



Directiva NIS2

Guía práctica



01

Titulares

01 Titulares



17 de octubre de 2024

Directiva traspasada obligatoriamente a los países miembros de la UE.



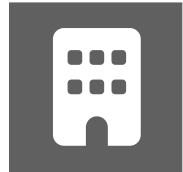
18 sectores directamente impactados

Diversos sectores se ven afectados, influyendo en la cadena de valor ya que los proveedores de estos sectores también están bajo la obligación de cumplimiento.



Empresas medianas y grandes

La normativa se aplica a empresas con más de 50 empleados y una facturación superior a 10 millones de euros.



Pequeñas empresas en sectores críticos

Las pequeñas empresas también pueden verse afectadas por la NIS2 si están en un sector crítico o son el único proveedor de un servicio esencial.



Cadena de suministro

Para que las empresas cumplan con la NIS2, es esencial que todas las empresas en su cadena de suministro también cumplan y que el ecosistema esté bajo control.

02

Sectores críticos

02 Sectores críticos

Primer eje

Energía	Banca	Mercados financieros	Salud	Transporte
Infraestructuras digitales	Agua potable	Aguas residuales	Administración pública	Gestión de servicios TIC
Investigación	Industria química	Alimentación	Servicios postales	Proveedores digitales
Fabricación	Gestión de residuos			

02 Sectores críticos

Primer eje



¿Si mi función está considerada como crítica y soy una pyme o micropyme, me afecta?



Si tu función es esencial y tiene un impacto significativo en terceros, estarías bajo las obligaciones del marco de la NIS2.

Por ejemplo, una pyme que ofrezca gestión de servicios de IT, servidores de dominios, productos en la nube B2B o servicios B2B que afecten de manera considerable a otras empresas.



03

Tamaño empresa

03 Tamaño empresa

Segundo eje

Mediana empresa



Gran empresa



03 Tamaño empresa


Segundo eje



A cualquier empresa que cumpla estos límites le afecta, sin importar el sector.



Más de 25,000 empresas, únicamente por su tamaño, ya están sujetas a las obligaciones de la NIS2.



Las empresas medianas y grandes colaboran con muchas empresas más pequeñas, las cuales deben evaluar y gestionar los riesgos cibernéticos para cumplir con la normativa.

04

Cadena de suministro

04 Cadena de suministro

Tercer eje



Se considera cadena de suministro a aquellas empresas que trabajen con las directamente afectadas por la NIS2.



Las empresas afectadas por la NIS2 tienen la obligación de mantener una relación sólida, trasladando controles y obligaciones a toda su cadena de proveedores.

A partir de ahora, un proveedor de Mercadona, Correos o Caixabank deberá asumir las responsabilidades de ciberseguridad que le indiquen estas empresas.



05

¿Me afecta directa o indirectamente?

05 ¿Me afecta directa o indirectamente?

Tercer eje

¿Cómo sé si me afecta la NIS2?



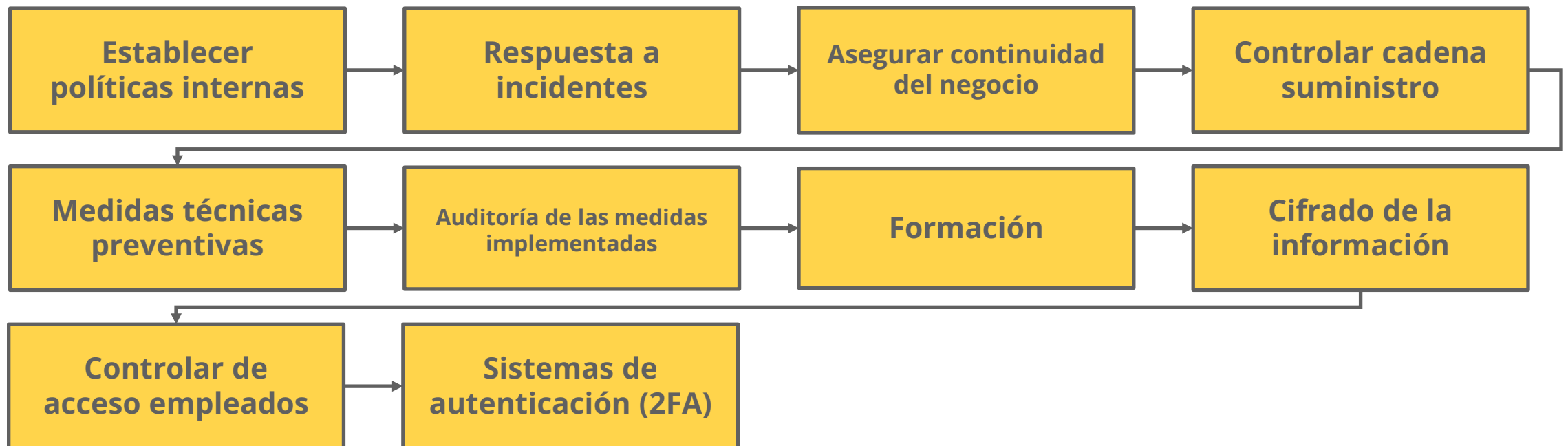
06

¿Qué obligaciones tengo?

06 ¿Qué obligaciones tengo?



Líneas a implementar obligatoriamente en mi empresa afectada por NIS2.



07

Detalles

07 Detalles

Artículo 21.2 a	Artículo 21.2 b	Artículo 21.2 c	Artículo 21.2 d	Artículo 21.2 e
Gestión de riesgos y política de seguridad <ul style="list-style-type: none">• Marco de gobierno de la ciberseguridad.• Roles y responsabilidades.• Postura de ciberseguridad.• Medidas para mitigar los riesgos.	Gestión de Incidentes <ul style="list-style-type: none">• Detección, notificación y respuesta.• Planes y procedimientos.	Continuidad de negocio <ul style="list-style-type: none">• Desarrollo de planes (crisis, continuidad, contingencias) que aseguren en caso de incidente.• Realizar formación y simulacros de continuidad de negocio.	Seguridad cadena <ul style="list-style-type: none">• Evaluar riesgos de ciberseguridad en la cadena de suministro.• Medidas de mitigación.• Evaluar riesgos e impactos en la cadena de suministro.	Adquisición, desarrollo y mantenimiento de sistemas y redes <ul style="list-style-type: none">• Escaneo de vulnerabilidades y test de penetración regulares.• Medidas de mitigación de vulnerabilidades.• Ciberhigiene y formaciones frecuentes.
Artículo 21.2 f	Artículo 21.2 g	Artículo 21.2 h	Artículo 21.2 i	Artículo 21.2 j
Eficacia de las medidas <ul style="list-style-type: none">• Políticas y procedimientos de evaluación de medidas.• Auditorías y pruebas frecuentes.	Concienciación y formación <ul style="list-style-type: none">• Programa integral de formación y concienciación.• Formación continua.• Formación y testeo aplicados para reforzar lo aprendido.	Cifrado <ul style="list-style-type: none">• Utilizar cifrado para preservar integridad, confidencialidad y autenticidad de los datos.• Implementar prácticas de gestión de claves.• Pruebas y formación sobre cifrado.	RRHH, Control de acceso, gestión de activos <ul style="list-style-type: none">• Procedimientos para empleados con acceso a información sensible.• Formación y pruebas sobre control de acceso.• Evaluar las medidas sobre el inventario de activos.	Autenticación y transferencia de información <ul style="list-style-type: none">• Implementar 2FA o autenticación continua para voz, vídeo y comunicaciones.



Las medidas a implementar deben ser proporcionales al tamaño y la actividad de la empresa. No se requiere el mismo nivel de cifrado para una entidad financiera que para una empresa del sector alimentario.

08

Sanciones

08 Sanciones



¿Habrá un marco sancionador en caso de incumplimientos?



Sí, existe un marco sancionador recomendado por la directiva de la UE, que es bastante estricto y se adapta a las leyes nacionales de cada país. **Novedad:** hay **responsabilidades penales** para los órganos de administración y directivos en casos de incumplimientos graves.

Máximo sanciones

10M

Hasta

2%

Volumen de negocio

7M

Hasta

1,4%

Volumen de negocio

Empresas Esenciales

Empresas Importantes



Estamos aquí para ayudarte a cumplir con la NIS2 y proteger tu negocio. Contacta con nosotros

Contactar

Más información

www.pistacero.es