GUÍA DE APLICACIÓN DEL NIS 2

Resumen

Introducción

La Directiva NIS 2 (Seguridad de las Redes y de la Información) representa un gran avance en la legislación europea sobre ciberseguridad, al imponer obligaciones específicas a una amplia gama de organizaciones consideradas esenciales o importantes para el funcionamiento de la sociedad y la economía. Su aplicación exige un planteamiento metódico para garantizar su cumplimiento, reducir los ciberriesgos y proteger las infraestructuras críticas.

Esta guía se ha creado para ayudar a las empresas a adaptarse a la norma NIS 2, centrándose en las diferencias entre las organizaciones que ya cuentan con la certificación ISO/IEC 27001 y las que no. El objetivo es proporcionar un camino claro y práctico para cada contexto.

Parte 1: Empresa con certificación ISO 27001

Las organizaciones que ya cuentan con la certificación ISO 27001 tienen una ventaja significativa, ya que muchas de las prácticas exigidas por la NIS 2 están alineadas con los requisitos de la norma ISO/IEC 27001. Sin embargo, se necesita un enfoque estratégico para colmar las lagunas e incorporar obligaciones reglamentarias adicionales.

Ventajas iniciales para las empresas certificadas :

- Estructura establecida: la presencia de un Sistema de Gestión de la Seguridad de la Información (SGSI) bien definido facilita la adaptación a los requisitos específicos de la SRI 2.
- Cumplimiento parcial: ya existen procesos como el análisis de riesgos, la gestión de vulnerabilidades y la supervisión continua.
- Cultura de seguridad: la certificación implica una mayor concienciación interna sobre la seguridad informática.

Principales medidas de adaptación :

1. Cartografía de los requisitos adicionales de la norma NIS 2: identificación de las diferencias con los requisitos de la norma ISO 27001, como la gestión de la cadena de suministro y la presentación de informes a los organismos competentes.
2. Compromiso de las partes interesadas: reforzar la colaboración con proveedores, socios y autoridades para cumplir los requisitos de información y resistencia de la NIS 2.
3. Actualización de la documentación: integración de los procesos existentes con los nuevos requisitos, como la gestión de crisis y los planes de contingencia.
4. Prueba de conformidad: comparar el estado actual del SGSI con el marco NIS 2 para identificar y resolver cualquier laguna.