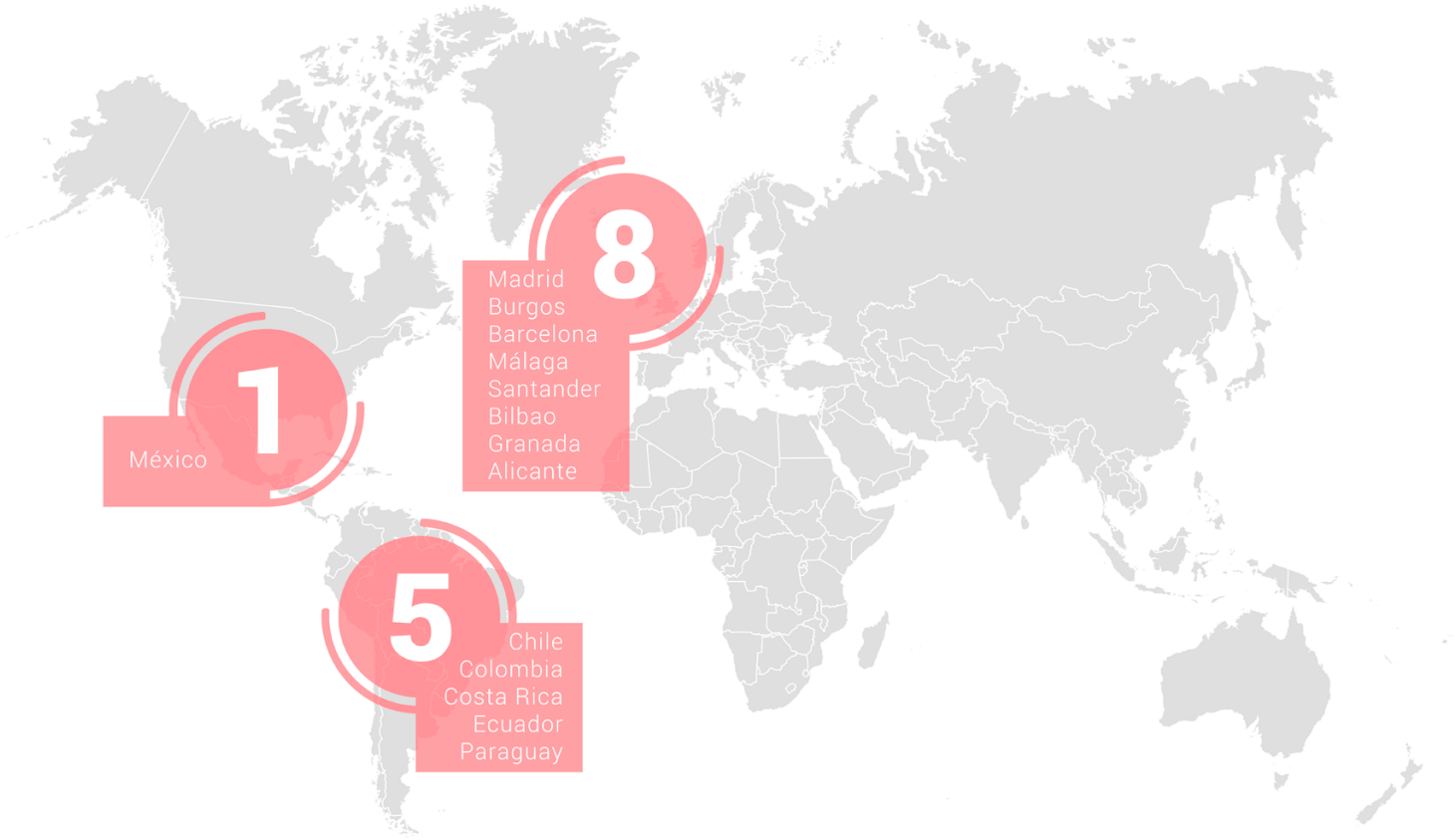
GrupoACMS
CONSULTORES

GRUPO ACMS Consultores

Directiva NIS2: Qué es y para qué sirve



AENOR
ER
Empresa Registrada
ISO 9001

(ER-0772/2013)

Alcance ISO 9001

Diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión de la calidad, medioambiental, de la prevención de riesgos laborales, protección de datos, seguridad alimentaria y de la calidad y competencia técnica en laboratorios clínicos.

Alcance ISO 27001

Los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión y el diseño, desarrollo y comercialización de software de sistemas de gestión de acuerdo con la declaración de aplicabilidad vigente.

AENOR
ER
Seguridad Información
ISO/IEC 27001

(SI-0021/2020)

Publicado el 04/04/2025

Actualización de la Directiva NIS 2

La Directiva NIS 2, recientemente actualizada, es una normativa de la Unión Europea que refuerza la seguridad de redes y sistemas de información en sectores críticos como la energía, transporte, salud y finanzas.

Su propósito es mejorar la capacidad de los Estados miembros y organizaciones para prevenir, gestionar y responder a ciberataques.

Principales diferencias entre NIS y NIS2

A continuación, te explicamos las principales diferencias y ventajas de esta actualización de manera sencilla y comprensible.

Principales Diferencias entre NIS y NIS2

- Ampliación del ámbito de aplicación:

NIS: Se centraba en operadores de servicios esenciales y proveedores de servicios digitales.

NIS2: Amplía su alcance a más sectores, incluyendo energía, transporte, salud, finanzas e infraestructura digital. Además, introduce las categorías de ?entidades esenciales? y ?entidades importantes? para una clasificación más clara. Esto significa que más organizaciones estarán obligadas a cumplir con los requisitos de ciberseguridad, asegurando una protección más amplia y uniforme.

- Requisitos de Seguridad más estrictos:

NIS: Tenía requisitos de seguridad menos específicos y dejaba mucho a la interpretación de los Estados miembros.

NIS2: Establece medidas de seguridad más rigurosas y uniformes, como la autenticación multifactor y la encriptación de datos. Estas medidas buscan asegurar que todas las organizaciones adopten prácticas de seguridad robustas, reduciendo así el riesgo de ciberataques exitosos.

- Notificación de incidentes:

NIS: Requería la notificación de incidentes significativos, pero con plazos y detalles menos definidos.

NIS2: Impone plazos estrictos para la notificación de incidentes: una advertencia inicial en 24 horas, un informe completo en 72 horas y un informe detallado en un mes. Esto permite una respuesta más rápida y coordinada ante incidentes de seguridad, minimizando el impacto potencial.

- Responsabilidad corporativa:

NIS: No especificaba claramente la responsabilidad de la alta dirección.

NIS2: La alta dirección debe aprobar y supervisar las medidas de ciberseguridad, siendo responsable de cualquier incumplimiento. Esto asegura que la ciberseguridad sea una prioridad a nivel ejecutivo, promoviendo una cultura de seguridad en toda la organización.

Beneficios que aporta la Directiva NIS2

Mayor Resiliencia y Seguridad:

La NIS2 proporciona un marco más robusto para la gestión de riesgos y la respuesta a incidentes, lo que ayuda a las organizaciones a estar mejor preparadas frente a ciberataques. Esto incluye la implementación de políticas y procedimientos que mejoran la capacidad de detectar, responder y recuperarse de incidentes de seguridad.

Uniformidad y Claridad:

Al clasificar las organizaciones de manera uniforme y establecer requisitos claros, se reduce la ambigüedad y se asegura una aplicación más consistente en toda la UE. Esto facilita el cumplimiento normativo y asegura que todas las organizaciones, independientemente de su ubicación, sigan los mismos estándares de seguridad.

Protección de Infraestructuras Críticas:

La inclusión de más sectores críticos bajo la NIS2 garantiza que servicios esenciales para la sociedad y la economía estén mejor protegidos. Esto es crucial para mantener la continuidad de servicios vitales como la energía, el transporte y la salud, que son fundamentales para el bienestar de la sociedad.

Mejora de la Cooperación Internacional:

La NIS2 fomenta una mayor cooperación entre los Estados miembros de la UE, lo que es crucial para enfrentar amenazas cibernéticas transfronterizas. Esta colaboración incluye el intercambio de información y mejores prácticas, así como la coordinación en la respuesta a incidentes de gran escala.

Sanciones Disuasorias:

La introducción de sanciones más severas por incumplimiento asegura que las organizaciones tomen en serio sus obligaciones de ciberseguridad. Las sanciones pueden incluir multas significativas, lo que incentiva a las organizaciones a cumplir con los requisitos y a invertir en medidas de seguridad adecuadas.

¿A quién aplica?

La nueva versión amplía los sectores cubiertos, introduce sanciones más estrictas y fomenta una cooperación más fuerte entre países.

Esta actualización es clave para proteger las infraestructuras esenciales frente a amenazas crecientes en el entorno digital.

A continuación, indicamos a quien aplica:

- Operadores de Servicios Esenciales (OES):

- Empresas e instituciones que operan en sectores críticos como:

- Energía (electricidad, gas, petróleo)

- Transporte (aéreo, ferroviario, marítimo, carreteras)

- Agua (abastecimiento y distribución)

- Salud (hospitales, clínicas)

- Infraestructuras financieras (bancos, mercados financieros)

- Infraestructuras digitales (proveedores de servicios de internet, centros de datos)

- Proveedores de Servicios Digitales (DSP). Empresas que ofrecen servicios digitales, como: servicios de computación en la nube, motores de búsqueda en línea, mercados en línea, plataformas de redes sociales.

- Pequeñas y medianas empresas que, aunque no forman parte de sectores críticos, pueden tener un impacto significativo en la seguridad cibernética si sus sistemas fueran comprometidos.

¿Cuáles son las exclusiones que contempla?

No aplica a microempresas (empresas con menos de 10 empleados o con un volumen de negocio anual inferior a 2 millones de euros). También están excluidas las instituciones gubernamentales que operan en sectores de defensa, seguridad nacional, seguridad pública y justicia.

Somos consultores en Seguridad de la Información

Como hemos visto, la Directiva NIS2 representa un paso adelante en la protección de las redes y sistemas de información en la UE.

Una vez que actualice la directiva, su empresa no solo cumplirá con la normativa, sino que también fortalecerá su capacidad para resistir y recuperarse de ciberataques, protegiendo así sus operaciones y la confianza de sus clientes.

En Grupo ACMS nos avalan más de 25 años de experiencia. Si necesita asesoramiento, consúltenos sin compromiso y le guiaremos en la mejor dirección.

Enlaces de interés:

INCIBE

Directiva NIS2 (Directiva (UE) 2022/2555 - BOE

Nos definimos como una compañía consultora independiente cuyo objetivo fundamental es suministrar servicios de consultoría en las áreas de Gestión empresarial, que representen para el cliente una solución excelente, que satisfaga sus necesidades explícitas o implícitas, tenga en cuenta las regulaciones y normas aplicables, y cumpla los objetivos de plazo y coste establecidos.

Madrid

C/ Campezo 3, nave 5 28022 Madrid

Tfno.: (+34) 91 375 06 80

Burgos

Centro de Empresas, 73 09007 Burgos

Tfno.: (+34) 947 041 645

Barcelona

C/ Plaça Universitat 3 08007 Barcelona

Tfno.: (+34) 93 013 19 49

Málaga

C/ Alejandro Dumas 17 29004 Málaga

Tfno.: (+34) 95 113 69 04

México

José González Varela 15 14700 Tlalpan

Tfno.: (+52) 5513 39 96 22

www.grupoacms.com
informacion@grupoacms.com