Directiva NIS 2

Contenido

1 ¿A qué sectores aplica la NIS2?

La UE considera que deben cumplir con esta normativa las empresas y organizaciones con más de 50 empleados y una facturación superior a 10 millones de euros.

Estos son los sectores a los que aplica, categorizados en tres grupos:

1.1 Críticos:

- **Energía:** empresas de suministro y distribución de electricidad, gas y petróleo.
- **Transporte:** operadores de transporte aéreo, ferroviario, marítimo y por carretera.
- **Banca y finanzas:** instituciones bancarias, proveedores de servicios y mercados financieros.
- **Salud:** hospitales, clínicas y otros proveedores de servicios de salud esenciales.
- **Agua potable y aguas residuales:** empresas que gestionan el suministro de agua potable y el tratamiento de aguas residuales.
- **Infraestructura digital:** proveedores de servicios de infraestructura digital, como centros de datos y redes de telecomunicaciones.
- **Administración pública:** entidades gubernamentales y organismos públicos que gestionan servicios esenciales.

1.2 Importantes:

- **Alimentación:** empresas de producción y distribución de alimentos.
- **Manufactura y producción industrial:** fabricantes de productos esenciales, incluyendo químicos y productos farmacéuticos.
- **Servicios postales y logísticos:** operadores de servicios postales y de logística esenciales.
- **Espacio:** proveedores de servicios relacionados con el espacio y la exploración espacial.
- **Tecnologías de la información y comunicación (TIC):** empresas que proporcionan servicios TIC, incluyendo proveedores de servicios de internet y empresas de software.

1.3 Proveedores de servicios digitales:

- **Servicios Cloud:** proveedores de servicios de computación en la nube y almacenamiento en la nube.
- **Mercados en línea:** plataformas de comercio electrónico que facilitan la venta de bienes y servicios.
- **Motores de búsqueda en línea:** empresas que operan motores de búsqueda en línea.

2 ¿Qué medidas hay que aplicar para cumplir con la NIS2?

Las empresas deben prepararse revisando sus políticas y procedimientos de ciberseguridad actuales, evaluando su conformidad con los requisitos de la NIS2 e implementando las mejoras necesarias. Las principales medidas incluyen:

2.1 Gestión de riesgos cibernéticos:

- **Evaluación de riesgos:** realizar evaluaciones periódicas de riesgos para identificar y mitigar posibles vulnerabilidades.
- **Planificación de contingencias:** desarrollar planes de contingencia y recuperación ante desastres para asegurar la continuidad operativa.

2.2 Higiene cibernética:

- **Actualización de sistemas:** mantener los sistemas y software actualizados para protegerlos contra vulnerabilidades conocidas.
- **Contraseñas seguras:** implementar políticas de contraseñas seguras y autenticación multifactor para todos los accesos críticos.

2.3 Respuesta a incidentes:

- **Protocolos de respuesta:** establecer procedimientos claros y detallados para la detección, respuesta y recuperación de incidentes de seguridad.
- **Notificación de incidentes:** informar a las autoridades competentes de cualquier incidente significativo en un plazo de 24 horas.

2.4 Seguridad en la cadena de suministro:

- **Evaluación de proveedores:** evaluar y monitorear la seguridad de los proveedores y socios comerciales.
- **Acuerdos de seguridad:** incluir cláusulas de seguridad en los contratos con proveedores para asegurar el cumplimiento de estándares de ciberseguridad.

2.5 Formación y concienciación:

- **Capacitación continua:** ofrecer programas de formación y concienciación en ciberseguridad para todos los empleados.
- **Simulacros:** realizar ejercicios regulares para evaluar y mejorar la preparación ante incidentes.

2.6 Implementación de medidas técnicas y organizativas:

- **Protección de datos:** implementar medidas técnicas como cifrado y control de acceso para proteger los datos sensibles.
- **Monitoreo y auditoría:** establecer sistemas de monitoreo continuo y realizar auditorías de seguridad regulares para detectar y corregir anomalías.