

CIBERSEGURIDAD

APLICADA A PYMES Y AUTÓNOMOS



Cumplimiento normativo y leyes sobre estafas, fraudes y riesgos sobre seguridad de la información.

Eleazar García. Experto en Derecho tecnológico y seguridad de la información.

TEGÖ



JUNTA DE EXTREMADURA



Transición de lo analógico a lo digital



- Era de la información (globalización).
- Trabajo vs. Conocimiento.
- Transformación digital.
- Situación pandémica (teletrabajo).



ExxonMobil

أرامكو السعودية
Saudi Aramco



Bank of America



2010



2020





Seguridad de la información

Conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

No confundir con seguridad informática que es menos amplia.

Información = **Activo más importante**



CIBERSEGURIDAD: un paso más en la evolución de la seguridad de la información.

Ahora el foco no está sólo en la información y su valor, también en la integridad de las personas (amenazas). Ejemplo claro, RGPD y derechos fundamentales.

La SEGURIDAD se construye con controles:

- Organizativos
- Procedimentales
- Técnicos
- Normativos // Compliance (Si no hay predisposición, ya habrá una norma)

Evaluar y gestionar el riesgo, seleccionando qué controles deben ser aplicados.

En esa evaluación de riesgos es CLAVE el **compliance**:

Identificación de las leyes, regulaciones y normas que se deben respetar y cumplir a lo largo de todas las fases del ciclo de vida del servicio, que incluye:

- Diseño
- Construcción
- Despliegue
- Mantenimiento
- Operación
- Retirada

Finalidad compliance: Gestión de los riesgos de cumplimiento, identificándolos e implementando las medidas y procedimientos necesarios para su prevención.

Por tanto, **Compliance en el ámbito de la información:**

Se pretende que la Entidad logre cumplir con las obligaciones legales, contractuales o éticas.

Políticas de compliance = Cultura de cumplimiento legal.

Política Compliance: Según Circular 1/2016 de la Fiscalía General del Estado es motivo de atenuante de responsabilidad penal (Conforme reforma CP 2015).

Últimos años, tendencia legislativa (nacional y europeo) en materia de seguridad y privacidad (importancia estratégica para UE, ayudas, etc.)

Entidades, balanza: POSITIVO / CRITERIO vs. RECELO / OBLIGACIONES



Responsabilidad de las entidades pueden proceder:

- Culpa in vigilando (omisión, negligencia)
- Culpa in eligendo (responsabilidad del empleador por error del empleado)
- Culpa organizativa

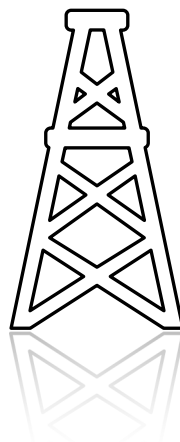
Importancia del plan de compliance y controles para su vigilancia y prevención (seguridad), podría atenuar o eximir responsabilidad penal.

Delitos con responsabilidad penal:

- **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos** (apoderarse de documentación, interceptar comunicaciones, etc.) Incluye secretos de empresa y daños a datos, programas o documentos electrónicos ajenos.
- **Delitos informáticos** (estafas mediante manipulación informática)
- **Delitos relacionados con el contenido** (pornografía de menores, discapacitadas)
- **Delitos relacionados con infracciones de la propiedad intelectual y derechos afines**

Esquema Nacional de Seguridad (ENS): Determina la política de seguridad en la utilización de medios electrónicos del Sector Público y sus proveedores tecnológicos del sector privado y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Ley de Protección de Infraestructuras Críticas (LPIC): Ley consecuencia de la mayor dependencia que la sociedad tiene del sistema de infraestructuras, que asegura el mantenimiento de los servicios esenciales (centrales energéticas, bancos, agua, transporte, etc.).



Directiva NIS de servicios esenciales y digitales: Pretende dar respuesta efectiva a los problemas de seguridad de las redes y sistemas de información. Planteamiento global en la UE que integra requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales.

La Ley de Gobernanza de Datos (DGA): Establece mecanismos sólidos para facilitar la reutilización de determinadas categorías de datos protegidos del Sector Público, aumentar la confianza en los servicios de intermediación de datos y fomentar el altruismo de datos en toda la Unión Europea.

Reglamento General de Protección de Datos (RGPD): Ante el tratamiento de datos personales por las Organizaciones existen una serie de obligaciones para respetar el derecho fundamental a la protección de datos de las personas titulares de los datos.

Obligaciones como: Mantener un RAT, Acuerdos de confidencialidad, Contratos de Encargo de Tratamiento, notificar las brechas de seguridad, medidas de seguridad que garanticen la confidencialidad (cifrado, control de accesos...), etc.

Sanciones económicas del 2% al 4% de la facturación anual o hasta 20 millones de euros



Leyes de Propiedad Intelectual e Industrial

Firma Electrónica: Reguladas mediante la Ley 6/2020 sobre determinados aspectos de los servicios electrónicos de confianza (Ley 59/2003 de Firma Electrónica derogada).

Comercio Electrónico (LSSI-CE): Regulado mediante la Ley de Servicios de la Información y de Comercio Electrónico. Esta Ley establece un régimen jurídico en lo referente a la prestación de servicios o contrataciones por vía electrónica.

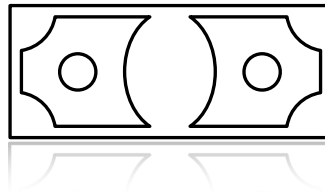
Telecomunicaciones (LGT): Empresas que ofrecen servicios de explotación de redes y/ o servicios de comunicaciones electrónicas se encuentran reguladas bajo la Ley General de Telecomunicaciones (alojamientos web, correo electrónico, servicios de telefónica, acceso a redes de datos, etc.).



Implantación del Payment Card Industry Data Security Standard (PCI- DSS): Estándar de seguridad impuesto por el PCI Security Standard Council. Establece un marco de pasos para empresas que realicen operaciones con tarjetas de crédito o débito.

Recoge las medidas de seguridad necesarias para tratar estos datos, así como también define políticas, diseño de software o procedimientos de seguridad con el fin de reducir fraudes o robos e incrementar la seguridad en el uso de estos dispositivos.

Sin importar que estos pagos se hagan de forma presencial u online (datáfonos, pasarelas, etc.).



Más allá de normativas nacionales, europeas e internacionales:

Normas de la serie ISO 27000 (Estándares)

Conjunto de buenas prácticas para la implantación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI) y que sirven como guía para implementar medidas y procedimientos para garantizar la seguridad de la información en la empresa.

En resumen:

- El compliance ayuda a mejorar la seguridad de las organizaciones (por incluir obligaciones derivadas de las normativas de seguridad).
- Identificar riesgos permite adoptar e incluir las medidas y procedimientos adecuados para prevenirlos o mitigar su impacto (proactividad).
- Clave medidas como: cifrado de datos, pruebas de pentesting, control de accesos, formación en ciberseguridad del personal, protocolo o política de protección de datos, la política de uso de dispositivos corporativos, teletrabajo, etc.
- Importancia de la Cultura del compliance y privacidad en la seguridad de la información de la empresa. Implicar a Dirección y Personal, especialmente, al departamento IT o encargados de la seguridad IT, responsables de aplicar el programa de cumplimiento normativo en esta área.

**¡MUCHAS GRACIAS
POR LA ASISTENCIA!**

**CIBERSEGURIDAD
APLICADA A PYMES Y AUTÓNOMOS**

