suplantación de identidad (14%) y el ciberacoso (5%), junto con un incremento significativo de las compras fraudulentas, que alcanzaron el 16% de las consultas.

Además de atender consultas, el Instituto Nacional de Ciberseguridad (INCIBE) se enfoca en la formación en buenas prácticas de ciberseguridad. A través de iniciativas como el *CyberCamp*[XV] y el *Cybersecurity Summer Bootcamp*[XVI], en 2023 el INCIBE formó a 117.000 personas, promoviendo una mayor conciencia y preparación frente a las amenazas de ciberseguridad. Estas iniciativas son fundamentales para fortalecer la ciberseguridad a escala individual y colectivo, y para capacitar a la población en la adopción de medidas preventivas y de respuesta ante posibles incidentes.

Situación actual de incidentes de ciberseguridad en Europa

Incremento de las amenazas de ciberseguridad

Entre julio de 2023 y junio de 2024, Europa vive un notable aumento en los incidentes de ciberseguridad, y refleja cómo los atacantes se vuelven cada vez más sofisticados y capaces de aprovechar vulnerabilidades tanto en infraestructuras críticas como en sistemas privados. Según la Agencia de la Unión Europea para la Ciberseguridad (ENISA), se ha producido un aumento de los incidentes en un 50% durante los primeros seis meses de 2024 en comparación con la segunda mitad de 2023, con 1.000 casos más registrados en ese período.

Impacto en ciudadanos y empresas

En 2023, los ciudadanos de países como Alemania, Francia e Italia se vieron gravemente afectados por incidentes de ciberseguridad centrados en la suplantación de identidad, fraudes financieros y *ransomware*. Estos ataques comprometieron la seguridad de millones de usuarios, exponiéndolos a pérdidas económicas y a la violación de su privacidad. En los años 2024 y 2025 los países continuaron viéndose significativamente afectados por incidentes de ciberseguridad, destacando el phishing como principal vector de intrusión, junto con el *ransomware* y otras formas de cibercriminalidad con motivación económica, que derivaron en filtraciones de datos, fraudes financieros y vulneraciones de la privacidad.[9]

En el ámbito empresarial, las pequeñas y medianas empresas fueron especialmente vulnerables debido a sus defensas menos sofisticadas. Sectores como la manufactura, la banca y la salud están entre los más afectados, enfrentando interrupciones operativas y pérdidas financieras significativas. La falta de recursos y la menor capacidad para implementar medidas de ciberseguridad robustas hicieron que estas empresas fueran objetivos clave para los ciberdelincuentes.[10]

[9] ENISA *Threat Landscape 2024*
[10] ENISA *Threat Landscape 2025*

Además, Europa registró un aumento en el número de sistemas expuestos y vulnerables, especialmente en infraestructuras críticas como redes de energía y transporte. Estas infraestructuras aún son objetivos prioritarios tanto para actores estatales como no estatales, lo que subraya la necesidad urgente de reforzar las defensas de ciberseguridad para proteger estos sistemas vitales y garantizar la seguridad y estabilidad de la región.[11]

Por otro lado, al desglosar los incidentes reportados por tipo de incidente se encuentra una base de datos de Eurostat publicada en 2019, donde se puede ver que el país que más uso fraudulento de sus tarjetas de crédito o débito sufrió fue Dinamarca, mientras que el que menos fue Irlanda.

Además, el país con más robo de identidad en línea fue Malta, y el que menos Bulgaria. Además, el país donde más *phishings* recibieron sus habitantes fue Dinamarca, y el que menos, Lituania. Y, por último, Malta fue el país que sufrió más pharming mientras que Bulgaria el que menos.[12]

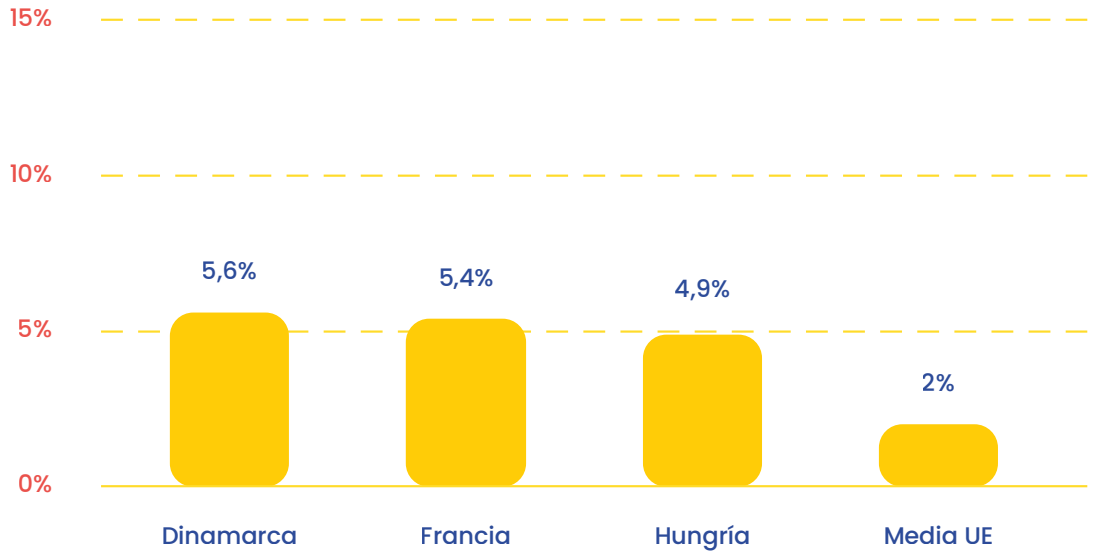


Figura 5
Porcentaje de individuos que han sufrido un uso fraudulento de la tarjeta de crédito[12]

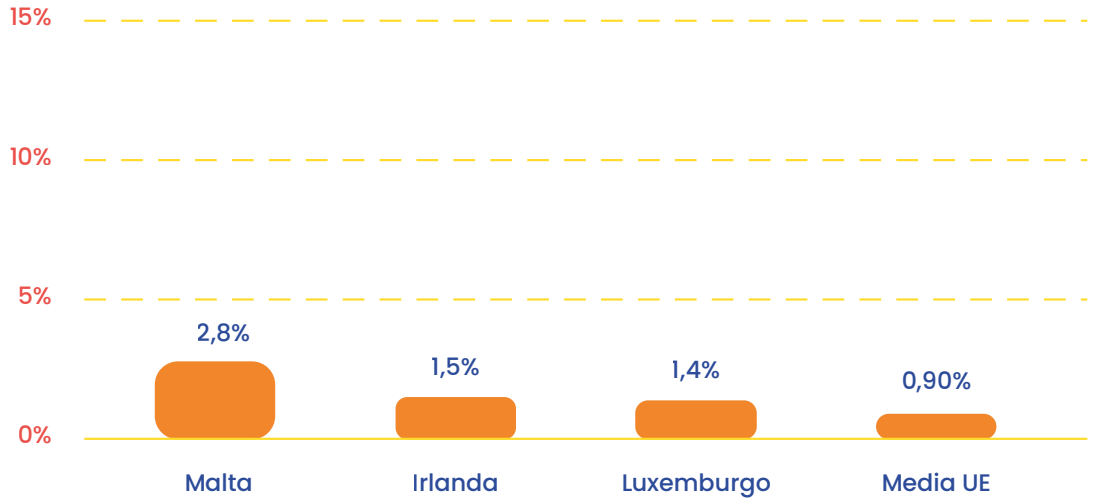


Figura 6
Porcentaje de individuos que han sufrido robo de identidad *online*[12]

[11] ENISA *Threat Landscape 2024*
[12] Eurostat de la base de datos *Security incidents and consequences by size class of enterprise.*

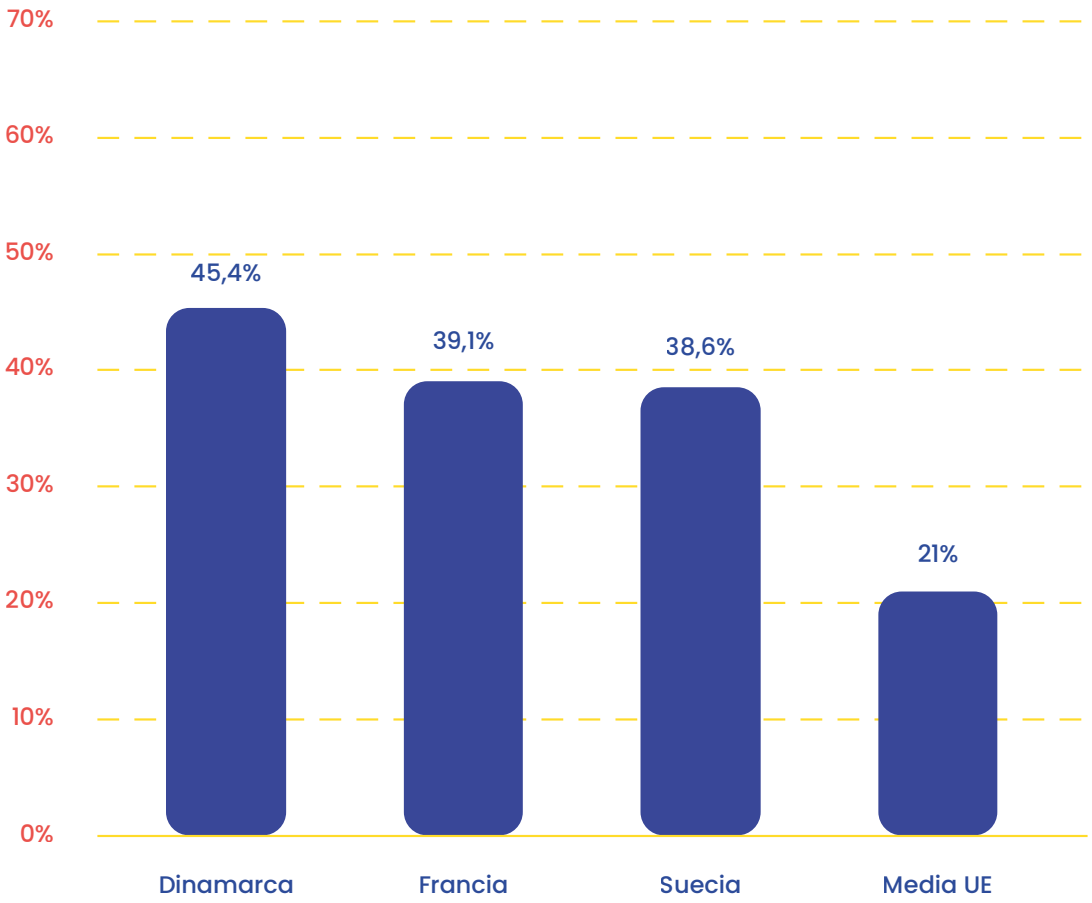


Figura 7
Porcentaje de individuos que han sufrido *phishing*[12]

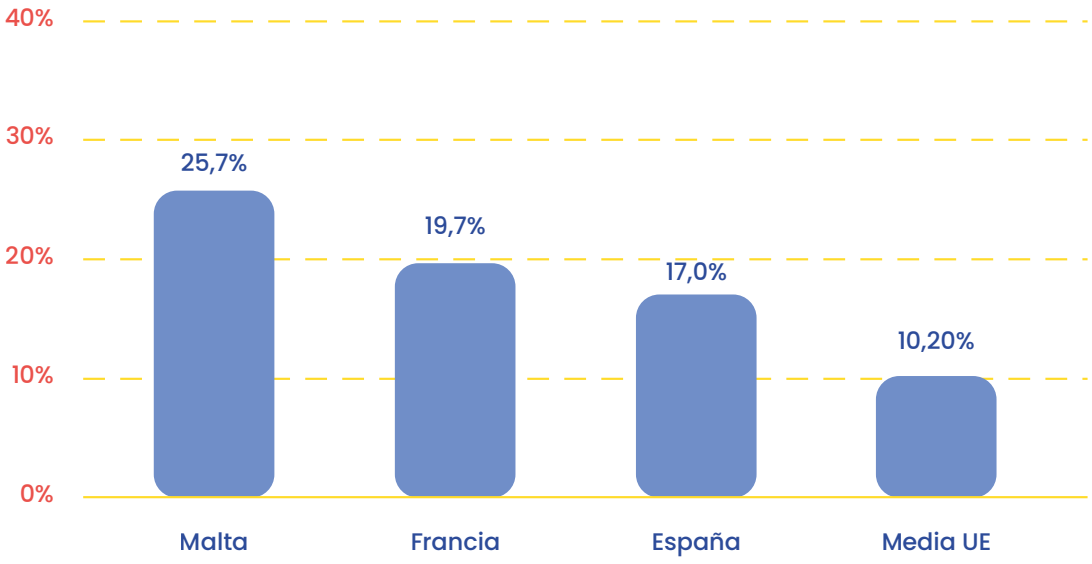


Figura 8
Porcentaje de individuos que han sufrido *pharming*[12]

[12] Eurostat de la base de datos *Security incidents and consequences by size class of enterprise.*

Por otro lado, en una estadística de Eurostat de 2024, se observa que el país en el que más incidentes han recibido las empresas es Finlandia con un 41%, mientras el país que menos ha sufrido ha sido Austria con un 11,2%[12].

Principales amenazas detectadas[13]

En 2023, el *ransomware* mantiene como una de las principales amenazas en Europa. Grupos como LockBit y Hive atacaron sistemas de gobiernos y grandes empresas, causando interrupciones importantes en servicios esenciales como la salud y el transporte en países como Francia y Alemania. Estos ataques, que bloqueaban el acceso a los datos y exigían rescates a cambio, generaron graves problemas operativos en estos sectores.

Las infraestructuras críticas también han estado en el punto de mira. En Alemania, varios ataques afectaron los sistemas ferroviarios, y causaron retrasos y pérdidas económicas. En Italia, el sector energético sufrió un incidente de ciberseguridad que expuso datos sensibles de clientes y complicó la operación de proveedores clave, dejando en evidencia la fragilidad de estas infraestructuras esenciales.

Los gobiernos europeos tampoco se salvan. Los incidentes de ciberseguridad contra redes gubernamentales aumentan. Algunos ataques están incluso vinculados a actores respaldados por Estados. Además, las campañas de desinformación[XVII], muchas de ellas a través de redes sociales y plataformas como Telegram, se utilizaron para influir en elecciones y sembrar desconfianza entre la población, intensificando la inestabilidad política y social.

Por otro lado, los servicios financieros enfrentan un impactante incremento en ataques de *phishing*. En países como los Países Bajos, Suecia y Bélgica, los delincuentes usan técnicas avanzadas, como correos electrónicos falsificados y dominios dinámicos[XVIII], para robar credenciales y dinero de personas usuarias, lo que mina la confianza en el sistema bancario y causa pérdidas significativas.

Esto muestra que Europa tiene la necesidad de reforzar su ciberseguridad, tanto para proteger infraestructuras críticas como para salvaguardar a la ciudadanía, empresas e instituciones frente a estas crecientes amenazas.

Sectores críticos en Europa[13]

En 2023, ENISA ha destacado varios sectores que fueron los más afectados por incidentes de ciberseguridad. Uno de los más vulnerables es el sector energético, con ataques constantes a redes eléctricas, especialmente en Europa del Este. Muchos de estos, atribuidos a actores estatales, buscan interrumpir el suministro como parte de conflictos geopolíticos, lo que pone en peligro la estabilidad energética de la región.

El sector del transporte también enfrenta graves problemas. Los sistemas logísticos y ferroviarios son un blanco de incidentes de ciberseguridad que afectan la movilidad en toda Europa, porque puede ocasionar, entre otros, retrasos significativos y pérdidas económicas.

Por otro lado, el sector salud tampoco se libra. Hospitales y sistemas médicos sufrieron ataques que interrumpieron servicios clave y expusieron datos sensibles de pacientes. Estas brechas de seguridad no solo afectaron la atención médica, sino que también comprometieron la privacidad y seguridad de las personas.

Por su parte, el sector financiero enfrenta un aumento en los ataques de *ransomware* y *phishing*. Bancos e instituciones financieras son objetivos frecuentes, con delincuentes buscando robar información sensible y fondos. Incluso los sistemas de pago y las transacciones electrónicas se ven comprometidos, lo que pone en cuestión la confianza en estos servicios y genera pérdidas económicas importantes.

[13] ENISA *Threat Landscape 2024*

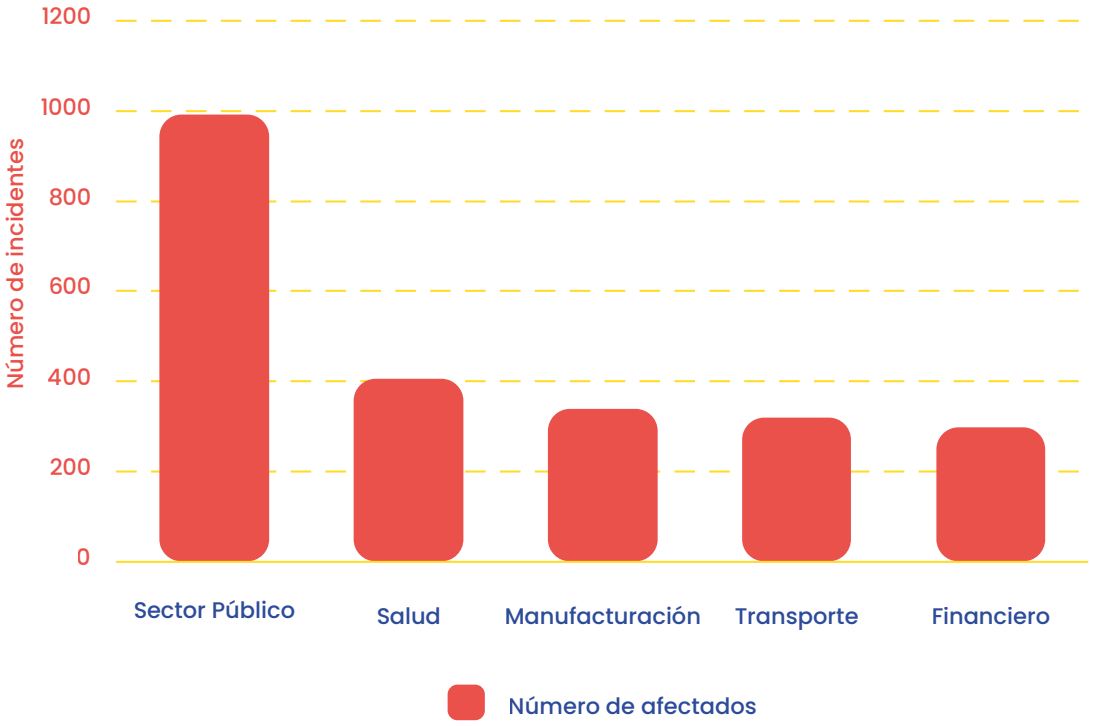


Figura 9
Sectores críticos más afectados por incidentes de ciberseguridad (Julio 2023- Junio 2024)[14]

Respuesta regional y colaboración

En la Unión Europea se han intensificado los esfuerzos para mejorar la ciberseguridad en la región. Una de las acciones clave ha sido la implementación de la **Directiva NIS2**[xix] , que amplía las obligaciones de ciberseguridad a más sectores esenciales y establece sanciones más severas para quienes incumplen las normativas. Además, se ha promovido la cooperación entre los Estados miembros a través de simulacros conjuntos de cibercrisis, como el ejercicio Cyber Europe 2023[xx] para fortalecer la respuesta ante ataques informáticos masivos.

En cuanto a la investigación, el programa ***Horizon Europe***[xxi] ha destinado fondos importantes para impulsar la ciberseguridad, con un enfoque particular en tecnologías avanzadas como la inteligencia artificial para la detección de amenazas y la criptografía.

Por otro lado, países como Suecia, Alemania y los Países Bajos han lanzado campañas nacionales de concienciación para educar tanto a la ciudadanía como a empresas sobre las mejores prácticas de seguridad digital. Estas iniciativas incluyen simulaciones de ataques de *phishing*, talleres de formación y la distribución de guías para proteger la información personal y empresarial en línea.

Resumen de la situación actual

Tanto en España como en el resto de Europa, la ciberseguridad ha emergido como un desafío estratégico, lo que pone de manifiesto una evolución constante en la sofisticación y el alcance de los incidentes de ciberseguridad. En España, el aumento del 24%[14] en incidentes gestionados por el INCIBE, destaca el impacto creciente en ciudadanía, empresas y operadores críticos, mientras que, a nivel europeo, los ataques de ransomware, interferencias en infraestructuras esenciales y campañas de desinformación, subrayan la amplitud de las amenazas.

Aunque las infraestructuras críticas como energía, transporte y sistemas sanitarios son objetivos clave en toda Europa, las iniciativas

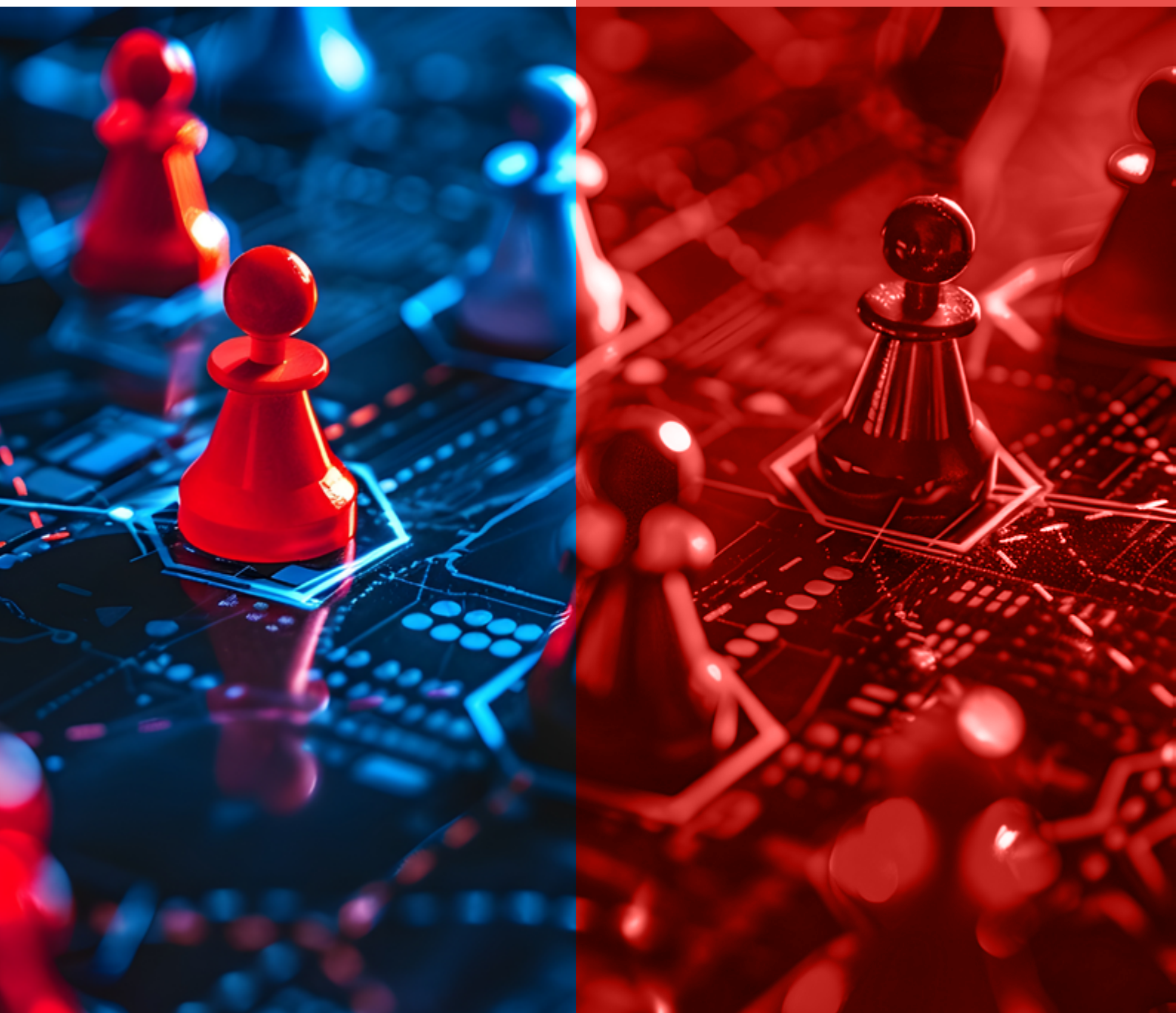
[14] ENISA *Threat Landscape 2024*

coordinadas, como la implementación de la Directiva NIS2 y los simulacros de cibercrisis, demuestran un compromiso regional por fortalecer la ciberresiliencia. Por otro lado, en España, la formación de más de 117.000 personas en ciberseguridad y la asistencia ciudadana proporcionada por *Tu Ayuda en Ciberseguridad* reflejan un enfoque proactivo para preparar a la población frente a los riesgos de ciberseguridad.[14]

En ambos contextos, la convergencia de amenazas tecnológicas, vulnerabilidades en sectores críticos y el uso de plataformas como Telegram para actividades ilícitas resaltan la importancia de una colaboración efectiva entre gobiernos, empresas y ciudadanos.

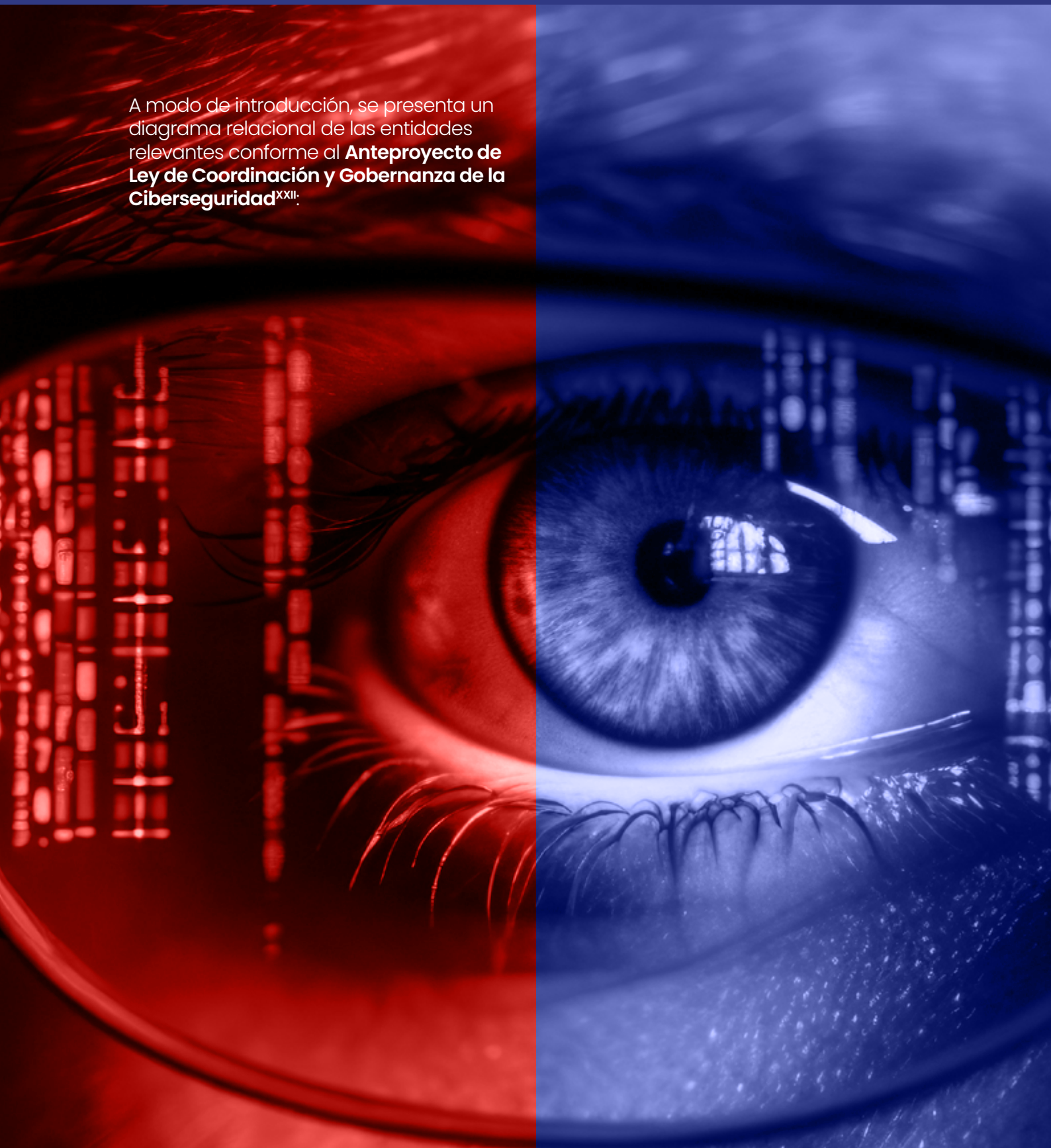
Fortalecer las defensas de ciberseguridad, invertir en tecnologías avanzadas y promover la educación continua en seguridad digital son pilares esenciales para enfrentar los desafíos futuros y proteger tanto a las personas como a las infraestructuras esenciales.

[14] ENISA *Threat Landscape 2024*



03

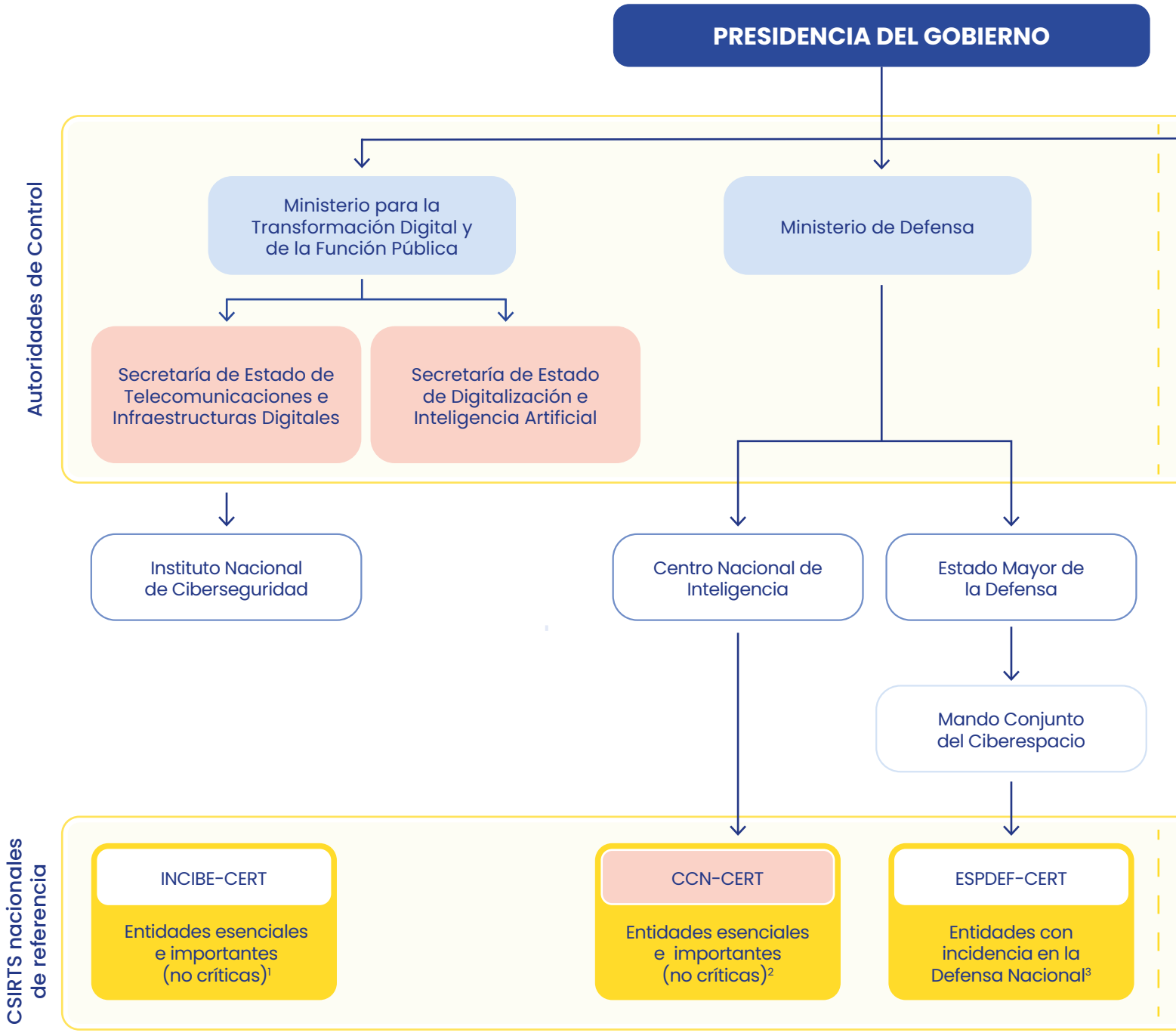
Normativas de gestión de incidentes de ciberseguridad



A modo de introducción, se presenta un diagrama relacional de las entidades relevantes conforme al **Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad**[XXII]:

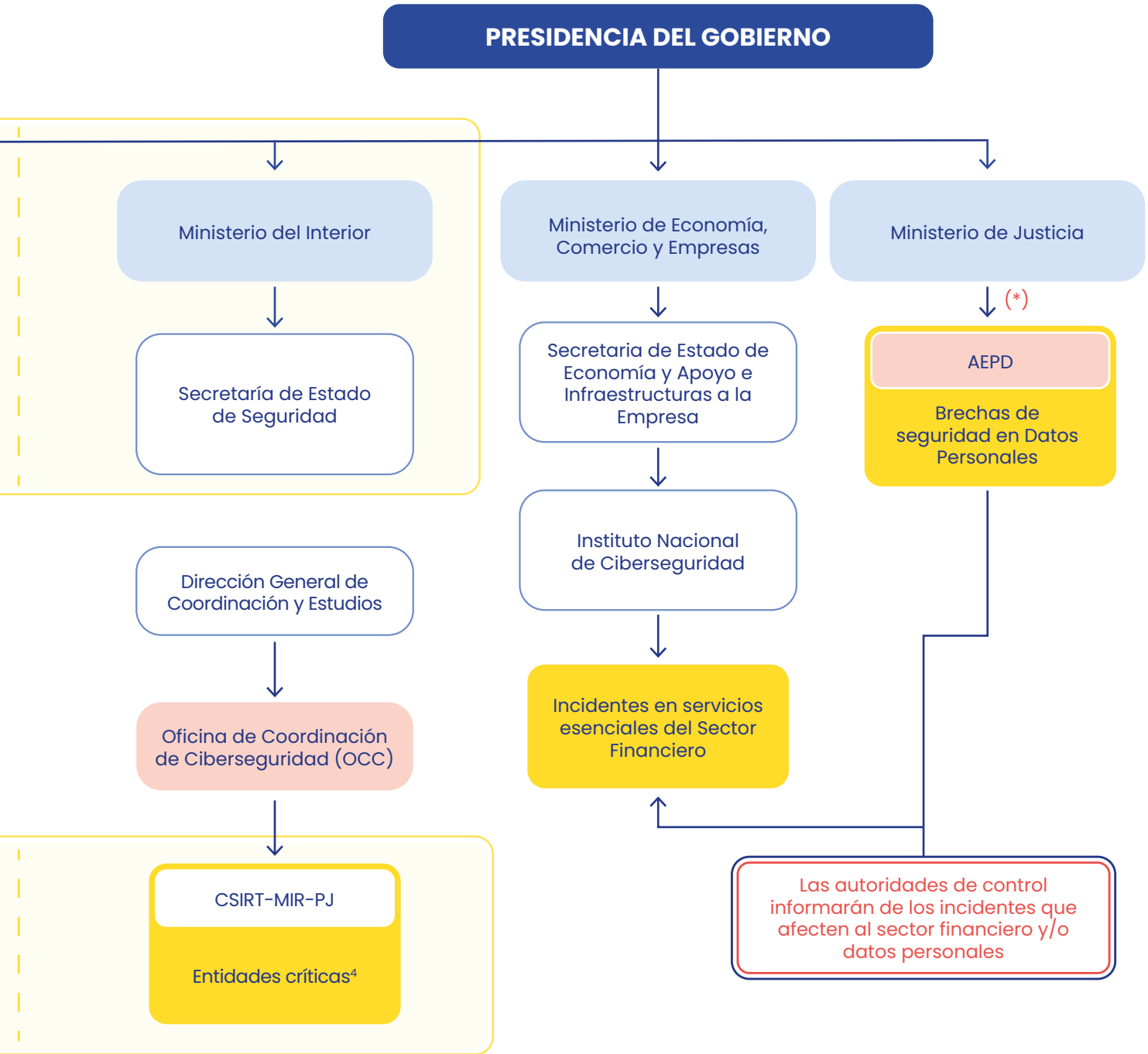
SITUACIÓN VIGENTE: 05/02/2025

Figura 10
Diagrama relacional de las entidades conforme al Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.



BANCO DE ESPAÑA

De acuerdo con la Disposición adicional segunda, las disposiciones de esta ley no afectan las competencias del Banco de España, el Banco Central Europeo ni del Sistema Europeo de Bancos Centrates, según lo establecido en el Tratado de Funcionamiento de la Unión Europea y otros marcos regulatorios, como el Reglamento (UE) 1024/2013 y la Ley 13/1994 sobre la autonomía del Banco de España.



(*) Información extraída del portal de transparencia de la AEPD

LEYENDA:

Autoridades de control que van a conformar el Centro Nacional de Ciberseguridad, de acuerdo con el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad

[1] Entidades esenciales e importantes de los sectores de Infraestructura Digital y Proveedores de Servicios Digitales, asi como de las entidades importantes del resto de sectores, que no se hayan designado como entidades criticas.

[2] Entidades no criticas deambito de aplicacion de la Ley 40/2015, de 1 de octubre, de Régimen Juridico del Sector Público.

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

[4] Ley 8/2011, de 28 de abril, por le que se esteblecen medidas para la protección de las infraestructuras críticas.

Situación nacional

El Gobierno de España asigna a diversos organismos públicos competencias en ciberseguridad para gestionar, conocer y responder a incidentes en las redes de información y comunicación del país. Estos organismos clave conforman la capacidad de respuesta a incidentes de ciberseguridad y atienden a distintos ámbitos:

- **CCN-CERT:** Dependiente del Centro Criptológico Nacional del CNI[XXIII], que a su vez depende del Ministerio de Defensa, se encarga del Sector Público (general, autonómico y local) y de sistemas con información clasificada.

- **INCIBE-CERT**: Gestionado por el Instituto Nacional de Ciberseguridad, es responsable de incidentes en el ámbito ciudadano y privado, además de instituciones afiliadas a la RedIRIS (red académica y de investigación) , en coordinación con CCN-CERT para organismos públicos. Este organismo depende de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETID) y de la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA), del Ministerio para la Transformación Digital y la Función Pública.

- **CNPIC:** Protege infraestructuras críticas y operadores estratégicos, proporcionando capacidades de respuesta técnica mediante CSIRT de referencia. También coordina operadores de servicios esenciales críticos, bajo la Oficina de Coordinación Cibernética según el Real Decreto-ley 12/2018[15], dependiente de la Dirección General de Coordinación y Estudios de la Secretaría de Estado de Seguridad del Ministerio del Interior.

- **ESP-DEF-CERT:** Dependiente del Mando Conjunto de Ciberdefensa (MCCE), que a su vez depende del Estado Mayor de la Defensa del Ministerio de Defensa, es el organismo responsable de la ciberseguridad en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas. También gestiona aquellas otras redes y sistemas que se le encomienden y que tengan impacto en la Defensa Nacional. Además, apoya a los operadores de servicios esenciales, especialmente aquellos con incidencia en la Defensa Nacional, según lo estipulado reglamentariamente. Este organismo refuerza la capacidad de respuesta de ciberseguridad en el ámbito militar y de defensa estratégica de España.

Se ha establecido una *Guía nacional de notificación y gestión de incidentes de ciberseguridad*, creada por el Ministerio del Interior en colaboración con el CCN, CNPIC, INCIBE y MCCE y aprobada por el Consejo Nacional de Ciberseguridad el 21 de febrero de 2020, como referencia oficial a nivel estatal para la notificación de este tipo de eventos. La guía se encuentra plenamente alineada con la normativa vigente en España, así como con las transposiciones de la legislación europea.

Además, establece las directrices destinadas a los Responsables de **Seguridad de la Información (RSI)**[XXVI] para garantizar el cumplimiento de las obligaciones relativas al reporte de incidentes de ciberseguridad que se produzcan en el ámbito de las Administraciones Públicas, las infraestructuras críticas y los operadores estratégicos bajo su responsabilidad, así como en el resto de las entidades incluidas en el ámbito de aplicación del Real Decreto-ley 12/2018.

A continuación, se presenta un esquema orientativo que detalla las autoridades competentes y los **CSIRTs** (Equipos de Respuesta a Incidentes de Seguridad Informática) de referencia aplicables.

[15] Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

El ecosistema de ciberseguridad articula una respuesta coordinada garantizando una notificación unificada y eficaz de incidentes

Autoridad competente de referencia

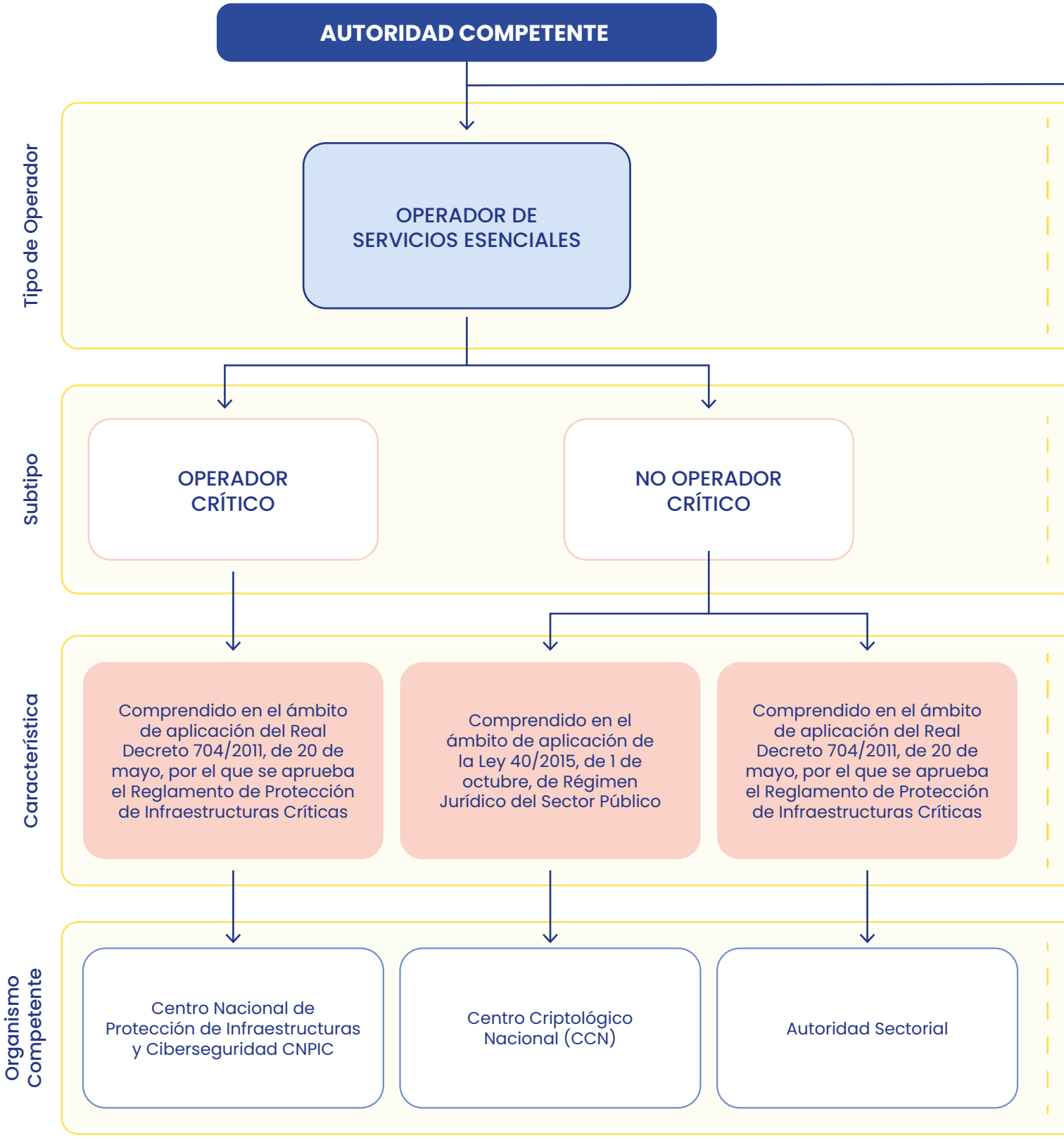
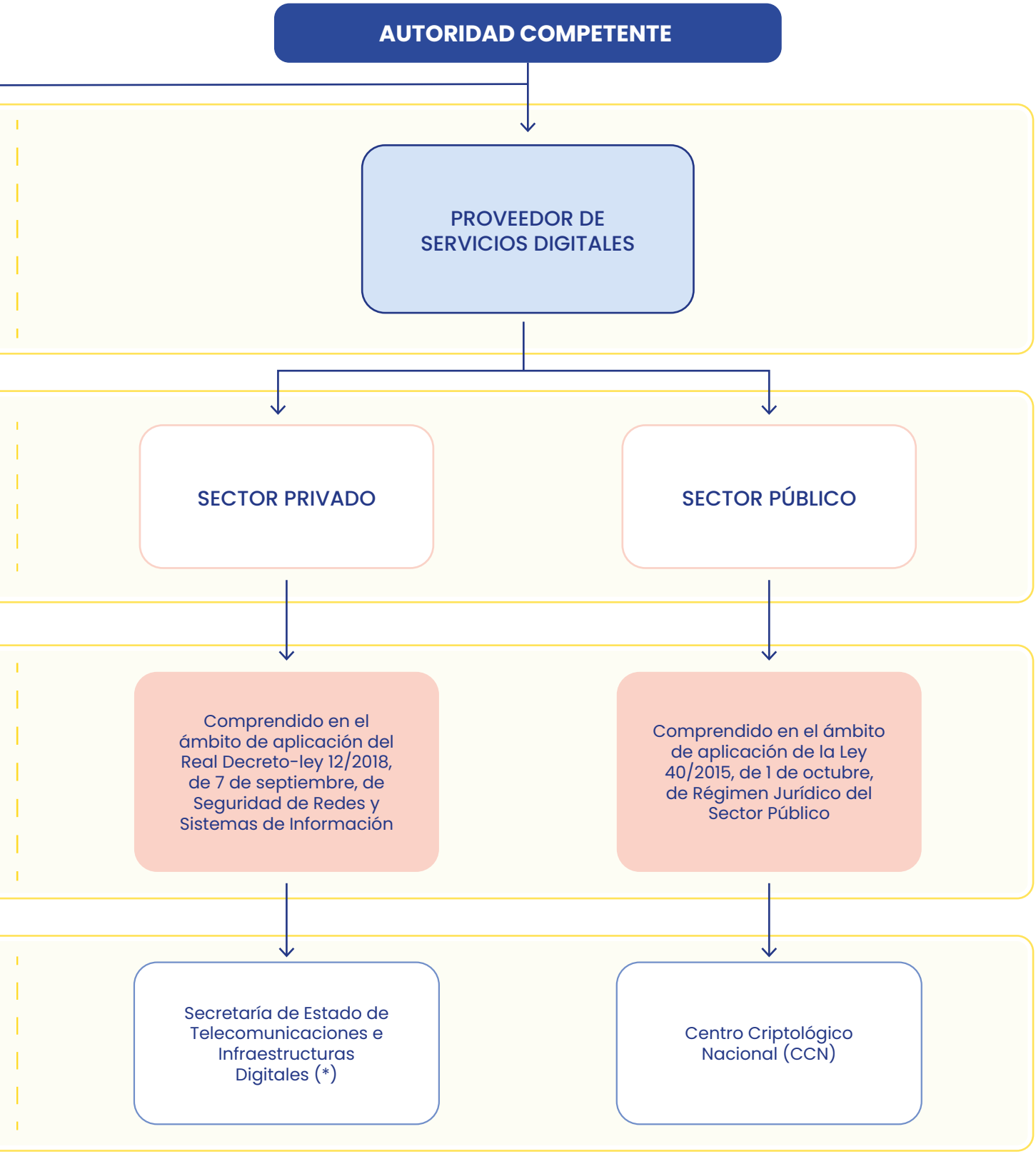


Figura 11
Organismo competente de referencia en función del tipo de Operador



(*)Cambio de competencias relativas a ciberseguridad de acuerdo con el Real Decreto 1185/2024, de 28 de roviembre, por el que se modifican el Real Decreto 210/2024, de 27 de febrero y el. Real Decreto 1009/2023, de 5 de diciembre

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

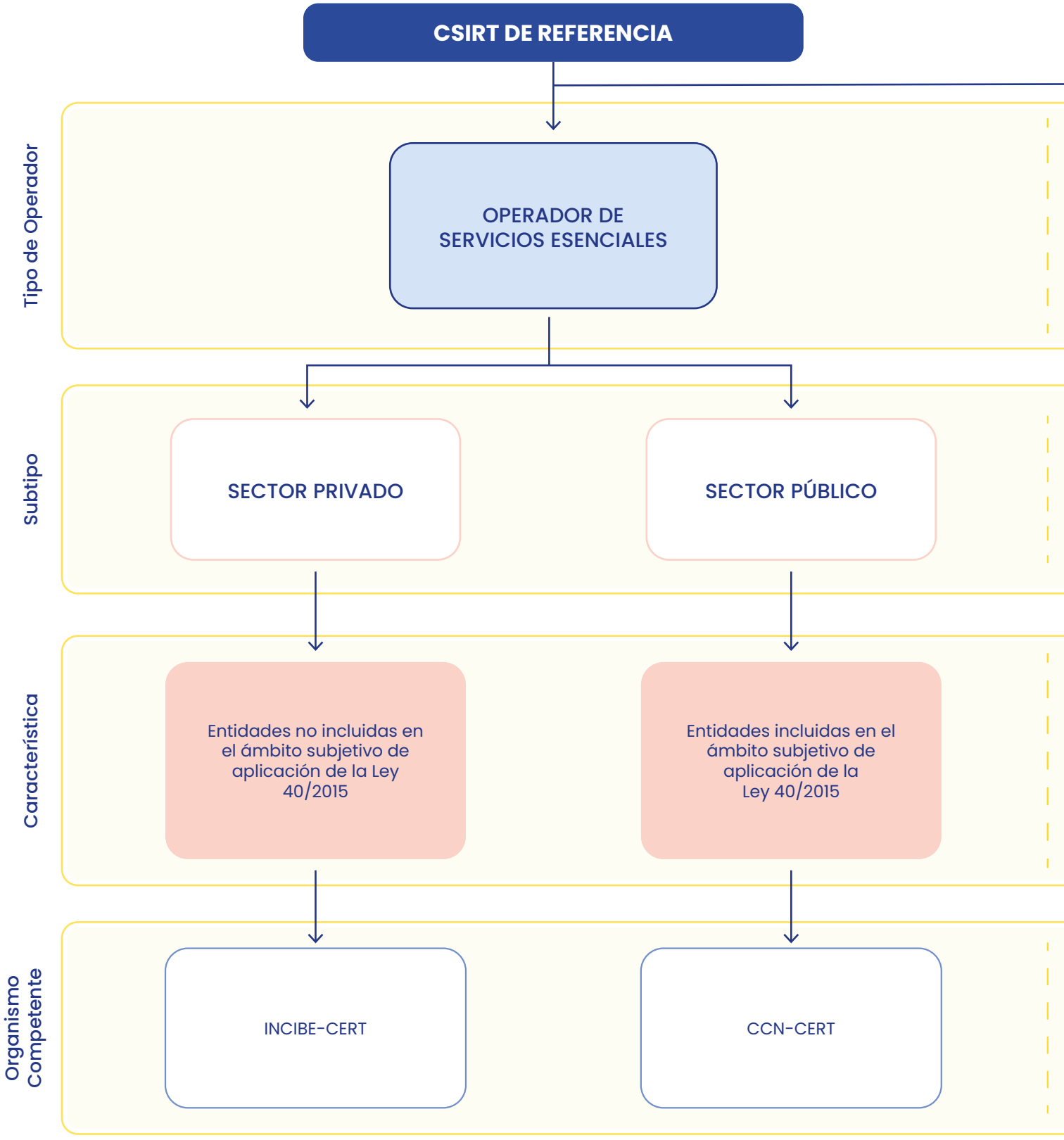
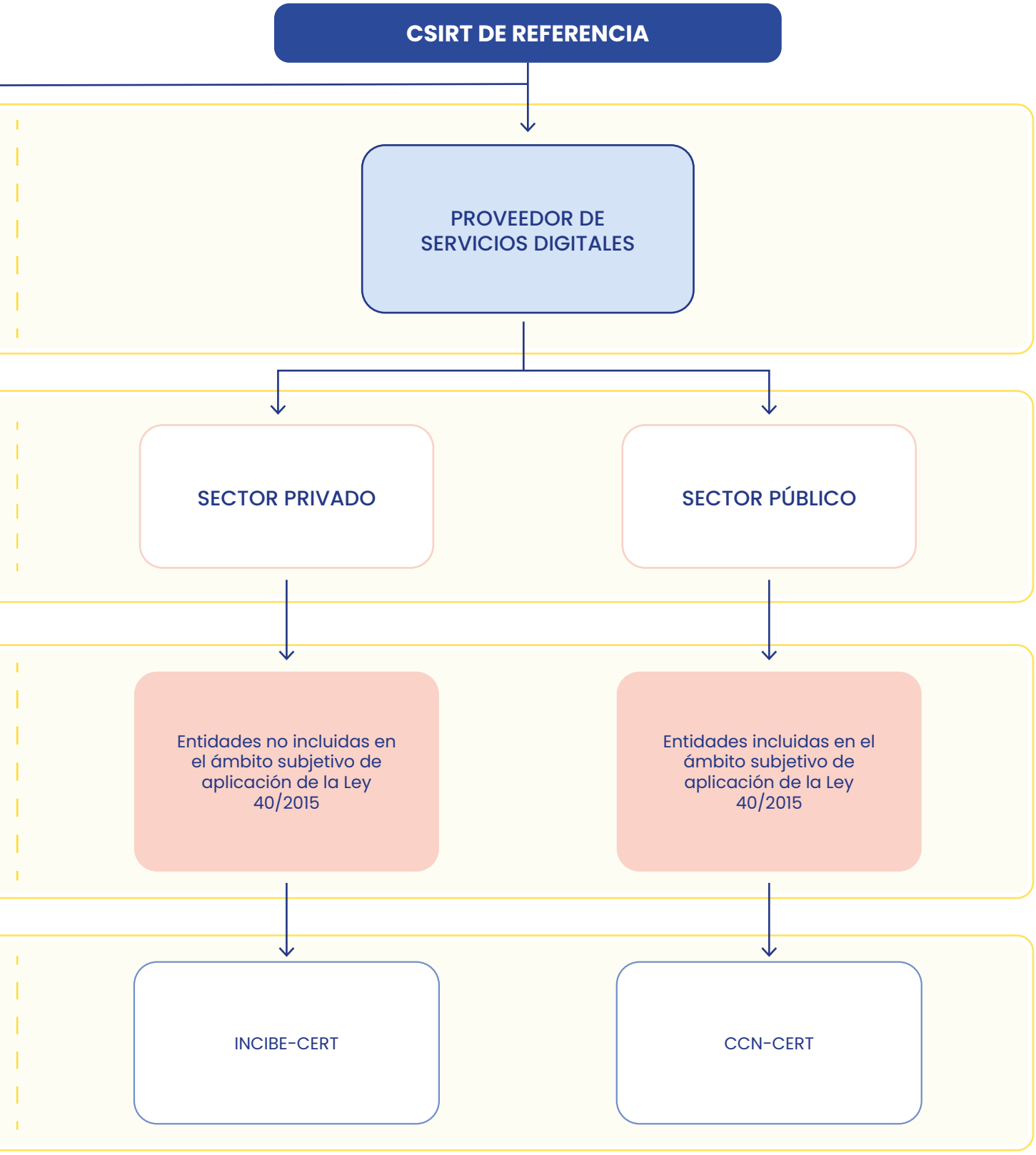


Figura 12
CSIRT de referencia en función del tipo de Operador

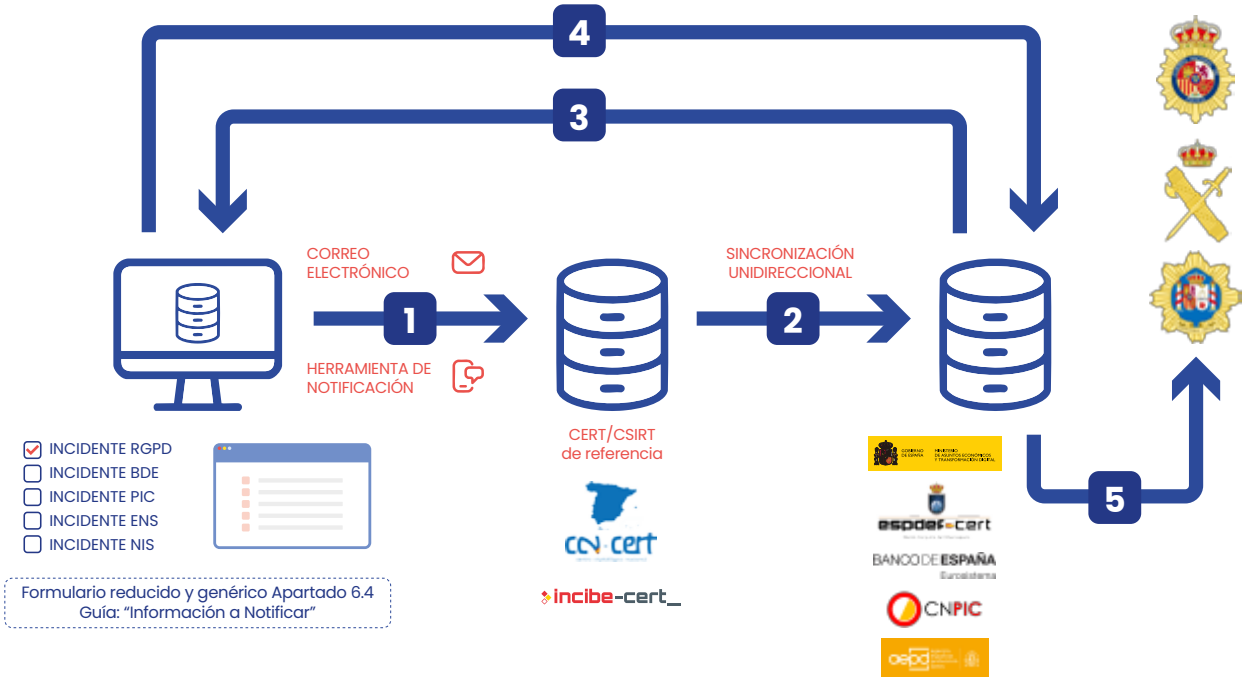

CSIRT DE REFERENCIA
PROVEEDOR DE SERVICIOS DIGITALES
SECTOR PRIVADO
SECTOR PÚBLICO
Entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015
Entidades incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015
INCIBE-CERT
CCN-CERT

La información relativa a un incidente de ciberseguridad deberá remitirse de acuerdo con el cauce establecido por la autoridad competente o CSIRT de referencia (tal y como se muestra en las tablas anteriores), todos estos reportes siguen la misma metodología: sistema de ventanilla única.

Metodología: Sistema de Ventanilla Única

La metodología de Ventanilla Única es un sistema centralizado que permite a las entidades y ciudadanía notificar los incidentes de ciberseguridad de manera unificada a una única plataforma, que luego se encarga de coordinar la comunicación con otras entidades relevantes, como el CCN-CERT, INCIBE-CERT, AEPD y otros organismos reguladores.

Este sistema busca simplificar el proceso de notificación, evitando que las organizaciones tengan que reportar un mismo incidente a diferentes autoridades a través de múltiples canales, lo que optimiza el tiempo y los recursos.



1 NOTIFICACIÓN INICIAL DEL INCIDENTE
A través del formulario de la guía Nacional de Notificación y Gestión de Ciberincidentes

2 SINCRONIZACIÓN DEL INCIDENTE
Con el organismo receptor implicado o autoridad competente

3 INICIO DE LA INVESTIGACIÓN DEL INCIDENTE

4 NOTIFICACIÓN COMPLETA DEL INCIDENTE
A través del formulario específico de organismo

5 INVESTIGACIÓN POLICIAL/JUDICIAL
Ministerio Fiscal. Fuerzas y Cuerpos de Seguridad del Estado

Figura 13
Metodología del sistema de ventanilla única CSIRT de referencia en función del tipo de Operador[16]

[16] *Guía Nacional de Notificación y Gestión de Incidentes de Ciberseguridad*

El procedimiento a seguir se detalla a continuación:

1. Notificación inicial.

El sujeto afectado envía un correo electrónico o ticket al CSIRT de referencia correspondiente para notificar el incidente.

2. Derivación del incidente.

El CSIRT de referencia, dependiendo del incidente, lo pone en conocimiento al organismo receptor implicado o a la autoridad nacional competente.

- Si afecta a la defensa nacional, al ESPDEF-CERT.
- Si afecta a una infraestructura crítica de la Ley PIC 8/2011, al CNPIC.
- Si afecta a la RGPD, a la AEPD.
- Incidentes en administraciones públicas bajo ENS con peligrosidad alta, muy alta o crítica: CCN-CERT.
- Si es un incidente de obligado reporte según el Real Decreto-Ley 12/2018, a la autoridad nacional correspondiente:
  - RGPD: se remite a la URL del portal de la AEPD.
  - BE: se remite la plantilla de notificación .XLS del BE (Banco de España).
  - PIC: se remite la plantilla de notificación .XLS del CNPIC.
  - ENS: se remite la plantilla de notificación .DOC al CCN-CERT.
  - NIS: se remite la plantilla de notificación del Centro Nacional de Ciberseguridad.

3. Solicitud de información.

El organismo receptor implicado o autoridad nacional competente se pone en contacto con el afectado para recabar información.

4. Transmisión de datos.

La persona afectada proporciona los datos necesarios al organismo receptor o autoridad competente.

5. Elevación a fuerzas de seguridad.

Si procede, desde la Oficina de Coordinación Cibernética (CNPIC), se pone la información a disposición de las Fuerzas y Cuerpos de Seguridad del Estado y Ministerio Fiscal para iniciar la investigación policial y judicial[17].

De acuerdo con el Artículo 11.2 del RD Ley 12/2018, de 7 de septiembre, en los supuestos de especial gravedad que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT.

[17] De acuerdo con el artículo 14.3 del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Clasificación y taxonomía de los incidentes de ciberseguridad

- Contenido abusivo:
  - **SPAM:** Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
  - **Delito de odio:** Contenido difamatorio o discriminatorio. Ejemplos: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
  - **Pornografía infantil, contenido sexual o violento inadecuado:** Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etcétera.
- Contenido dañino:
  - **Sistema infectado:** Sistema infectado con *malware*. Ejemplo: sistema, computadora o teléfono móvil infectado con un *rootkit*.[XXVII]
  - **Servidor C&C (Mando y Control):** Conexión con servidor de Mando y Control (C&C) mediante *malware* o sistemas infectados.
  - **Distribución de *malware*:** Recurso usado para distribución de *software* malicioso[XXVIII]. Ejemplo: recurso de una organización empleado para distribuir *malware*.
  - **Configuración de *malware*:** Recurso que aloje ficheros de configuración de *malware*. Ejemplo: ataque de webinjects para troyano[XXIX].
  - ***Malware* dominio DGA:** Tipo de *software* que emplea un DGA (Algoritmo de Generación de Dominio) para crear de forma automática una gran cantidad de nombres de dominio que sirven como puntos de contacto con servidores de comando y control (C2), para poder así comunicarse con el servidor del sistema infectado y recibir órdenes o enviar datos robados.
- Obtención de información:
  - **Escaneo de redes (*scanning*):** Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ejemplos: peticiones DNS, ICMP, SMTP, escaneo de puertos.
  - **Análisis de paquetes (*sniffing*):** Observación y grabación del tráfico de redes.
  - **Ingeniería social:** Técnica de manipulación psicológica empleada para engañar a los usuarios con el objetivo de que revelen información confidencial o permitan el acceso no autorizado a sus sistemas o dispositivos. Ejemplos: *phishing, vhishing*[XXX], *baiting*[XXXI].
- Intento de intrusión:
  - **Explotación de vulnerabilidades conocidas:** Intento de atacar un sistema empleando fallos de seguridad ya identificados en CVE (*Common Vulnerabilities and Exposures*), un sistema de identificación de vulnerabilidades de *hardware* y *software* *ya conocidas.* Ejemplos: desbordamiento de *buffer*[XXXII], puertas traseras[XXXIII], *cross site scripting* (XSS)[XXXIV].
  - **Intento de acceso con vulneración de credenciales:** Múltiples intentos de vulnerar credenciales. Ejemplos: intentos de ruptura de contraseñas, ataque por fuerza bruta.
  - **Ataque desconocido:** ataque empleando una explotación desconocida, es decir, un código, programa o técnica que aprovecha una vulnerabilidad en un sistema para realizar acciones maliciosas.
- Intrusión:
  - **Compromiso de cuenta con privilegios:** Compromiso de un sistema en el que el atacante ha adquirido privilegios.
  - **Compromiso de cuenta sin privilegios:** Compromiso de un sistema empleando cuentas sin privilegios.

- **Compromiso de aplicaciones:** Compromiso de una aplicación mediante la explotación de vulnerabilidades de *software*. *Ejemplo: inyección SQL.*
- **Robo:** intrusión física. *Ejemplo: acceso no autorizado a Centro de Proceso de Datos y sustracción de equipo.*

- Disponibilidad:
  - **DoS (Denegación de Servicio):** Ataque de Denegación de Servicio. Ejemplo: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
  - **DDoS (Denegación Distribuida de Servicio):** Ataque de Denegación Distribuida de Servicio. Ejemplos: inundación de paquetes SYN (es un tipo de ataque DoS, consistente en un intento de sobrecargar un servidor al enviarle una gran cantidad de solicitudes de conexión falsas).
  - **Sabotaje:** sabotaje físico. Ejemplos: cortes de cableados de equipos o incendios provocados.
  - **Interrupciones:** Interrupciones por causas externas. Ejemplo: desastre natural.

- Compromiso de la información:
  - **Acceso no autorizado a información:** Acceso no autorizado a información. Ejemplos: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
  - **Modificación no autorizada de información:** Modificación no autorizada de información. Ejemplo: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante *ransomware.*
  - **Pérdida de datos:** pérdida de información. Ejemplo: pérdida por fallo de disco duro o robo físico.

- Fraude:
  - **Uso no autorizado de recursos:** Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. *Ejemplo: uso de correo electrónico para participar en estafas piramidales.*
  - **Derechos de autor:** Ofrecimiento o instalación de *software* carente de licencia u otro material protegido por derechos de autor. Ejemplo: Warez[xxxv].
  - **Suplantación:** Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
  - ***Phishing*:** Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.

- Vulnerable:
  - **Criptografía débil:** Servicios accesibles públicamente que pueden presentar criptografía débil. Ejemplo: servidores web susceptibles de ataques POODLE/FREAK (aquellos con vulnerabilidades relacionadas con versiones antiguas de protocolos de seguridad y cifrado como SSL y TLS).
  - **Amplificador DDoS:** Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques *DDoS.* Ejemplos: DNS open-resolvers (servidor DNS configurado para resolver cualquier consulta DNS, sin restringir el acceso) o Servidores NTP (*Network Time Protocol*) con monitorización monlist (la función monlist devuelve una lista de los últimos 600 clientes que se han conectado a ese servidor NTP).
  - **Servicios con acceso potencial no deseado:** Servicios accesibles públicamente potencialmente no deseados. Ejemplos: Telnet, RDP o VNC.
  - **Revelación de información:** Acceso público a servicios en los que potencialmente pueda revelarse información sensible. Ejemplos:

SNMP o Redis.

- **Sistema vulnerable:** Sistema vulnerable. Ejemplos: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.

- Otros:
  - **Otros:** Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
  - **APT:** Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.
  - **Ciberterrorismo:** Uso de redes o sistemas de información con fines de carácter terrorista.
  - **Daños informáticos PIC:** Borrado, dañado, alteración, supresión o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una infraestructura crítica. Conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.

Notificación de incidentes

En cada **notificación inicial** de un incidente, será necesario proporcionar toda la información disponible que el sujeto obligado pueda conocer en relación con los siguientes campos:

- **Asunto:** Frase que describa de forma general el incidente. Este campo lo heredarán todas las notificaciones asociadas al incidente.
- **OSE/PSD:** Denominación del operador de servicios esenciales o proveedor de servicios digitales que notifica.
- **Sector estratégico:** Energía, transporte, financiero, etcétera.
- **Fecha y hora del incidente:** Indicar con la mayor precisión posible cuándo ha ocurrido el incidente de ciberseguridad.
- **Fecha y hora de detección del incidente:** Indicar con la mayor precisión posible cuándo se ha detectado el incidente de ciberseguridad.
- **Descripción:** Describir con detalle lo sucedido.
- **Recursos tecnológicos afectados:** Indicar la información técnica sobre el número y tipo de activos afectados por el incidente de ciberseguridad, incluyendo direcciones IP, sistemas operativos, aplicaciones, versiones, etcétera.
- **Origen del incidente:** Indicar la causa del incidente si se conoce. Apertura de un fichero sospechoso, conexión de un dispositivo USB, acceso a una página web maliciosa, etcétera.
- **Taxonomía (clasificación):** Posible clasificación y tipo de incidente de ciberseguridad en función de la taxonomía descrita.
- **Nivel de peligrosidad:** Especificar el nivel de peligrosidad asignado a la amenaza.
- **Nivel de impacto:** Especificar el nivel de impacto asignado al incidente.
- **Impacto transfronterizo:** Indicar si el incidente tiene impacto transfronterizo en algún Estado miembro de la Unión Europea. Especificar.
- **Plan de acción y contramedidas:** Actuaciones realizadas hasta el momento en relación con el incidente de ciberseguridad. Indicar el Plan de acción seguido junto con las contramedidas implantadas.
- **Medios necesarios para la resolución (J-P):** Capacidad empleada en la resolución del incidente en Jornadas-Persona.
- **Impacto económico estimado:** Costes asociados al incidente, tanto de carácter directo como indirecto.
- **Extensión geográfica:** Local, autonómico, nacional, supranacional...
- **Daños reputacionales:** Afectación a la imagen corporativa del operador.
- **Adjuntos:** Indicar la relación de documentos adjuntos que se aportan para ayudar a conocer la causa del

problema o a su resolución (capturas de pantalla, ficheros de registro de información, correos electrónicos...)

- **Regulación afectada:** ENS, RGPD, NIS, PIC u otros.
- Si se requiere actuación de **Fuerzas y Cuerpos de Seguridad del Estado**: (sí/no).

Una vez el CSIRT de referencia recibe el aviso sobre un posible incidente, deberá llevar a cabo un análisis para determinar si el caso será gestionado por él mismo.

Si aplica la gestión del incidente de ciberseguridad, se registra la información reportada y se le asigna un identificador único que debe estar presente en todas las comunicaciones relacionadas con el incidente. Asimismo, se le deberá asignar una clasificación y unos valores de peligrosidad e impacto, que se detallan a continuación.

Tal y como se define en la *Guía nacional de notificación y gestión de incidentes de ciberseguridad*, el **nivel de peligrosidad** indica la potencial amenaza que supondría la materialización del incidente, se encuentran definidos cinco niveles de peligrosidad: crítico, muy alto, alto, medio y bajo.

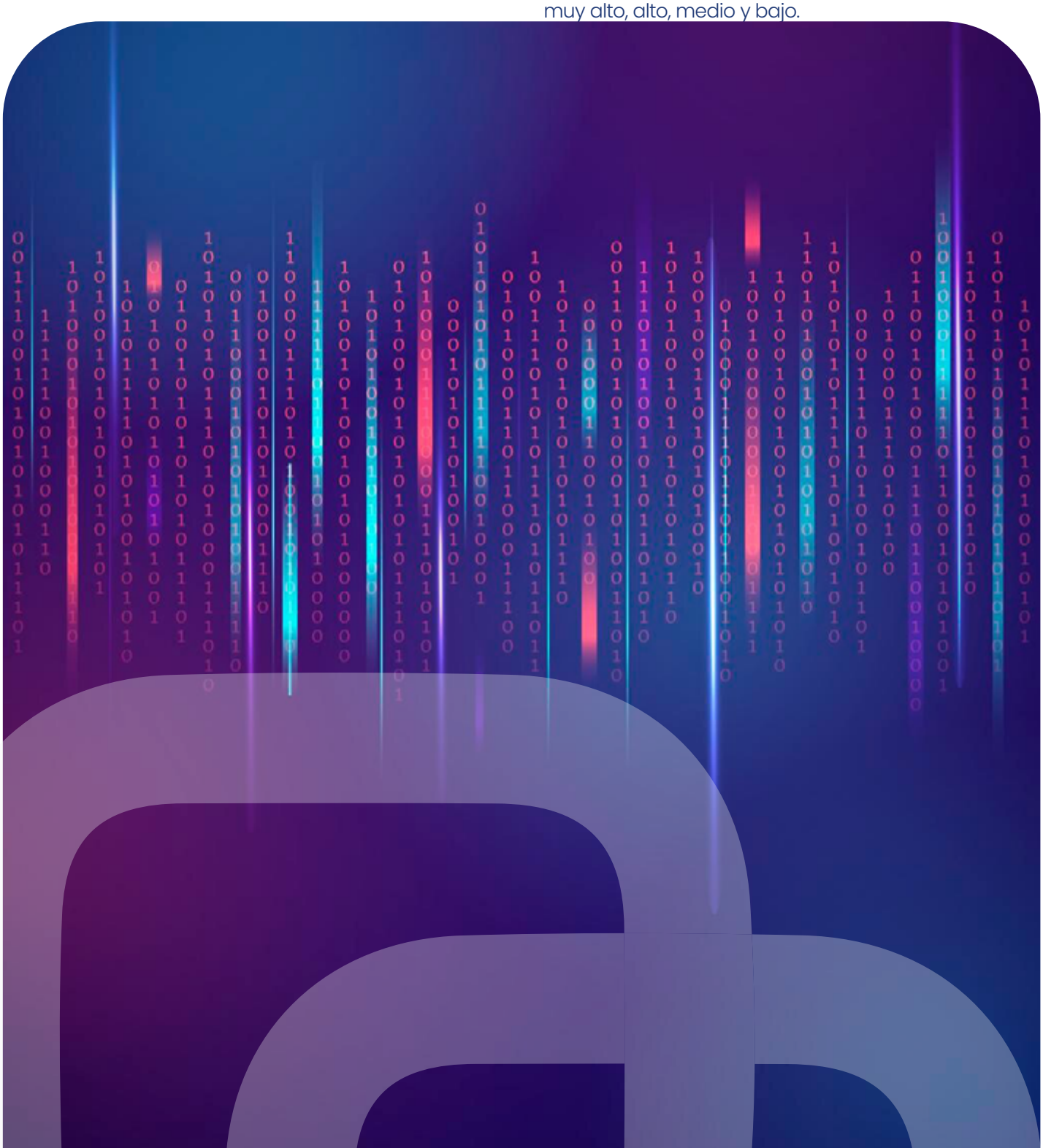


Tabla 1 Clasificación de incidentes de ciberseguridad por nivel de peligrosidad[18]

Nivel	Clasificación	Tipo de incidente
Crítico	Otros	APT[XXXVI]
Muy alto	Código dañino	Distribución y configuración de *malware*
	Intrusión	Robo
	Disponibilidad	Sabotaje Interrupciones
Alto	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
	Código dañino	Sistema infectado Servidor C&C (Mando y Control)
	Intrusión	Compromiso de aplicaciones
	Intento de intrusión	Compromiso de cuentas con privilegios Ataque desconocido
	Disponibilidad	*DoS* (Denegación de servicio) *DDoS* (Denegación distribuida de servicio)
	Compromiso de la información	Acceso no autorizado a datos Modificación no autorizada de información Pérdida de datos
Medio	Contenido abusivo	Discurso de odio
	Obtención de información	Ingeniería social
	Intento de intrusión	Explotación de vulnerabilidades conocidas Acceso con vulneración de credenciales
	Intrusión	Compromiso de cuentas sin privilegios
	Disponibilidad	Mala configuración
	Fraude	Uso no autorizado de recursos Derechos de autor Suplantación
	Vulnerable	Criptografía débil Servicios con acceso potencial no deseado Revelación de información
Bajo	Contenido abusivo	*Spam*
	Obtención de información	Escaneo de redes *(scanning)* Análisis de paquetes *(sniffing)*

[18] *Guía Nacional de Notificación y Gestión de Incidentes de Ciberseguridad*

Respecto al **nivel de impacto**, para determinarlo, se debe atender a los siguientes parámetros:

- Impacto en la seguridad nacional o en la ciudadana.
- Efectos en la prestación de un servicio esencial o en una infraestructura crítica.
- Tipología de la información o sistemas afectados.
- Grado de afectación a las instalaciones de la organización.
- Posible interrupción en la prestación del servicio normal de la organización.
- Tiempo y costes propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones.
- Pérdidas económicas y daños reputacionales asociados.
- Extensión geográfica afectada.

Se encuentran definidos seis niveles de impacto asociados a un incidente de ciberseguridad: crítico, muy alto, alto, medio, bajo y sin impacto.

Tabla 2
Clasificación de incidentes de ciberseguridad por nivel de impacto[19]

Nivel	Clasificación
Crítico	Afecta apreciablemente a la Seguridad Nacional y ciudadana. Afecta a una Infraestructura crítica. Afecta a sistemas clasificados SECRETO. Afecta a más del 90% de los sistemas de la organización. Interrupción en la prestación del servicio superior a 24 horas y al 50% de personas usuarias El incidente de ciberseguridad precisa para resolverse más de 100 Jornadas-Persona. Impacto económico superior al 0,1% del Producto Interior Bruto (PIB) actual. Extensión geográfica supranacional. Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.
Muy alto	Afecta a la seguridad ciudadana con potencial peligro para bienes materiales. Afecta apreciablemente a actividades oficiales o misiones en el extranjero. Afecta a un servicio esencial. Afecta a más del 75% de los sistemas de la organización. Interrupción en la prestación del servicio superior a 8 horas y superior al 35% de los usuarios. El incidente de ciberseguridad precisa para resolverse entre 30 y 100 Jornadas-Persona. Impacto económico entre el 0,07% y el 0,1% del PIB. actual. Extensión geográfica superior a cuatro CCAA (Comunidades Autónomas) o una T.I.S (Infraestructura de Tecnologías de la Información y la Seguridad) Daños reputacionales a la imagen del país (marca España). Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.
Alto	Afecta a más del 50% de los sistemas de la organización. Interrupción en la prestación del servicio superior a una hora y al 10% de personas. El incidente de ciberseguridad precisa para resolverse entre cinco y 30 Jornadas–Persona. Impacto económico entre el 0,03% y el 0,07% del PIB actual. Extensión geográfica superior a 3 CCAA Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.

[19] *Guía Nacional de Notificación y Gestión de Incidentes de Ciberseguridad*

Nivel	Clasificación
Medio	Afecta a más del 20% de los sistemas de la organización. Interrupción en la presentación del servicio superior al 5% de usuarios. El incidente de ciberseguridad precisa para resolverse entre una y cinco Jornadas-Persona. Impacto económico entre el 0,001% y el 0,03% del PIB actual. Extensión geográfica superior a dos CCAA Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).
Bajo	Afecta a los sistemas de la organización. Interrupción de la prestación de un servicio. El incidente de ciberseguridad precisa para resolverse menos de una Jornadas-Persona. Impacto económico entre el 0,0001% y el 0,001% del PIB actual. Extensión geográfica superior a una CCAA Daños reputacionales puntuales, sin eco mediático
Sin impacto	No hay ningún impacto apreciable

Sector Privado

Instituto Nacional de Ciberseguridad - *Computer Emergency Response Team*

Las entidades de derecho privado deberán notificar los incidentes de ciberseguridad al **INCIBE-CERT**, según recoge el artículo 11 del Real Decreto-ley 12/2018, de 7 de septiembre, sobre la seguridad de las redes y sistemas de información. Dicha notificación se realizará a través de los canales y herramientas que el INCIBE-CERT establezca.

El **INCIBE-CERT**, operado por el Instituto Nacional de Ciberseguridad (INCIBE) (organismo dependiente del Ministerio para la Transformación Digital y de la Función Pública, a través de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales), opera como el centro de referencia para la gestión de incidentes de seguridad dirigidos a ciudadanos y entidades de derecho privado en España. Acorde al Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, se encuentra conjuntamente operado por **INCIBE y CSIRT-MIR-PJ** de la OCC, Oficina de coordinación de ciberseguridad del Ministerio del Interior.

Criterios y obligatoriedad de notificación

El proceso para notificar incidentes al **INCIBE-CERT** puede ser realizado por cualquier persona o entidad afectada, utilizando los medios habilitados por el **CERT** para este propósito.

Estas notificaciones se manejan por niveles de prioridad: baja, media, alta y crítica, cada uno con una respuesta diferenciada. La prioridad es asignada durante el registro del incidente, en función de su peligrosidad e impacto.

- **Prioridad baja y media:** Los incidentes de ciberseguridad se atienden por orden de llegada, a menos que se requiera la atención de un incidente de prioridad superior.
- **Prioridad alta:** Los incidentes de ciberseguridad requieren atención antes que otros, incluso si se detectan después. En el caso de un volumen elevado de incidentes, no se gestionarán otros casos de prioridad inferior mientras que los de alta prioridad no hayan sido atendidos.
- **Prioridad crítica:** La gestión de estos incidentes de ciberseguridad no admite demora y para su resolución se emplearán todos los recursos disponibles.

En los casos de entidades afiliadas a RedIRIS, hay un procedimiento específico para incidentes con prioridad alta, en el cual se intenta contactar con la institución responsable de la dirección IP implicada en el incidente para que tome las acciones correctivas oportunas, tanto por correo como por teléfono.

Primero se contacta con el responsable de seguridad de la institución y, a continuación, con el PER (Punto de Enlace de RedIRIS) de la institución. Si se trata de una institución conectada a una red regional o autonómica, se pone en copia de todos los mensajes a los responsables de seguridad de la red autonómica.

Si se trata de un incidente de prioridad crítica, que afecte a la red troncal de RedIRIS, se aplican medidas correctivas sin notificar previamente a la institución afectada o a la red autonómica, con el objetivo de proteger la infraestructura y garantizar su funcionamiento normal.[20]

Registro y reporte del incidente de ciberseguridad

Para contactar y reportar un incidente, si se realiza a través de correo electrónico, las direcciones para las notificaciones son:

- De la ciudadanía: incidencias@incibe-cert.es
- Empresas: incidencias@incibe-cert.es
- Instituciones afiliadas a la red académica y de investigación española (IRIS): iris@incibe-cert.es
- Operadores esenciales y de infraestructuras críticas: pic@incibe-cert.es
- Empresas proveedoras de servicios digitales: incidencias@incibe-cert.es

[20] INCIBE. *Procedimiento de gestión de incidentes de ciberseguridad para el sector privado y la ciudadanía.*

En todos los casos, se recomienda cifrar la información enviada por correo electrónico utilizando la clave PGP (*Pretty Good Privacy*, por sus siglas en inglés) correspondiente al buzón. Esta clave *Pretty Good Privacy*, que en castellano significa bastante buena privacidad, es un sistema de cifrado de clave pública, empleado para asegurar la privacidad y autenticidad de las comunicaciones electrónicas y los datos, puede descargarse de la página oficial del INCIBE. Además del correo, INCIBE-CERT ofrece vías adicionales de reporte, como formularios de contacto, portal web o el teléfono 017, para complementar el proceso de notificación.

Periodo de entrega

De acuerdo con el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, todos los sujetos afectados por un incidente de notificación obligatoria deberán remitirlo, en función de su nivel de peligrosidad o impacto, en los siguientes plazos:

- **Crítico:** Notificación inicial inmediata, notificación intermedia entre 24 y 48 horas y notificación final en 20 días.
- **Muy alto:** Notificación inicial inmediata, notificación intermedia en 72 horas y notificación final en 40.
- **Alto:** Notificación inicial inmediata, notificación inmediata y final no tienen plazo establecido.
- Para nivel **medio** y **bajo** no hay plazo de notificación establecido.

Sector público

Centro Criptológico Nacional - Computer Emergency Response Team

Los organismos del sector público notificarán los incidentes al Equipo de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT), adscrito al Centro Nacional de Inteligencia (CNI), dependiente del Ministerio de Defensa, según especifica la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad publicada en el *BOE nº 95 de 19 de abril de 2018* y la *Guía CCN-STIC 817 de Gestión de Incidentes de Ciberseguridad*.[21]

Criterios y obligatoriedad de notificación

La guía establece que los incidentes de ciberseguridad con niveles de peligrosidad **alto, muy alto o crítico** deben notificarse al CCN-CERT de manera inmediata tras su detección y verificación.

La notificación inicial debe contener la información esencial disponible en ese momento y puede ser complementada posteriormente a medida que se obtengan más detalles.

[21] Elaborada por el CCN, establece directrices para la identificación, clasificación y gestión de incidentes de ciberseguridad en entidades públicas, en cumplimiento del Esquema Nacional de Seguridad.

Para incidentes de **menor peligrosidad**, aunque no se requiere una notificación inmediata, se recomienda reportarlos al CCN-CERT lo antes posible, especialmente si existe la posibilidad de que escalen en gravedad o afecten a otras entidades.

Registro y reporte del incidente de ciberseguridad

Para reportar los incidentes de ciberseguridad, se emplearán las herramientas o vías específicamente desarrolladas por el CCN para tal notificación:

- **Herramienta LUCIA** (Listado Unificado de Coordinación de Incidentes y Amenazas), para aquellas entidades del ámbito del Esquema Nacional de Seguridad.
  - Se trata de una herramienta desarrollada por el CCN-CERT para la gestión de incidentes de ciberseguridad en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. LUCIA permite gestionar incidentes localmente en cada organismo y sincronizar esta información con el CCN-CERT, consolidando y coordinando la respuesta a escala nacional.
  - El objetivo es comunicar y sincronizar incidentes de ciberseguridad entre el CCN-CERT y su comunidad de organismos, y mejorar así los procedimientos con aquellos adscritos a los Sistemas de Alerta Temprana de Internet (SAT-INET), Sistemas de Control Industrial (SAT-ICS) y Red SARA (SAT-SARA).

El Centro Criptológico Nacional, adscrito CNI, es quien pone a disposición las herramientas o vías para reportar incidentes

- A través del correo electrónico: incidentes@ccn-cert.cni.es
  - Se deberá ofrecer una descripción detallada del posible incidente y la información de contacto (mínimo una dirección de correo electrónico y un teléfono). Además, deberán cifrarse los mensajes con una clave PGP disponible en la página web. Esta clave es un sistema de cifrado de clave pública, empleado para asegurar la privacidad y autenticidad de las comunicaciones electrónicas y los datos.

Las notificaciones efectuadas por las entidades comprendidas en el ámbito de aplicación de la mencionada instrucción técnica de seguridad al **Centro Criptológico Nacional (CCN)** se realizarán de acuerdo con lo dispuesto en los artículos 33 y 34, del capítulo IV sobre capacidad de respuesta a incidentes de seguridad, del Real Decreto 311/2022, de 3 de mayo.[22]

Una vez notificado el incidente al organismo afectado por parte del sistema de alerta temprana de Red SARA (SAT-SARA), de Internet (SAT-INET) o para los sistemas de control industrial (SAT-ICS) del CCN-CERT, se realizará un seguimiento de este, asignándole un estado determinado. Este seguimiento se realiza en función del nivel de peligrosidad o impacto del incidente de seguridad.

Periodo de entrega

De acuerdo con el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, todos los sujetos afectados por un incidente de notificación obligatoria deberán remitirlo, en función de su nivel de peligrosidad o impacto, en los siguientes plazos:

- **Crítico:** Notificación inicial inmediata, notificación intermedia entre 24 y 48 horas y notificación final en 20 días.
- **Muy alto:** Notificación inicial inmediata, notificación intermedia en 72 horas y notificación final en 40 días.

[22] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

- **Alto:** Ni la notificación inicial inmediata, la notificación inmediata ni la final tienen plazo establecido.
- Para **nivel medio y bajo** no hay plazo de notificación establecido.

Sector infraestructuras críticas

Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)

Cualquier incidente que afecte a una Infraestructura crítica de la *Ley PIC 8/2011*[23], deberá ponerse en conocimiento del **Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)**.

De acuerdo con el artículo 2 de la Ley 8/2011, son **operadores críticos**: "Entidades u organismos responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica con arreglo a la presente ley".

De acuerdo con el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, todos los operadores que sean considerados críticos tienen como autoridad competente a la Secretaría de Estado de Seguridad del Ministerio del Interior, a través del **CSIRT-MIR-PJ**, de la **Oficina de Coordinación de Ciberseguridad (OCC)**[24].

Criterios y obligatoriedad de notificación

- La notificación de incidentes de ciberseguridad se basa inicialmente en el **Nivel de peligrosidad** asignado al incidente. Durante su desarrollo, mitigación o resolución, puede reclasificarse según su **nivel de impacto**. Esto podría requerir su comunicación al CNPIC a través del CSIRT correspondiente. Estos niveles de peligrosidad e impacto se han detallado a lo largo del documento conforme a la *Guía Nacional de Notificación de Gestión de Incidentes.*
- Es obligatorio notificar los incidentes clasificados como **críticos, muy altos** o **altos**, y considerar su nivel correspondiente.
- El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, puede exigir la notificación de incidentes en redes o sistemas que soporten servicios esenciales, según el **Nivel de Alerta Antiterrorista (NAA)** o el **Nivel de Alerta en Infraestructuras Críticas (NAIC)** aplicable.

Cuando un incidente tenga indicios de **infracción penal,** el Centro Nacional de Protección de Infraestructuras y Ciberseguridad informará al respecto, a través de la Oficina de Coordinación Cibernética del Ministerio del Interior, al Ministerio Fiscal y a las Fuerzas y Cuerpos de Seguridad del Estado, con el fin de que se tomen las medidas oportunas, y proporcionar toda la información disponible relacionada con el suceso.

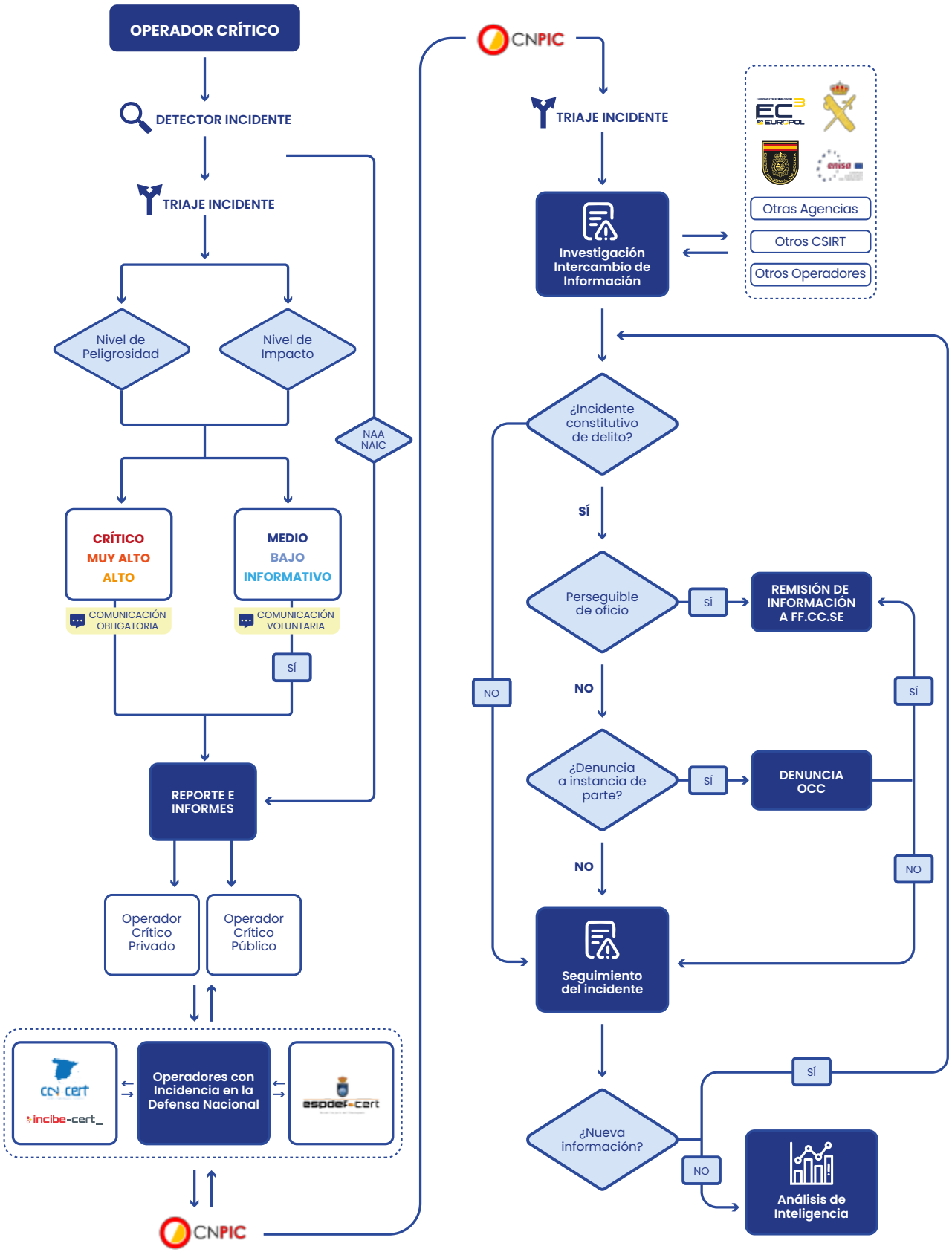
Registro y reporte del incidente de ciberseguridad

El correo electrónico para notificar incidentes de ciberseguridad al CERT del CNPIC es **cert@cnpic.interior.es.** A continuación, se muestra el flujo del proceso de gestión y notificación de un incidente en el ámbito PIC.

Los incidentes susceptibles de ser infracción penal el Centro Nacional de Protección de Infraestructuras y Ciberseguridad informará a través de la Oficina de Coordinación Cibernética del Ministerio del Interior, Fiscal y Cuerpos de Seguridad del Estado

[23] Ley de Protección de las Infraestructuras Críticas que establece el marco jurídico para proteger las infraestructuras críticas en España frente a amenazas y riesgos que puedan afectar su funcionamiento.
[24] Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.

Figura 14
Proceso de gestión de un incidente de ciberseguridad en el ámbito PIC



Autoridad nacional

Centro Nacional de Ciberseguridad

La información que se presenta a continuación se fundamenta en el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, elaborado por el Ministerio del Interior y aprobado el 14 de enero de 2025. A fecha de la redacción del presente documento , esta Ley se encuentra en estado de anteproyecto, por lo que podrían existir modificaciones una vez se encuentre aprobada como Ley.

Según recoge el artículo 6[25], el **Centro Nacional de Ciberseguridad** ejercerá como **Autoridad Nacional** de gestión de crisis y punto de contacto único, y asumirá la superior dirección y coordinación de las autoridades de control y puntos de contacto sectoriales en el desarrollo de sus funciones de ejecución y supervisión, así como de los CSIRT nacionales de referencia. Dentro de su ámbito de aplicación, abarca tanto a las entidades públicas como privadas con residencia fiscal en España y que se encuentren dentro de sectores de alta criticidad.

Criterios y obligatoriedad de notificación

Las entidades esenciales e importantes deben notificar **sin demora indebida**, a través de su CSIRT nacional de referencia, cualquier incidente significativo que afecte a su operativa o prestación de servicios.

La definición de **incidente significativo** es que se trata de un hecho que compromete la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad de los datos o servicios relacionados con redes y sistemas de información. Y se considera significativo si se da:

- **Impacto operativo o económico:** Ha causado o puede causar graves perturbaciones operativas de los servicios y/o genera pérdidas económicas importantes para la entidad afectada.
- **Afectación a terceros:** Ha afectado o puede afectar a otras personas físicas o jurídicas al provocar perjuicios materiales o inmateriales considerables.
- Incidente con **repercusiones transfronterizas.**
- Afectación a **redes críticas**.

Registro y reporte del incidente de ciberseguridad

La notificación de incidentes de ciberseguridad se realizará preferiblemente a través de la **Plataforma Nacional de Notificación y Seguimiento de Incidentes de Ciberseguridad**, disponible ininterrumpidamente 24 horas al día, todos los días del año.

Esta plataforma será adaptada, mantenida y gestionada por el CCN-CERT bajo la dirección del Centro Nacional de Ciberseguridad sin perjuicio de los mecanismos de colaboración necesarios con el INCIBE-CERT y el ESPDEF-CERT.

De acuerdo con el artículo 7.a) del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, las autoridades de control deberán establecer canales de comunicación operativos y seguros con las entidades catalogadas como esenciales e importantes.

Uno de estos canales será la **Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (PNNSC)**, que actuará como canal adicional a los ya existentes de cada autoridad de control. En este sentido, este canal no sustituirá los actualmente habilitados, sino que los complementará, al formar parte del conjunto de mecanismos disponibles para la notificación y seguimiento de incidentes de ciberseguridad. A fecha de informe, la Plataforma se encuentra creada pero no está en funcionamiento.

Plazo de entrega

- **Alerta temprana:** En un plazo máximo de **24 horas** tras detectar un incidente significativo, tras indicar si es ilícito o tiene repercusiones transfronterizas.
- **Notificación completa:** Dentro de las **72 horas** siguientes, proporcionando detalles más amplios, como la evaluación inicial de peligrosidad e impacto.
- **Informe final:** En un plazo máximo de **un mes**, en el que se incluya una descripción detallada del incidente, la posible causa del incidente, las medidas paliativas aplicadas e Indicadores de Compromiso (IoCs).

[25] Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.

Para **prestadores de servicios de confianza**, cuando el incidente afecte a la prestación de sus servicios, el plazo de notificación completa es de **24 horas**.

Defensa nacional

Centro de Respuesta ante Incidentes del Ministerio de Defensa (ESPDEF-CERT)

El **ESPDEF-CERT** (Equipo de Respuesta a Incidentes de Seguridad de la Información del Ministerio de Defensa) es el equipo especializado en ciberseguridad de las Fuerzas Armadas de España. Está integrado en el Mando Conjunto del Ciberespacio (**MCCE**) y tiene como misión principal garantizar la ciberseguridad de los sistemas de información y comunicaciones del Ministerio de Defensa y de las Fuerzas Armadas.

Criterios y obligatoriedad de notificación

Según el *Real Decreto-ley 12/2018, de 7 de septiembre*[26], el **ESPDEF-CERT**, del Ministerio de Defensa, cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que estos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos operadores que tengan incidencia en la Defensa Nacional y que reglamentariamente se determinen.

Y de acuerdo con el *Real Decreto 43/2021*, se consideran **operadores con incidencia en la Defensa Nacional** a los proveedores de servicios esenciales para el **Ministerio de Defensa** o las **Fuerzas Armadas**, que son designados por la Comisión Nacional para la Protección de las Infraestructuras Críticas, a propuesta del Ministerio de Defensa.

Los CSIRT de referencia serán informados de la identidad de estos operadores y de cualquier cambio, como altas o bajas, en su designación.

Registro y reporte del incidente de ciberseguridad

Si un operador relacionado con la Defensa Nacional experimenta un incidente que podría afectar al Ministerio de Defensa o a las Fuerzas Armadas, deberá comunicarlo a su CSIRT de referencia, quien a su vez lo informará al ESPDEF-CERT del Mando Conjunto del Ciberespacio. Este último deberá ser informado sobre la evolución de la gestión del incidente.

La comunicación con ESPDEF-CERT se realizará por correo electrónico mediante mensajería cifrada con la clave pública PGP. La dirección habilitada para ello es:
espdef-cert@mde.es

En caso de urgencia, podrá contactarse con el Oficial de Servicio (teléfono+34 638 76 96 98).

Periodo de entrega

Todos los sujetos afectados por un incidente de notificación obligatoria deberán remitirlo, en función de su nivel de peligrosidad o impacto, en los siguientes plazos:

- **Crítico:** Notificación inicial inmediata, notificación intermedia entre 24 y 48 horas y notificación final en 20 días.
- **Muy alto:** Notificación inicial inmediata, notificación intermedia en 72 horas y notificación final en 40 días.
- **Alto:** Notificación inicial inmediata, notificación inmediata y final no tienen plazo establecido.
- Para nivel **medio** y **bajo** no hay plazo de notificación establecido.

Sector financiero

Banco de España

Según el *Real Decreto 43/2021, de 26 de enero*[27], el **Banco de España (BE)** desempeña un papel crucial en el ecosistema de ciberseguridad del sector financiero, al actuar como regulador, supervisor y coordinador. Su función en este ámbito se centra en garantizar que las entidades financieras y otras instituciones bajo su supervisión gestionen adecuadamente los riesgos de ciberseguridad y cumplan con las normativas aplicables.

El BE colabora con otros organismos nacionales, como el **CCN-CERT**, el **INCIBE-CERT**, y el **CNPIC**, para garantizar una respuesta coordinada a los incidentes de ciberseguridad que puedan tener un impacto sistémico.

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

En el contexto europeo, trabaja estrechamente con otras autoridades de supervisión financiera actuando como canal único, de forma que el Banco de España es el encargado de hacer llegar las notificaciones al resto de autoridades como el Banco Central Europeo (BCE), la Autoridad Bancaria Europea (EBA) y los CSIRTs establecidos conforme a la NIS2.

Las entidades supervisadas deben notificar al BE cualquier incidente grave que afecte la seguridad de sus sistemas de información, conforme a lo establecido en el Reglamento (UE) 2022/2554[28] . De acuerdo con el Reglamento, se considera incidente grave a "un incidente relacionado con las TIC con graves repercusiones negativas en las redes y sistemas de información que sustentan funciones esenciales o importantes de la entidad financiera".

Según el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, el Banco de España continuará y mantendrá las competencias y funciones que tiene asignadas.

Mientras que las autoridades de control y CSIRTs de referencia deberán informar a la Secretaría de Estado de Economía y Apoyo a la Empresa, del Ministerio de Economía, Comercio y Empresa, sobre aquellos incidentes que tengan efectos significativos en los servicios esenciales del sistema financiero.

Criterios y obligatoriedad de notificación

Cuando el incidente se considere grave. En caso de no ser grave, pero sí relevante, también es obligatorio notificarlo. Un incidente se considera grave cuando afecta a todas las entidades financieras sujetas al Reglamento (UE) 2022/2554 (DORA); y se considera relevante cuando afecta solo a las entidades bajo supervisión directa del Banco de España.

La documentación relativa al Banco de España sobre notificación de incidentes de ciberseguridad se presenta, exclusivamente, por vía telemática.

Los criterios de la documentación a enviar se especifican en los campos de la plantilla disponible en la Sede Electrónica del Banco de España correspondiente a la Notificación de incidentes graves y ciberamenazas importantes bajo normativa DORA, en el apartado *Tramitación*.

Además, se dispone de una guía para ayudar en todos los pasos a completar en el procedimiento de notificación del incidente (*Guía del proceso de notificación de incidentes graves y/o ciberamenazas bajo normativa DORA*), disponible en el apartado *Otra información de interés* de la web.

Tienen la obligación de notificar incidentes graves relacionados con las TIC y los incidentes operativos o de seguridad graves relacionados con los servicios de pago: las entidades de crédito, entidades de pago, entidades de pago exentas en virtud de la Directiva (UE) 2015/2366[29], proveedores de servicio de información sobre cuentas y entidades de dinero electrónico.

Registro y reporte del incidente de ciberseguridad

Como requisito inicial para la **notificación** de un incidente grave de ciberseguridad se ha de realizar el proceso de adhesión al servicio electrónico **PIR - Notificación y delegación de notificación de incidentes graves y amenazas importantes bajo normativa DORA.**

Es necesario disponer de un certificado electrónico expedido por alguna de las Autoridades de Certificación aceptadas por el BE.

Tras realizar la adhesión al servicio electrónico, se ha de descargar la *Plantilla de informe de incidente grave DORA* y rellenarla según las instrucciones incluidas en la propia plantilla. Si la intención es notificar una amenaza de ciberseguridad, el usuario o la usuaria deberá descargarse la *Plantilla de notificación de ciberamenazas importantes DORA*.

Tras rellenarla, se manda a través del canal de envío de Internet-ITW (canal web para el intercambio telemático de archivos). Una vez enviado, se puede comprobar si ha sido recibido por el Banco de España a través de un canal de seguimiento.

[28] Reglamento (UE) 2022/2554 de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero.
[29] Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) nº 1093/2010 y se deroga la Directiva 2007/64/CE.

La plantilla es un documento Excel con la siguiente estructura:

1. **General:** Se indica el tipo de informe que se va a enviar.
2. **A-Initial report:** Se trata del informe inicial, donde han de rellenarse todos los campos indicados.
3. **B-Intermediate report:** Es el contenido del informe intermedio, para cumplimentarlo, deberá haberse rellenado previamente el inicial.
4. **C-Final report:** Se trata del informe final, que deberá rellenarse tras haber cumplimentado los dos informes anteriores.
5. **Explanatory notes:** Hoja explicativa con todos los campos que hay que rellenar y su descripción.

Los campos sombreados en rojo son aquellos obligatorios de cumplimentar y los sombreados de gris los que no deben rellenarse.

Para información con más detalle sobre el contenido de la plantilla, puede consultarse la *Guía del proceso de notificación de incidentes graves y/o ciberamenazas importantes bajo normativa DORA*, disponible en la Sede Electrónica del Banco de España. Y para cualquier duda o consulta, el usuario puede ponerse en contacto a través del correo electrónico **ciberincidentes@bde.es**.

Periodo de Entrega

El plazo de presentación consta de tres fases, incrementales en cuanto al contenido en función de la situación del incidente de ciberseguridad y estructurados en torno a, proceso "PIR":

- **Informe inicial:** El plazo para su entrega es de cuatro horas desde que el incidente se clasifica como grave y no más de 24 horas desde que se conoce.
- **Informe intermedio:** El plazo para su entrega es de 72 horas desde el envío de la notificación inicial. Este informe puede ser enviado de forma simultánea con el informe inicial.
- **Informe final:** Se dispone de un plazo no superior a un mes desde que se envió el último informe intermedio.
- **Informe de incidente reclasificado como no grave**: Debe enviarse en cuanto se haya comprobado que el incidente ya no cumple los requisitos para ser clasificado como grave.

Protección de datos personales

Agencia Española de Protección de Datos (AEPD)

Cualquier incidente que afecte o guarde relación con el cumplimiento del **Reglamento General de Protección de Datos (RGPD)** deberá ser reportado e informado a la Agencia Española de **Protección de Datos (AEPD)**.

El RGPD define, de un modo amplio, las **brechas de datos personales** como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".

No tendrán consideración de brecha de datos personales sujetas a los artículos 33 y 34 del RGPD aquellos incidentes que:

- No afecten a datos personales, es decir, a datos que no sean de personas físicas identificadas o identificables.
- No afecten a tratamientos de datos personales llevados a cabo por un responsable o un encargado.
- Ocurran en tratamientos llevados a cabo por una persona física en el ámbito doméstico.

Criterios y obligatoriedad de notificación

Según el artículo 33 del RGPD, los responsables del tratamiento de datos personales tienen la **obligación** de notificar a la autoridad de control competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas.

El **responsable del tratamiento** debe evaluar cuidadosamente el nivel de riesgo asociado a una brecha de datos personales. Si existe algún riesgo, está obligado a notificarlo a la autoridad de control.

Además, de acuerdo con el artículo 34 del RGPD, si no se puede garantizar que la brecha no afectará, de forma reversible o irreversible, los derechos fundamentales o las libertades públicas de las personas, también deberá informar a los afectados.

Este mismo artículo establece que, en caso de que la brecha de datos personales suponga un alto riesgo para los **derechos y libertades** de las personas físicas, la comunicación a las personas **afectadas** deberá realizarse sin dilación indebida.

Ámbito de aplicación

· **Ámbito privado:** Los responsables del tratamiento afectados por una brecha de datos personales deberán notificar a la AEPD:

- Cuando su único establecimiento esté localizado en España.
- Si tienen varios establecimientos en la Unión Europea, únicamente cuando el establecimiento principal esté localizado en España.
- Si no tienen establecimiento principal en la Unión Europea, solo en el caso de que hayan designado un representante en España.
- Si no tienen establecimiento ni representante en la Unión Europea, en el caso de que la brecha de datos personales cuente con afectados en España.

· **Ámbito público:** Con carácter general, las Administraciones Públicas, deben notificar las brechas de datos personales a la Agencia Española de Protección de Datos a excepción del caso de las Comunidades Autónomas de Andalucía, Cataluña y País Vasco, cuando las brechas de datos personales se produzcan en entidades **del sector público bajo su competencia.**

- Cataluña: A la Autoridad Catalana de Protección de Datos (**https://apdcat.gencat.cat/es/inici/**) a través de su sede electrónica.
- País Vasco: A la Agencia Vasca de Protección de Datos mediante el correo electrónico: **avpd@avpd.eus**.
- Andalucía: Al Consejo de Transparencia y Protección de Datos de Andalucía a través de su ventanilla electrónica (**https://www.ctpdandalucia.es/ventanilla-electronica**)

Registro y reporte del incidente de ciberseguridad

Se realiza a través de un **formulario** disponible en la página web de la AEPD.

El **contenido** de la notificación que ha de incluirse en el formulario es el siguiente: carácter de la notificación, información general (duración, número total de personas y ámbito geográfico), intencionalidad y origen (interno o externo), fecha de inicio de la brecha, medio de detección de la brecha, medidas de seguridad antes del incidente, acciones tomadas, comunicación a las personas afectadas, identificación de quienes intervengan y, si es necesario, documentación adjunta.

Además, es esencial identificar el suceso que desencadena la brecha de datos personales para determinar sus causas, evaluar las consecuencias y prevenir incidentes similares. Las brechas de datos pueden clasificarse según las dimensiones de seguridad afectadas: **confidencialidad, disponibilidad e integridad**.

- **Confidencialidad:** Ocurre cuando terceros no autorizados acceden a los datos personales, como en casos de exfiltración de información (proceso de robar datos de un sistema o dispositivo de forma no autorizada), errores de envío, pérdida de dispositivos o ataques de *ransomware*. Si los datos estaban cifrados o anonimizados, el riesgo puede mitigarse.
- **Disponibilidad:** Se refiere a la inaccesibilidad temporal o permanente de los datos personales para quienes tienen derecho

a tratarlos. Esto incluye cifrado malicioso por *ransomware*, pérdida de documentación o problemas de acceso a sistemas. Recuperar los datos y sistemas afectados es clave para reducir el impacto.

- **Integridad:** Se ve comprometida cuando los datos son alterados de forma ilegítima, lo que causa posibles daños a las personas afectadas, como la modificación de información bancaria o calificaciones académicas. Es crucial evaluar si los datos alterados pueden ocasionar perjuicios y si estos son reversibles.

El análisis y clasificación de estas tipologías ayudan a determinar el nivel de riesgo y a establecer medidas preventivas y correctivas. En el **formulario** de notificación de brechas, se considera un listado con diferentes sucesos como son: datos personales eliminados, modificación no autorizada de datos, revelación verbal no autorizada, correo postal perdido...

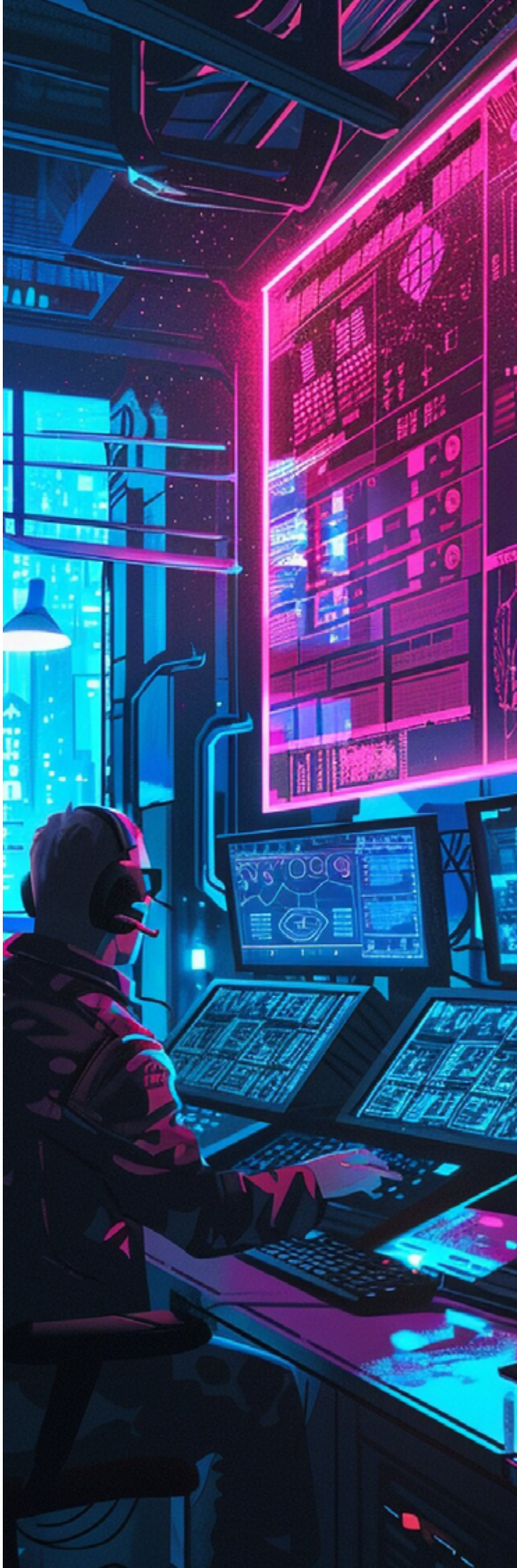
Asimismo, en la notificación a la AEPD se consideran diferentes categorías como datos básicos, de contacto y económicos, medios de pago, credenciales de acceso, religión, origen racial, etcétera.

Con el fin de facilitar este proceso la AEPD pone a disposición dos **herramientas**:

- **ASESORA BRECHA:** Un recurso útil para evaluar de manera eficaz la necesidad de notificar la brecha sin demora innecesaria. La herramienta es accesible desde el siguiente enlace.
- **Comunica-Brecha RGPD:** Herramienta que permite evaluar la obligación de notificar a las personas físicas afectadas por una brecha de seguridad en sus datos personales. Se encuentra disponible en la siguiente página web de la AEPD.

Periodo de entrega

El **plazo** para notificar a la autoridad de control es de **72 horas** desde que la organización tiene constancia de la brecha, de acuerdo con el Reglamento General de Protección de Datos.



Resumen y conclusión

En términos generales, los **CSIRT (CCN-CERT, ESPDEF-CERT** e **INCIBE-CER**T) y las entidades como el **BE** y el **CSIRT-MIR-PJ** tienen roles complementarios pero diferenciados. **CCN-CERT** actúa como el organismo principal para incidentes de seguridad nacional, **INCIBE-CERT** se encarga de coordinar con el sector privado, el **BE** supervisa la ciberseguridad del sistema financiero, y el **CSIRT-MIR-MJ** de la **OCC** se centra en la protección de infraestructuras críticas, incluyendo aquellas con impacto en la Defensa.

AEPD gestiona específicamente los incidentes que implican datos personales, mientras que el **ESPDEF-CERT** se ocupa de los incidentes de ciberseguridad dentro de las Fuerzas Armadas y la Defensa Nacional.

En la **figura 10** se definen las relaciones entre las autoridades y entidades en función del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.

Normativas y guías de referencia

Estas entidades y autoridades actúan dentro de un marco normativo y siguiendo guías de referencia para garantizar una gestión adecuada de los incidentes de ciberseguridad:

- **Real Decreto-ley 12/2018, de 7 de septiembre**, de seguridad de las redes y sistemas de información.
- **Real Decreto 43/2021**, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- *Guía nacional de notificación y gestión de incidentes de ciberseguridad.*

Además, de manera individual, cada entidad se rige por las siguientes normativas y guías:

- **CCN-CERT:** Guía CCN-STIC 817 de Gestión de Incidentes de Ciberseguridad.
- **INCIBE-CERT:** Procedimiento de gestión de incidentes de ciberseguridad para el sector privado y la ciudadanía.
- **AEPD:** Reglamento General de Protección de Datos (RGPD).
- **BE:** Procedimiento de notificación de incidentes de ciberseguridad relevantes de las entidades de crédito bajo supervisión directa del Banco de España.
- **Centro Nacional de Ciberseguridad:** Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.

A continuación, a modo de resumen, se lista el conjunto de CSIRT y entidades de referencia en función de su ámbito competencial, así como la relación entre ellos.

Tabla 3
Alcance, Competencia y Relación entre Entidades en la Gestión de Incidentes de Ciberseguridad

Entidad	Normativa	Competencia
INCIBE-CERT	-	Protección de la ciberseguridad nacional, apoyo a empresas y ciudadanía, formación y sensibilización.
CCN-CERT	• Esquema Nacional de Seguridad - Real Decreto 311/2022, de 3 de mayo	Protección de infraestructuras críticas, gestión de incidentes de ciberseguridad en el ámbito público y sectores estratégicos.
CSIRT-MIR-PJ	• Ley 8/2011, de 28 de abril, de protección de infraestructuras críticas • Real Decreto 704/2011, de 20 de mayo, Reglamento PIC • Anteproyecto de Ley de Protección y Resiliencia de Entidades Críticas • CER2 - Directiva (UE) 2022/2557	Protección de infraestructuras críticas (energía, telecomunicaciones...), coordinación de incidentes en estos sectores.
Centro Nacional de Ciberseguridad	• Directiva NIS2 - Directiva (UE) 2022/2555	Autoridad nacional competente y punto único de contacto en materia de gobernanza de ciberseguridad.
ESPDEF-CERT	• Ley Orgánica 5/2005, de 17 de noviembre, Defensa Nacional • Ley 36/2015, de 28 de septiembre, Seguridad Nacional	Ciberseguridad y respuesta ante incidentes dentro del ámbito de la Defensa Nacional.
BE	• Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito • DORA - Reglamento (UE) 2022/2554 • eIDAS 2 - Reglamento (UE) 2024/1183	Ciberseguridad en el sector financiero, supervisión de la resiliencia del sistema financiero.
AEPD	• Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales, LOPDGDD • (Ley Orgánica 3/2018, de 5 de diciembre) • Reglamento General de Protección de Datos, RGPD • Reglamento (UE) 2016/679	Protección de datos personales, supervisión de incidentes relacionados con violaciones de privacidad.

Alcance	Relación con otras entidades
Empresas privadas, ciudadanía y pymes.	Colabora con el CCN-CERT en incidentes de impacto público-privado, y con el ESPDEF-CERT en infraestructuras críticas vinculadas a la defensa. Coordina con el CSIRT-MIR-PJ de la OCC para gestionar incidentes en operadores críticos, notifica fugas de datos a la AEPD e informa al BE sobre incidentes de ciberseguridad en el sector financiero
Sector público, infraestructuras críticas, organismos gubernamentales, y defensa nacional.	Coordina con INCIBE-CERT casos donde el sector público colabore con entidades privadas, ESPDEF-CERT si afecta a la defensa nacional, el CSIRT-MIR-PJ de la OCC a incidentes en infraestructuras críticas y la AEPD en casos de fugas de datos personales en el sector público.
Infraestructuras críticas de sectores como energía, telecomunicaciones, transporte, y sector público.	Colabora con CCN-CERT, ESPDEF-CERT, e INCIBE-CERT en incidentes que afectan operadores críticos y la continuidad de servicios esenciales. Con AEPD si afecta a protección de datos y el BE sobre infraestructuras del sector financiero.
Entidades públicas o privadas que se encuentren dentro de sectores de alta criticidad.	De acuerdo con el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, será el punto de contacto para los CSIRTs nacionales de referencia.
Fuerzas Armadas, Ministerio de Defensa, infraestructuras y operaciones militares.	Colabora con CCN-CERT, CSIRT-MIR-PJ e INCIBE-CERT en la gestión de incidentes que afecten a la Defensa Nacional y las Fuerzas Armadas.
Entidades financieras y sistemas de pago, con énfasis en infraestructuras críticas del sistema financiero.	Trabaja con INCIBE-CERT y el CSIRT-MIR-PJ de la OCC sobre incidentes de ciberseguridad que puedan afectar servicios financieros críticos. AEPD en brechas de datos que afectan al sistema financiero y junto al CCN-CERT en incidentes graves que involucren instituciones públicas.
Todos los sectores que gestionan datos personales.	Recibe notificaciones de fugas de datos desde CCN-CERT, INCIBE-CERT y operadores críticos coordinados por el CSIRT-MIR-PJ de la OCC. Colabora con el BE si afecta a datos financieros de clientes.

Adicionalmente, a modo resumen, se lista la obligación de notificación en función del nivel de peligrosidad del incidente y el plazo de reporte a través de los canales de contacto establecidos.

Tabla 4
Plazo, Obligación de Notificación y Canal de Contacto de las Entidades para la Gestión de Incidentes de Ciberseguridad

Entidad	Obligación de notificación	Plazo de notificación	Canal de Contacto
INCIBE-CERT	Cuando el incidente tenga nivel de peligrosidad crítico, muy alto o alto. **Según el Real Decreto 43/2021, de 26 de enero*	La notificación inicial para incidentes críticos, muy altos y altos deberá ser inmediata. Para medio y bajo será de carácter voluntario, aunque recomendado. **Según el Real Decreto 43/2021, de 26 de enero*	• Formulario web • Correo electrónico: ▪ Ciudadanos, empresas y proveedores de servicios digitales: incidencias@incibe-cert.es ▪ Instituciones afiliadas a RedIRIS: iris@incibe-cert.es ▪ Operadores esenciales y de infraestructuras críticas: pic@incibe-cert.es
CCN-CERT	Cuando el incidente tenga nivel de peligrosidad crítico, muy alto o alto. **Según el Real Decreto 43/2021, de 26 de enero*	La notificación inicial para incidentes críticos, muy altos y altos deberá ser inmediata. Para medio y bajo será de carácter voluntario, aunque recomendado. **Según el Real Decreto 43/2021, de 26 de enero*	▪ Correo electrónico: incidentes@ccn-cert.cni.es Herramienta: LUCIA
CSIRT-MIR-PJ (OCC)	Cuando el incidente tenga nivel de peligrosidad crítico, muy alto o alto. **Según el Real Decreto 43/2021, de 26 de enero*	La notificación inicial para incidentes críticos, muy altos y altos deberá ser inmediata. Para medio y bajo será de carácter voluntario, aunque recomendado. **Según el Real Decreto 43/2021, de 26 de enero*	▪ Correo electrónico: cert@cnpic.interior.es
Centro Nacional de Ciberseguridad	Cuando el incidente se considere significativo. **Según el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad*	• Alerta temprana: 24 horas • Notificación completa: 72 horas • Informe final: Plazo máximo de un mes **Según el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad*	• Plataforma Nacional de Notificación y Seguimiento de Incidentes de Ciberseguridad (web) **Según el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad* *(La plataforma aún no se encuentra en funcionamiento)*

Entidad	Obligación de notificación	Plazo de notificación	Canal de Contacto
ESPDEF-CERT	Para incidentes relacionados con la Defensa Nacional o las Fuerzas Armadas que puedan afectar la seguridad nacional. **Según el Real Decreto 43/2021, de 26 de enero*	La notificación inicial para incidentes críticos, muy altos y altos deberá ser inmediata. Para medio y bajo será de carácter voluntario, aunque recomendado. **Según el Real Decreto 43/2021, de 26 de enero*	• Correo electrónico: espdef-cert@mde.es
BE	Cuando el incidente se considere grave. En caso de no ser grave, pero sí relevante, también es obligatorio notificarlo. Un incidente se considera grave cuando afecta a todas las entidades financieras sujetas al Reglamento (UE) 2022/2554 (DORA) y se considera relevante cuando afecta solo a las entidades bajo supervisión directa del BE.	Desde que se considera relevante el incidente: Carácter inmediato Desde que se considera grave el incidente: 1º Informe: 4 horas 2º Informe: 72 horas 3º Informe: Un mes **Conforme al Procedimiento de Notificación de incidentes graves y amenazas importantes bajo normativa DORA*	• Plantilla de informe de incidente grave DORA en formato Excel. • Correo electrónico: Ciberincidentes@bde.es
AEPD	Todas las brechas de seguridad, a excepción de aquellas en las que el responsable pueda garantizar que es improbable que supongan un riesgo para los derechos y las libertades de las personas físicas. **Según el Reglamento General de Protección de Datos*	En las primeras 72 horas desde la detección del incidente. **Según el Reglamento General de Protección de Datos*	• Formulario de notificación de brechas de datos personales en línea a través de la página web de la AEPD

Según lo establecido en el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, la Plataforma Nacional de Notificación y Seguimiento de Cibereincidentes se integrará como un canal adicional y complementario a los canales de comunicación correspondientes a las autoridades de control recogidas en la presente tabla. A fecha de informe, la Plataforma se encuentra creada pero no está en funcionamiento.

Por otro lado, cabe destacar lo establecido en la Disposición Transitoria Tercera del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, que indica lo siguiente:

> *"Régimen transitorio: Hasta que inicie sus actividades el Centro Nacional de Ciberseguridad, conservarán transitoriamente su vigencia las disposiciones del Real Decreto-ley 12/2018, de 7 de septiembre, y del Real Decreto 43/2021, de 26 de enero, relativas a las autoridades competentes, CSIRT nacionales de referencia y punto de contacto único".*

Esta previsión normativa da lugar, en la práctica, a dos escenarios diferenciados:

- Hasta la **entrada en funcionamiento del Centro Nacional de Ciberseguridad**, se mantienen vigentes las disposiciones del Real Decreto-ley 12/2018 y del Real Decreto 43/2021 en lo relativo a autoridades competentes, CSIRT de referencia y punto de contacto único.
- Una vez esté **operativo el Centro Nacional de Ciberseguridad**, aunque no se establece expresamente en la disposición, el Real Decreto 43/2021 continuará siendo aplicable a aquellas entidades que queden fuera del ámbito de aplicación de la nueva ley, es decir, aquellas entidades que no estén clasificadas como entidades esenciales o importantes conforme a la Directiva NIS2, mientras no se apruebe un régimen específico para ellas.

Situación de la UE

La notificación de incidentes de ciberseguridad en la UE es fundamental para proteger infraestructuras críticas, servicios esenciales y datos sensibles ante las crecientes amenazas digitales. Establecida principalmente por la Directiva NIS2, esta obligación busca asegurar que los incidentes importantes sean informados de manera rápida y efectiva a las autoridades competentes, permitiendo una respuesta ágil y coordinada.

La Directiva NIS2 amplía el alcance de su predecesora, la Directiva NIS[XXXVII], incluye tanto al sector público como privado en áreas clave como la energía, el transporte, las telecomunicaciones y la salud. Esta normativa regula tanto los plazos como el contenido de las notificaciones, promoviendo la armonización y el intercambio de información entre los Estados miembros.

Gracias a herramientas como **Red de CSIRT**[XXXVIII], el **EU-CyCLONe**[XXXIX] y las plataformas nacionales, la Unión Europea ha creado un sistema sólido que no solo facilita la gestión de incidentes, sino que también ayuda en el análisis y prevención de futuros ataques. Una notificación eficaz contribuye a mejorar la resiliencia de ciberseguridad de la región, asegurar la continuidad de los servicios esenciales y fortalecer la confianza de los ciudadanos en un entorno cada vez más digitalizado.

Marco normativo

En la UE, la notificación de incidentes de ciberseguridad está regulada por varias leyes y directivas que determinan lo que deben hacer las entidades cuando se enfrentan a estos incidentes, obligándolas a informar a las autoridades correspondientes. Estas normativas tienen como objetivo asegurar una respuesta rápida y coordinada ante las amenazas de ciberseguridad y mejorar constantemente las defensas digitales en toda la región.

Tabla 5
Marco Normativo Europeo para la notificación de incidentes de seguridad[30]

Directiva	Descripción	Alcance
NIS1 **Directiva (UE) 2016/1148 del parlamento europeo y del consejo**	La Directiva NIS de la Unión Europea establece medidas para mejorar la ciberseguridad en redes y sistemas de información, protegiendo servicios esenciales como energía, transporte, banca y salud. Exige que los operadores de servicios esenciales y proveedores de servicios digitales implementen medidas de seguridad y notifiquen incidentes significativos a las autoridades competentes o a los equipos de respuesta ante incidentes (CSIRT).	Entidades recogidas en el anexo II
NIS2 **Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo**	La Directiva NIS2 refuerza y amplía la Directiva NIS para mejorar la ciberseguridad en la Unión Europea. Establece medidas más estrictas para proteger sectores esenciales y relevantes, como energía, transporte, salud y servicios digitales. Exige a los operadores de servicios esenciales y proveedores de servicios digitales notificar incidentes significativos a las autoridades competentes o a los equipos de respuesta ante incidentes (CSIRT) y aplicar medidas de seguridad más robustas, garantizando una cooperación transfronteriza más eficaz.	Entidades recogidas en el anexo I y anexo II
DORA **Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo**	La Ley DORA (*Digital Operational Resilience Act*) es una regulación de la Unión Europea que busca reforzar la seguridad de las Tecnologías de la Información y Comunicación (TIC) en instituciones financieras como bancos, aseguradoras y corredurías de inversión.	Servicios TIC a entidades financieras
eIDAS **Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo**	Regulación de la Unión Europea destinada a estandarizar la identificación, los servicios electrónicos de confianza y las transacciones de comercio electrónico en la UE.	Se aplica a toda la Unión Europea y se adapta a algunas entidades fuera de la UE
eIDAS 2 **Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo**	Introduce una extensa renovación de la Regulación eIDAS introduciendo un marco efectivo a escala de la UE para los esquemas de la Cartera de identidad Digital Europea.	General y transfronterizo, diseñado para todos los ciudadanos y empresas de la UE, cubriendo tanto servicios públicos como privados bajo una identidad digital común.

[30] 2024 *Report on the State of the Cybersecurity in the Union.*

Artículo sobre la notificación Nacional	Transposición Española
Artículo 14: Los operadores de servicios esenciales (OES) deben notificar a la autoridad competente o al CSIRT los incidentes con un impacto significativo en la continuidad de sus servicios. **Artículo 16**: Los proveedores de servicios digitales (DSP), como mercados en línea, motores de búsqueda y servicios de computación en la nube, deben informar sobre incidentes con un impacto sustancial en la prestación de sus servicios.	Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre
Artículo 23: establece la obligación de los Estados miembros de garantizar que las entidades esenciales e importantes incidente que tenga un impacto significativo en la prestación de sus servicios.	Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad
El artículo 19 establece que, en caso de una violación de la seguridad de los datos personales, el responsable del tratamiento debe notificarlo al Supervisor Europeo de Protección de Datos.	Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011.
El artículo 19 establece la obligación de los prestadores de servicios de confianza cualificados y no cualificados de notificar cualquier violación de la seguridad o pérdida de integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales conservados en el mismo	Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
El artículo 19 bis: los prestadores no cualificados notificarán al organismo de supervisión, a las personas afectadas identificables, al público si es de interés público y, cuando proceda, a otras autoridades competentes pertinentes cualquier violación de la seguridad o interrupción en la prestación del servicio. **El artículo 24.2**: los prestadores cualificados notificarán al organismo de supervisión, a las personas afectadas identificables, al público si es de interés público y, cuando proceda, a otras autoridades competentes pertinentes cualquier violación de la seguridad o interrupción en la prestación del servicio.	Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital.

Directiva	Descripción	Alcance
EECC **Directiva (UE) 2018/ del Parlamento Europeo y del Consejo**	Garantizar que los proveedores de redes y servicios de comunicación adopten medidas técnicas y organizativas adecuadas para gestionar los riesgos de seguridad.	Proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público
CER2 **Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo**	Establecer obligaciones y normas con el fin de que las entidades críticas aumenten su resiliencia en el mercado interior, así como sus capacidades para prevenir, proteger, responder y recuperarse ante posibles incidente	El alcance abarca once sectores: energía, transporte, banca, infraestructuras de los mercados financieros, banca, sanidad, agua potable, aguas residuales, infraestructura digital, administración pública, espacio y producción, transformación y distribución de alimentos
Regulación (EU) 2018/1725 del Parlamento Europeo y del Consejo	Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos	Tratamiento de datos personales por parte de todas las instituciones y organismos de la Unión
Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo	Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos	Tratamiento de datos personales por parte de las autoridades competentes
Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo	Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos	Tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero

Artículo sobre la notificación Nacional	Transposición Española
El artículo 40 establece la obligación de los Estados miembros de garantizar que los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público notifiquen los incidentes de seguridad que tengan un impacto significativo en el funcionamiento de las redes o servicios. Cabe señalar que el artículo 40-41 del EECC queda derogado por la NIS2.	Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas.
El artículo 15 establece que los Estados miembros se asegurarán de que las entidades críticas notifiquen sin demora indebida a la autoridad competente los incidentes que perturben o puedan perturbar de forma significativa la prestación de servicios esenciales. Para ello, las entidades críticas deben presentar en un plazo de 24 horas una notificación inicial, seguida de un informe detallado en el plazo máximo de un mes.	Anteproyecto de Ley de Protección y Resiliencia de las Entidades Críticas (Ley CER2) **A fecha de informe no se encuentra transpuesta*
Artículo 34 exige al responsable del tratamiento, en caso de violación de seguridad de datos personales, se notifique al Supervisor Europeo de Protección de Datos.	Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) nº 45/2001 y la Decisión nº 1247/2002/CE.
Artículo 30 dispone que, en caso de una violación de la seguridad de los datos personales, el responsable del tratamiento debe notificarlo a la autoridad de control correspondiente.	Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
Artículo 33 establece que, en caso de una violación de la seguridad de los datos personales, el responsable del tratamiento debe notificarlo a la autoridad de control competente.	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

El marco legal de la Unión Europea para la notificación de incidentes de ciberseguridad es clave para asegurar una respuesta rápida y coordinada ante las amenazas de ciberseguridad. Normativas como la Directiva NIS2, la Regulación eIDAS, la ley DORA, el Código Europeo de Comunicaciones Electrónicas (EECC), la Directiva CER2 y las leyes de protección de datos crean un conjunto de obligaciones que refuerzan la ciberseguridad en toda la región.

Estas leyes fomentan la colaboración entre los países de la UE y las autoridades competentes, garantizando la protección de infraestructuras críticas y manteniendo la confianza de los ciudadanos en un entorno digital cada vez más complejo.

Proceso de notificación de la NIS2[31]

El objetivo de La Directiva NIS2 es crear un marco sólido para garantizar la ciberseguridad en la Unión Europea. Según el artículo 8.4, cada país de la UE debe designar un punto de contacto único, encargado de coordinar la cooperación con los puntos de contacto de otros países. Este sistema permite una respuesta rápida y coordinada ante incidentes de ciberseguridad a escala europea.

Ámbito de actuación de la NIS2

La Directiva NIS2 amplía considerablemente lo que cubría la Directiva NIS original, implementando medidas más estrictas para asegurar la ciberseguridad en sectores clave. Esta nueva normativa está destinada a aplicarse a organizaciones que cumplen con ciertos criterios de relevancia estratégica, como aquellas que son el único proveedor de un servicio esencial en un país o aquellas cuyo cese de actividades pueda tener graves consecuencias para la seguridad pública, el orden o la salud pública.

La NIS2 regula dos tipos de sectores: los denominados sectores esenciales y los sectores importantes, que abarcan una gama más amplia de actividades económicas y sociales que son cruciales.

A continuación, se presentan los sectores afectados, clasificados en estas dos categorías.

1. Sectores esenciales

Los sectores esenciales abarcan actividades cuya interrupción o fallo podría tener un impacto significativo en la sociedad, la economía o la seguridad nacional. Estos sectores están detallados en el anexo I de la NIS2 e incluyen, entre otros:

1. Energía:
   - Electricidad (incluida la generación, distribución y transmisión).
   - Petróleo (infraestructuras y oleoductos).
   - Gas (incluido el almacenamiento y transporte).
2. Transporte:
   - Transporte aéreo (aerolíneas, aeropuertos, servicios de navegación aérea).
   - Transporte ferroviario (operadores y redes).
   - Transporte marítimo (puertos, operadores de servicios marítimos y fluviales).
   - Transporte por carretera (operadores y sistemas de gestión del tráfico).
3. Banca y servicios financieros:
   - Banca digital y servicios de pago electrónico.
   - Infraestructuras digitales.
4. Proveedores de servicios de Internet:
   - Centros de datos y redes de telecomunicaciones.
   - Servicios de computación en la nube.
5. Agua potable y aguas residuales:
   - Sistemas de abastecimiento y tratamiento de aguas.

[31] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo.

6. Gestión de servicios de TIC:
   - Proveedores de servicios gestionados.
   - Proveedores de servicios de seguridad gestionados.
7. Salud:
   - Hospitales y otros proveedores de asistencia sanitaria.
   - Laboratorios de análisis médicos.
   - Centros de investigación biomédica.
8. Administración pública:
   - Organismos gubernamentales clave que gestionan servicios esenciales.
9. Espacio:
   - Operadores de infraestructuras terrestres donde la propiedad, gestión y explotación descansa en los Estados miembros.
   - Entidades privadas que apoyan la prestación de servicios espaciales.

2. Sectores importantes

Los sectores importantes comprenden actividades económicas críticas que, aunque no se consideran esenciales, son fundamentales para la seguridad y el buen funcionamiento de la economía. Estos sectores están enumerados en el **anexo II** de la NIS2 e incluyen, entre otros:

1. Fabricación y producción
   - Fabricación de productos farmacéuticos.
   - Producción de dispositivos médicos.
   - Industria alimentaria, en especial empresas de distribución y procesamiento.
2. Proveedores de servicios digitales
   - Motores de búsqueda.
   - Mercados en línea.
3. Residuos y gestión de residuos
   - Gestión de residuos peligrosos y reciclaje.
4. Servicios postales y de mensajería
   - Empresas que operan en la logística de envíos y paquetes esenciales.
5. Investigación y desarrollo
   - Centros de innovación tecnológica relacionados con sectores críticos.
6. Producción, transformación de alimentos
   - Empresas que operan en la producción de alimentos, en su transformación y su distribución.

Incidentes cubiertos por las obligaciones de notificación

En la Directiva NIS2 se establece que las entidades deben informar sobre los incidentes que sean considerados graves, es decir, que interrumpan de forma significativa servicios esenciales o importantes, y afecten a la continuidad de operaciones clave o la seguridad de datos sensibles.

Esta medida tiene como objetivo asegurar que los incidentes que puedan afectar a la sociedad o a sectores cruciales sean atendidos de manera rápida y coordinada.

Algunos de los incidentes más frecuentes que deben ser notificados incluyen:

1. **Ataques de *ransomware*** dirigidos a infraestructuras críticas, como hospitales, sistemas de transporte o redes de energía, donde la paralización puede tener consecuencias severas para la población.

1. **Fallos técnicos** originados por la explotación de vulnerabilidades conocidas, que pueden derivar en la interrupción de servicios esenciales, como telecomunicaciones o suministro de agua.

Proceso de notificación

Se establece que las entidades están obligadas a reportar un incidente en un plazo máximo de 24 horas desde su detección. Esto es muy importante para garantizar una respuesta temprana y coordinar las acciones necesarias para mitigar el impacto del ataque.

La notificación inicial no requiere incluir todos los detalles del incidente; pudiéndose limitar a un informe preliminar que describa la situación de manera general.

Posteriormente, una vez recopilados todos los datos relevantes, se deberá presentar un informe completo con información detallada sobre el incidente y las medidas adoptadas.

1. **Notificación inicial:**

En las primeras 24 horas desde la detección del incidente, la entidad afectada debe presentar al CSIRT o a la autoridad competente una alerta temprana. Esta notificación indicará la sospecha de un incidente significativo, el cual podría deberse a acciones ilícitas o malintencionadas, y, en su caso, incluirá la posibilidad de repercusiones transfronterizas.

2. **Informe inicial:**

En un plazo máximo de 72 horas, la entidad afectada debe presentar una notificación ampliada del incidente. Este informe debe actualizar la información previamente enviada y complementarla con una evaluación inicial del incidente significativo, incluyendo:

- La gravedad y el impacto del incidente.
- Los indicadores de compromiso identificados.

3. **Informe final:**

En un plazo máximo de un mes desde la presentación del informe inicial, la entidad deberá entregar un informe completo que incluya los siguientes elementos:

- Una descripción detallada del incidente, su gravedad e impacto.
- El tipo de amenaza o la causa principal que probablemente haya desencadenado el incidente.
- Las medidas paliativas aplicadas y las que estén en curso.
- Las repercusiones transfronterizas del incidente, si las hubiera.

En el caso de que el incidente siga en curso en el momento de la presentación del informe final, los Estados miembros se encargarán de que las entidades afectadas presenten un informe de situación en ese momento y un informe final a partir de que hayan gestionado el incidente.

Mecanismos de comunicación para la cooperación

La Unión Europea ha implementado un sistema de colaboración integral que busca garantizar una respuesta eficaz y coordinada ante incidentes de ciberseguridad. Este enfoque incluye diversas plataformas, normativas y organismos que trabajan conjuntamente para compartir información técnica, coordinar acciones y gestionar crisis de manera eficiente.

Ley de Cibersolidaridad de la UE (CSA)

La Ley de Cibersolidaridad de la UE (*Cyber Solidarity Act*), en vigor desde el 4 de febrero de 2025, establece un marco para mejorar la resiliencia cibernética de la UE, al fortalecer la detección, preparación y respuesta ante incidentes de ciberseguridad. Sus componentes principales son:

- **Sistema europeo de alerta de ciberseguridad:** Creación de una red de Centros de Operaciones de Seguridad (SOC) nacionales y transfronterizos que emplean tecnologías avanzadas para detectar y compartir alertas sobre amenazas cibernéticas en tiempo real.
- **Mecanismo de emergencia en ciberseguridad:** Acciones de preparación para detectar posibles

vulnerabilidades, la creación de una reserva de ciberseguridad de la UE con proveedores de servicios de respuesta a incidentes y ofrecer asistencia mutua entre Estados miembro afectados por los incidentes.

- **Mecanismo de revisión de incidentes de ciberseguridad:** La Agencia de Ciberseguridad de la UE (ENISA) será la responsable de revisar los incidentes de ciberseguridad significativos o a gran escala y, tras ello, deberá presentar un informe que incluya lecciones y recomendaciones para mejorar la respuesta ante estos incidentes.

Para asegurar una correcta interoperabilidad técnica, ENISA, junto a la Comisión Europea, deben emitir unas directrices de interoperabilidad, teniendo como plazo máximo el 5 de febrero de 2026, que especifiquen los formatos y protocolos de puesta en común de información de los centros cibernéticos transfronterizos.

Red de CSIRTs: intercambio y coordinación operativa

La Red de CSIRTs (Equipos de Respuesta a Incidentes de Seguridad Informática) es una herramienta clave para gestionar los incidentes de ciberseguridad en la Unión Europea. Conecta a los equipos nacionales de respuesta a incidentes de ciberseguridad de los Estados miembros, facilitando el intercambio continuo de información técnica en tiempo real.

Gracias a esta red, se pueden identificar y analizar nuevas amenazas, compartir datos sobre ataques en curso y coordinar estrategias para minimizar sus efectos. Su estructura operativa permite una respuesta rápida y efectiva, especialmente en situaciones que requieren cooperación entre países. Así, la Red de CSIRTs actúa como un puente vital entre los equipos técnicos de diferentes naciones, garantizando una gestión coherente y eficiente de los incidentes de ciberseguridad.

NIS Cooperation Group: colaboración estratégica y buenas prácticas

A nivel estratégico, el NIS Cooperation Group juega un papel clave en mejorar la ciberseguridad en toda la región. Este grupo reúne a representantes de los países miembros para fomentar la cooperación más allá de la respuesta inmediata a los incidentes.

Su objetivo principal es promover el intercambio de experiencias, conocimientos y buenas prácticas entre los países. También trabaja en la creación de procedimientos comunes para la notificación de incidentes, lo que ayuda a estandarizar y hacer más eficaz la respuesta a las amenazas de ciberseguridad. Así, el NIS Cooperation Group proporciona una base sólida para reforzar la resiliencia de la Unión Europea frente a los retos digitales.

EU-CyCLONe: gestión de crisis de ciberseguridad complejas

En situaciones de gran envergadura, como las crisis de ciberseguridad que afectan a varios países o sectores, entra en juego el EU-CyCLONe (*EU Cyber Crises Liaison Organisation Network*). Este organismo se diseñó con el fin de coordinar la respuesta a incidentes de gran impacto, asegurando que todos los países involucrados actúen de manera conjunta.

El EU-CyCLONe se encarga de gestionar la comunicación operativa a nivel estratégico, al crear un canal directo entre los responsables de la toma de decisiones en cada país. Su objetivo es garantizar que las respuestas sean rápidas, coherentes y adaptadas a las características de cada crisis. Además, trabaja para reducir el impacto de los incidentes y restaurar la normalidad en los sistemas afectados lo más rápido posible.

Centralización de los datos y el papel de ENISA en la ciberseguridad europea

ENISA juega un papel clave a la hora de mejorar la ciberseguridad en toda la región al ser el centro donde se recopilan, analizan y coordinan la información sobre incidentes

de ciberseguridad. No solo centraliza los datos proporcionados por las autoridades nacionales competentes, sino que también les da un enfoque estratégico, lo que ayuda a identificar tendencias, patrones y amenazas emergentes que podrían afectar a varios países miembros.

Centralización de datos y análisis estratégico

ENISA recoge los datos que provienen de las notificaciones enviadas por los puntos de contacto únicos de cada país miembro. Para facilitar su análisis, esta información se presenta de forma estandarizada, lo que permite a la agencia consolidarla de forma eficiente y detectar patrones comunes en los incidentes reportados. Este enfoque no solo ayuda a entender mejor el panorama de ciberseguridad europeo, sino que también a identificar vulnerabilidades clave y áreas prioritarias para prevenir futuras amenazas.

Gracias a este proceso de centralización y análisis, ENISA juega un papel crucial en la coordinación de estrategias futuras, al asegurar que las respuestas y medidas preventivas sean coherentes y se basen en información sólida. Esto fortalece la capacidad de los países miembros para anticiparse a las amenazas y reducir los riesgos antes de que se conviertan en problemas mayores.

Informes periódicos y colaboración internacional

La integración de datos no se limita al análisis interno. ENISA también promueve la transparencia y la colaboración entre los Estados miembros mediante la elaboración de informes periódicos que consolidan y comparten los hallazgos clave:

- **Cada tres meses**, los puntos de contacto únicos envían a ENISA resúmenes anonimizados y agregados sobre incidentes significativos, amenazas de ciberseguridad e incluso incidentes potenciales o cuasi-incidentes. Estos informes proporcionan una visión general de la actividad de ciberseguridad reciente y permiten a ENISA identificar tendencias y patrones emergentes.
- **Cada seis meses**, ENISA elabora un informe consolidado basado en la información recibida. Este documento se comparte con el NIS Cooperation Group y la Red de CSIRTs, fomentando una colaboración más estrecha entre los países miembros y mejorando la ciberseguridad en toda la región.

Proceso de notificación DORA[32]

El proceso de notificación de incidentes graves relacionados con las tecnologías de la información y la comunicación (TIC), regulado por el Reglamento de Resiliencia Operativa Digital (Reglamento (UE) 2022/2554), establece cómo las entidades financieras deben informar sobre problemas que afecten sus sistemas tecnológicos.

El objetivo de este procedimiento es asegurarse de que las autoridades competentes sean notificadas de manera rápida, para que puedan responder de forma eficaz y coordinada, al reducir los riesgos y minimizando el impacto de estos incidentes.

Ámbito de actuación de DORA

El presente reglamento se aplica a una amplia gama de entidades relacionadas con el sector financiero y tecnológico, denominadas colectivamente entidades financieras, así como a proveedores terceros de servicios de tecnologías de la información y comunicación (TIC).

Proceso de notificación

Las entidades financieras deben notificar los incidentes graves relacionados con las TIC a la autoridad competente. De acuerdo con el reglamento, un incidente grave es "un incidente relacionado con las TIC con graves repercusiones negativas en las redes y sistemas de información que sustentan funciones esenciales o importantes de la entidad financiera".

[32] Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo.

1. **Notificación inicial:**
   Las entidades financieras deben presentar un informe preliminar tras detectar un incidente grave relacionado con las TIC. Este informe inicial incluye información necesaria para evaluar la importancia del incidente y sus posibles efectos transfronterizos.
2. **Informe intermedio:**
   Si la situación del incidente evoluciona o se dispone de información adicional relevante, se deben emitir actualizaciones. Estas también se generan cuando la autoridad competente lo solicita.
3. **Informe final:**
   Una vez concluido el análisis del incidente, se presenta un informe completo. Este incluye la causa subyacente, los impactos reales, y las medidas adoptadas para mitigar el problema y prevenir incidentes futuros.

Reporte a autoridades

Una vez que la autoridad competente reciba la notificación inicial y los informes relacionados, debe facilitar información detallada sobre el incidente grave relacionado con las TIC a las siguientes partes destinatarias, en función de sus competencias respectivas:

- Autoridades no financieras públicas, como las designadas en virtud de la Directiva NIS2 (UE) 2022/2555.
- Autoridades de protección de datos nacionales, cuando el incidente afecte la privacidad o seguridad de los datos personales.
- Autoridades policiales, en caso de que el incidente tenga un carácter delictivo.
- Equipos de respuesta a incidentes de seguridad informática (CSIRTs), para garantizar asistencia técnica rápida y eficiente.

Cualquier otra autoridad relevante designada según la legislación de la UE o de los Estados miembros que aplique al incidente. Esta distribución asegura una coordinación adecuada y la gestión eficiente de los riesgos relacionados con las TIC.

Proceso de notificación eIDAS 2[33]

El Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del **marco europeo de identidad digital (Reglamento eIDAS 2)** tiene por objeto garantizar el correcto funcionamiento del mercado interior y la existencia de un nivel de seguridad adecuado de los medios de identificación electrónica y los servicios de confianza utilizados en toda la UE.

Con la finalidad de permitir y facilitar que las personas físicas y jurídicas ejerzan el derecho a participar en la sociedad digital de una forma segura y a acceder a los servicios del sector público y privado en línea en toda la Unión Europea.

De acuerdo con el artículo 46, cada Estado miembro debe nombrar un punto de contacto único responsable de coordinar la cooperación con los puntos de contacto de otros países. Para facilitar este trabajo conjunto y el intercambio de información, la Comisión Europea creará el Grupo de Cooperación sobre la Identidad Digital Europea[XL].

Ámbito de actuación de la eIDAS 2

El Reglamento amplía el ámbito de aplicación del **marco de identidad digital en la Unión Europea**, por lo que promueve una infraestructura digital armonizada, facilitando de esta forma la identificación electrónica transfronteriza, y fortaleciendo la confianza en lo que respecta a los servicios digitales.

Para ello se implanta un marco de identidad digital armonizado que reduzca los obstáculos digitales entre los Estados miembros y capacite a la ciudadanía de la Unión Europea y a cuantos residen en ella para que gocen de los beneficios de la digitalización, al mismo tiempo que se incrementa la transparencia y la protección de sus derechos.

[33] Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo.

Proceso de notificación

El proceso de notificación depende del tipo de entidad afectada:

- En caso de que un **prestador cualificado de servicios de confianza** detecte un incidente de seguridad que tenga un impacto significativo en la prestación o fiabilidad del servicio, deberá notificarlo sin demora indebida a la autoridad supervisora nacional competente.

  Si el incidente afecta directa o indirectamente a la seguridad, confidencialidad o integridad de los datos de las personas usuarias, el prestador o prestadora también deberá informar a las personas afectadas y adoptar las medidas necesarias para mitigar el daño y restaurar el servicio.

- Si se produce una violación de seguridad que compromete parcial o totalmente la fiabilidad de las **Carteras de Identidad Digital Europeas (EUDI Wallets)**, el Estado miembro responsable deberá suspender de forma inmediata la provisión y el uso de dichas carteras. Además, deberá notificar a cuantos resulten afectados, al punto de contacto único nacional designado y a la Comisión Europea (si el incidente tiene impacto transfronterizo o gravedad elevada). Si la violación de seguridad no ha sido resuelta en el plazo de **tres meses**, el Estado miembro debe proceder a la retirada definitiva de las carteras y revocar su validez, así como informar de nuevo a las usuarias y los usuarios afectados y al punto único de contacto. Una vez resuelto el incidente, el Estado miembro puede restablecer la provisión y el uso de las carteras europeas de identidad digital e informará de ello a los usuarios afectados y a su punto de contacto único.

Proceso de notificación CER2[34]

La **Directiva (UE) 2022/2557**, conocida como Directiva de Resiliencia de Entidades Críticas (CER2) y por la que se deroga la Directiva (UE) 2008/114/CE del Consejo (Directiva CER1), tiene como objetivo establecer obligaciones y normas con el fin de que las entidades críticas aumenten su resiliencia en el mercado interior, así como sus capacidades para prevenir, proteger, responder y recuperarse ante posibles incidentes.

Cada Estado miembro deberá designar una o varias autoridades competentes que serán responsables de asegurar una correcta aplicación de la presente directiva, así como un punto de contacto único que servirá como enlace y unión entre los otros puntos de los Estados miembros.

En lo que respecta a la **transposición nacional** de la presente Directiva, cuyo plazo era el 17 de octubre de 2024, el 27 de mayo de 2025 el Consejo de Ministros aprueba el anteproyecto de Ley de Protección y Resiliencia de las Entidades Críticas (Ley CER2). Una vez aprobada definitivamente, esta norma traspondrá al ordenamiento jurídico español la Directiva (UE) 2022/2557.

Ámbito de actuación de la CER2

La presente Directiva amplía su alcance respecto a la predecesora, a **11 sectores esenciales** (energía, transporte, banca, infraestructuras de los mercados financieros, sanidad, agua potable, aguas residuales, infraestructura digital, administración pública, espacio y producción, transformación y distribución de alimentos), y amplía así el ámbito de solo incluir infraestructuras físicas a incluir tanto infraestructuras físicas como digitales.

De acuerdo con el artículo 6, los Estados miembros tienen como fecha límite el 17 de julio de 2026 para identificar las entidades críticas de los once sectores indicados.

[34] Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo.

Proceso de notificación

Las entidades críticas deben establecer procedimientos para notificar a las autoridades competentes incidentes que perturben la prestación de servicios esenciales. El plazo establecido para una **notificación inicial** es de 24 horas desde el momento que se tiene conocimiento del incidente y un mes como máximo, para un **informe detallado**.

La información a especificar es la siguiente:

- El número y porcentaje de personas afectadas por la perturbación.
- La duración de la perturbación.
- La zona geográfica afectada, teniendo en cuenta si la zona está aislada geográficamente.

Si el incidente afecta a seis o más Estados miembros, las autoridades competentes deberán notificarlo a la Comisión Europea.

Proceso de notificación Protección de Datos

En el ámbito de la protección de datos, se encuentra el **Reglamento (UE) 2016/679** del Parlamento Europeo y del Consejo, también conocido como Reglamento General de Protección de Datos o RGPD, que regula la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos.

Además, se encuentran otras regulaciones para la protección de datos en ámbitos más específicos, como son:

- La **Reglamento (UE) 2018/1725**, que se encarga de la protección de los datos personales de las personas físicas en el contexto de las instituciones, órganos y organismos de la Unión Europea.
- La **Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo**, que regula la protección de los datos personales en lo que respecta al tratamiento realizado por las autoridades competentes, con fines de prevención, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales.
- **El Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo**, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos). Conocido como *Data Governance Act* (DGA), regula el intercambio seguro de datos entre sectores y países en la UE.

A continuación, se detallará cuáles son las obligaciones en lo que respecta a una violación de seguridad de los datos personales de acuerdo con cada directiva y reglamento.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

Este reglamento, conocido como Reglamento General de Protección de Datos o RGPD, regula la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

En caso de una violación de seguridad de los datos personales que represente un riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento deberá notificar el incidente a la **Autoridad de Control competente**, de conformidad con el **artículo 55**, dentro de un plazo máximo de 72 horas desde que se conozca.

Si la notificación no se realiza dentro del plazo estipulado, deberá incluir una justificación que explique la demora.

La notificación deberá incluir, como mínimo, la siguiente información:

- Una descripción detallada de la violación de seguridad, e incluir las categorías y el número aproximado de interesados afectados, así como las categorías y el número aproximado de registros de datos personales comprometidos.
- Los datos de contacto del delegado o delegada de protección de datos o el punto de contacto pertinente.
- Una descripción de las posibles consecuencias de la violación de seguridad de los datos personales.
- Las medidas adoptadas o propuestas por el responsable del tratamiento para remediar la violación, incluyendo, si procede, las acciones implementadas para mitigar los posibles efectos negativos.

Además, el responsable del tratamiento deberá **documentar detalladamente cualquier violación de seguridad de los datos personales**, e incluir los hechos relacionados con el incidente, sus efectos y las medidas correctivas adoptadas. Esta documentación permitirá a la **Autoridad de Control** verificar el cumplimiento de las obligaciones legales establecidas en este artículo.

Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo

Este reglamento regula la protección de personas físicas relativas al tratamiento de datos personales por parte de las instituciones, órganos y organismos de la UE.

En caso de una violación de seguridad de los datos personales que implique un riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento deberá notificarla al **Supervisor Europeo de Protección de Datos** dentro de un plazo de 72 horas desde que tenga constancia de su existencia.

Si la notificación no se realiza dentro del plazo establecido, deberá adjuntarse una justificación que explique la demora.

La notificación deberá incluir, como mínimo, la siguiente información:

- Una descripción detallada de la violación de seguridad, e incluir las categorías y el número aproximado de interesados afectados, así como las categorías y el número aproximado de registros de datos personales comprometidos.
- Los datos de contacto del delegado de protección de datos o el punto de contacto pertinente.
- Una descripción de las posibles consecuencias de la violación de seguridad de los datos personales.
- Las medidas adoptadas o propuestas por el responsable del tratamiento para remediar la violación, incluyendo, si procede, las acciones implementadas para mitigar los posibles efectos negativos.

El responsable del tratamiento deberá también documentar cualquier violación de la seguridad de los datos personales, e incluir los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Esta documentación permitirá al Supervisor Europeo de Protección de Datos verificar el cumplimiento de las disposiciones establecidas en este artículo.

Si no es posible proporcionar toda la información de manera simultánea, esta podrá ser facilitada gradualmente a medida que se disponga de ella.

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo

Esta directiva regula la protección de personas físicas relativas al tratamiento de datos personales por parte de las autoridades competentes para los fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

En caso de una violación de seguridad de los datos personales que implique un riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento deberá notificarla a la **Autoridad de control** dentro de un plazo de 72 horas desde que tenga constancia del hecho.

Si la notificación no se realiza dentro del plazo establecido, deberá adjuntarse una justificación que explique la demora.

La notificación deberá incluir, como mínimo, la siguiente información:

- Una descripción detallada de la violación de seguridad, incluyendo las categorías y el número aproximado de interesados afectados, así como las categorías y el número aproximado de registros de datos personales comprometidos.
- Los datos de contacto del delegado o delegada de protección de datos o el punto de contacto pertinente.
- Una descripción de las posibles consecuencias de la violación de seguridad de los datos personales.
- Las medidas adoptadas o propuestas por el responsable del tratamiento para remediar la violación, incluyendo, si procede, las acciones implementadas para mitigar los posibles efectos negativos.

Además, el responsable o la responsable del tratamiento deberá **documentar detalladamente cualquier violación de seguridad de los datos personales**, incluyendo los hechos relacionados con el incidente, sus efectos y las medidas correctivas adoptadas. Esta documentación permitirá a la **Autoridad de Control** verificar el cumplimiento de las obligaciones legales establecidas en este artículo.

De acuerdo con el artículo 7 del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, las autoridades de control deberán establecer canales de comunicación operativos y seguros con las entidades catalogadas como esenciales e importantes.

Uno de estos canales será la **Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes**, concebida como un sistema centralizado para recibir, gestionar y hacer seguimiento de los incidentes de ciberseguridad que afecten a estas entidades. Aunque esta plataforma aún **no está en funcionamiento**, sí se han habilitado y presentado otras plataformas específicas que dependen de cada autoridad de control competente, y que actualmente se utilizan para la notificación de incidentes.

Asimismo, los Estados miembros dispondrán que, cuando la violación de seguridad de los datos personales esté relacionada con datos que hayan sido transmitidos por o hacia un responsable del tratamiento en otro Estado miembro, la información comunicada a la autoridad de control también sea notificada al responsable del tratamiento del otro Estado sin demora indebida.

Si no es posible proporcionar toda la información de manera simultánea, esta podrá ser facilitada gradualmente a medida que se disponga de ella.

Situación de la transposición de la NIS2

A fecha de este informe, España lleva un considerable retraso en la transposición de la Directiva NIS2 con respecto a otros Estados miembro. No ha sido hasta el pasado 14 de enero de 2025, cuando se publica el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, como propuesta legislativa para la transposición de la NIS2 al ordenamiento jurídico nacional.

A continuación, se muestra una tabla para mostrar los países de la Unión Europea que a día 10 de marzo de 2026 han completado la transposición de la Directiva NIS2, donde se indica la fecha de cuando se realizó, así como el nombre de la legislación donde se recoge, la entidad responsable y el canal para reportar incidentes.

Tabla 6
Datos de países que han Implementado la Directiva NIS2

País	Entidad Responsable	Canal de Comunicación	Fecha de transposición a la NIS2	Legislación
Hungría	CERT-Hungary, Equipo de Respuesta a Emergencias perteneciente al Centro Nacional de Seguridad Cibernética de Hungría (NKI).	• Formulario en línea anónimo en la web. • Correo electrónico: CSIRT@nki.gov.hu *(*Con clave PGP para envío de datos altamente sensibles)* • Teléfono para casos críticos que requieran una acción inmediata: *+36 1 279 6271*	01/2024	2023. évi XXIII. törvény
Letonia	CERT.LV, Equipo de Respuesta a Emergencias perteneciente al Instituto de Matemáticas e Informática de la Universidad de Letonia, operativo bajo el Ministerio de Defensa de la República de Letonia.	• Correo electrónico: 1. Informe de incidentes y spam: abuse@cert.lv 2. Reportar vulnerabilidad: cvd@cert.lv • Teléfono: *+371 67085888*	01/09/2024	Nacionālās kiberdrošības likums
Italia	CSIRT Italia, centro operativo dentro de la Agencia Nacional de Ciberseguridad (ACN).	• Formulario en línea disponible en la web. • Correo electrónico para enviar *malware* o email malisioso: infected@csirt.gov.it	04/09/2024	DECRETO LEGISLATIVO 4 settembre 2024, n. 138
Bélgica	CCB (Center for Cyber security Belgium) actúa como el CSIRT nacional.	• Formulario en línea disponible en la web. • Correo electrónico: info@ccb.belgium.be • Teléfono: +32 (0)2 501 05 60 (Solo para Emergencias de Operadores o Entidades Esenciales)	18/10/2024	Loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique [2024/202344]
Rumania	CERT-RO, Equipo Nacional de Respuesta a Incidentes de Seguridad Informática de Rumanía (FIRM-RO)	• Formulario en línea disponible en la web	31/12/2024	ORDONANȚĂ DE URGENȚĂ nr. 155 din 30 decembrie 2024

País	Entidad Responsable	Canal de Comunicación	Fecha de transposición a la NIS2	Legislación
Eslovaquia	CSIRT.SK, unidad gubernamental que actúa como el Equipo de Respuesta a Emergencias de la República Eslovaca. SK-CERT Actividades clave en la gestión de la seguridad de ciberseguridad incluyen el análisis de amenazas, la coordinación de incidentes a nivel nacional, y la promoción de la enseñanza, educación, capacitación e investigación en el ámbito de ciberseguridad.	• Correo electrónico: incident@csirt.sk	01/01/2025	69/2018 Coll.
Croacia	CERT.hr Organismo nacional para la prevención y protección contra las amenazas informáticas a la seguridad de los sistemas de información pública en la República de Croacia	• Correo electrónico: incident@cert.hr	07/02/2024	Zakona o kibernetičkoj sigurnosti (NN 14/24)
Lituania	CERT-LT institución gubernamental encargada de ofrecer orientación y apoyo sobre cómo mitigar las amenazas de seguridad informática	• Formulario en línea disponible en la web. • Correo electrónico: cert@nksc.lt • Teléfono: *+370 706 84 116*	11/07/2024	Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas
Grecia	NCERT-GR GR-CSIRT buque insignia del estado en lo que respecta a la defensa de ciberseguridad, la respuesta a incidentes y la integración operativa EL-CSIRT función reguladora/ regulatoria, supervisora, coordinadora, consultiva, auditora y sancionadora.	• Formulario en línea disponible en la web.	26/11/2024	Νόμος 5160/2024

País	Entidad Responsable	Canal de Comunicación	Fecha de transposición a la NIS2	Legislación
Bulgaria	Ministerio de Gobernanza Electrónica.	• Correo electrónico para notificación de incidentes (CSIRT nacional): cert@govcert.bg • Teléfono: +359 (2) 949 23 01 • Correo del punto único de contacto NIS: NSPOC@e-gov.bg	05/02/2026	
República Checa	Agencia Nacional de Ciberseguridad y Seguridad de la Información (NÚKIB) CERT Nacional	• Formulario / canal oficial de notificación (NÚKIB) • Correo electrónico (punto único de contacto NIS): nckb@nukib.cz • Teléfono: +420 541 110 777	04/08/2025	Ley de ciberseguridad / Ley n.º 264/2025
Suecia	Agencia Sueca de Contingencias Civiles (MSB)	• Correo electrónico del CSIRT nacional: cert@cert.se • Teléfono de contacto: +46 (0)10 240 40 40 • Correo del punto único de contacto NIS (MSB): spoc.nis@msb.se	17/12/2025	Ley de ciberseguridad
Finlandia	Centro Nacional de Seguridad Cibernética	• Formulario / servicio electrónico de notificación NIS2 • Correo electrónico del CSIRT nacional: cert@ncsc.fi • Teléfono: +358 295 345 630	08/04/2025	Ley de ciberseguridad
Países Bajos	Centro Nacional de Ciberseguridad (CNCS), incluido CERT.PT	• Formulario de notificación / canal oficial NIS2 (NCSC – 24/7) • Correo electrónico para notificación de incidentes: cert@ncsc.nl • Teléfono (24/7): +31 70 751 55 75	04/12/2025	Decreto-Ley n.º 125/2025

País	Entidad Responsable	Canal de Comunicación	Fecha de transposición a la NIS2	Legislación
Alemania	Oficina Federal de Seguridad de la Información. BSI (Bundesamt für Sicherheit in der Informationstechnik).	• Portal oficial de notificación de incidentes (obligatorio): BSI Portal / Melde und Informationsportal (MIP) https://www.bsi.bund.de/ • Formulario online para entidades aún no registradas: disponible a través del BSI Portal • Correo electrónico del CSIRT nacional (no sustitutivo del portal): cert@bsi.bund.de	05/12/2025	Ley que implementa la Directiva NIS-2 y regula los principios esenciales de la gestión de la seguridad de la información en la administración federal
Polonia	Ministro de Asuntos Digitales. Cuatro tipos de CSIRT: • CSIRT LUN. • CSIRT NASK. • CSIRT GOV. • CSIRT sectoriales.	• Correo electrónico del punto único de contacto NIS: ppk_ksc@mc.gov.pl • Correo electrónico para entidades digitales (DSP): duc_ksc@mc.gov.pl • Teléfono de contacto: +48 22 245 59 22	02/03/2026	Ley por la que se modifica la Ley del Sistema Nacional de Ciberseguridad
Portugal	· Autoridad competente y CSIRT nacional: Centro Nacional de Ciberseguridad (CNCS), incluido CERT.PT · Autoridad nacional para la gestión de crisis e incidentes de ciberseguridad a gran escala: Secretario General del Sistema de Seguridad Interior. · Autoridades nacionales de ciberseguridad sectoriales y autoridades nacionales especiales de ciberseguridad	• Canales oficiales del CNCS (notificación NIS2): https://www.cncs.gov.pt/ • Correo electrónico del CSIRT nacional (CERT.PT): cert@cert.pt • Teléfono de contacto: +351 210 497 399 • Teléfono de emergencia (fuera de horario): +351 910 601 102	04/12/2025	Decreto-Ley n.º 125/2025

País	Entidad Responsable	Canal de Comunicación	Fecha de transposición a la NIS2	Legislación
Dinamarca	Ministro de Protección Civil y Planificación de Emergencias El Ministro de Protección Civil y Planificación de Emergencias, en consulta con otros ministros sectoriales	• Portal oficial de notificación NIS2 (obligatorio): Virk.dk – solución digital de registro y notificación • https://www.virk.dk/ • Correo electrónico del CSIRT nacional (CFCS): cert@cert.cfcs.dk • Teléfono de contacto (24/7): +45 33 32 55 80	01/07/2025	Ley n.º 434, Ley de medidas para garantizar un alto nivel de ciberseguridad (Ley NIS 2)
Eslovenia	Oficina de Seguridad de la Información del Gobierno de la República de Eslovenia. CSIRT SI-CERT. CSIRT de la Administración Estatal	• Canales oficiales de notificación de la autoridad competente (URSIV): • https://www.gov.si/en/state-authorities/government-office-for-information-security/ • Correo electrónico del CSIRT nacional (SI CERT): cert@cert.si	19/06/2025	Ley de seguridad de la información (ZInfV-1)
Austria	Oficina Federal de Ciberseguridad, dependiente del ministro Federal del Interior. Centro Nacional de Coordinación de Ciberseguridad.	• Portal de notificación NIS: https://nis.cert.at/ • Teléfono: +43 1 505 64 16 78	23/12/2025	Ley de seguridad de redes y sistemas de información de 2026

Conclusión de la notificación en la UE

La UE ha creado un **conjunto de normas** para la notificación de incidentes de ciberseguridad con el objetivo de proteger infraestructuras clave, servicios esenciales y datos personales frente a las crecientes amenazas digitales.

Herramientas como la Directiva NIS2, el Reglamento de Resiliencia Operativa Digital (DORA) y el Reglamento eIDAS 2 ayudan a las entidades públicas y privadas a gestionar y reducir riesgos, estableciendo procedimientos claros para la notificación de incidentes, plazos específicos de respuesta y un sistema sólido de cooperación entre países.

Este enfoque no solo permite dar una **respuesta coordinada ante incidentes graves**, sino que también permite fortalecer la resiliencia de ciberseguridad en toda Europa, mejora la confianza de los ciudadanos en los servicios digitales y refuerza la posición de la UE como líder mundial en ciberseguridad.

La constante actualización de estas normativas asegura que las medidas sigan siendo efectivas frente a los desafíos cambiantes del entorno digital.

04
Referencias

• *Ministerio del Interior. (s. f.). Informe sobre cibercriminalidad en España 2023. En* https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf.

• *INE - Instituto Nacional de Estadística. (n.d.). Seguridad TIC. INE.* https://www.ine.es/jaxi/Datos.htm?tpx=53970

• *Seguridad TIC. (s/f). INE.* https://www.ine.es/jaxi/Datos.htm?tpx=53970

• *Eurostat (n.d.). Security related problems experienced when using the Internet. Eurostat.* https://doi.org/10.2908/ISOC_CISCI_PB

• *Eurostat (n.d.). Security incidents and consequences by size class of enterprise. Eurostat.* https://doi.org/10.2908/ISOC_CISCE_IC

• *2024 Report on the State of the Cybersecurity in the Union | ENISA.* (s.f.). Home | ENISA. https://enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

• *CCN-CERT - Directrices para la gestión de incidentes.* (s.f.). CCN-CERT - Inicio. https://www.ccn-cert.cni.es/es/gestion-de-incidentes/directrices-para-la-gestion-de-incidentes.html

• *ENISA Threat Landscape 2023 | ENISA.* (s.f.). Home | ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

• *CCN-CERT IA-04/24 Ciberamenazas y Tendencias. edición 2024.* (s. f.). https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024

• (s.f.).https://www.incibe.es/sites/default/files/2024-08/Infografía_balance_de_ciberseguridad_INCIBE_2023_0.pdf

• *INCIBE presenta su balance de ciberseguridad 2024 con más de 97.000 incidentes gestionados. (s/f). Incibe.es.* https://www.incibe.es/incibe/sala-de-prensa/incibe-presenta-su-balance-de-ciberseguridad-2024-con-mas-de-97000-incidentes

• *(S/f). Incibe.es.* https://www.incibe.es/sites/default/files/2026-02/Balance%20de%20ciberseguridad%202025%20INCIBE/BalanceCiberseguridad2025_INCIBE.pdf

• *Notificación de brechas de datos personales a la Autoridad de Control | AEPD.* (s.f.). AEPD. https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-datos-personales-notificacion

• *Reglamento General de Protección de Datos.* (s/f). Boe.es. https://www.boe.es/doue/2016/119/L00001-00088.pdf

• *Ministerio del Interior. (2025). Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.* https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/participacion-ciudadana/Participacion-publica-en-proyectos-normativos/Audiencia-e-informacion-publica/01_2025_Anteproyecto_ley_coordinacion_gobernanza_ciberseguridad.pdf

• *BOE-A-2018-12257 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.* (s.f.). BOE.es - Agencia Estatal Boletín Oficial del Estado. https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257

• *BOE-A-2021-1192 Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.* (s.f.). BOE. es - Agencia Estatal Boletín Oficial del Estado. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192

• *BOE-A-2018-5370 Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.* (s.f.). BOE. es - Agencia Estatal Boletín Oficial del Estado. https://www.boe.es/buscar/act.php?id=BOE-A-2018-5370

Guía Nacional de notificación y gestión de incidentes de ciberseguridad. (s/f). Incibe.es https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

• *INCIBE-CERT.* (s.f.). https://www.incibe.es/incibe-cert/incidentes/procedimientos

• *Sede Electrónica del Banco de España - Catálogo de trámites - Supervisión.* (s/f). https://sedeelectronica.bde.es/sede/es/menu/tramites/supervision/notificacion-incidentes-graves-ciberamenazas-importantes-p314.html

• *Regulation - EU - 2024/1183 - EN - EUR-Lex.* (s.f.). The official portal for European data | data.europa.eu. http://data.europa.eu/eli/reg/2024/1183/oj

• *Directive - 2016/680 - EN - Law Enforcement Directive; LED - EUR-Lex.* (s.f.). The official portal for European data | data.europa.eu. http://data.europa.eu/eli/dir/2016/680/oj

• *Directive - 2022/2555 - EN - EUR-Lex.* (s.f.). The official portal for European data | data.europa.eu. http://data.europa.eu/eli/dir/2022/2555/oj

• *Directive - 2016/1148 - EN - EUR-Lex.* (s.f.). The official portal for European data | data.europa.eu. http://data.europa.eu/eli/dir/2016/1148/oj

• *Regulation - EU - 2018/1725 - EN - EUR-Lex.* (s.f.). The official portal for European data | data.europa.eu. http://data.europa.eu/eli/reg/2018/1725/oj

• *Regulation - 2016/679 - EN - gdpr - EUR-Lex.* (s.f.-a). The official portal for European data | data.europa.eu. http://data.europa.eu/eli/reg/2016/679/oj

• *Regulation - 2022/2554 - EN - DORA - EUR-Lex.* (s. f.). The official portal for European data | data.europa.eu. https://eur-lex.europa.eu/eli/reg/2022/2554/oj

• *Directive - 2022/2557 - EN – CER2 - EUR-Lex.* (s/f). The official portal for European data | data.europa.eu. https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

• *Directive - 2016/680 - EN - law enforcement directive; LED - EUR-Lex.* (s/f). The official portal for European data | data.europa.eu. https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng

• *CSIRT Italia - ACN.* (s.f.). ACN. https://www.acn.gov.it/portale/csirt-italia

• *CERT.LV.* (s.f.). CERT.LV. https://www.cert.lv/lv/

• *Nahlásiť incident | CSIRT.SK.* (s. f.). https://csirt.sk/nahlasit-incident.html

• *Enhanced National Cyber Security Services and Capabilities for Interoperability – eCSI.* (s. f.). https://ecsi.cert.ro/

• *CERT.hr. (2024, 11 abril).* CERT.hr. CERT.hr -. https://www.cert.hr/

• *CERT-LT.* (s. f.). https://www.nksc.lt

• *Cert-Ro.* (s. f.). https://www.cert.ro

• *Főoldal.* (s. f.). Nemzeti Kibervédelmi Intézet. https://nki.gov.hu/

• *GR-CSIRT. (s. f.).* https://csirt.cd.mil.gr

• *HunCERT csoport. (s.f.).* HunCERT csoport. https://cert.hu/

índice de tablas

índice de figuras

glosario

Guía sobre la notificación de Incidentes de Ciberseguridad

Glosario

[I] **Incidente de ciberseguridad**: Acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traducen en un efecto real o potencialmente adverso sobre un sistema de información y/o la información que trata o los servicios que presta.

[II] ***Phishing***: Método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño o la picaresca, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio.

[III] ***DDoS***: *Distributed Denial-of-Service*, por sus siglas en inglés, que en castellano corresponde a denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma no permitir que sus legítimos usuarios puedan utilizar los servicios por prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.

[IV] ***Ransomware***: Código malicioso para secuestrar datos, una forma de explotación en el cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado.

[V] **Ciberacoso**: Acoso que se lleva a cabo a través de Internet.

[VI] ***Pharming***: Ataque informático que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP (Internet Protocol, por sus siglas en inglés, que en castellano corresponde a protocolo de Internet) legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a otra dirección IP donde se aloja una página web falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad.

[VII] **Corrupción de datos**: Alteración de la información digital, de manera que se vuelve inaccesible, incorrecta o inutilizable. Puede ser tanto por fallos del *hardware* o *software*, por ataques de incidentes de ciberseguridad, por infección por *malware* o por error humano.

[VIII] **Servicios *Botnet***: Conjunto de recursos de ciberseguridad, los cuales son controlados de forma remota, estos son conocidos como "*bot*", que son dispositivos infectados por un *malware*. Esto se usa para hacer ataques masivos, como *DDoS* entre otros.

[IX] **Grupo *hacktivista***: Grupo de activistas que usan técnicas de hacking para promover sus causas.

[X] **Infraestructura crítica**: Conjunto de sistemas, activos y recursos esenciales para el funcionamiento de la sociedad. En caso de interrupción o destrucción tendría un impacto significativo.

[XI] **Datos sensibles**: Toda información que, si se divulga, puede causar daño a la persona.

[XII] **Ciberdelincuente**: Persona que delinque a través de Internet.

[XIII] **Fuga de información**: Pérdida de la confidencialidad de los datos sensibles, de manera accidental o intencionado.

[XIV] **Tu Ayuda en Ciberseguridad**: Servicio nacional, gratuito y confidencial que INCIBE pone a disposición de los usuarios de Internet y la tecnología con el objetivo de ayudarles a resolver los problemas de ciberseguridad que puedan surgir en su día a día.

[XV] ***CyberCamp***: Evento referente para el desarrollo de la ciberseguridad y la confianza digital de la ciudadanía y entidades.

[XVI] ***Cybersecurity Summer BootCamp***: Programa internacional de capacitación especializado en ciberseguridad dirigido a Fuerzas y Cuerpos de Seguridad, Ministerio Fiscal, Jueces y Magistrados, actores políticos, reguladores, legislativos y Especialistas de Centros de Respuesta a Incidentes Cibernéticos.

[xvii] **Campaña de desinformación**: Estrategia para difundir información falsa o incompleta con el fin de influir en la opinión pública.

[xviii] **Dominio dinámico** (en el contexto de *phishing*): Dominio web que cambia con frecuencia. Esta práctica es utilizada en ataques de *phishing*.

[xix] **NIS2**: *Network and Information Security*, por sus siglas en inglés, que en castellano corresponde a seguridad de redes y sistemas de información. La Directiva NIS2 (Directiva (UE) 2022/2555) surge como respuesta a esa necesidad de actualización y fortalecimiento de las medidas establecidas en la Directiva NIS1, erigiéndose como un marco normativo estratégico para abordar los retos actuales en materia de ciberseguridad en el marco de la Unión Europea.

[xx] ***Cyber Europe 2023***: Evento de dos días que proporciona una plataforma para que expertos en ciberseguridad y *startups* compartan conocimientos y colaboren en la lucha contra la creciente amenaza de los incidentes de ciberseguridad en el entorno tecnológico.

[xxi] ***Horizon Europe***: Programa de financiación clave de la Unión Europea para la investigación y la innovación.

[xxii] **Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad**: Anteproyecto para la transposición de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, conocida como NIS2, que incluye una serie de medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión Europea.

[xxiii] **Centro Nacional de Inteligencia** (CNI): es el organismo público responsable de facilitar al presidente del Gobierno y al Gobierno de la nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o la integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones.

[xxiv] **RedIRIS**: Real Academia y de Investigación Española. Es una red de comunicaciones avanzadas que da servicio a la comunidad científica y académica española.

[xxv] **OCC**: Oficina de Coordinación de Ciberseguridad, entidad encargada de coordinar y supervisar las políticas y estrategias relacionadas con la ciberseguridad a nivel nacional.

[xxvi] **Responsables de Seguridad de la Información**: Profesionales encargados de garantizar la protección, confidencialidad, integridad y disponibilidad de la información dentro de una organización.

[xxvii] ***Rootkit***: Conjunto de *software* dañino que permite el acceso privilegiado a áreas de una máquina, mientras que al mismo tiempo se oculta su presencia mediante la corrupción del Sistema Operativo u otras aplicaciones. Denotar que por máquina se entiende todo el espectro de sistemas IT, desde *smartphones* hasta ICS (Sistemas de Control Industrial). El propósito por tanto de un *rootkit* es enmascarar eficazmente *payloads* (cargas útiles) y permitir su existencia en el sistema.

[xxviii] ***Malware***: Palabra que deriva de los términos malicious y *software*. Cualquier pieza de *software* que lleve a cabo acciones como extracción de datos u otro tipo de alteración de un sistema puede categorizarse como *malware*. Así pues, *malware* es un término que engloba varios tipos de programas dañinos.

[xxix] **Webinjects**: Herramienta gratuita y de código abierto diseñada principalmente para automatizar la prueba de las aplicaciones y servicios web.

[xxx] ***Vishing***: Término similar a *phishing*. Se utiliza cuando una estafa se realiza a través de una llamada telefónica en la cual se emplean técnicas de ingeniería social. El atacante finge ser una entidad u organización reconocida.

[xxxi] ***Baiting*** (cebo): Técnica de incidente de ciberseguridad en la que los delincuentes atraen a las víctimas ofreciendo algo tentador, como un archivo gratuito, un *software*, o un regalo, con el fin de que descarguen o accedan a un enlace malicioso.

[xxxii] ***Buffer Overflow***: En castellano, desbordamiento de *buffer*. Situación en la que un programa en ejecución intenta escribir datos fuera del *buffer* de memoria que no está destinado a almacenar esos datos.

[xxxiii] ***Backdoors***: En castellano, puertas traseras. Pasaje secreto en un sistema operativo que permite al atacante un acceso remoto sin ser detectado.

[XXXIV] ***Cross Site Scripting* (XSS)**: Ataque que trata de explotar una vulnerabilidad presente en aplicaciones web, por la cual un atacante inyecta sentencias mal formadas o cadenas que el receptor no espera o controla debidamente.

[XXXV] ***Warez***: *Software* que se copia, piratea o comparte ilegalmente. Por ejemplo: videojuegos, programas, películas...

[XXXVI] **Incidente APT**: Amenaza Persistente Avanzada. Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

[XXXVII] **NIS**: Legislación de la Unión Europea que establece medidas para mejorar la ciberseguridad de las infraestructuras críticas y los servicios esenciales dentro de los estados miembros.

[XXXVIII] **Red de CSIRT**: Red compuesta por los CSIRTs designados de los Estados miembros de la UE y CERT-EU.

[XXXIX] **EU-CyCLONe**: Red de cooperación para las autoridades nacionales de los Estados miembros encargadas de la gestión de crisis de ciberseguridad.

[XL] **Identidad Digital Europea**: Sistema de identificación y autenticación digital propuesto por la Unión Europea que permite a la ciudadanía, residentes y empresas acceder a servicios públicos y privados en línea de forma segura, utilizando una única identidad digital válida en todos los países miembros.

Las definiciones de los términos de este glosario han sido extraídas de las siguientes fuentes oficiales: Guía Nacional de Notificación de Gestión de Incidentes de ciberseguridad, Real Academia Española, Gobierno de España, CNI, ENISA, Comisión Europea y European Cyber Security Organisation (ECSO), salvo alguna excepción que ha sido elaborada por el propio autor del informe.

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es · ontsi · incibe_ · Plan de Recuperación, Transformación y Resiliencia

guía sobre la notificación de incidentes de ciberseguridad

observaciber