POTENCIAL DIGITAL

CDTIC Centro Demostrador TIC

CIBERSEGURIDAD PARA UN FUTURO CONECTADO

PROTECCIÓN EN LA ERA DIGITAL

“Aspectos legales. Evita las Cibermultas millonarias en tu empresa”.

Eleazar García. Director

03/06/2025

TEGÕ legal

CDTIC Centro Demostrador TIC

JUNTA DE EXTREMADURA
Consejería de Economía, Empleo y Transformación Digital

Cofinanciado por la Unión Europea

¿Quién soy y por qué estoy aquí?

- Eleazar, abogado especializado en derecho tecnológico y ciberseguridad (Derecho, GAP, Máster Ejerc.)
- Fundador **TEGÕ Legal**, despacho boutique para empresas que no quieren sorpresas legales.
- Ayudo a traducir leyes y normas técnicas al idioma empresa.
- Auditor Interno ISO27001 Certificado / Delegado de Protección de Datos.
- Profesor UEX 5 ediciones Curso de Derecho Tecnológico e Informática Forense DTIF.
- Mentor en legal y ciberseguridad (Extremadura OF, Circular FAB, USAL, MentorDay, PreIncubadora, IRIA).
- Cibercooperante en INCIBE.

TEGÕ legal

Protección de Datos

Registrar Marca

Delegado de Protección de Datos

Mercantil, M&A y Contratos

Comercio Electrónico

Contratos tecnológicos

¿Qué es la ciberseguridad... legalmente hablando?

- No se trata solo de firewalls y antivirus.
- Implica el **cumplimiento normativo** que protege derechos, datos, operaciones.
- Concepto clave: **seguridad de la información** (confidencialidad, integridad y disponibilidad).
- Base jurídica: **principio de responsabilidad proactiva**.

Principales normas aplicables

- **Constitución Española**
- **Normativa de seguridad nacional:** *Ley de Seguridad Nacional; Esquema Nacional de Seguridad, Ley CNI, Ley de Secretos Empresariales, Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, etc.*
- **Infraestructuras críticas:** *Ley de medidas para la protección de infraestructuras críticas, Reglamento, etc.*
- **Normativa de seguridad:** *Estructura orgánica y funciones de la Dirección General de la Policía, Ley Orgánica de protección de la seguridad ciudadana, Ley de Seguridad Privada y su Reglamento, etc.*
- **Equipo de respuesta a incidentes de seguridad:** *Ley de servicios de la sociedad de la información y de comercio electrónico; Centro Criptológico Nacional; Organización Fuerzas Armadas, etc.*

Principales normas aplicables

- **Telecomunicaciones y usuarios:** *LSSICE; Ley General de Telecomunicaciones; Ley servicios electrónicos de confianza; ENS de redes y servicios 5G; Ley conservación de datos de comunicaciones electrónicas y redes públicas.*
- **Ciberdelincuencia:** *Código Penal; Ley Enjuiciamiento Criminal; Ley responsabilidad penal de los menores.*
- **Protección de datos:** *RGPD; LOPDGDD.*
- **Relaciones con la Administración:** *Ley del Procedimiento Administrativo Común de las AAPP; Ley Régimen Jurídico del Sector Público.*

Principales normas aplicables

- Reglamento General de Protección de Datos (**RGPD**)
- Ley Orgánica de Protección de Datos y garantía de los derechos digitales (**LOPDGDD**)
- Ley de Servicios de la Sociedad de la Información (**LSSI**)
- Esquema Nacional de Seguridad (**ENS**)
- Directiva Network and Information Security (**NIS**)
- Normas ISO 27001, 27002… (**no obligatorias pero muy recomendables**)

Principales normas aplicables

Reglamento General de Protección de Datos (**RGPD**)

- **Definición:** Reglamento de la Unión Europea para la protección de datos personales.
- **Objetivo:** Proteger la privacidad de los ciudadanos de la UE y armonizar las leyes de privacidad de datos en Europa.
- Requisitos clave:
  - **Base legal** (contrato, consentimiento, etc.): Necesidad de obtener base legal para procesar datos.
  - **Derecho al acceso**: Los usuarios pueden solicitar acceso a sus datos personales.
  - **Derecho al olvido**: Los usuarios pueden solicitar la eliminación de sus datos personales.
  - **Notificación de brechas**: Obligación de notificar a las autoridades y a los usuarios sobre las violaciones de datos en un plazo de 72 horas.

Principales normas aplicables

Ley Orgánica de Protección de Datos y garantía de los derechos digitales (**LOPDGDD**)

- **Definición**: Ley española que adapta el RGPD al ordenamiento jurídico español y garantiza derechos digitales.

- **Objetivo**: Proteger los datos personales y los derechos digitales de los ciudadanos en España.

- Requisitos Clave:
  - Derecho a la intimidad en uso de dispositivos digitales: Protección de la privacidad en el ámbito laboral.
  - Derecho a la desconexión digital: Garantía del tiempo de descanso fuera del horario laboral.
  - Protección de menores: Normas específicas para el tratamiento de datos de menores de edad.

Principales normas aplicables

Directiva Network and Information Security (**NIS**)

- **Definición**: Directiva de la UE que establece medidas para garantizar un alto nivel común de seguridad de las redes y sistemas de información en la UE.

- **Objetivo**: Mejorar la ciberseguridad en toda la Unión Europea mediante la cooperación entre estados miembros y la implementación de medidas de seguridad adecuadas.

- **Requisitos clave**:
  - Operadores de Servicios Esenciales (OSE): Identificación y protección de infraestructuras críticas.
  - Proveedores de Servicios Digitales (DSP): Obligación de adoptar medidas de seguridad y notificar incidentes.
  - Cooperación: Establecimiento de CSIRTs (Equipos de Respuesta a Incidentes de Seguridad Informática) y una red de cooperación entre ellos.

Principales normas aplicables

Directiva Network and Information Security (**NIS**)

- **Directiva NIS 2**: Diciembre 2022 (17/01/2023 comenzó transposición hasta 17/10/2024. Máximo el 17/01/2025 España debió comunicar el régimen sancionador (7-10 mill. € o 1,4 - 2%) y 17/04/2025 lista de entidades esenciales) **Retraso**, aún en *Anteproyecto de la Ley de Coordinación y Gobernanza de la Ciberseguridad* en enero de 2025, no se desvía de la Directiva.

- **Aplicación**:
  - Sectores de Alta Criticidad (11 sectores): energía, banca, infraestructuras de mercados financieros, sector sanitario, transporte, infraestructura digital, aguas potables, aguas residuales, administración pública (con exclusión del poder judicial, parlamentos y bancos centrales), gestión de servicios TIC (Business to Business) y espacio.
  - Otros sectores críticos (7 sectores): investigación, química, alimentación, servicios postales, proveedores digitales, fabricación y gestión de residuos.
  - Empresas afectadas:
    - Mediana empresa: 50-250 empleados y 10-50 millones de euros de volumen negocio anual.
    - Gran empresa: +250 empleados y 50 millones de euros de volumen negocio anuales.
    - Indep. del tamaño: actividad crítica; único proveedor servicio esencial en un Estado, etc.

Obligaciones legales básicas

- **Analizar riesgos** y documentarlos.
- Implantar **medidas técnicas y organizativas adecuadas**.
- Disponer de un **procedimiento de gestión de incidentes**.
- Establecer **contratos con encargados del tratamiento**.
- Notificar brechas de seguridad (y no hacer el avestruz).
- Formar y concienciar a las personas empleadas.

¿Y si no cumplo?

Multas, sí. Pero no solo eso.

- Hasta **20 millones de euros** o el 4% de la facturación global.
- **Reclamaciones** de clientes, pérdida de reputación, responsabilidades civiles e incluso penales.
- **Ejemplos**:
  - Empresa multada por no cifrar datos de clientes tras una brecha.
  - Personas empleadas compartiendo contraseñas en un Excel = brecha + sanción.

Casos reales en empresas (con nombres cambiados o no 😅)

- **"Tecnoconstrucciones S.L.":** multa de 60.000€ por no tener medidas tras pérdida de un pendrive.
- **"CloudLimpio":** SaaS que sufrió brecha y no notificó. Alguien lo denunció → multa + pérdida de clientes.
- **Pequeña tienda online:** usaban Google Forms para pedidos con datos de tarjeta. ¿Resultado? Sanción.

Casos reales en empresas (con nombres cambiados o no 😅)

Ciberataques en España en 2025, mes a mes

- Enero 2025: Ataque de phishing a universitarios en Baleares
- Enero 2025: Brecha de datos en la Guardia Civil y las Fuerzas Armadas
- Enero 2025: Telefónica sufre un ciberataque en su sistema de ticketing
- Febrero 2025: Filtración de datos personales en DKV
- Marzo 2025: Quedan expuestos datos de clientes de El Corte Inglés
- Marzo 2025: Ataque prorruso a webs de diputaciones y ayuntamientos en España
- Abril 2025: robo de los datos de las federaciones de autónomos ATA
- Abril 2025: La compañía Aigües de Mataró sufre un ciberataque
- Abril 2025: Ransomware dirigido al Ayuntamiento de Badajoz
- Mayo 2025: Dos informáticos acceden a los equipos de miembros del Senado

Claves para evitar sustos legales

- Hacer una **auditoría de riesgos legales y técnicos**.
- Diseñar e implantar **protocolos claros** (accesos, contraseñas, copias de seguridad, etc.).
- Redactar y aplicar políticas: privacidad, uso del correo, BYOD…
- **Formación periódica** para el personal.
- **Simulacros de brechas** y revisión de procedimientos..

Herramientas legales que toda empresa debería tener

- **Política de seguridad** de la información.
- **Contratos** con proveedores TIC con cláusulas de seguridad (RGPD, DORA, etc.).
- Registro de actividades de tratamiento.
- Protocolos internos de actuación ante incidentes.
- Plan de continuidad de negocio / recuperación ante desastres.

¿Qué puede hacer un abogado por ti?

- **Traducir** la ley al lenguaje de tu empresa.
- Diseñar tu "traje legal" en ciberseguridad.
- **Reaccionar** rápido ante incidentes legales o regulatorios.
- Prepararte para una **inspección** (o mejor, evitarla).

PREVENCIÓN

Conclusión

La ciberseguridad no es solo cosa del informático

- Es una cuestión estratégica y legal.
- Cuesta menos prevenir que remediar y pagar multas.
- Y si no sabes por dónde empezar… pide ayuda.

Contacto

¡Muchas gracias por tu asistencia y atención!

¿Hablamos?

- eleazar@tegolegal.es
- www.tegolegal.es
- 654 42 68 86

"No es paranoia si de verdad están intentando hackearte"