CYBASQUE

Directiva NIS2 en las TICs

¿A quién le afecta?

Independientemente de su tamaño

- Registros de nombres de dominio de primer nivel
- Proveedores de servicios de sistema de nombres de dominio
- Prestadores de servicios de confianza
- Proveedores de redes públicas de comunicaciones electrónicas
- Proveedores de servicios de comunicaciones electrónicas disponibles para el público

50 o más empleados y más de 10 millones de euros de volumen de negocios anual o balance general anual

- Proveedores de servicios de computación en nube
- Proveedores de servicios de centro de datos
- Proveedores de redes de distribución de contenidos
- Proveedores de servicios gestionados
- Proveedores de servicios de seguridad gestionados
- Proveedores de mercados en línea
- Proveedores de motores de búsqueda en línea
- Proveedores de plataformas de servicios de redes sociales

Proveedores de empresas obligadas por NIS 2

NIS2 obliga a todas las empresas de los sectores afectados (energía, transporte, banca, sanitario, fabricación, etc.) a que realicen una adecuada gestión de su cadena de suministro desde el punto de vista de la seguridad. En consecuencia, si una empresa TIC no obligada conforme a los puntos anteriores presta servicios a empresas obligadas por NIS2, es altamente probable que sus clientes le exijan el cumplimiento de las medidas de seguridad establecidas por NIS2

Las multas puede llegar hasta los 10M€ o el 2% del volumen de negocio anual en entidades esenciales o hasta 7M€ o el 1,4% del volumen de negocio anual para entidades importantes.

Retos y comparación

Retos

Uno de los retos más complejos es el de la cadena de suministro, ya que exige asegurar no solo la propia infraestructura, sino también la de terceros clave. Por otra parte y mencionando al anteproyecto de ley: "Las **medidas** de **seguridad** tomarán como base las contempladas tanto en el **Esquema Nacional de Seguridad** como en **normas técnicas europeas** e **internacionales equivalentes**; garantizarán un **nivel adecuado de seguridad** de las **redes** y **sistemas de información**, así como de su **entorno físico**, adecuado en relación con los riesgos planteados".

Puntos en común entre NIS2 y el Esquema Nacional de Seguridad Alto

Gestión de riesgos
Medidas técnicas y organizativas
Gobernanza y responsabilidad
Gestión y notificación de incidentes
Formación y concienciación
Continuidad de negocio
Colaboración y cooperación

Importancia en el sector TIC

Cómo norma general las empresas dedicadas a este sector suelen estar a la última en tecnología y con una seguridad bastante robusta. Si no están en el ámbito de aplicación es probable que sean parte de la cadena de suministro de alguna empresa afectada, por lo que tendrán que hacer implementaciones.

Por otro lado, aquellas compañías que deban cumplir con la directiva y no lo hagan, correrán el riesgo de ser multados.

Cumplir con el ENS o la ISO27001 no supone automaticamente cumplir con todos los requisitos de la NIS2

El anteproyecto de ley habla de la creación de un Centro Nacional de Ciberseguridad (CNC) entidad que se encargará del cumplimiento de las obligaciones de ciberseguridad por parte de las entidades esenciales e importantes.

Desde Europa se le da mucha importancia a la notificación de incidentes, con un total de tres avisos por cada incidente. También señalarán al equipo directivo como responsable de los ataque.

Implementaciones técnicas

Aunque de momento no hay una ley oficial ni sus implementaciones sean las finales, esta es una lista de los puntos a tener en cuenta:

1. Gestión de riesgos y seguridad en la cadena de suministro
2. Protección de activos críticos
3. Monitorización y detección de amenazas
4. Gestión de incidentes y notificación
5. Continuidad de negocio y recuperación
6. Seguridad en el desarrollo y adquisición de sistemas
7. Formación y concienciación
8. Gobernanza y responsabilidades
9. Actuación y gestión de vulnerabilidades
10. Colaboración y cooperación

CYBASQUE