Cumplimiento legal

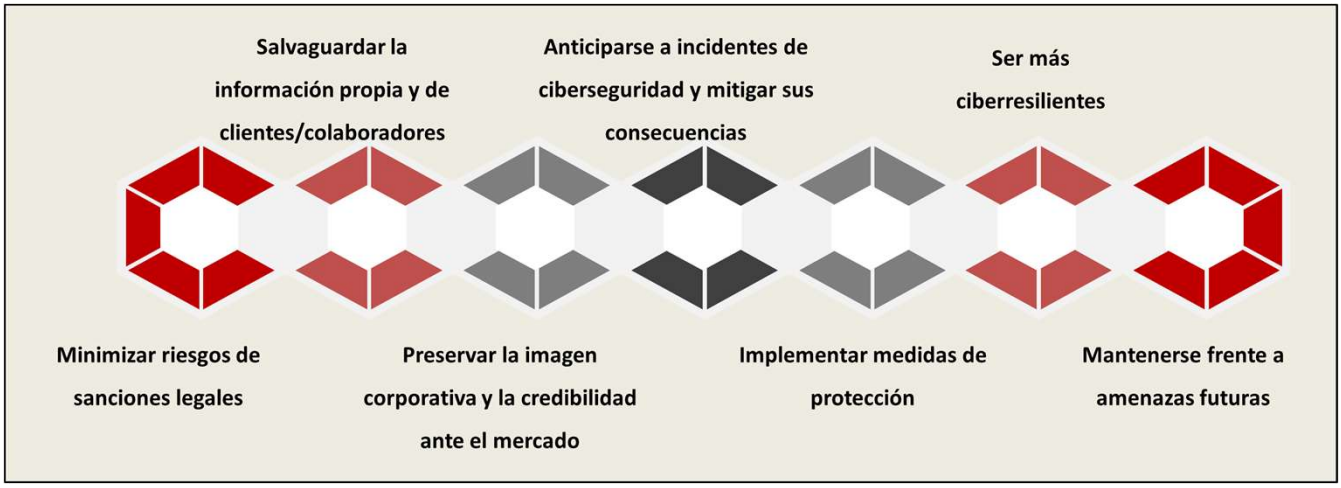
Consultoría en capacidades de Ciberseguridad

Descripción del Servicio

El cumplimiento legal en materia de ciberseguridad engloba las disposiciones legales y regulaciones que las organizaciones deben aplicar para resguardar sus sistemas, la información que manejan y sus canales de comunicación. Más allá de ser un requisito jurídico, constituye una estrategia esencial para reducir vulnerabilidades y fortalecer la confianza tanto de clientes como de aliados comerciales.

El cumplimiento normativo en ciberseguridad persigue **un doble propósito**:

- Proteger la información de la organización y de las personas vinculadas a ella
- Garantizar que las empresas actúan de manera responsable frente a los riesgos digitales



¿Por qué resulta clave cumplir con la normativa de ciberseguridad?

El incremento constante y la creciente sofisticación de las amenazas digitales hacen que respetar las regulaciones en materia de ciberseguridad sea una obligación estratégica para cualquier empresa. No se trata de una opción, sino de un requisito esencial para garantizar la protección y la continuidad del negocio.

Ignorar estas normas puede derivar en consecuencias críticas, como:

- **Multas y responsabilidades legales**: las compañías que incumplen la legislación vigente pueden enfrentarse a **sanciones económicas**, demandas judiciales o incluso a la suspensión de sus licencias.
- **Pérdida de confianza y reputación**: una brecha de seguridad puede **afectar gravemente la imagen corporativa** y provocar que los clientes dejen de confiar en la organización.
- **Impacto en la operativa**: las vulnerabilidades no atendidas pueden ocasionar **interrupciones en los sistemas**, pérdidas económicas y exposición de datos sensibles.

Tipos de Servicio

Adecuación normativa
Implementar de forma práctica medidas jurídicas, técnicas y organizativas en ciberseguridad, conforme a legislación como RGPD, NIS2, CRA y ENS.

Representación y defensa legal
Defender a la empresa frente a inspecciones o sanciones, mediante la preparación de documentación y pruebas de cumplimiento.

Diseño de políticas y procedimientos internos
Traducir las obligaciones legales en reglas internas claras, mediante la redacción de políticas de seguridad de la información adaptadas (ej. RGPD, NIS2).

Auditorías legales
Realizar la revisión documental, entrevistas con responsables de seguridad y legal, y análisis de procesos de gestión de incidentes y protección de datos.

Certificaciones necesarias

DPO (Delegado de Protección de Datos)
Garantiza el cumplimiento del GDPR, asesorando y supervisando la protección de datos personales en la organización.

NIS2 Implementer
Habilita la correcta aplicación de la Directiva NIS2, reforzando la ciberseguridad y resiliencia de entidades esenciales y críticas.

CISA (Certified Information Systems Auditor – ISACA)
Certifica la pericia en la auditoría, control, aseguramiento y seguridad de los sistemas de información empresariales.

Director de Seguridad Privada
Gestiona y lidera la seguridad integral, física y lógica, especialmente en entornos de infraestructuras críticas.

Normativas

NORMAS PRINCIPALES

Esquema Nacional de Seguridad (ENS)

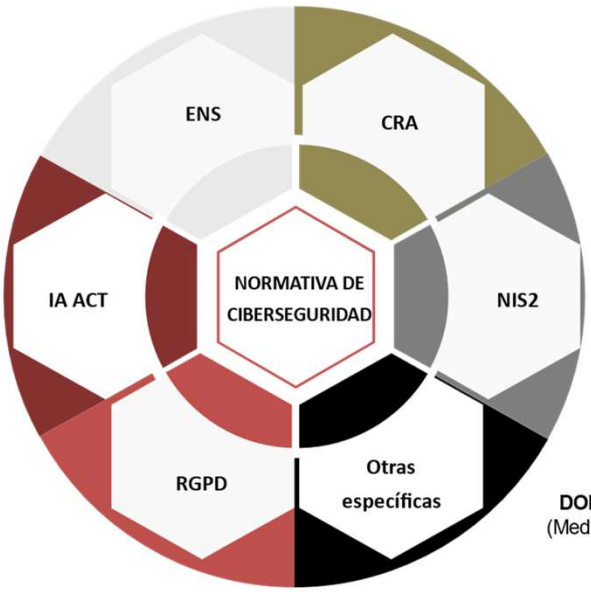
Regulación española (Real Decreto 311/2022) que establece principios y requisitos mínimos de seguridad para sistemas de información de las Administraciones Públicas y sus proveedores.

Artificial Intelligence Act

Aprobado en 2024, establece un marco legal para el desarrollo y uso de sistemas de inteligencia artificial en la UE, con enfoque en riesgos y transparencia.

Reglamento General de Protección de Datos (RGPD/GDPR)

Norma europea que regula la protección de datos personales y la privacidad en la UE.



Cyber Resilience Act – CRA

Aprobada desde 2024. Busca garantizar que los productos con componentes digitales cumplan requisitos mínimos de seguridad durante todo su ciclo de vida.

Directiva (UE) 2022/2555, conocida como NIS2

Aprobada en 2022, y pendiente de trasposición en España, establece un marco común para reforzar la ciberseguridad en la UE, aplicando a los sectores críticos y exigiendo medidas de gestión de riesgos y notificación de incidentes con el objetivo de garantizar la continuidad y protección de servicios esenciales.

DORA, TISAX, UNECE R155, R156, MDR (Medicar Device resilience), **Infraestructuras críticas, etc.**

Gobierno de Navarra | Nafarroako Gobernua