La Directiva NIS2

Análisis de las claves de la Directiva y desafíos para los CISO

José Antonio Sánchez Durán
Senior Consultant & Advisor
Govertis, parte de Telefónica Tech.

CLUB CISO AEC

GOVERTIS
Part of Telefónica Tech

Contenido

GOVERTIS
Part of Telefónica Tech

La Directiva NIS2

Una visión global de la Directiva UE 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS 2) y como debemos los CISOs orientar y preparar a la organización para su cumplimiento.

Una directiva **publicada** en el DOUE el 27 de diciembre de 2022, con **entrada en vigor** el 16 de enero de 2023, que debe ser **transpuesta** a la normativa nacional antes del 17 de octubre y con **aplicación** en toda la UE a partir del 18 de octubre de 2024.

Nos enfrentamos a una normativa con requisitos precisos y estrictos en la gestión de los riesgos y la notificación de los incidentes, ampliando en el alcance a **nuevos sectores** críticos que no estaban contemplados en la normativa anterior NIS, y por último, con la aplicación de sanciones mucho más severas, efectivas, proporcionadas y disuasorias ante **cualquier incumplimiento** de las disposiciones nacionales adoptadas al amparo de la directiva.

En concreto, el considerando 133 detalla que *'las autoridades competentes deben estar facultadas para **suspender temporalmente** o solicitar la suspensión temporal de una **certificación o autorización** referente a una **parte o la totalidad** de los servicios pertinentes prestados o a las actividades realizadas por una entidad esencial y solicitar la **imposición de una prohibición temporal** de que una **persona física** ejerza funciones de dirección a nivel de director general o representante legal'* y el art. 20 Gobernanza, expone que los Estados miembros velarán por que los **Órganos de Dirección**:

a) **Aprueben** las medidas para la gestión de riesgos de ciberseguridad adoptadas,
b) **Supervisen** su puesta en práctica, y
c) **Respondan** por el **incumplimiento.**

Sectores afectados por NIS2

Lo primero que debemos conocer es su ámbito de aplicación. La directiva es de aplicación a aquellas **entidades públicas o privadas** que:

1º Están incluidas en alguno de los tipos mencionados en los **anexos I y II** y son consideradas **medianas empresas**, empresas que ocupan a menos de 250 personas y cuyo volumen de negocios anual no excede de 50 millones de euros o cuyo balance general anual no excede de 43 millones de euros; o **superan los límites máximos para las medianas empresas**, y prestan sus servicios o llevan a cabo sus actividades en la UE.

2º **Independientemente de su tamaño**, cualquier entidad que esté incluida en alguno de los tipos mencionados en los anexos I y II, y cumplen alguna de las siguientes condiciones:

   a. Prestan servicios como proveedores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas públicas, son prestadores de servicios de confianza[1], o son registros de nombres de dominio de primer nivel y proveen servicios de sistema de nombres de dominio.

   b. sea el único proveedor existente en un Estado miembro de un servicio esencial.

   c. Una perturbación en el servicio prestado por la entidad pudiera tener repercusiones significativas sobre la seguridad pública, el orden público o la salud pública, o inducir riesgos sistémicos significativos, en particular para los sectores con repercusiones de carácter transfronterizo.

   d. Sea crítica por su importancia específica a nivel nacional o regional para el sector o tipo de servicio concreto o para otros sectores interdependientes en el Estado miembro.

   e. Sea una entidad de la Administración pública central, o en el caso de ser regional, si tras la evaluación de riesgo, una perturbación podría tener un impacto significativo en actividades sociales o económicas críticas.

3º **Independientemente de su tamaño**, cualquier entidad identificada como **entidad crítica** de acuerdo a la Directiva UE 2022/2557, que cumple lo siguiente:

   a. Presta uno o más **servicios esenciales**[2] (la lista la elabora cada Estado miembro).

[1] **Prestador de servicios de confianza** es una persona física o jurídica que proporciona y conserva certificados digitales para crear y validar firmas electrónicas y autenticar a sus firmantes, así como sitios web en general. Del mismo modo verifica la identidad de usuarios, clientes o negocios y aprueba operaciones de firma electrónica a través de la emisión y el almacenamiento de certificados digitales.

[2] **Servicio esencial:** servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas. Art.2 Definiciones Ley 8/2011 LPIC.

b. Opera en el territorio del Estado miembro y su **infraestructura crítica**[3] está situada en él.

c. Un incidente tendría efectos perturbadores significativos.

4º **Independientemente de su tamaño**, cualquier entidad que preste servicios de registro de nombres de dominio. En España, Dominios.es es la unidad responsable de la gestión del **registro de nombres de dominio** de Internet bajo el código de país ".es" y está integrada en la Entidad Pública Empresarial Red.es del Gobierno de España.

5º Entidades de la **Administración pública local,** o **centros de enseñanza**, en particular aquellos que realicen **actividades críticas de investigación**, por disposición del Estado miembro.

[3] **Infraestructuras críticas**: las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales, cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Art.2 Definiciones Ley 8/2011 LPIC.

Exclusiones a la NIS2

La aplicación de la norma se entenderá **sin perjuicio** de las responsabilidades de los Estados miembros de **salvaguardar la seguridad nacional**, garantizar la **integridad territorial** del Estado o mantener el **orden público**.

No se aplicará a las entidades de la Administración pública que lleven a cabo sus actividades en los ámbitos de la **seguridad nacional**, la **seguridad pública**, la **defensa** o la garantía del **cumplimiento de la ley**, incluidas la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales.

Los Estados miembros **podrán eximir a las entidades específicas** que llevan a cabo actividades en los ámbitos de la defensa, la seguridad nacional, la seguridad pública o la garantía del cumplimiento de la ley, o que prestan servicios exclusivamente a entidades de la Administración pública

No se aplicará a las entidades que los Estados miembros hayan excluido del ámbito de aplicación del Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital del sector financiero (DORA), de conformidad con el artículo 2, apartado 4, (entidades a que se refiere el artículo 2, apartado 5, puntos 4 a 23, de la Directiva 2013/36/UE), en España, **al Instituto de Crédito Oficial (ICO)**. **No implica el suministro de información** cuya divulgación sea contraria a los intereses esenciales de los Estados miembros en materia de seguridad nacional, seguridad pública o defensa.

Clasificación de las entidades

Entidades esenciales

Se considerarán entidades esenciales:

a) Aquellas entidades de algunos de los tipos mencionados en el **anexo I que superen los límites para medianas empresas** (ocupan a menos de 250 personas y cuyo volumen de negocios anual no excede de 50 millones de euros o cuyo balance general anual no excede de 43 millones de euros).

b) **prestadores cualificados de servicios de confianza** y **registros de nombres de dominio** de primer nivel, así como proveedores de servicios de DNS, independientemente de su tamaño.

c) **proveedores de redes públicas de comunicaciones electrónicas** o de servicios de comunicaciones electrónicas disponibles para el público que sean consideradas medianas empresas.

d) entidades de la **Administración pública central o regional**.

e) cualquier entidad identificada por el Estado miembro como **entidad esencial**.

f) las entidades identificadas como **entidades críticas**.

g) las entidades identificadas por el Estado miembro como **operadoras de servicios esenciales**.

Entidades Importantes

Se considerarán entidades importantes todas las entidades de uno de los tipos mencionados en los **anexos I o II** que no puedan considerarse entidades esenciales, incluidas las identificadas como tal por un Estado miembro.

Sectores de aplicación Anexo I y II

SECTORES DE ALTA CRITICIDAD (Anexo I)

- Energía
- Transporte
- Banca
- Infraestructuras Mercados Financieros
- Sector Sanitario
- Agua Potable
- Aguas Residuales
- Infraestructura Digital
- Gestión de Servicios TIC
- Administración Pública
- Espacio

OTROS SECTORES CRÍTICOS (Anexo II)

- Servicios Postales y de mensajería
- Gestión de Residuos
- Fabricación, producción y distribución de Sustancias Químicas
- Producción, transformación y distribución de alimentos
- Fabricación
- Proveedores de Servicios Digitales
- Investigación

Afectación de la normativa NIS2 por sectores

Anexo I Sectores de Alta Criticidad

Sector Energía

El sector energético es uno de los más afectados por la Directiva NIS2 ya que proporcionan servicios esenciales a la sociedad y se ha convertido en el foco principal de ataques cibernéticos para las organizaciones cibercriminales.

Por ello, la Directiva establece requisitos de cumplimiento para todos los sectores a través de las medidas para la gestión de riesgos de ciberseguridad, y que son aplicables especialmente en las empresas del sector energético al objeto de salvaguardar sus redes y los sistemas de información.

El sector energía incluye a los subsectores de:

- **Electricidad**.
  - Empresas eléctricas que efectúan la función de suministro.
  - Gestores de la red de distribución.
  - Gestores de la red de transporte.
  - Productores de energía eléctrica.
  - Operadores del mercado eléctrico.
  - Participantes en el mercado eléctrico que presten servicios de agregación, respuesta de demanda o almacenamiento de energía.
  - Operadores responsables de la gestión y explotación de puntos de recarga al usuario final.
- **Sistemas urbanos de calefacción y refrigeración.**
  - Operadores.
- **Crudo.**
  - Operadores de oleoductos de transporte.
  - Operadores de producción, instalaciones de refinado y tratamiento, almacenamiento y transporte.
  - Entidades centrales de almacenamiento.
- **Gas.**
  - Empresas suministradoras de gas.
  - Gestores de la red de distribución.
  - Gestores de la red de transporte.
  - Gestores de almacenamiento.
  - Gestores de la red de gas natural licuado (GNL).
  - Compañías de gas natural.
  - Operadores de instalaciones de refinado y tratamiento de gas natural.
- **Hidrógeno.**
  - Operadores de producción, almacenamiento y transporte.

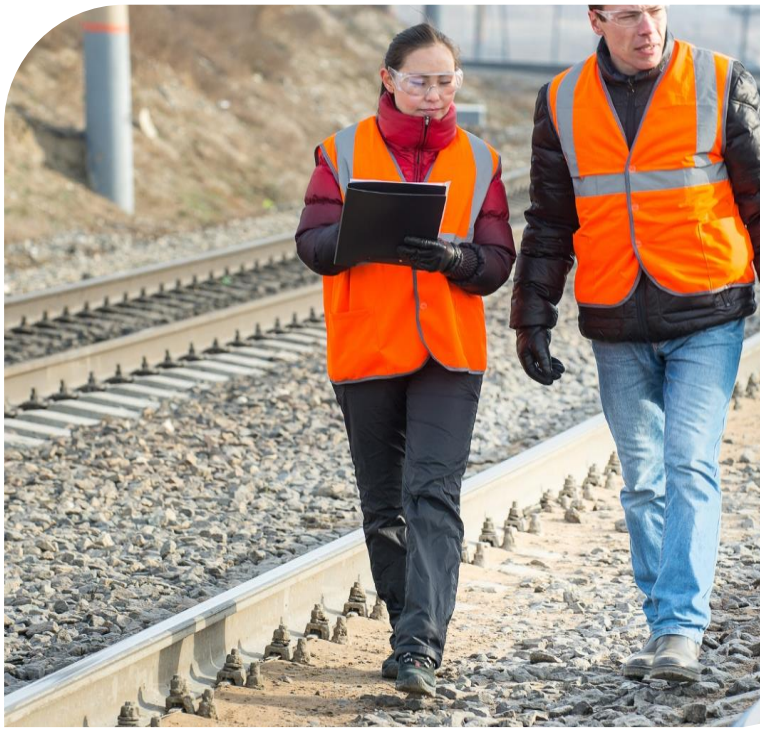
Sector Transporte

El sector de transporte ofrece la infraestructura y los servicios necesarios para unir los núcleos de producción, industrias y empresas con la sociedad. Abarca todos los medios y sistemas de transporte tanto de personas como de mercancías y es el pilar alrededor del cual gira la sociedad y la economía.

Está considerado como un sector esencial puesto que cualquier interrupción podría causar efectos dramáticos en toda la sociedad con una afectación en cascada en los sectores dependientes. Como ejemplo solo tenemos que ver el impacto que ocasiona una huelga de transportistas de mercancías con el consiguiente desabastecimiento de materias primas, paralización de las cadenas de producción, e incremento de los precios.

La Directiva exige la evaluación, análisis y control de las posibles ciberamenazas de seguridad, tanto propias como de proveedores externos, fabricantes de componentes críticos o prestadores de servicios TIC. En el sector de transporte es esencial verificar que los sistemas y equipamientos cumplen con la normativa de seguridad, y ofrecen capacidad de resistencia y recuperación ante ataques cibernéticos.

Este sector depende en gran medida de la comunicación de datos en tiempo real entre sistemas, como es el caso de los sistemas de control de tráfico aéreo, por ello la directiva exige que los canales de comunicación estén debidamente protegidos para evitar el acceso no autorizado o su manipulación. Entre los requisitos específicos están la implementación del cifrado, los controles de acceso, la autenticación multifactor, implementación de firewalls, sistemas IDS/IPS, sistemas EDR o la monitorización continua y el registro de eventos.



El sector transporte incluye a los subsectores de:

- **Aéreo.**
  - Compañías aéreas.
  - Entidades gestoras de aeropuertos, aeropuertos y entidades que explotan instalaciones anexas dentro de los recintos de los aeropuertos.
  - Operadores de control de la gestión del tráfico aéreo.
- **Ferrocarril.**
  - Administradores de infraestructuras.
  - Empresas ferroviarias, incluidos los explotadores de instalaciones de servicio.

- **Marítimo y fluvial.**
  - Empresas de transporte marítimo, fluvial y de cabotaje, tanto de pasajeros como de mercancías, sin incluir buques particulares explotados por estas empresas.
  - Organismos gestores de puertos incluidas sus instalaciones portuarias, y entidades que operan obras y equipos que se encuentran en los puertos.
  - Operadores de servicios de tráfico de buques (STB).
- **Por carretera.**
  - Autoridades viarias responsables del control de la gestión del tráfico, excluidas las entidades públicas para las cuales la gestión del tráfico o la explotación de sistemas de transporte inteligentes sea una parte no esencial de su actividad general.
  - Operadores de sistemas de transporte inteligentes (ITS), conjunto de aplicaciones informáticas y sistemas tecnológicos creados con el objetivo de mejorar la seguridad y eficiencia en el transporte terrestre, facilitando la labor de control, gestión y seguimiento (mapas, planificación de rutas, guías en ruta, información de la red de transporte en tiempo real, etc.).

Sector banca y sector infraestructuras mercados financieros

Dentro del sector de la banca e infraestructuras de mercados financieros, se incluyen además de las instituciones bancarias y las empresas de inversión, a las compañías aseguradoras que gestionan y garantizan el flujo de capital en la Unión Europea.

El sector financiero ha ido aplicando e implementando durante los últimos años muchas normativas regulatorias específicas que han permitido aumentar su capacidad de resiliencia y estabilidad del sector. Con esta directiva se ven abocados a examinar las medidas de ciberseguridad que ya tienen implementadas y realizar los cambios que sean necesarios para adaptarse a los nuevos requerimientos de disponibilidad, confidencialidad e integridad, al cifrado de los datos tanto en tránsito como en reposo, a la monitorización continua de cualquier intento de acceso o manipulación no autorizado y el registro y análisis de eventos, a disponer de los planes de contingencia, continuidad de negocio y recuperación ante desastres que permitan minimizar el impacto de cualquier disrupción.

La interconexión de los sistemas financieros con terceros que les prestan servicios exige la evaluación y gestión de los riesgos derivados de la cadena de suministros, adecuando contratos y acuerdos de nivel de servicio, y analizando y auditando los niveles de ciberseguridad de los sistemas de sus proveedores.

Tenemos que tener presente que estos sectores realizan transacciones financieras de muy alto valor, con la transmisión de

información crítica y confidencial, que en caso de comprometerse y sufrir una violación de seguridad podría llegar a tener un impacto demoledor para las partes que están involucradas, y para el sistema financiero de un país.

Estos sectores incluyen a:

- Entidades de crédito.
- Gestores de centros de negociación.
- Entidades de contrapartida central (ECC), personas jurídicas que intermedia entre las contrapartes de los contratos negociados en uno o varios mercados financieros, actuando como compradora frente a todo vendedor y como vendedora frente a todo comprador.

Sector sanitario

Este es un sector vital para la sociedad y la economía de la Unión Europea. Los potenciales efectos que podría tener un ciberataque exitoso, provocando tiempos de inactividad o fallos en los sistemas críticos de atención médica, serían fatales llegando a afectar a vidas humanas. Por ello, es un sector sometido estrictamente a los requisitos y obligaciones recogidas en la directiva, destacando la de garantizar la continuidad de sus servicios esenciales.

Estamos hablando de un sector que tiene en sus manos la vida de las personas, lo que implica una enorme responsabilidad para garantizar la protección de sus servicios, sistemas, información y la seguridad de sus usuarios y pacientes. Una violación de seguridad puede comprometer la información con el resultado de un daño considerable a las personas. Es por ello que estas entidades están sujetas a estrictas regulaciones de privacidad como el RGPD o la LOPDGDD, y la directiva NIS2 lo que hace es añadir una capa adicional a las regulaciones en el ámbito de la ciberseguridad.

La Directiva está enfocada a implementar las medidas de gestión de riesgos cibernéticos, notificación de incidentes y hacer cumplir estrictamente los estándares de ciberseguridad para todos los operadores de servicios esenciales, muy en especial, los incluidos en este sector sanitario.

Estos sectores incluyen a:

- Prestadores de asistencia sanitaria, toda persona física o jurídica que dispense legalmente asistencia sanitaria en el territorio de un Estado miembro.
- Laboratorios de referencia de la UE responsables de la coordinación de la red de laboratorios nacionales de referencia.
- Entidades que realizan actividades de investigación y desarrollo de medicamentos.
- Entidades que fabrican productos farmacéuticos de base y especialidades farmacéuticas.
- Entidades que fabrican productos sanitarios que se consideran

esenciales en situaciones de emergencia de salud pública.

Sector agua potable y sector aguas residuales

El sector del suministro de agua potable es vital para la subsistencia humana. Proporcionar a la sociedad agua potable de forma segura y realizar la gestión y tratamiento de las aguas residuales es transcendental en la Unión Europea. La interrupción o manipulación de estos servicios puede llegar a tener consecuencias muy graves en la vida de las personas. Recordemos que es un sector con una gran dependencia de sistemas OT que regulan la dosificación de componentes químicos y los niveles de presión de la canalización. Ya existen casos en los que los atacantes han utilizado como vector de ataque estos componentes y sistemas OT con fatales consecuencias.

La Directiva da gran importancia a la protección de las infraestructuras críticas y su capacidad de resistencia y resiliencia ante las amenazas de ciberseguridad. Por ello, entre las medidas que exige, están la de actualizar la tecnología, implementar herramientas de seguridad y formar y concienciar a los empleados.

En el caso de las infraestructuras críticas uno de los puntos clave de la Directiva es la importancia de la coordinación y cooperación entre las entidades sectoriales para facilitar información relevante en el ámbito de la ciberseguridad.

Estos sectores incluyen a:

- Suministradores y distribuidores de aguas destinadas al consumo humano, excluidos los distribuidores para los que la distribución de aguas destinadas al consumo humano sea una parte no esencial de su actividad general de distribución de otros bienes y productos básicos.
- Empresas dedicadas a la recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas o industriales, excluidas las empresas para las que la recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas o industriales sea una parte no esencial de su actividad general.

Sector infraestructura digital y sector gestión de servicios TIC (de empresa a empresa)

Nos estamos refiriendo a unos sectores sin los cuales la sociedad no habría podido evolucionar y lograr la transición digital. Es muy difícil imaginarse un mundo actual sin una infraestructura que nos permita estar interconectados de forma global.

Con un crecimiento exponencial de la dependencia de las nuevas tecnologías (*Cloud*, IA, *Big Data*, etc.) se está convirtiendo este sector en la base sobre la que se sustenta la sociedad, y dado este valor, las organizaciones cibercriminales buscan focalizar sus esfuerzos en atacar, perturbar y causar daños sobre este sector y las entidades involucradas.

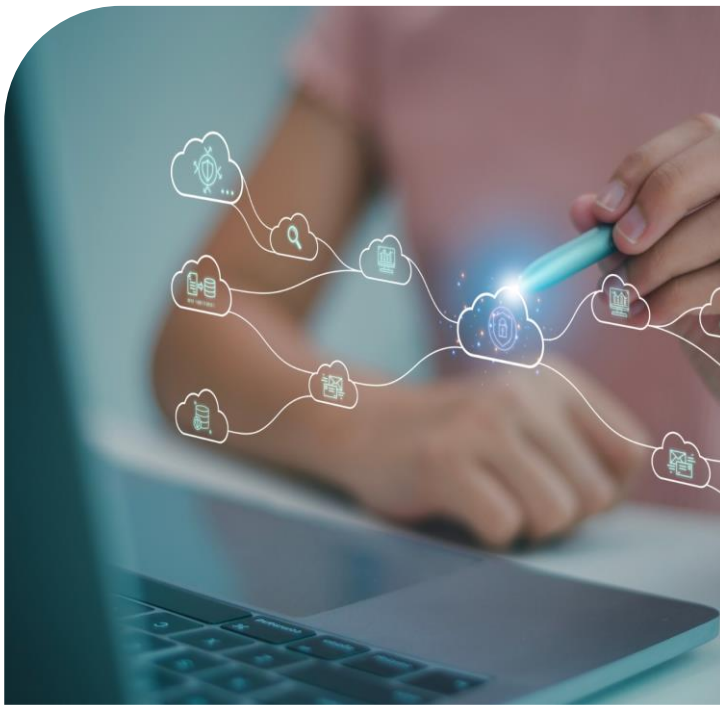
Entre las medidas que requiere la Directiva se incluyen aquellas que incumben a las amenazas a la seguridad física como resultado de una evaluación y análisis de riesgos sobre las infraestructuras digitales.

Al igual que en el resto de sectores, las infraestructuras digitales deberán disponer de planes de gestión de incidentes, de continuidad de negocio y de recuperación ante desastres, identificando de forma precisa las personas responsables y los equipos de respuesta, fijando los canales de comunicación internos y externos, y estableciendo los procedimientos necesarios.

Por otra parte, este es un sector que experimentará una mayor supervisión en el cumplimiento de las nuevas normativas regulatorias que le son de afectación, entre otras por ejemplo las regulaciones sobre Inteligencia Artificial, *BlockChain*, etc.

Estos sectores incluyen a:

- Proveedores de puntos de intercambio de internet.
- Proveedores de servicios de DNS, organizaciones que administran un base de datos de nombres de dominio y sus direcciones IP asociadas, excluidos los operadores de servidores raíz.
- Registros de nombres de dominio de primer nivel.
- Proveedores de servicios de computación en nube.
- Proveedores de servicios de centro de datos.
- Proveedores de redes de distribución de contenidos (CDN), una red de servidores interconectados que acelera la carga de las páginas web para las aplicaciones que tienen un uso intensivo de datos.
- Prestadores de servicios de confianza, persona física o jurídica que proporciona y conserva certificados digitales para crear y validar firmas electrónicas y autenticar a sus firmantes, así como sitios web en general. Del mismo modo verifica la identidad de usuarios, clientes o negocios y aprueba operaciones de firma electrónica a través de la emisión y el almacenamiento de certificados digitales.
- Proveedores de redes públicas de comunicaciones electrónicas.
- Proveedores de servicios de comunicaciones electrónicas disponibles para el público.
- Proveedores de servicios gestionados.
- Proveedores de servicios de seguridad gestionados.



Sector Administración Pública
(con exclusión del poder judicial, los parlamentos y los bancos centrales)

Cuando hablamos de la Administración Pública tenemos que tener presente los servicios esenciales que ofrecen a los ciudadanos, servicios sociales, de seguridad, económicos, de representación, etc., vitales y críticos para la sociedad europea.

Este sector maneja toda la información personal de sus ciudadanos, información confidencial que administran y gestionan, y a la que las organizaciones cibercriminales tienen puesto el foco de interés. Solo por poner un ejemplo de consecuencias directas en la sociedad son los ataques que sufren entidades públicas en la gestión de los censos y recuentos electorales, pudiendo cambiar el designio político de un Estado.

Como objetivo principal de la Directiva está la de garantizar la estabilidad de las infraestructuras críticas esenciales ante ataques cibernéticos y para ello exige la implementación de las medidas necesarias por parte de la Administración Pública de forma que se evite poner en peligro la información de sus ciudadanos, perturbar los servicios públicos esenciales o desestabilizar la sociedad a nivel local, regional o nacional.

La Directiva exige a la Administración Pública la implementación de las medidas de ciberseguridad, al igual que el resto de los sectores, ya que deben ser garantes de la protección de la información sensible de sus ciudadanos, la información financiera y los datos de sus infraestructuras críticas, ante posibles ataques cibernéticos que busquen el robo de información con fines maliciosos.

Entre las medidas incluidas en la Directiva están la obligación de llevar a cabo evaluaciones de riesgos de forma periódica en materia de ciberseguridad, y la de formar y concienciar a los funcionarios en ciberseguridad, algo ciertamente importante dado los diferentes niveles y grados de concienciación y motivación existentes en la Administración.

Este sector incluye a:

- Entidades de la Administración pública central.
- Entidades de la Administración pública a escala regional.

Sector espacio

Este sector es esencial en la economía de la Unión Europea dada la implicación y dependencia para muchas industrias como las de Telecomunicaciones, las de Navegación Aérea o la Seguridad Nacional. Esta importancia lo convierte en un objetivo prioritario para los ciberatacantes en busca de acceder a datos secretos, confidenciales, o alterar sistemas críticos.

En los últimos días hemos podido tener conocimiento que se están generando interferencias en las tecnologías de posicionamiento, localización y seguimiento GPS en el mar Báltico (Estonia, Letonia y Lituania) y norte de Noruega que impactan directamente en la operativa de los aeropuertos próximos a la frontera con Rusia, representando un peligro para la aviación civil.

Entre los requisitos de la Directiva NIS2 están la de informar de cualquier incidente que pueda afectar a su infraestructura, incluidos satélites y estaciones de seguimiento terrestres. Esto les obligará, entre otras medidas, a implementar sistemas mucho

más precisos de monitorización, detección y respuesta ante incidentes cibernéticos; a practicar una mayor colaboración pública y privada compartiendo información e inteligencia sobre amenazas con los organismos reguladores; y a realizar e implementar una estricta gestión de riesgos en su cadena de suministros.

Este sector incluye a:

- Operadores de infraestructuras terrestres, cuya propiedad, gestión y explotación descansa en los Estados miembros o en entidades privadas, que apoyan la prestación de servicios espaciales, excepto los proveedores de redes públicas de comunicaciones electrónicas.

Anexo II Otros sectores críticos

Sector servicios postales y de mensajería

El servicio postal y de mensajería, con la transformación digital, depende esencialmente de los sistemas y redes digitales para lleva a cabo la gestión y prestación de sus servicios postales, lo que lleva implícito una mayor exposición a ciberamenazas.

Estos operadores manejan gran cantidad de información y datos personales por lo que la Directiva les exige que garanticen la seguridad de estos datos implementando medidas como el cifrado, los controles de acceso y la autenticación multifactor.

La Directiva, respecto a este sector, también exige que las entidades tomen las medidas necesarias para garantizar una ciberseguridad resistente y resiliente.

Este sector incluye a:

- Proveedores de servicios postales, incluidos los proveedores de servicios de mensajería.

Sector gestión de residuos

Este sector es el responsable de proteger el medio ambiente, la sostenibilidad y mantener la salud pública, lo que lo convierte en parte esencial en la economía de la UE. El sector, debido a la variedad de actividades que realiza (recolección, transporte, tratamiento y eliminación) es ampliamente vulnerable a ciberataques que podrían llegar a causar consecuencias nefastas en la sociedad.

Uno de los requisitos de la Directiva es la exigencia a las entidades de la integración de

la ciberseguridad en todo el ciclo de vida de la gestión de residuos, es decir, desde la recogida hasta la eliminación de los residuos, teniendo en consideración también el manejo de residuos peligrosos.

Otro de los requisitos importantes de la Directiva es la obligación de realizar de forma periódica evaluaciones y análisis de riesgos de ciberseguridad y el establecimiento de las medidas necesarias para mitigar los riesgos que hayan sido identificados.

Este sector incluye a:

- Empresas que realizan la gestión de residuos, excepto aquellas para las que la gestión de residuos no es su principal actividad económica.

Sector fabricación, producción y distribución de sustancias y mezclas químicas

Uno de los sectores más importantes en la UE es la industria química al proporcionar una amplia gama de productos químicos, petroquímicos, polímeros, inorgánicos, especialidades y productos químicos de consumo.

Además, es un punto de apoyo a otros sectores industriales como la construcción, el transporte, la energía o la agricultura. Una interrupción en el suministro de sus productos podría tener serias consecuencias en la sociedad, lo que le convierte en objetivo conveniente para los atacantes cibernéticos.

Este es uno de los sectores que está bastante regulado en la UE y el cumplimiento de la Directiva obligará a las entidades a realizar una considerable inversión en recursos financieros, tecnológicos y humanos relacionados con sus infraestructuras TI y con la ciberseguridad.

Este sector incluye a:

- Empresas que realizan la fabricación de sustancias y la distribución de sustancias o mezclas químicas, y empresas que realizan la producción de artículos a partir de sustancias y mezclas químicas.

Sector producción, transformación y distribución de alimentos

Hablamos posiblemente de una de las industrias más importantes y mayores dentro de la UE, desde la obtención de materias primas de alimentación (agricultura, ganadería y pesca), al procesado, envasado, transporte y venta al por mayor y por menor. Con la evolución de la tecnología, esta industrial, al igual que el resto, se ha transformado digitalmente con una mayor interconexión, lo que la ha vuelto más expuesta a las amenazas de ciberseguridad.

La Directiva en el caso de este sector exige que se lleven a cabo evaluaciones de riesgos considerando las amenazas y vulnerabilidades únicas del sector, como son los ataques físicos a sus infraestructuras, o la presencia de elementos contaminantes en la cadena de suministro de alimentos.

Para ello las entidades deberán exigir que sus proveedores cumplan con los mismos niveles de ciberseguridad que ellos cumplen.

Este sector incluye a:

- Empresas alimentarias que se dediquen a la distribución al por mayor

y a la producción y transformación industriales.

Sector fabricación

Este sector es esencial en la economía de la UE, desde la producción de las pequeñas industrias manufactureras hasta los procesos industriales a gran escala.

La industria está sufriendo una enorme transformación digital, lo que viene a denominarse Industria 4.0, favorecida por una hiperconectividad de redes, sistemas y componentes, y que a su vez supone una mayor exposición a las amenazas cibernéticas.

Una de las cuestiones que tiene presente la Directiva para este sector es la dependencia con los proveedores, por lo que exige que los fabricantes prioricen la seguridad de la cadena de suministros mediante la evaluación, análisis y gestión de los riesgos de ciberseguridad en un horizonte de amenazas en continua evolución.

Este sector incluye a los subsectores de:

- **Fabricación de productos sanitarios y productos sanitarios para diagnóstico *in vitro*.**
    - Entidades que fabrican los productos sanitarios y entidades que fabrican los productos sanitarios para diagnóstico in vitro, excepto las entidades que fabrican productos sanitarios que se consideran esenciales en situaciones de emergencia de salud pública, que estaría incluida en el Anexo I Sector Sanitario.
- **Fabricación de productos informáticos, electrónicos y ópticos.**
    - Empresas que realizan cualquiera de las siguientes actividades económicas:
        - Fabricación de componentes electrónicos y circuitos impresos ensamblados.
        - Fabricación de ordenadores y equipos periféricos.
        - Fabricación de equipos de telecomunicaciones.
        - Fabricación de productos electrónicos de consumo (TV, radios, videos, etc.).
        - Fabricación de instrumentos y aparatos de medida, verificación y navegación.
        - Fabricación de relojes.
        - Fabricación de equipos de radiación, electromédicos y electroterapéuticos.
        - Fabricación de instrumentos de óptica y equipo fotográfico.
        - Fabricación de soportes magnéticos y ópticos.
- **Fabricación de material eléctrico.**
    - Empresas que realizan cualquiera de las siguientes actividades económicas:
        - Fabricación de motores, generadores y transformadores eléctricos.
        - Fabricación de aparatos de distribución y control eléctrico.

- Fabricación de pilas y acumuladores eléctricos.
- Fabricación de cables y dispositivos de cableado.
- Fabricación de cables de fibra óptica.
- Fabricación de otros hilos y cables electrónicos y eléctricos.
- Fabricación de dispositivos de cableado.
- Fabricación de lámparas y aparatos eléctricos de iluminación.
- Fabricación de electrodomésticos.
- Fabricación de aparatos domésticos no eléctricos.
- Fabricación de otro material y equipo eléctrico.

- **Fabricación de maquinaria y equipo no comprendidos en otras partes (n.c.o.p.).**
  - Empresas que realizan cualquiera de las siguientes actividades económicas:
    - Fabricación de motores y turbinas, excepto los destinados a aeronaves, vehículos automóviles y ciclomotores.
    - Fabricación de equipos de transmisión hidráulica y neumática.
    - Fabricación de otras bombas y compresores.
    - Fabricación de otra grifería y válvulas.
    - Fabricación de cojinetes, engranajes y órganos mecánicos de transmisión.
    - Fabricación de hornos y quemadores.
    - Fabricación de maquinaria de elevación y manipulación.
    - Fabricación de máquinas y equipos de oficina, excepto equipos informáticos.
    - Fabricación de herramientas eléctricas manuales.
    - Fabricación de maquinaria de ventilación y refrigeración no doméstica.
    - Fabricación de otra maquinaria de uso general n.c.o.p.
    - Fabricación de maquinaria agraria y forestal.
    - Fabricación de máquinas herramienta para trabajar el metal y otras máquinas herramienta.
    - Fabricación de otra maquinaria para usos específicos para la industrias.

- **Fabricación de vehículos de motor, remolques y semirremolques.**
  - Empresas que realizan cualquiera de las siguientes actividades económicas:
    - Fabricación de vehículos de motor.

- Fabricación de carrocerías para vehículos de motor; fabricación de remolques y semirremolques.
- Fabricación de equipos eléctricos y electrónicos para vehículos de motor.
- Fabricación de otros componentes, piezas y accesorios para vehículos de motor.

- **Fabricación de otro material de transporte.**
  - Empresas que realizan cualquiera de las siguientes actividades económicas:
    - Construcción de barcos y estructuras flotantes.
    - Construcción de embarcaciones de recreo y deporte.
    - Fabricación de locomotoras y material ferroviario.
    - Construcción aeronáutica y espacial y su maquinaria.
    - Fabricación de vehículos militares de combate,
    - Fabricación de motocicletas.
    - Fabricación de bicicletas y de vehículos para personas con discapacidad.
    - Fabricación de otro material de transporte n.c.o.p.

Sector proveedores de servicios digitales

Hablamos de un sector que ha transformado la forma en la que nos comunicamos, la forma en que las empresas operan a nivel mundial, realizan transacciones comerciales y acceden a información en línea en tiempo real. No cabe duda de que es una parte fundamental en la economía actual en la Unión Europea de la que dependen millones de ciudadanos.

Una de las prioridades de la Directiva es la colaboración entre los proveedores de servicios digitales y las autoridades competentes de ciberseguridad. La Directiva exige que para cumplir con los requisitos se deba informar de los incidentes significativos y mantener un registro y seguimiento de las medidas de seguridad aplicadas.

Entre las medidas que exige la Directiva está el cumplimiento de las normas de privacidad de datos, interrelacionada con el RGPD, y la obligación de informar ante cualquier incidente de seguridad.

Este sector incluye a:

- Proveedores de mercados en línea.
- Proveedores de motores de búsqueda en línea.
- Proveedores de plataformas de servicios de redes sociales.

Sector proveedores de servicios digitales

Este es un sector altamente internacionalizado con colaboraciones y asociaciones multinacionales. El cumplimiento de la Directiva NIS2 dependerá

de cada transposición a la normativa de cada país en el cual la entidad opere, pudiéndose dar el caso de tener que cumplir con requisitos específicos de varios países bajo una misma directiva.

Este sector maneja un gran volumen de información confidencial, en muchos casos datos personales, y por ello deben cumplir con múltiples regulaciones sobre privacidad y protección de datos como es el RGPD. En este caso la Directiva NIS2 establece una capa más de protección en el ámbito de la ciberseguridad.

Qué mejor objetivo para los ciberdelincuentes que intentar robar datos de investigaciones, espiar o alterar los resultados o los propios sistemas críticos de las entidades de investigación e innovación.

Este sector incluye a:

- Organismos de investigación.

Retos para los CISOs

Falta de Capacitación, Formación y Concienciación

Como CISOs tenemos la responsabilidad de exigir la capacitación del personal involucrado en la ciberseguridad, y fomentar, apoyar y divulgar la formación y concienciación de todo el personal. No debemos olvidar que la primera defensa en ciberseguridad en cualquier organización son los empleados, que a través de la Inteligencia Artificial y la Ingeniería Social ofrecen un vector de ataque ampliamente extendido entre los ciberdelincuentes.

Escasez de profesionales en Ciberseguridad

Uno de los retos a los que nos enfrentamos los CISOs es la escasez de profesionales capacitados y con experiencia en el ámbito de la Ciberseguridad. Esto conduce a generar una sobrecarga sobre el personal existente, y a la vez, un aumento en la rotación de este personal en busca de empresas que ofrezcan mejores condiciones laborales.

Interconexión de Sistemas y componentes Internos y Externos

Las empresas, para llevar a cabo el control de su infraestructura crítica, dependen de forma extensa de la interconexión de los sistemas, redes y dispositivos, como por ejemplo los sistemas SCADA, DCS, la conectividad con los RTU, IIoT, actuadores, sensores, robots y maquinarias, o sistemas de seguimiento de vehículos, localizadores GPS, etc., aumentando el riesgo de ciberataques y la filtración de datos.

Seguridad de los Sistemas de Control

Los CISOs somos conscientes de que un ataque cibernético dirigido tipo *Ransomware* puede llegar a interrumpir y bloquear la operación de los Sistemas de Información y de Control con el correspondiente impacto que suponer la imposibilidad de acceder a los datos y sistemas, la interrupción de las operaciones y la posibilidad de realizar las tareas críticas. Los daños que se pueden causar si se ven comprometidos los sistemas críticos como por ejemplo, sistemas de control de tráfico ferroviario, o sistemas de

navegación aérea o marítima, son impredecibles, no solo a nivel económico, sino en vidas humanas.

Vulnerabilidades de los Sistemas

Otra de las pesadillas es mantener los equipos y sistemas actualizados evitando y/o corrigiendo sus vulnerabilidades. Uno de los principales vectores de ataque que utilizan los ciberdelincuentes es la explotación de estas vulnerabilidades para conseguir sus objetivos. Por desgracia, los medios económicos y recursos técnicos y humanos que disponen estas organizaciones les permite investigar y hallar vulnerabilidades Zero-Day incluso antes que los propios fabricantes, y publicarlas en la Deep/Dark Web a cambio de interesantes compensaciones económicas.

En el caso del sector espacial, la amenaza de explotar alguna vulnerabilidad de sus activos, satélites o estaciones de seguimiento terrestre, es más significativa ya que podría suponer la interrupción de las comunicaciones espaciales y los servicios críticos dependientes.

Obsolescencia de los equipos

En especial en el sector industrial, las empresas mantienen en operación sistemas legacy que no disponen de soporte ni actualizaciones de seguridad de sus fabricantes, o incluso éstos han desaparecido del mercado. Esto es una de las razones que convierten a los sistemas y equipos en extremadamente vulnerables imposibilitando dar una respuesta efectiva ante un ataque cibernético.

Falta de estandarización

Dentro de cada sector, las organizaciones utilizan diferentes sistemas y fabricantes que en muchas ocasiones no cumplen con una normativa estandarizada en el desarrollo de sus sistemas y componentes, como por ejemplo el uso de protocolos propietarios de fabricantes. Esto ocasiona una mayor dificultad a la hora de aplicar medidas de seguridad unificadas y consistentes.

Infraestructuras basadas en servicios y tecnologías Web

No cabe duda de que uno de los principales objetivos de ataque se produce explotando las vulnerabilidades de las aplicaciones web y sistemas on-line, robando información, comprometiendo credenciales de acceso, inyectando código malicioso, suplantando páginas web reales, etc.

Otro de los retos en el entorno Web son los ataques DDoS que provocan la inactividad de la operativa con graves consecuencias económicas y de confianza.

No debemos olvidar que otro de los objetivos principales en los que están centrando sus esfuerzos las organizaciones cibercriminales son las amenazas a los servicios basados en la tecnología Cloud. Objetivo que viene motivado por el traspaso de sistemas y servicios on-premise al entorno Cloud con Infraestructuras como servicio (IaaS), Plataformas como servicios (PaaS) o Software como servicio (SaaS).

Limitación en la Inversión en Ciberseguridad

Las organizaciones tienen a optimizar recursos y eficiencia con la mínima inversión. Según estudios recientes la Dirección de las empresas son conscientes de la necesidad de adoptar medidas de ciberseguridad, pero a la hora de plasmarlo en sus presupuestos no es una prioridad, generando presupuestos limitados, insuficiencia de recursos y un aumento en la exposición a brechas de seguridad.

Amenazas Persistentes Avanzadas (APT)

En una época tan convulsa, con una situación geopolítica tan complicada, los actores-estado, ataques 'patrocinados' por un estado, sofisticados, complejos y con recursos financieros, están favoreciendo y apoyando a grupos organizados que se dedican a realizar este tipo de ataques denominados APT. El sector energético, sanitario y la Administración Pública están demostrando ser objetivos principales de sus ataques por la gran repercusión que puede tener el comprometer las infraestructuras críticas, interrumpir los servicios y afectar a la seguridad y bienestar de los ciudadanos.

Insiders

Nos referimos a las actuaciones maliciosas, intencionadas o no, realizadas por los empleados por desconocimiento, o por estar insatisfechos o descontentos, o por empleados de subcontratas con capacidad de acceso a los sistemas críticos y que pueden originar fallas en los sistemas, interrupciones, configuraciones incorrectas, fuga de datos o cualquier otro incidente de seguridad.

Dentro de este apartado podemos incluir a los saboteadores, actores maliciosos que tratan de dañar o inutilizar sistemas o equipos críticos dentro de las instalaciones provocando interrupciones significativas en los procesos operativos.

Cadena de Suministros

Todas las normativas que se están publicando actualmente (NIS2, CER, NIST, ISO, etc.) hacen hincapié en la necesidad de controlar con mayor rigurosidad la cadena de suministros, es decir, la conectividad con sistemas de terceros, con empresas suministradoras o proveedoras de servicios a través de las cuales a los ciberdelincuentes

les es más fácil aprovechar la debilidad en seguridad de sus sistemas y redes para penetrar en la red de la organización.

Protección de la información

Son muchas las entidades incluidas en los sectores de aplicación de la Directiva NIS2 que manejan información sensible, crítica y confidencial. En el sector financiero por ejemplo se manejan datos personales y económicos muy relevantes, en el sector de la salud, las entidades sanitarias manejan información de pacientes o historiales médicos de alto valor para los atacantes cibernéticos, y con un impacto adverso para las personas afectadas.

Robo de la propiedad Intelectual

Otro de los retos a los que nos enfrentamos es disponer en los sistemas, tanto en reposo como en tránsito, de información, procedimientos, patentes, estudios, etc., clasificados como propiedad intelectual y que es de alto valor para las organizaciones, y es algo que los ciberdelincuentes y las organizaciones cibercriminales buscan robar para beneficio propio o espionaje patrocinado por actores-Estado.

Objetivo de la Directiva

El principal objetivo de la norma es elevar el nivel de ciberseguridad y resiliencia de los sistemas de toda la UE frente a ciberamenazas a través de **Estrategias Nacionales de Ciberseguridad** (en España data del 2019, con la aprobación en 2022 del Plan Nacional de Ciberseguridad), **medidas para la gestión de riesgos** de ciberseguridad, **obligaciones de notificación** para las entidades, y normas y obligaciones relativas al **intercambio de información** sobre ciberseguridad.

Requisitos de cumplimiento

Gobernanza (art.20)

Los órganos de dirección de las entidades esenciales e importantes **aprobarán las medidas** para la gestión de riesgos de ciberseguridad adoptadas para dar cumplimiento a la Directiva, **supervisarán** su puesta en práctica y **responderán por su incumplimiento**; sin perjuicio a las normas sobre responsabilidad aplicables a las instituciones públicas, así como a la responsabilidad de los funcionarios públicos y los cargos electos o designados.

Los órganos de dirección de las entidades esenciales e importantes **deberán asistir a formaciones** y ofrecerán **formaciones similares a sus empleados periódicamente** al objeto de adquirir conocimientos y destrezas suficientes que les permitan detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados por la entidad.

Medidas para la gestión de riesgos de ciberseguridad (art. 21)

La normativa NIS2 exige que las entidades esenciales e importantes **adopten medidas organizativas, técnicas y operativas** adecuadas para prevenir, detectar y responder ante incidentes que afecten a su

seguridad y continuidad, gestionando los riesgos que se planteen para la seguridad de los sistemas de redes, de información y el entorno físico que utilizan dichas entidades en sus operaciones o en la prestación de sus servicios, previniendo o minimizando el impacto de los incidentes en los destinatarios de sus servicios y en otros servicios dependientes.

Teniendo en consideración la situación y el coste de su aplicación, las medidas garantizarán un **nivel de seguridad y protección** de los **sistemas de redes** e **de información** y el **entorno físico** de dichos sistemas, adecuado y proporcionado en relación con los peligros, riesgos, grado de exposición de la entidad, su tamaño, la probabilidad y la gravedad social y económica de su impacto.

Las **medidas organizativas, técnicas y operativas** requeridas para la protección de la infraestructura crítica, los datos, la privacidad y la disponibilidad de los servicios incluirán al menos los siguientes elementos:

- Políticas de Seguridad de los Sistemas de Información (SGSI) y análisis de riesgos.
- Gestión de Incidentes.
- Gestión de Crisis, Planes de Continuidad de Negocio (BCP) y Planes de Recuperación ante Desastres (DRP).
- Seguridad en la Cadena de Suministros.
- Seguridad en la Adquisición, Desarrollo y Mantenimiento de Sistemas de Redes y de Información.
- Políticas y Procedimientos de evaluación de la eficacia de las medidas de gestión de riesgos de ciberseguridad.
- Mejores Prácticas en ciberseguridad, Formación y Concienciación.
- Políticas y Procedimientos de utilización de criptografía y cifrado de la información y los datos.
- Seguridad de los Recursos Humanos.
- Políticas de Control de Acceso y Gestión de Activos.
- Autenticación multifactorial (MFA).
- Seguridad en las comunicaciones (voz, video y texto).
- Implementación de sistemas seguros de comunicación de emergencia.

Obligaciones de notificación (art. 23)

Las entidades esenciales e importantes **notificarán, sin demora indebida**, a su CSIRT o, en su caso, a la autoridad competente, cualquier incidente que tenga un **impacto significativo** en la prestación de sus servicios, es decir, si:

a) Ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada.

b) Ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables.

Cuando proceda, las entidades afectadas, sin demora indebida, **notificarán** a los destinatarios de sus servicios **los incidentes significativos** susceptibles de afectar

negativamente a la prestación de dichos servicios, y comunicarán, en caso de que puedan verse **afectados por una ciberamenaza significativa**, las **medidas o soluciones** que dichos destinatarios pueden aplicar **en respuesta a la amenaza**.

A los efectos de la notificación las entidades afectadas presentarán:

1. En el plazo de **veinticuatro horas** desde que se haya tenido constancia del incidente significativo, una **alerta temprana** en la que se indicará, cuando proceda, si cabe sospechar que el incidente significativo responde a una acción ilícita o malintencionada o puede tener repercusiones transfronterizas.
2. En el plazo de **setenta y dos horas** desde que se haya tenido constancia del incidente significativo, una **notificación del incidente** en la que se actualizará, cuando proceda, la información anterior y se expondrá una evaluación inicial del incidente significativo, incluyendo su gravedad e impacto, así como indicadores de compromiso, cuando estén disponibles.
3. A instancias de un CSIRT o, en su caso, de la autoridad competente, un **informe intermedio** con las actualizaciones pertinentes sobre la situación.
4. Un **informe final**, a más tardar **un mes después** de presentar la notificación del incidente; en el caso de que el incidente siga en curso en el momento de la presentación del informe final las entidades afectadas presenten un **informe de situación** en ese momento y un **informe final** en el plazo de **un mes** a partir de que hayan **gestionado el incidente**.

El CSIRT o la autoridad competente ofrecerá, sin demora indebida y, cuando sea posible, **en el plazo de veinticuatro horas** tras la recepción de la **alerta temprana**, una **respuesta** a la entidad notificante, en particular sus comentarios iniciales sobre el incidente significativo y, a instancias de la entidad, una **orientación o asesoramiento operativo** sobre la aplicación de posibles medidas paliativas.

Cuando el **conocimiento del público** sea necesario para evitar un incidente significativo o hacer frente a un incidente significativo en curso, o cuando la divulgación del incidente significativo redunde en el interés público, el CSIRT o la autoridad competente podrán **informar al público**, después de consultarlo con la entidad afectada, del incidente significativo o exigir a la entidad que lo haga.

Notificación voluntaria de información pertinente (art. 30)

Además de las obligaciones de notificación, pueden ser presentadas a los CSIRT o autoridades competentes de forma voluntaria por entidades esenciales e importantes en el caso de incidentes, ciberamenazas y cuasi incidentes; y por las entidades distintas de las mencionadas, independientemente de si están o no comprendidas en el ámbito de aplicación de la Directiva, en el caso de incidentes, ciberamenazas o cuasi incidentes significativos.

Mecanismos de intercambio de información sobre ciberseguridad (art. 29)

Los Estados miembros velarán por que las entidades comprendidas en el ámbito de aplicación y, cuando proceda, otras entidades no comprendidas en el ámbito de aplicación de la Directiva NIS2 **intercambiarán entre sí de forma voluntaria información relevante** sobre ciberseguridad, en particular la relativa a ciberamenazas, cuasi incidentes, vulnerabilidades, técnicas y procedimientos, indicadores de compromiso, tácticas de los adversarios, información específica del agente de riesgo, alertas de ciberseguridad y recomendaciones sobre configuraciones de las herramientas de seguridad para detectar ciberataques, siempre que:

1. tenga como objetivo prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión,
2. reforzar el nivel de ciberseguridad, en particular al concienciar sobre las ciberamenazas, limitar o impedir la capacidad de tales amenazas para propagarse, o respaldar una batería de capacidades de defensa, corrección y divulgación de las vulnerabilidades, técnicas de detección, contención y prevención de amenazas, estrategias de mitigación, o etapas de respuesta y recuperación, o
3. fomentar la investigación de ciberamenazas en colaboración con entidades públicas y privadas.

Entidades esenciales: supervisión y ejecución

Las medidas que se impondrán a las entidades esenciales en relación con sus obligaciones serán efectivas, proporcionadas y disuasorias, teniendo en cuenta las circunstancias de cada caso individual.

Supervisión

Las competencias de las autoridades en el ejercicio de sus **funciones de supervisión** serán, como mínimo:

a) **Inspecciones** in situ y supervisión a distancia, incluidos controles aleatorios.

b) **Auditorías de seguridad** periódicas y específicas.

c) **Auditorías ad-hoc** cuando lo justifique un incidente significativo[4] o un incumplimiento.

d) **Análisis de seguridad** basados en criterios de evaluación del riesgo objetivos, no discriminatorios, justos y transparentes.

e) **Solicitudes de información** necesaria para evaluar las medidas para la gestión de riesgos de ciberseguridad adoptadas por la entidad afectada, en particular las políticas de ciberseguridad documentadas, así como el cumplimiento de la obligación de presentar información a las autoridades competentes.

f) **Solicitudes de acceso** a datos, documentos e información necesaria.

g) **Solicitudes de pruebas** de la aplicación de las políticas de ciberseguridad.

Ejecución

Las competencias de las autoridades en el ejercicio de sus **facultades de ejecución** sobre las entidades afectadas serán, como mínimo:

a) **Apercibir** por incumplimiento.

b) **Adoptar instrucciones vinculantes**, en particular sobre las medidas necesarias para prevenir o subsanar un incidente, así como **plazos para la ejecución** de esas medidas y notificar su aplicación, o una **orden de requerimiento** para que las entidades afectadas subsanen las deficiencias detectadas o los incumplimientos.

c) **Exigir que pongan fin a las conductas** que infringen la Directiva y que se abstengan de repetirlas.

d) **Exigir que se garantice que las medidas** para la gestión de riesgos de ciberseguridad son conformes con lo dispuesto o que cumplan las obligaciones de notificación de una

[4] **Incidente significativo**: todo hecho que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos y que tenga un impacto significativo al **causar o poder causar graves perturbaciones operativas** de los servicios o **pérdidas económicas** para la entidad afectada; o **afecte o pueda afectar a otras personas físicas o jurídicas** al causar **perjuicios materiales o inmateriales** considerables.

manera específica y en un plazo concreto.

e) **Ordenar que se informe a las personas físicas o jurídicas** a las que prestan servicios o realizan actividades y que puedan verse afectadas por una ciberamenaza significativa, sobre la naturaleza de la amenaza, así como sobre cualquier posible medida correctora o de protección que puedan adoptar en respuesta a la amenaza.

f) **Ordenar que apliquen las recomendaciones** formuladas a raíz de una auditoría de seguridad en un plazo razonable.

g) **Designar un responsable de supervisión** con funciones claramente definidas para que supervise, durante un período determinado, el cumplimiento de sus obligaciones.

h) **Ordenar que hagan públicos** determinados aspectos del incumplimiento de una manera específica.

i) **Imponer o solicitar la imposición** por parte de los organismos u órganos jurisdiccionales competentes de acuerdo con la legislación nacional de una **multa administrativa**.

Cuando las medidas de ejecución adoptadas resulten ineficaces, las autoridades competentes estarán facultadas para **fijar un plazo** en el que se requerirá a la entidad esencial que adopte las medidas necesarias para subsanar las deficiencias o cumplir los requisitos de dichas autoridades.

Si las medidas requeridas no se adoptan dentro del plazo establecido, las autoridades competentes estarán facultadas para:

a) **Suspender temporalmente** una certificación o autorización referente a **una parte o la totalidad de los servicios o actividades** prestados por la entidad esencial.

b) Solicitar que **prohíban temporalmente a cualquier persona** que ejerza responsabilidades de **dirección** a nivel de director general o representante legal de la entidad esencial **ejercer funciones** de dirección en dicha entidad.

Las suspensiones o las prohibiciones temporales impuestas se aplicarán únicamente hasta que la entidad afectada adopte las medidas necesarias para subsanar las deficiencias o cumplir los requisitos de la autoridad competente.

Las medidas de ejecución previstas en el presente apartado **no serán aplicables a las entidades de la Administración pública** sujetas a la presente Directiva.

Responsabilidad de la Dirección

Cualquier persona física responsable de una entidad esencial o que actúe como representante de ella con facultades para representarla, con autoridad para tomar decisiones en su nombre o ejercer control sobre ella, tendrá las competencias para velar por el cumplimiento de la Directiva.

Dichas personas físicas se considerarán **responsables por el incumplimiento** de su deber de garantizar el cumplimiento de la Directiva.

En el caso de entidades de la **Administración pública**, se entenderá sin perjuicio en materia de responsabilidad de los funcionarios y cargos electos o designados.

Consideraciones agravantes y atenuantes

a) La **gravedad** del incumplimiento y la **importancia** de las disposiciones infringidas. Constituyen incumplimientos graves:

   i. Incumplimientos reiterados.

   ii. Ausencia de notificación o subsanación de los incidentes significativos.

   iii. Ausencia de subsanación de deficiencias tras recibir instrucciones vinculantes.

   iv. Obstrucción de las auditorías o actividades de control tras la constatación de un incumplimiento.

   v. Suministro de información falsa o manifiestamente imprecisa en relación con las medidas de gestión del riesgo de ciberseguridad o las obligaciones de notificación.

b) La **duración** del incumplimiento.

c) Todo **incumplimiento anterior** relevante cometido por la entidad afectada.

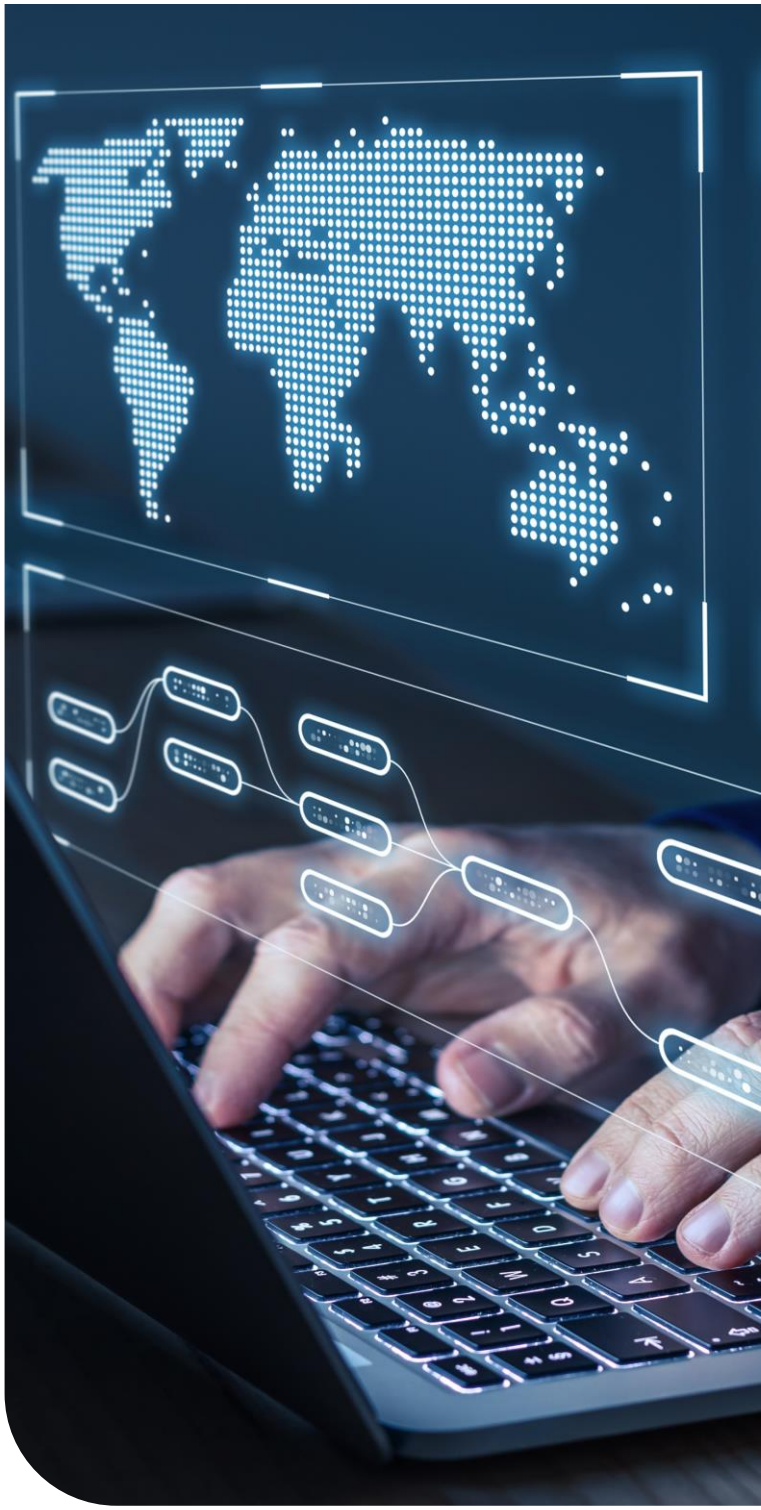
d) Todo **perjuicio material o inmaterial causado**, incluidas las pérdidas financieras o económicas, los **efectos** para otros servicios y el **número de usuarios afectados**.

e) Cualquier **intencionalidad** o **negligencia**

f) Cualesquiera **medidas adoptadas** por la entidad para **prevenir o reducir los perjuicios** materiales o inmateriales.

g) Cualquier **adhesión a códigos de conducta** o a **mecanismos de certificación** aprobados.

h) El **grado de cooperación** de las personas físicas o jurídicas.



Entidades importantes: supervisión y ejecución

Cuando se dispongan de pruebas, indicios o información de que una entidad importante presuntamente no cumple la Directiva, las autoridades competentes actuarán, cuando proceda, a través de **medidas de supervisión a posteriori**.

Las medidas serán efectivas, proporcionadas y disuasorias, teniendo en cuenta las circunstancias de cada caso.

Supervisión

Las competencias de las autoridades en el ejercicio de sus **funciones de supervisión** serán, como mínimo:

a) **Inspecciones** in situ y supervisión **a posteriori** a distancia, incluidos controles aleatorios.

b) **Auditorías de seguridad** específicas;

c) **Análisis de seguridad** basados en criterios de evaluación del riesgo objetivos, no discriminatorios, justos y transparentes.

d) **Solicitudes de información** necesaria para evaluar **a posteriori** las medidas para la gestión de riesgos de ciberseguridad adoptadas por la entidad afectada, en particular las políticas de ciberseguridad documentadas, así como el cumplimiento de la obligación de presentar información a las autoridades competentes.

e) **Solicitudes de acceso** a datos, documentos e información necesaria.

f) **solicitudes de pruebas** de la aplicación de las políticas de ciberseguridad.

Ejecución

Las competencias de las autoridades en el ejercicio de sus **facultades de ejecución** sobre las entidades afectadas serán, como mínimo:

a) **Apercibir** por incumplimiento.

b) **Adoptar instrucciones vinculantes**, o una **orden de requerimiento** para que las entidades afectadas subsanen las deficiencias detectadas o los incumplimientos.

c) **Exigir que pongan fin a las conductas** que infringen la Directiva y que se abstengan de repetirlas.

d) **Ordenar que se garantice que las medidas** para la gestión de riesgos de ciberseguridad son conformes con lo dispuesto o que cumplan las obligaciones de notificación de una manera específica y en un plazo concreto.

e) **Ordenar que se informe a las personas físicas o jurídicas** a las que prestan servicios o realizan actividades y que puedan verse afectadas por una ciberamenaza significativa, sobre la naturaleza de la amenaza, así como sobre cualquier posible medida correctora o de protección que puedan adoptar en respuesta a la amenaza.

f) **Ordenar que apliquen las recomendaciones** formuladas a raíz de una auditoría de seguridad en un plazo razonable.

g) **ordenar que hagan públicos** determinados aspectos del incumplimiento de una manera específica;

h) **imponer o solicitar la imposición** por parte de los organismos u órganos jurisdiccionales competentes de acuerdo con la legislación nacional de una **multa administrativa**.

Responsabilidad de la Dirección

En los mismos términos que para las entidades esenciales aplicando el principio *mutatis mudandis* (RAE: cambiando lo que se deba cambiar).

Consideraciones Agravantes y Atenuantes

Se adoptarán las mismas consideraciones que para las entidades esenciales aplicando el principio *mutatis mudandis* (RAE: cambiando lo que se deba cambiar).

Multas administrativas

Serán efectivas, proporcionadas y disuasorias, teniendo en cuenta las circunstancias de cada caso individual, y se impondrán a título adicional respecto a cualquiera de las medidas contempladas en la Directiva.

A la hora de decidir la imposición de una multa administrativa y su cuantía en cada caso particular se tendrán debidamente en cuenta, como mínimo, las consideraciones agravantes y atenuantes detalladas anteriormente.

Los Estados miembros podrán prever la facultad de **imponer multas coercitivas** para obligar a una entidad esencial o importante a poner fin a un incumplimiento de la Directiva de conformidad con una decisión previa de la autoridad competente.

Entidades Esenciales

Las **entidades esenciales** sean sancionadas por el incumplimiento de las medidas para la gestión de riesgos de ciberseguridad o las obligaciones de notificación, con multas administrativas de un máximo de, **al menos, 10 000 000 EUR** o de un máximo de, al menos, **el 2 % del volumen de negocios anual total a nivel mundial** de la empresa a la que pertenece la entidad esencial durante el ejercicio financiero anterior, optándose por **la de mayor cuantía**.

Entidades Importantes

Las **entidades importantes** sean sancionadas por el incumplimiento de las medidas para la gestión de riesgos de ciberseguridad o las obligaciones de notificación, con multas administrativas de un máximo de, **al menos, 7.000.000 EUR** o de un máximo de, al menos, **el 1,4 % del volumen de negocios anual total a nivel mundial** de la empresa a la que pertenece la entidad importante durante el ejercicio financiero anterior, optándose por **la de mayor cuantía**.

Entidades de la Administración Pública

Cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida,

imponer multas administrativas a las **entidades de la Administración pública**.

Incumplimientos con violación de la seguridad de los datos personales

Cuando las autoridades competentes tengan constancia en el transcurso de ejercicio de sus funciones de supervisión o ejecución, de que el incumplimiento de las obligaciones puede conllevar una violación de la seguridad de los datos personales informarán sin demora indebida a las autoridades de control establecidas en el RGPD / LOPDGDD.

No se impondrán multas administrativas en el caso de que ya sea impuesta por la autoridad de control en virtud del RGPD, pero sí podrán imponer el resto de las medidas de ejecución previstas en la Directiva.

Sanciones

Cada Estado miembro establecerá el régimen de sanciones aplicables a cualquier incumplimiento de las disposiciones nacionales adoptadas al amparo de la Directiva y adoptarán todas las medidas necesarias para garantizar su ejecución. Tales sanciones serán efectivas, proporcionadas y disuasorias. Recordemos que en España la Directiva NIS2 aún no ha sido transpuesta a la normativa nacional

Esquemas europeos de certificación de la ciberseguridad

Para demostrar la conformidad con determinados requisitos expuestos anteriormente, los Estados miembros podrán exigir a las entidades esenciales e importantes que utilicen productos, servicios y procesos de TIC particulares, desarrollados por la entidad o adquiridos a terceros, que estén certificados en virtud de un esquema europeo de certificación de la ciberseguridad. En España, **ENAC** (Entidad Nacional de Acreditación) está en disposición de acreditar a laboratorios de acuerdo a los requisitos del nuevo esquema europeo de ciberseguridad EUCC.

El **esquema europeo de certificación basado en *Common Criteria*** (**EUCC**), elaborado por la Agencia de Ciberseguridad de la Unión Europea (ENISA), se ha convertido en el primer esquema de certificación de ciberseguridad adoptado en la UE dentro del marco del **Reglamento (UE) 2019/881**, popularmente conocido como ***Cybersecurity Act***, y tiene por objetivo elevar el nivel de ciberseguridad de los productos, servicios y procesos de TIC en el mercado comunitario. En concreto, este esquema, permite a los proveedores del sector que deseen demostrar la seguridad de sus productos TIC, tales como componentes tecnológicos (chips, tarjetas inteligentes), *hardware* y *software*, someterse a un proceso de evaluación común de la UE para certificar estos productos.

Govertis, parte de Telefónica Tech

www.govertis.com | info@govertis.com | 902 900 231

GOVERTIS
Part of Telefónica Tech