Deloitte.

Directiva NIS 2

Directiva (UE) 2022/2555
relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión

Contenidos

Introducción

En agosto de 2016 entró en vigor la primera versión de la Directiva NIS (Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión) cuyo objetivo era estandarizar las medidas de seguridad de los miembros de la Unión Europea. A partir de ella, se realizó la transposición de la Directiva NIS en España a través del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, y posteriormente se publicó el desarrollo reglamentario de la misma a través del Real Decreto 43/2021, de 26 de enero.

El pasado 27 de diciembre de 2022 se publicó la nueva "Directiva (UE) 2022/2555 del parlamento europeo y del consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión" (en adelante, Directiva NIS 2), cuyo objetivo es mejorar las medidas destinadas a garantizar un adecuado nivel común de ciberseguridad.

El presente artículo tiene como objetivo resumir los aspectos principales de la Directiva NIS 2, identificando sus principales impactos, especialmente para las entidades esenciales e importantes. De esta manera, se pretende contestar a las siguientes preguntas:

- ¿Qué sectores se encuentran bajo la aplicabilidad de la Directiva NIS 2?
- ¿A quién aplica la Directiva NIS 2?
- ¿Cuáles son los principales organismos vinculados a la Directiva NIS 2?
- ¿Qué impacto tendrá la Directiva NIS 2 sobre las entidades afectadas?
- ¿Qué requerimientos de notificación de incidentes tendrán que cumplir las entidades afectadas?
    - ¿Qué es un incidente con impacto significativo?
    - ¿Cuál es el flujo de notificación propuesto?
- ¿Cuáles serán las funciones y competencias de las autoridades competentes de cada Estado miembro?
- ¿Cómo será el régimen sancionador en los Estados miembro?
- ¿Cuáles son los próximos pasos?

¿Qué **sectores** se encuentran bajo la **aplicabilidad** de la Directiva NIS 2?

La Directiva NIS 2 diferencia dos tipos de sectores de aplicación: **"Sectores de Alta Criticidad"** y **"Otros sectores críticos"**. En total, hay 18 sectores a los que aplica la Directiva, siendo 11 los sectores de alta criticidad y 7 el resto de sectores críticos. Además, la Directiva NIS 2 divide algunos sectores en subsectores específicos que facilitan la identificación por parte de las propias entidades. Así, por ejemplo, dentro del sector de energía, se encuentran los subsectores de electricidad, sistemas urbanos de calefacción y de refrigeración, crudo, gas e hidrógeno. Si bien es cierto que se ha aumentado el número total de sectores contemplados en la Directiva NIS 2, hay sectores que ya lo estaban en la Directiva anterior (energía, banca, infraestructura de mercados financieros, sector sanitario, transporte, infraestructura digital y aguas potables).

En este sentido, cabe recalcar que muchos de estos nuevos sectores ya habían sido contemplados adicionalmente en la regulación nacional que se elaboró con motivo de la transposición de la Directiva NIS (Real Decreto-ley 12/2018 y Real Decreto 43/2021), por lo que el cambio en nuestro país no es tan grande como puede serlo en otros.

Ilustración 1 - Sectores de alta criticidad y otros sectores críticos contemplados en NIS 2

¿**A quién aplica** la Directiva NIS 2?

La Directiva NIS 2 aplicará, de forma general y sin entrar en las excepciones concretas establecidas en la propia Directiva, a las entidades públicas o privadas que pertenezcan a alguno de los sectores de alta criticidad u otros sectores críticos que superen los límites máximos[1] considerados para las mismas.

Asimismo, independientemente del tamaño, la Directiva NIS 2 aplicará a las entidades cuando los servicios sean prestados por:

- Proveedores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles para el público;
- Prestadores de servicio de confianza;
- Registros de nombres de dominio de primer nivel y proveedores de servicio de sistema de nombres de dominio;
- Entidades que sean el único proveedor en un Estado miembro de un servicio esencial;
- Entidades en las que una perturbación del servicio prestado pudiera tener repercusiones significativas sobre la seguridad pública, el orden público o la salud pública;
- Entidades en las que una perturbación del servicio prestado pudiera incluir riesgos sistemáticos significativos, en particular para los sectores en los que tal perturbación podría tener repercusiones de carácter transfronterizo;
- Entidades que sean críticas a la luz de su importancia específica a nivel nacional o regional;
- Entidades de la administración pública central o regional definida por un Estado miembro;
- Entidades identificadas como entidad crítica con arreglo a la "Directiva (UE) 2022/2557 relativa a la resiliencia de las entidades críticas" (en adelante, Directiva CER);
- Entidades que presten servicios de registro de nombres de dominio;
- Si así lo dispone el Estado miembro, entidades de la Administración pública a nivel local o centros de enseñanza, en particular cuando lleven a cabo actividades críticas de investigación.

Es importante señalar que la Directiva NIS 2, para aquellas entidades afectadas por el "Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital del sector financiero" (en adelante, Reglamento DORA), ha definido un conjunto de disposiciones en las que, deben aplicarse aquellas reflejadas Reglamento DORA, en concreto aquellas relativas a las medidas de gestión de los riesgos de las tecnologías de la información y de las comunicaciones (TIC), la gestión de los incidentes relacionados con las TIC y, en particular, la notificación de incidentes graves relacionados con las TIC, así como las pruebas de la resiliencia operativa digital, los mecanismos de intercambio de información y los riesgos de terceros relacionados con las TIC.

La Directiva NIS 2 cambia la denominación anterior de Operadores de Servicios Esenciales (por sus siglas, OSE) y Proveedores de Servicios Digitales (por sus siglas, PSD). Ahora, se distinguen dos tipos de entidades, las cuales quedan diferenciadas de la siguiente manera:

- **Entidades esenciales,** que serán aquellas que pertenezcan a los sectores de alta criticidad que superen los límites máximos previstos, así como los prestadores cualificados de servicios de confianza y registros de nombres de dominio de primer nivel y proveedores de servicios de DNS, independientemente de su tamaño. También serán entidades de este tipo los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicación electrónicos disponibles para el público que sean consideradas medianas empresas, entidades de la Administración pública, cualquier otra entidad perteneciente a otros sectores críticos que el Estado miembro identifique como entidad esencial, las entidades críticas identificadas por la Directiva CER, y, si así lo dispone el Estado miembro, las entidades identificadas como operadores de servicios esenciales de conformidad con la anterior Directiva NIS.
- **Entidades importantes,** que serán todas aquellas entidades que pertenezcan a los sectores de alta criticidad o a otros sectores críticos que no pueden considerarse entidades esenciales.

1 *Microempresas, pequeñas empresas y medianas empresas de menos de 250 personas y cuyo volumen anual de negocios no exceda los 50 millones de euros o cuyo balance general anual no exceda los 43 millones de euros.*

¿Cuáles son los principales **organismos vinculados** a la Directiva NIS 2?

- **Autoridades competentes,** cuyo cometido será la supervisión de las entidades a través de inspecciones, análisis de seguridad o auditorías. Deberá esperarse hasta la transposición de la Directiva NIS 2 por el Estado miembro, para saber cuáles serán estas Autoridades Competentes, aunque a nivel nacional ya se anticiparon con la Directiva NIS.

- **Equipos de respuesta a incidentes de seguridad informática (CSIRT),** que deberán prestar asistencia a las entidades esenciales e importantes afectadas por cualquier incidente. Asimismo, los CSIRTs deberán difundir alertas, avisos e información sobre ciberamenazas, vulnerabilidades e incidentes entre las entidades implicadas en la Directiva NIS 2. Para ello, deberán garantizar una gran disponibilidad de los canales de comunicación, estar dotadas de un sistema de gestión de solicitudes que garantice la efectividad y eficiencia y garantizar la confidencialidad y fiabilidad de sus operaciones.

- **Red de CSIRTs,** que estará formada por representantes de los CSIRTs y el Equipo de Respuesta a Emergencias Informáticas de las instituciones, órganos y organismos de la Unión (CERT-EU). El principal cometido de la red de CSIRTs será el intercambio de información de incidentes, cuasincidentes, ciberamenazas, etc.

- **Punto de contacto único,** designado por el Estado miembro y cuyo cometido será asegurar la cooperación transfronteriza entre todas las Autoridades Competentes designadas en dicho Estado.

- **Grupo de Cooperación** formado por representantes de los Estados miembro, la Comisión y ENISA, y cuyo objetivo será proporcionar a las autoridades competentes orientación con la transposición y aplicación de la Directiva, desarrollo y ejecución de políticas sobre divulgación coordinada de vulnerabilidades, intercambio de buenas prácticas e información relacionada con la aplicación de la Directiva, ciberamenazas, vulnerabilidades, etc.

- **Red europea de organizaciones de enlace para la crisis de ciberseguridad (EU-CyCLONe)** estará formada por la Autoridades de Gestión de Crisis de Ciberseguridad de los Estados miembro y la Comisión, que tendrá un papel de observador en caso de que un ciberincidente pueda tener un impacto significativo en los servicios y actividades incluidos en la Directiva NIS 2. El principal cometido de la EU-CyCLONe será respaldar la gestión coordinada de los incidentes y crisis de ciberseguridad a gran escala.

¿Qué **impacto** tendrá la Directiva NIS 2 sobre las **entidades afectadas**?

Las entidades esenciales e importantes deberán tener en consideración distintos aspectos, como son la gobernanza, las medidas que deberán aplicar para la gestión de riesgos de ciberseguridad, la gestión y notificación de incidentes (que será tratada en un apartado independiente), o el intercambio de información de ciberseguridad.

Gobernanza

En el artículo 20 se menciona la relevancia y las responsabilidades que van a adquirir los Órganos de Dirección de las entidades, poniendo el foco principalmente en dos puntos:

- Los Órganos de Dirección de las entidades esenciales e importantes serán quienes deberán aprobar las medidas para la gestión de riesgos de ciberseguridad y supervisarán su puesta en práctica, ya que en el caso de incumplimiento de la presente Directiva serán quienes respondan ante ello.

- Los integrantes de dichos Órganos de Dirección deberán asistir a formaciones de gestión de riesgos de ciberseguridad de manera periódica. Del mismo modo, los empleados, alentados por los Órganos de Dirección, deberán también, de manera periódica, adquirir conocimientos y destrezas suficientes que les permitan detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad (concienciación, formación, etc.).

Medidas para la gestión de riesgos de ciberseguridad

El artículo 21 es uno de los más relevantes dentro de la Directiva, ya que establece que las entidades esenciales e importantes deben gestionar los riesgos que se planteen para la seguridad de sus sistemas de información y prevenir o minimizar las repercusiones de los incidentes. A la hora de establecer dichas medidas, las entidades deberán tener en cuenta el grado de exposición, su tamaño y la probabilidad de ocurrencia, así como la gravedad de la posible materialización de una perturbación.

Las entidades deberán, como mínimo, teniendo en cuenta lo que dicte la transposición del Estado miembro, adoptar medidas relativas a los siguientes puntos:

- Establecer políticas de seguridad de los sistemas de información y análisis de riesgos.

- Contar con un proceso completo de gestión de incidentes.

- Contemplar la continuidad de las actividades, considerando la gestión de copias de seguridad, la recuperación en caso de catástrofe y la gestión de crisis.

- Contemplar la seguridad de la cadena de suministros, incluyendo los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores.

- Considerar la seguridad en la adquisición, el desarrollo y el mantenimiento de redes y sistemas de información, incluyendo la gestión y divulgación de vulnerabilidades.

- Establecer políticas y procedimientos para evaluar la eficacia de las medidas de gestión de riesgos de ciberseguridad.

- Contar con prácticas básicas de ciberhigiene[2] y formación en ciberseguridad.

- Establecer políticas y procedimientos sobre el uso de la criptografía y el cifrado.

- Contemplar la seguridad relativa a los recursos humanos, políticas de control de acceso y la gestión de activos.

- Hacer uso de soluciones de autenticación multifactor o de autenticación continua.

Como se mencionaba anteriormente, estás medidas deberán ser aprobadas por los Órganos de Dirección, siendo éstos quienes supervisarán su correcta aplicación.

---

2 *Las políticas de ciberhigiene proporcionan la base para proteger la seguridad de las infraestructuras de los sistemas de redes y de información, del hardware, del software, de las aplicaciones en línea, así como los datos comerciales o de usuarios finales de los que dependen las entidades. Estas políticas de ciberhigiene permiten establecer un marco proactivo de preparación y seguridad global en caso de incidentes o ciberamenazas.*

Mecanismos de intercambio de información sobre ciberseguridad

En el artículo 29 se mencionan cuáles serán los mecanismos de intercambios de información, y las circunstancias en las que las entidades sometidas a la Directiva deberán realizar dichos intercambios.

El principal objetivo de estos intercambios de información es prevenir, detectar o responder ante incidentes, recuperarse de ellos o reducir, en la medida de lo posible, su repercusión, reforzando así el nivel de ciberseguridad de las entidades. Para ello, los Estados miembro facilitarán el establecimiento de los mecanismos de intercambio de información sobre ciberseguridad, y establecerán la exigencia de que se formalicen acuerdos para que se lleven a cabo de manera segura entre los participantes.

Cualquier participación en este tipo de acuerdos, o mecanismo, deberá ser notificado por parte de las entidades esenciales e importantes a las autoridades competentes, así como su retirada, cuando proceda. En este intercambio de información también podrán participar entidades que no entren del ámbito de aplicación de la Directiva NIS 2 de forma voluntaria.

¿Qué requerimientos de **notificación de incidentes** tendrán que cumplir las entidades afectadas?

El artículo 23 de la Directiva NIS 2 estipula que los Estados miembro deberán asegurarse de que las entidades esenciales e importantes notifiquen a su CSIRT de referencia, o a la autoridad competente, cualquier incidente que tenga un impacto significativo en la prestación de sus servicios. En el caso de que el incidente pueda afectar a usuarios de ese servicio esencial, la entidad deberá notificarlo también a dichos usuarios.

También se deberá comunicar a los destinatarios del servicio que pueden verse afectados por una ciberamenaza significativa, las medidas o soluciones que dichos destinatarios pueden aplicar en respuesta a la amenaza.

¿Qué es un incidente con impacto significativo?

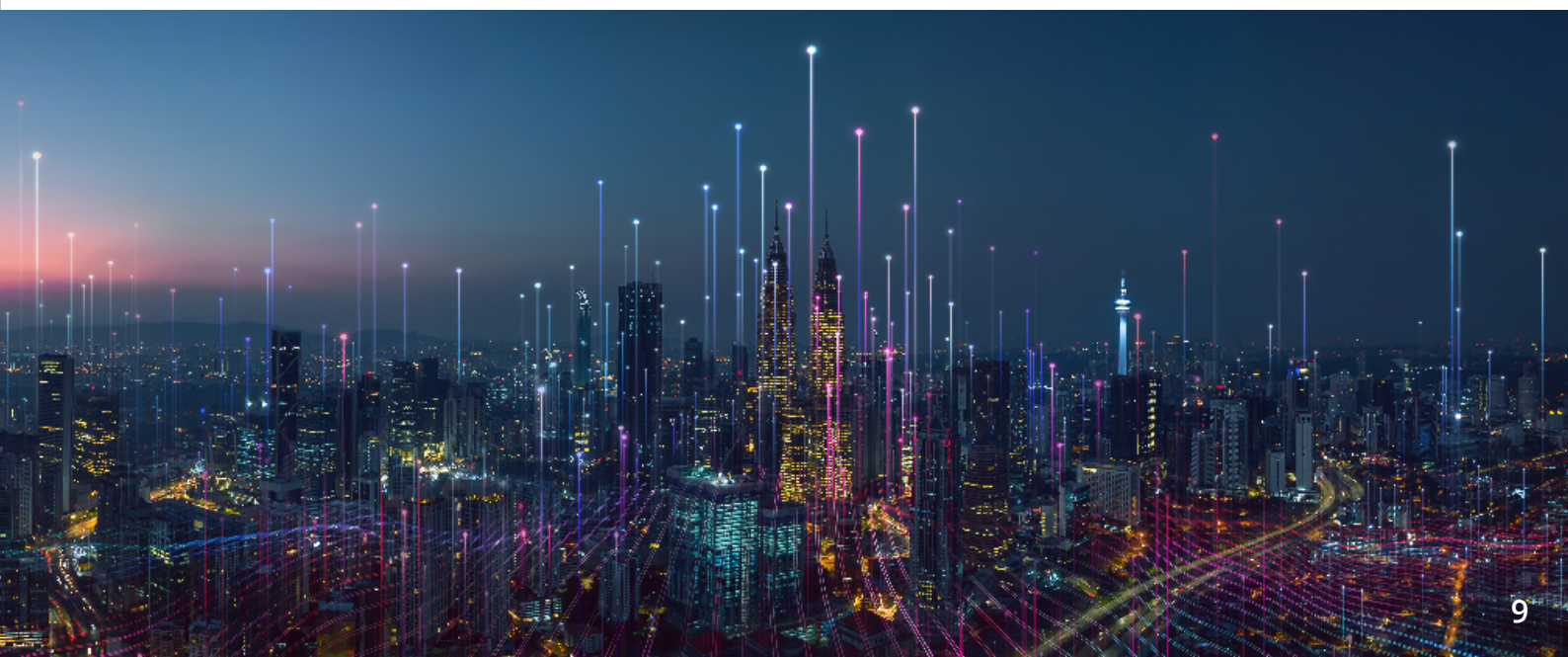
Un incidente con impacto significativo es aquel que ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada y ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables.

¿Cuál es el flujo de notificación propuesto?

Las entidades afectadas por un incidente con impacto significativo deberán notificar, sin demora indebida, al CSIRT o, en su defecto, a la autoridad competente, en un plazo de 24 horas desde que se haya tenido constancia del incidente, 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. Ante esta situación, en un plazo de 24 horas tras esta notificación de alerta temprana, el CSIRT o autoridad competente ofrecerán orientación o asesoramiento operativo sobre la aplicación de posibles medidas paliativas.

Pasadas 72 horas desde la detección del incidente, las entidades deberán actualizar el estado del incidente, exponiendo una evaluación inicial del incidente significativo en el que se incluye su gravedad e impacto, así como indicadores de compromiso siempre que estén disponibles.

Por último, a más tardar un mes después de la notificación del incidente, las entidades deberán presentar un informe final que recoja una descripción detallada del mismo, incluyendo su gravedad e impacto, el tipo de amenaza o causa principal que probablemente haya desencadenado el incidente, las medidas paliativas aplicadas y en curso y, cuando proceda, las repercusiones transfronterizas del incidente. Es importante considerar que, en el caso de que el incidente siga en curso en el momento de la presentación del informe final, los Estados miembro velarán por que 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 se haya gestionado el incidente.



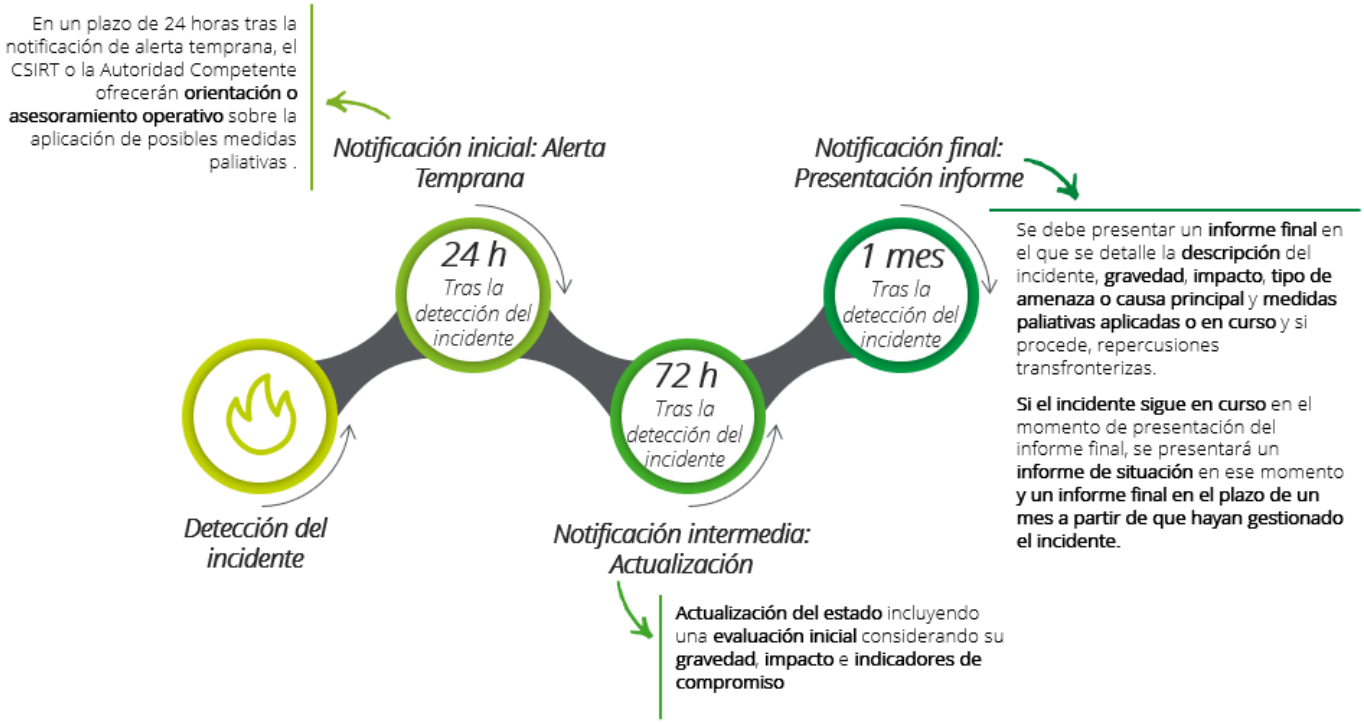


Ilustración 2 - Periodos de notificación de incidentes con impacto significativo

¿Cuáles serán las **funciones y competencias** de las **autoridades competentes** de cada Estado miembro?

Los artículos 32 y 33 están relacionados con las medidas de supervisión y ejecución de las entidades esenciales e importantes respectivamente, siendo estas medidas comunes en ambos casos. La diferencia es que, para las entidades esenciales, las medidas de supervisión se aplicarán de forma proactiva por parte de las autoridades competentes mientras que, para las entidades importantes, se aplicarán a posteriori, es decir, cuando se proporcionen pruebas o indicios del incumplimiento de las obligaciones establecidas de la Directiva NIS 2.

A continuación, se muestran las funciones de supervisión, y las principales competencias, de las autoridades competentes:

Funciones de supervisión de las autoridades competentes

Inspecciones in situ y supervisión a distancia
Auditorías de seguridad o ad-hoc[3]
Análisis de seguridad basados en criterios de evaluación del riesgo objetivo
Solicitudes de información necesarias para evaluar las medidas de gestión de riesgos de ciberseguridad
Solicitud de acceso a datos, documentación e información
Solicitudes de pruebas de la aplicación de las políticas de ciberseguridad

Tabla 1 - Funciones de supervisión de las autoridades competentes

Principales competencias de las autoridades competentes

Imponer multas administrativas a los Órganos de Dirección
Suspender temporalmente una parte o la totalidad de los servicios o actividades prestadas por una entidad esencial
Prohibir temporalmente a cualquier persona de la dirección, a nivel de director general o representante legal de la compañía, ejercer las funciones de dirección[4]

Tabla 2 - Principales competencias de las autoridades competentes

3 *Los costes de la auditoría serán sufragados por la entidad auditada salvo que la autoridad competente decida lo contrario.*

4 *Las suspensiones o prohibiciones temporales impuestas se aplicarán hasta que la entidad afectada adopte las medidas necesarias para subsanar las deficiencias o cumplir los requisitos de la Autoridad Competente.*

¿Cómo será el **régimen sancionador** en los Estados miembro?

De acuerdo con los artículos 34 y 36, los Estados miembro tendrán la posibilidad de imponer sanciones administrativas a las entidades que incumplan con los requisitos de la Directiva NIS 2, en especial los requisitos establecidos en los artículos 21 y 23, relativos a las medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación respectivamente.

Las sanciones deberán ser efectivas, proporcionales y disuasorias teniendo en cuenta las circunstancias en cada caso particular. A la hora de realizar la transposición y establecer el régimen sancionador los Estados miembro tomarán como referencia las siguientes cuantías en función del tipo de entidad:

- Para las entidades esenciales, las sanciones podrán ser, optándose por la de mayor cuantía, de hasta:
  - 10.000.000 €.
  - Máximo de un 2% del volumen de negocio anual total a nivel mundial del ejercicio financiero anterior.
- Para las entidades importantes, las sanciones podrán ser, optándose por la de mayor cuantía, de hasta:
  - 7.000.000 €.
  - Máximo de un 1.4% del volumen de negocio anual total a nivel mundial del ejercicio financiero anterior.

Los Estados miembro tendrán como fecha límite el 17 de enero de 2025 para comunicar el régimen de sanciones aplicables por incumplimiento a la Comisión Europea.

¿Cuáles serán los **próximos pasos**?

A fecha de 17 de enero de 2023, ha comenzado el periodo de transposición de la Directiva para los Estados miembro de la UE a su legislación nacional. Este plazo finalizará, a más tardar, el 17 de octubre de 2024, momento en el cual ya se deberán haber completado las labores de adaptación y publicación de las transposiciones.

De la misma forma, con fecha límite de 17 de enero de 2025, los Estados miembro deberán haber comunicado el régimen sancionador aplicable por incumplimiento de la presente Directiva a la Comisión Europea.

En este periodo de tiempo, los Estados miembro establecerán qué entidades se consideran esenciales e importantes teniendo en cuenta su legislación nacional, el detalle sobre las medidas de gestión de riesgos de ciberseguridad que estas deberán cumplir y las obligaciones en cuanto a notificación de incidentes.

Además, los Estados miembro tendrán el 17 de abril de 2025 como fecha límite para la elaboración de las listas de entidades esenciales e importantes.
Es por todo esto que las entidades deben tener en cuenta la actualización de la presente Directiva NIS 2 para poder adecuarse durante los próximos meses, tanto aquellas a las que ya les aplicaba la regulación anterior como las nuevas a las que les aplicará.

Además, deberán estar atentas a la actualización de las leyes actuales a nivel nacional a medida que vayan adecuándose a esta nueva Directiva, lo que permitirá aclarar las dudas principales que pueden haber quedado pendientes actualmente.

Finalmente, esta normativa no debe considerarse aislada, sino vinculada a otras regulaciones a nivel europeo que permiten dibujar la estrategia de seguridad de la UE. Entre ellas, se encuentran la propia Estrategia de Ciberseguridad Europea, el Reglamento DORA, la Directiva CER, el Reglamento sobre la Ciberseguridad y sus esquemas de certificación, o el futuro Reglamento para la Ciberresiliencia. Todas estas regulaciones tienen como objetivo elevar el nivel de resiliencia de la Unión para hacer frente a las amenazas crecientes y cada vez más complejas.

Deloitte.