Directiva NIS2
Guía Esencial para Empresas

Descubre en este Ebook una guía comprensible sobre la Directiva NIS2, su impacto en las empresas y las obligaciones que introduce en materia de seguridad de la información.

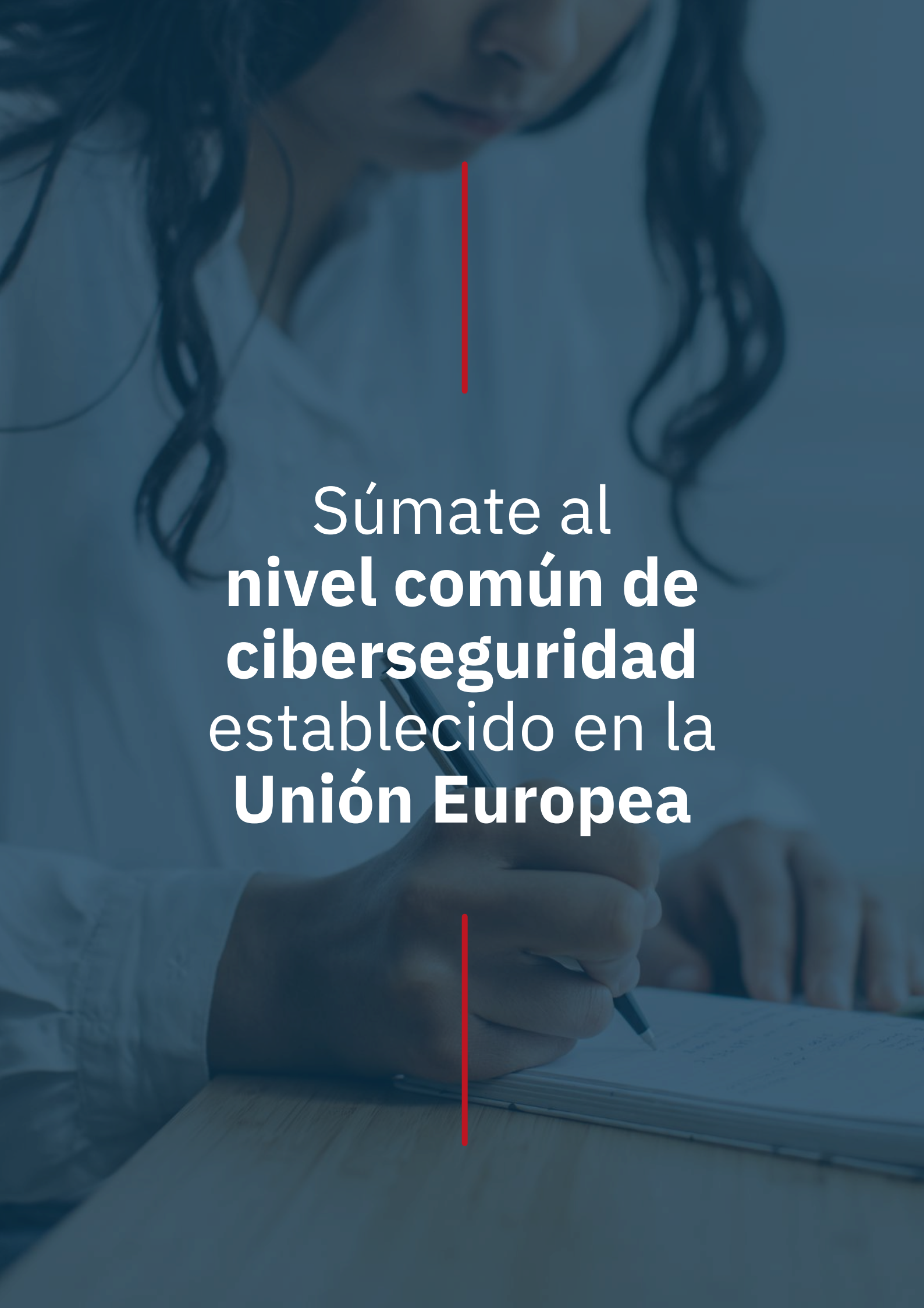
Leer más >>

ingertec

Sobre nosotros

Grupo Ingertec es una consultora de ámbito nacional e internacional, especializada en **servicios de cumplimiento normativo y seguridad de la información**.

Nuestros consultores de TI están especializados en la **aplicación de medidas de ciberseguridad obligatorias exigidas por la Directiva NIS2**.



Súmate al
nivel común de ciberseguridad
establecido en la
Unión Europea

¿Qué es la **Directiva NIS2**?

Directiva (UE) 2022/2555, también conocida como NIS2, es una **normativa europea** que establece nuevas **reglas sobre la seguridad de redes y sistemas de información** para **mejorar la ciberseguridad** dentro de la Unión Europea.

Aprobada en diciembre de 2022, esta normativa **actualiza la primera Directiva NIS** de 2016, ampliando su **ámbito de aplicación y reforzando las medidas de seguridad obligatorias** para las organizaciones de diversos sectores críticos.

OBJETIVO

El objetivo de la Directiva NIS2 es **asegurar un alto nivel de ciberseguridad en sectores clave y garantizar la resistencia de las infraestructuras críticas ante ciberataques**.

Todo ello, estandarizando y eliminando divergencias en materia de ciberseguridad entre todos los estados miembros.

Para ello se establecen:

- **Obligaciones de ciberseguridad para los Estados Miembros.**
- **Obligaciones en la toma de medidas para la gestión de riesgos de ciberseguridad de entidades.**
- **Obligaciones de notificación para las entidades.**
- **Obligaciones relativas al intercambio de información sobre seguridad.**
- **Obligaciones de supervisión y ejecución de los estados.**

Empresas afectadas por NIS2

Las empresas se verán afectadas por la Directiva NIS2 siempre que cumplan estos 3 criterios:

UBICACIÓN	Empresas que **ofrecen sus servicios o desarrollan su actividad** en cualquier país miembro de la **Unión Europea**.
TAMAÑO	• **Medianas empresas**: entre 50 y 250 personas trabajadoras 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. • **Grandes empresas**: más de 250 personas trabajadoras 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.
SECTOR	Se aplica a 18 sectores los cuales divide entre **sectores de alta criticidad** y otros **sectores críticos**.

Dentro de estas empresas afectadas se consideran **entidades esenciales** todas las grandes empresas de los sectores de alta criticidad del anexo I de la Directiva (UE) 2022/2555. Además, también se considerarán entidades esenciales:

- Los prestadores cualificados de servicios de confianza y registros de nombres de dominio de primer nivel y los proveedores de servicios de DNS, independientemente de su tamaño.
- Los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles para el público, dentro de las medianas empresas.
- Las entidades identificadas como críticas con arreglo a la Directiva (UE) 2022/2557 que ha de trasponerse a la legislación nacional en las mismas fechas que la NIS2, independientemente de su tamaño.
- Los operadores de servicios esenciales de conformidad con la Directiva (UE) 2016/1148 o el derecho nacional designados por el Estado miembro.

Por otro lado, se consideran **entidades importantes** todas aquellas empresas mencionadas en los anexos I o II de la Directiva (UE) 2022/2555 que no puedan considerarse entidades esenciales.

Un Estado miembro puede identificar a una entidad, **independientemente de su tamaño**, como esencial o importante cuando:

- La entidad es el único proveedor en un Estado miembro de un servicio esencial para el mantenimiento de actividades sociales o económicas críticas.
- Una perturbación del servicio prestado por la entidad pudiera tener repercusiones significativas sobre la seguridad pública, el orden público o la salud pública.
- Una perturbación del servicio prestado por la entidad pudiera inducir riesgos sistémicos significativos, en particular para los sectores en los que tal perturbación podría tener repercusiones de carácter transfronterizo.
- La entidad sea crítica a la luz de su importancia específica a nivel nacional o regional para el sector o tipo de servicio en concreto o para otros sectores interdependientes en el Estado miembro.

Los Estados miembros deben elaborar **antes del 17/04/2025** una **lista de entidades esenciales e importantes**, incluyendo en ella las entidades que prestan servicio de registro de nombres de dominios. Esta lista se deberá **actualizar periódicamente**, al menos cada 2 años y podrá establecer **mecanismos nacionales de autorregistro**.

¿TU EMPRESA HA DE CUMPLIR CON EL NIS2?

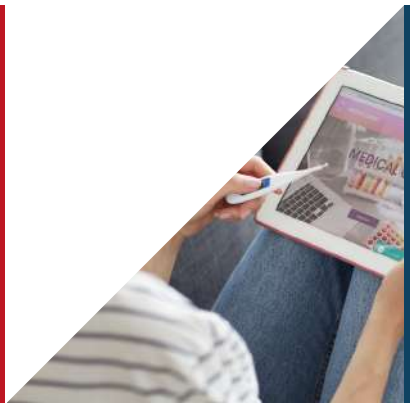
Para saber si tu organización está obligada a cumplir con esta normativa y tomar las medidas adecuadas, hemos preparado un formulario rápido y sencillo.

Tras rellenarlo, nuestro equipo de consultores lo revisará y contactará contigo.

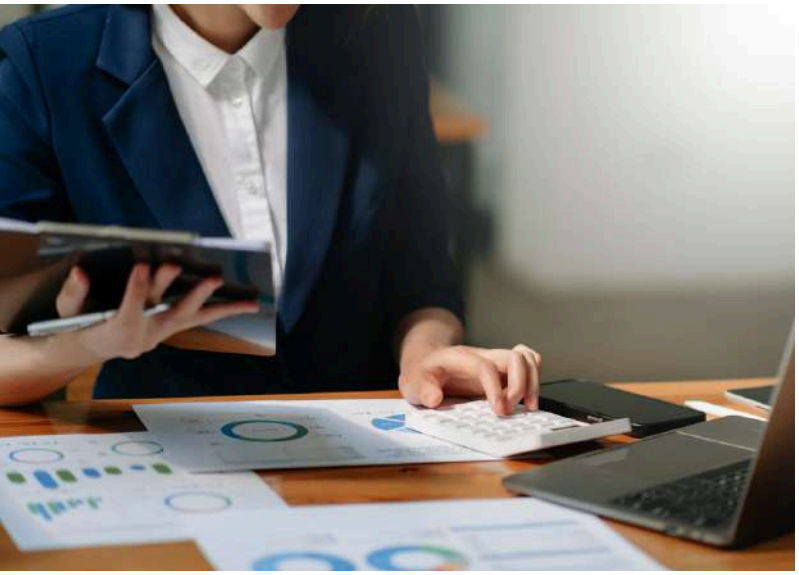
Rellenar el Formulario

Independientemente del tamaño de la empresa la Directiva NIS 2 **aplicará a las organizaciones que presten los siguientes servicios**:

- 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.

Organismos **vinculados**

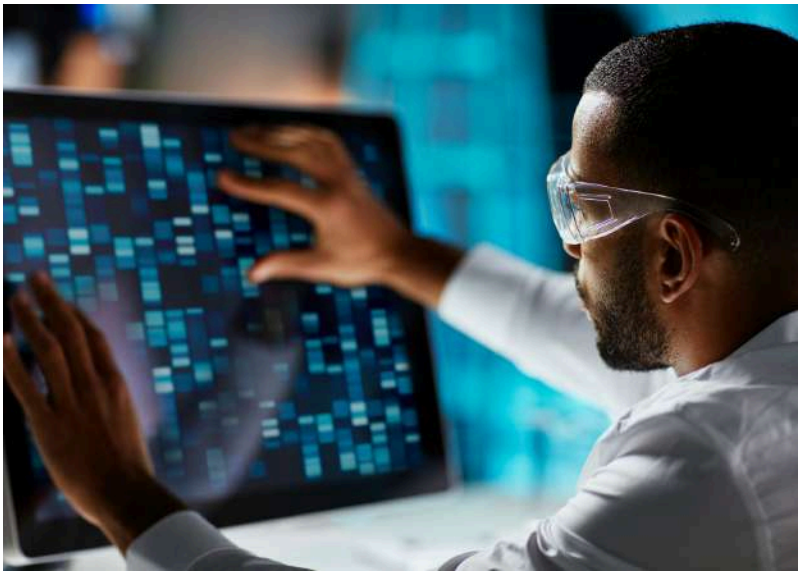


AUTORIDADES COMPETENTES

Realizarán inspecciones, análisis de seguridad o auditorías hacia las empresas interesadas en la Directiva.

CSIRT

Se trata de los equipos de respuesta a incidentes de seguridad informática, quienes prestarán asistencia a las entidades esenciales y afectadas ante cualquier incidente.



RED DE CSIRTS

Formado por representantes de los CSIRTs y el Equipo de Respuesta a Emergencias Informáticas de las instituciones, órganos y organismos de la Unión (CERT-EU), para intercambiar información de incidentes, ciberamenazas y otras cosas de interés.

PUNTO DE CONTACTO ÚNICO

Asegurará 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, para 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.

EU-CYCLONE

Red europea de organizaciones de enlace para la crisis de ciberseguridad (EU-CyCLONe), formada por la Autoridades de Gestión de Crisis de Ciberseguridad de los Estados miembro y la Comisión, para respaldar la gestión coordinada de los incidentes y crisis de ciberseguridad a gran escala en caso de ciberincidentes.

Multas por incumplimiento

La cuantía de las sanciones económicas varia si la empresa es considerada como entidad esencial o importante:

Un máximo de 10.000.000 euros o hasta el 2% del volumen de negocios total anual a escala mundial de la empresa a la que pertenezca la **entidad esencial** en el ejercicio precedente, optándose por la de mayor cuantía.

Un máximo de 7.000.000 euros o el 1,4% del volumen de negocios total anual a nivel mundial de la empresa a la que pertenece la **entidad importante** en el ejercicio precedente, optándose por la de mayor cuantía.

Relación con **ISO 27001** y **Esquema Nacional de Seguridad**

ISO 27001

La Directiva NIS2 **no exige la certificación de la empresa en ISO 27001** de Seguridad de la Información, ni el seguimiento de sus políticas y controles.

Sin embargo, menciona la serie ISO/IEC 27000 como **una forma de abordar el riesgo basándose en las mejores prácticas de gestión de riesgos de ciberseguridad**.

De hecho, ISO 27001 proporciona un **marco excelente para cumplir con la gestión de riesgos de ciberseguridad** requerida en esta Directiva.

ENS

El Centro Criptológico Nacional (CCN) ha publicado la *"Guía CCN-STIC 892. Perfil de Cumplimiento Específico"* para organizaciones en el ámbito de aplicación de la Directiva NIS2.

El objeto de este documento es **mostrar el perfil que se ha desarrollado para dar respuesta a las disposiciones de la directiva europea** por parte de aquellas organizaciones que se encuentran en el ámbito de aplicación del Esquema Nacional de Seguridad (ENS).

Estructura de NIS2

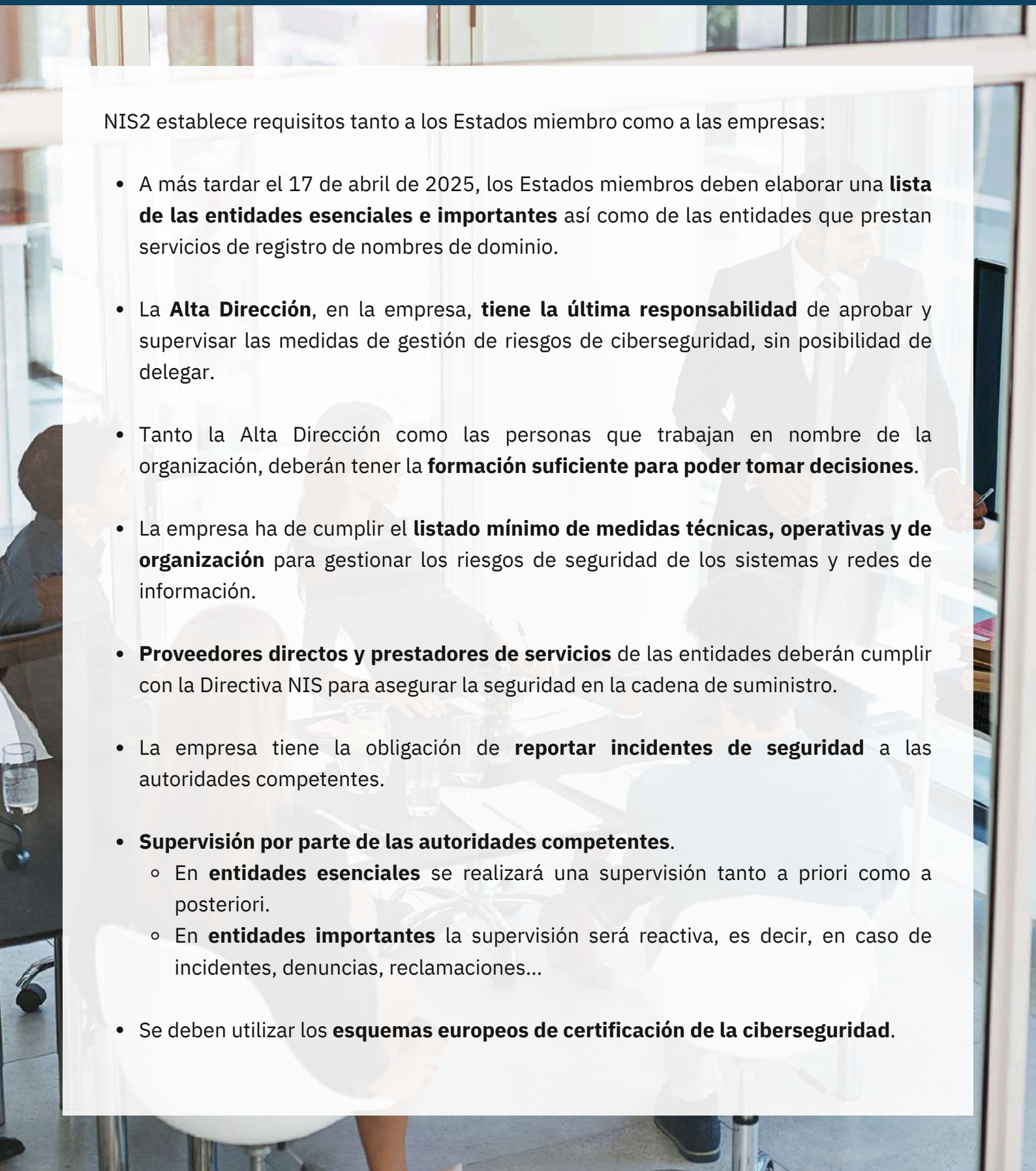
NIS 2 está estructurada en 46 artículos, sin embargo los más importantes se encuentran dentro del ***Capítulo IV "Medidas para la Gestión de Riesgos de Ciberseguridad y Obligaciones de Notificación"***.

Este capítulo define cuáles son los plazos, mecanismos y organismos vinculantes, entre otros, para la notificación en caso de incidentes tanto en para las entidades esenciales como las importantes. En él se concentran los siguientes artículos:

Artículo 20. Gobernanza.
Artículo 21. Medidas para la gestión de riesgos de ciberseguridad.
Artículo 22. Evaluaciones coordinadas de los riesgos de seguridad de las cadenas de suministro críticas a escala de la Unión.
Artículo 23. Obligaciones de notificación.
Artículo 24. Utilización de esquemas europeos de certificación de la ciberseguridad. (certificaciones no son obligatorias)
Artículo 25. Normalización.

El resto de capítulos especifican las obligaciones de los Estados Miembros respecto de las acciones de coordinación, registro de entidades, evaluación del cumplimiento, etc.

Requisitos del NIS2



NIS2 establece requisitos tanto a los Estados miembro como a las empresas:

- A más tardar el 17 de abril de 2025, los Estados miembros deben elaborar una **lista de las entidades esenciales e importantes** así como de las entidades que prestan servicios de registro de nombres de dominio.

- La **Alta Dirección**, en la empresa, **tiene la última responsabilidad** de aprobar y supervisar las medidas de gestión de riesgos de ciberseguridad, sin posibilidad de delegar.

- Tanto la Alta Dirección como las personas que trabajan en nombre de la organización, deberán tener la **formación suficiente para poder tomar decisiones**.

- La empresa ha de cumplir el **listado mínimo de medidas técnicas, operativas y de organización** para gestionar los riesgos de seguridad de los sistemas y redes de información.

- **Proveedores directos y prestadores de servicios** de las entidades deberán cumplir con la Directiva NIS para asegurar la seguridad en la cadena de suministro.

- La empresa tiene la obligación de **reportar incidentes de seguridad** a las autoridades competentes.

- **Supervisión por parte de las autoridades competentes**.
  - En **entidades esenciales** se realizará una supervisión tanto a priori como a posteriori.
  - En **entidades importantes** la supervisión será reactiva, es decir, en caso de incidentes, denuncias, reclamaciones...

- Se deben utilizar los **esquemas europeos de certificación de la ciberseguridad**.

Listado mínimo de medidas técnicas, operativas y de organización

Las medidas exigidas, indicadas como mínimas, serán proporcionales a los riesgos y al tamaño de las entidades. Éstas son:

01. Las políticas de seguridad de los sistemas de información y análisis de riesgos.
02. La gestión de incidentes.
03. La continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis.
04. La seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos.

Las entidades han de tener en cuenta:

- **Las vulnerabilidades específicas de cada proveedor y prestador de servicios directo.**
- **La calidad general de los productos y servicios prestados.**
- **Las prácticas en materia de ciberseguridad de sus proveedores y prestadores de servicios, incluidos sus procedimientos de desarrollo seguro.**

05. La seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información, incluida la gestión y divulgación de las vulnerabilidades.
06. Las políticas y los procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad.
07. Las prácticas básicas de ciberhigiene y formación en ciberseguridad.
08. Las políticas y procedimientos relativos a la utilización de criptografía y, en su caso, de cifrado.
09. La seguridad de los recursos humanos, las políticas de control de acceso y la gestión de activos.
10. El uso de soluciones de autenticación multifactorial o de autenticación continua, comunicaciones de voz, vídeo y texto seguras y sistemas seguros de comunicaciones de emergencia en la entidad, cuando proceda.

A más tardar el **17 de octubre de 2024**, la Comisión deberá adoptar actos de ejecución por los que se establezcan los **requisitos técnicos y metodológicos de las medidas detalladas anteriormente**.

La Comisión intercambiará asesoramiento y colaborará con el Grupo de Cooperación y la ENISA, por lo que reflejará un gran nivel de seguridad.

Comienza el
proceso de implementación de medidas de seguridad
obligatorias
según la
Directiva NIS2

¡Cuenta con
Grupo Ingertec!

Contacta con nosotros

900 897 931

www.ingertec.com

info@ingertec.com