BLINDAJE DIGITAL

Protección de Datos y Ciberseguridad

Curso de Formación Interna • 30–45 min

RGPD / Ciberseguridad / Buenas Prácticas

La información es un activo vital — protegerla es nuestra responsabilidad compartida

Agenda del Curso

01

~10 min

El Marco Legal — RGPD

Los 6 principios del art. 5: licitud, minimización, exactitud, conservación, integridad

02

~10 min

Fundamentos de Ciberseguridad

Tríada CIA: Confidencialidad, Integridad y Disponibilidad con medidas técnicas

03

~10 min

Amenazas y Ataques

Phishing, Malware, Ingeniería Social, Fugas de datos — cómo reconocerlos

04

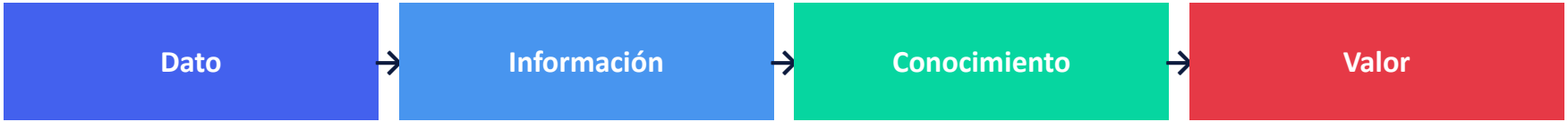
~10 min

Buenas Prácticas

Protección en entornos laborales y personales, externalización responsable

¿Por qué proteger la información?

La información es un activo vital para cualquier organización — y necesita ser protegida adecuadamente.



Velocidad

Los incidentes tecnológicos se propagan de forma instantánea a escala global.

Conexión mundial

Un mundo conectado crea vacíos jurisdiccionales y nuevas superficies de ataque.

Sin fronteras

Los ataques no entienden de fronteras; afectan a cualquier organización.

Falta de seguridad

Las medidas de protección se aplican aún de forma reactiva, tras el incidente.

PARTE 1

Reglamento General de Protección de Datos

El Marco Legal: RGPD

Los 6 principios del art. 5 que toda organización debe conocer y aplicar

¿Qué es el RGPD?

Reglamento (UE) 2016/679

En vigor desde mayo de 2018 en toda la UE. En España complementado por la LOPDGDD.

Aplica a cualquier organización

Que trate datos de personas físicas en la UE, independientemente de su tamaño o sector.

Derechos del ciudadano

Acceso, rectificación, supresión, portabilidad, limitación y oposición al tratamiento.

Multas: hasta 20M€ o 4% facturación

El incumplimiento puede acarrear sanciones millonarias y grave daño reputacional.

Los 6 Principios del RGPD — art. 5

1

Licitud, lealtad y transparencia

Tratamiento legal, leal y transparente

2

Limitación de la finalidad

Fines determinados, explícitos y legítimos

3

Minimización de datos

Adecuados, pertinentes y no excesivos

4

Exactitud

Exactos y actualizados; rectificar si no

5

Limitación del plazo

Solo el tiempo necesario para la finalidad

6

Integridad y confidencialidad

Seguridad apropiada: técnica y organizativa

Principio 1

Licitud, Lealtad y Transparencia

Base legal del tratamiento

Debe existir un fundamento jurídico válido: consentimiento, contrato, obligación legal, interés vital, público o legítimo.

Lealtad hacia el interesado

El tratamiento debe ser honesto, sin engañar ni perjudicar a las personas cuya información se trata.

Transparencia informativa

Informar de forma clara y accesible sobre qué datos se recogen, con qué fin y quién es el responsable.

Principios 2 y 3 — Finalidad y Minimización

2

Limitación de la Finalidad

Los datos se recogen con fines determinados, explícitos y legítimos.

Determinados: el fin debe estar definido antes de recoger los datos.

Explícitos: los interesados deben ser informados con precisión.

Legítimos: el fin debe estar amparado por la ley.

3

Minimización de Datos

Solo se tratan los datos estrictamente necesarios.

Adecuados: relevantes para la finalidad concreta.

Pertinentes: guardan relación directa con el propósito.

No excesivos: limitados a lo mínimo necesario.

Principios 4, 5 y 6 — Exactitud · Plazo · Integridad

4

Exactitud

Exactos y actualizados

Los datos deben mantenerse exactos. Si un dato es inexacto debe ser rectificado o suprimido sin dilación.

5

Limitación del Plazo

Solo el tiempo necesario

No conservar más tiempo del necesario. Pasado ese plazo: eliminación o anonimización sin excepción.

6

Integridad y Confidencialidad

Seguridad adecuada

Medidas técnicas y organizativas que garanticen la protección de los datos frente a accesos no autorizados.

RGPD → Ciberseguridad

El Principio 6 exige Integridad y Confidencialidad

¿Cómo se garantiza en la práctica?

Con medidas de Ciberseguridad: control de accesos, cifrado, monitorización, copias de seguridad y planes de respuesta a incidentes.

▼ **A continuación: los fundamentos técnicos de la Ciberseguridad** ▼

PARTE 2

Confidencialidad · Integridad · Disponibilidad

Fundamentos de Ciberseguridad

Los tres pilares sobre los que se construye toda medida de seguridad de la información

La Tríada CIA — Los tres pilares de la Seguridad

CONFIDENTIALITY

Confidencialidad

Solo el personal autorizado puede acceder a la información que le corresponde. Cada persona: solo lo que necesita.

INTEGRITY

Integridad

La información no ha sido modificada de forma no autorizada. Garantiza exactitud, credibilidad y confianza.

AVAILABILITY

Disponibilidad

Los sistemas y recursos están accesibles cuando los usuarios autorizados los necesitan. Sin interrupciones no autorizadas.

Confidencialidad — Solo para quien corresponde

Prevenir el acceso no autorizado. Cada usuario accede únicamente a los recursos necesarios.

Autenticación de usuarios

Contraseñas robustas + MFA. Identidad verificada antes de cualquier acceso.

Gestión de privilegios

Principio de mínimo privilegio: cada usuario solo puede leer/editar lo estrictamente necesario.

Cifrado y encriptación

La información resulta ilegible para usuarios no autorizados.

Integridad — Fidelidad y exactitud de la información

Prevenir modificaciones no autorizadas. Abarca información y origen: exactitud, credibilidad, confianza.

Monitorización del tráfico

Detectan intrusiones o comportamientos anómalos en la red en tiempo real.

Control de registros (logs)

Quién accede, cuándo y qué hace. Esencial para auditorías y detección de incidentes.

Control de cambios

Verificación de archivos mediante checksums/hashes para detectar modificaciones.

Disponibilidad — Acceso cuando se necesita

Prevenir interrupciones. De poco sirven la confidencialidad e integridad sin acceso a la información.

Acuerdos de nivel de servicio (SLA)

Garantizan porcentajes de uptime y tiempos de respuesta ante incidencias.

Balanceadores de carga

Distribuyen peticiones entre varios servidores para evitar caídas por sobrecarga.

Copias de seguridad y redundancia

Backups periódicos y sistemas alternativos garantizan continuidad.

PARTE 3

Phishing · Malware · Ingeniería Social · Fugas de datos

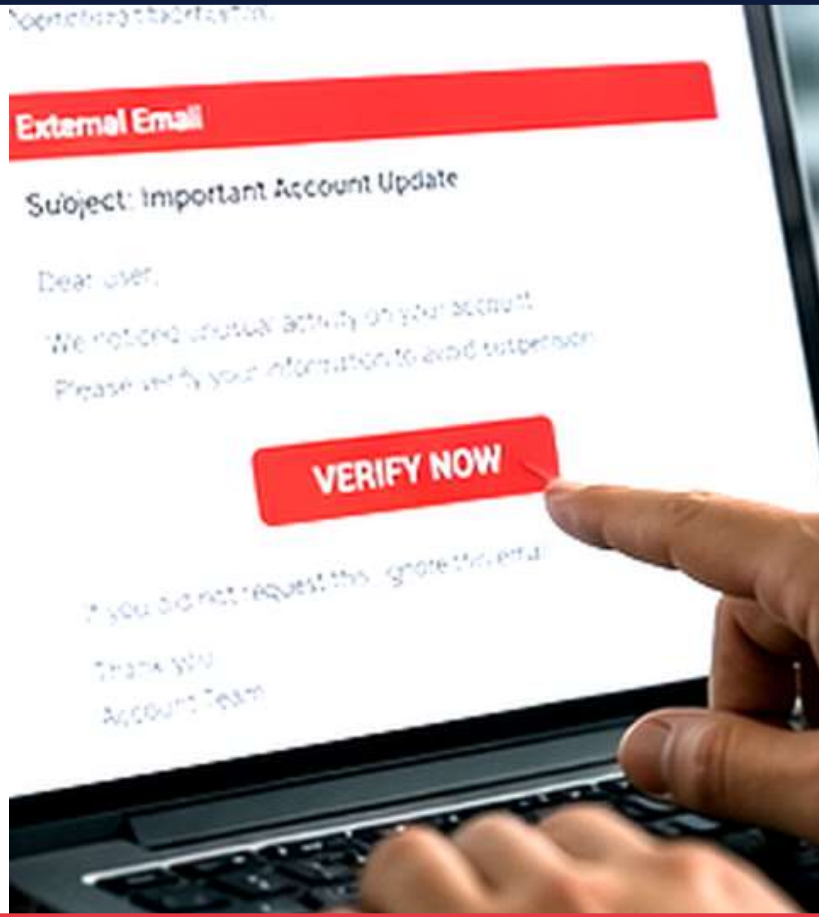
Amenazas y Ataques

Los principales riesgos cibernéticos que debes conocer y saber detectar antes de que ocurran

Phishing y Fraudes Online

¿Cómo detectar un correo o mensaje falso?

1. Dirección sospechosa que imita una legítima (ej: soporte@micr0soft.com)
2. Errores ortográficos o gramaticales en el mensaje
3. Asunto alarmista: 'Tu cuenta será suspendida', 'Acción urgente'
4. Solicitud de contraseñas, datos bancarios o personales con urgencia
5. Ofertas demasiado buenas o premios inesperados
6. URLs que no coinciden con el texto del enlace al pasar el ratón
7. Adjuntos inesperados: .exe, .zip, .docm — no abrir sin verificar



Malware — Virus, Ransomware, Spyware, Troyanos

Software malicioso diseñado para dañar, interrumpir o acceder sin autorización a sistemas.

Virus

Se replica en archivos legítimos y se propaga cuando el usuario los ejecuta.

Ransomware

Cifra todos los archivos y pide rescate económico. Puede paralizar organizaciones enteras.

Spyware

Espía en silencio: captura teclas, contraseñas y datos personales sin que la víctima lo note.

Troyanos

Se disfrazan de software legítimo. Al instalarse, abren puertas traseras para el atacante.

Fugas de Datos e Ingeniería Social

Fugas de Datos y Robo de Identidad

¿Qué son? Exposición de datos personales accidental o por ataque.

¿Consecuencias? Suplantación, fraude financiero, daño reputacional.

¿Prevención? Cifrado, control de accesos, formación y detección temprana.

Ingeniería Social

Manipulación psicológica para que la víctima revele información o realice acciones perjudiciales.

Pretexting: Inventar escenarios falsos para ganarse la confianza de la víctima.

Vishing: Llamadas suplantando a técnicos de soporte o directivos.

Baiting: Dejar USBs infectados en lugares visibles para que alguien los conecte.

PARTE 4

Cómo protegerte en el día a día

Buenas Prácticas

Medidas concretas para tu entorno laboral y personal — la seguridad empieza en ti

Consejos para Proteger tus Datos Personales

Contraseñas seguras

Mínimo 12 caracteres con mayúsculas, minúsculas, números y símbolos. Una contraseña diferente por servicio.

Autenticación multifactor

Activa el doble factor (MFA) en correo, banca y redes sociales. Un código extra que el atacante no tiene.

Evita redes Wi-Fi públicas

Sin VPN, no uses redes públicas para trabajo. Los atacantes pueden interceptar todo el tráfico.

HTTPS y dominios correctos

Verifica que la URL comienza por https:// y el dominio es exacto antes de introducir cualquier dato.

Actualiza tus dispositivos

Las actualizaciones corrigen vulnerabilidades. Mantén al día el sistema operativo y las apps.

Solo apps de fuentes oficiales

App Store o Google Play únicamente. Revisa siempre los permisos que solicita cada aplicación.

Protección en el Entorno Laboral

Pequeños descuidos pueden tener grandes consecuencias legales y reputacionales.

✓ SÍ HACER	✗ NO HACER
Bloquea la pantalla al alejarte del puesto	Email corporativo para asuntos personales
Usa solo dispositivos y redes corporativas	Conectar USB o dispositivos no autorizados
Reporta cualquier incidente de seguridad	Compartir credenciales de acceso con nadie
Clasifica documentos según confidencialidad	Acceder a datos más allá de lo necesario
Destruye físicamente los papeles sensibles	Hablar de información confidencial en público

Externalización — Encargados del Tratamiento (art. 28)

Cuando un proveedor trata datos por tu cuenta, el RGPD te obliga a garantizar las mismas garantías.

Contrato de encargo del tratamiento

Obligatorio con cualquier proveedor que acceda a datos personales. Finalidad, datos, medidas de seguridad y obligaciones.

Due diligence del proveedor

Antes de contratar, verifica que aplica medidas adecuadas. Solicita certificaciones ISO 27001 o auditorías.

Cadena de subencargados

El encargado no puede subcontratar sin tu autorización previa. Debes conocer toda la cadena de acceso a los datos.

Lo que debes recordar

Conclusiones clave

1

El RGPD no es solo burocracia

Es un marco de derechos fundamentales. Cumplirlo protege a las personas y a tu organización.

2

CIA: el núcleo de la seguridad

Confidencialidad, Integridad y Disponibilidad son los tres pilares de toda medida de seguridad.

3

El factor humano es la primera línea

La mayoría de incidentes empiezan con un error humano. La formación es la mejor defensa.

4

Reporta — no ocultes incidentes

Si detectas algo sospechoso, comunícalo de inmediato. El RGPD obliga a notificar brechas en 72 horas.

¿Preguntas?

Dudas, sugerencias o comentarios

luis@leynetconsultores.com

Gracias por vuestra atención
La seguridad es responsabilidad de todos