REQUERIMIENTOS DE LA DIRECTIVA NIS2

Directiva UE 2022/2555
Ley de Coordinación y Gobernanza de la Ciberseguridad

¿Qué exige a las **entidades afectadas**?

Las organizaciones dentro del ámbito de NIS 2 deben cumplir una serie de **obligaciones de ciberseguridad** destinadas a reducir riesgos y proteger sus servicios frente a amenazas e incidentes.

Según los **artículos 20-23** de la directiva NIS2, los requerimientos clave son los siguientes:

Gobernanza y responsabilidades

Establecer funciones claras en materia de ciberseguridad y asegurar la implicación de la alta dirección.

Medidas técnicas y organizativas

Adoptar controles adecuados para prevenir, detectar y responder a incidentes.

Análisis y gestión de riesgos

Identificar y evaluar los riesgos, vulnerabilidades y dependencias que puedan afectar a la seguridad.

Continuidad de negocio

Establecer planes y procedimientos para garantizar la prestación de servicios ante incidentes.

Formación y sensibilización

Establecer programas de formación y concienciación para todo el personal.

Seguridad en la cadena de suministro

Evaluar y controlar los riesgos derivados de proveedores y terceros.

Gestión de políticas de acceso y cifrado

Aplicar controles de acceso, segmentación de redes y cifrado de datos según riesgos.

Evaluación de las medidas

Desarrollar políticas y procedimientos para revisar si las medidas aplicadas funcionan correctamente.

Notificación de incidentes

Obligación de comunicar incidentes relevantes en un plazo máximo de 24 horas desde su detección.

CCN centro criptológico nacional

Puedes encontrar más información en:
https://www.ccn.cni.es
https://www.ccn-cert.cni.es