

# GUÍA DE CIBERSEGURIDAD Y BUENAS PRÁCTICAS PARA EMPRESAS

---

Medidas esenciales para proteger la información, los sistemas y el trabajo diario de la empresa.



**LEGALDPO**

Consultoría especializada en RGPD

Documento interno de apoyo para empresas

## FUENTES Y REFERENCIAS UTILIZADAS

La presente guía ha sido elaborada por el Departamento Jurídico de LegalDPO, tomando como referencia las recomendaciones de la AEPD, INCIBE, OSI y CCN-CERT.

Su finalidad es concienciar sobre los principales riesgos de ciberseguridad y ofrecer medidas básicas para prevenir incidentes y brechas de seguridad en las organizaciones.

Referencias principales: RGPD, LOPDGDD, AEPD, INCIBE, OSI y CCN-CERT.

## ÍNDICE

1. Introducción
2. Principales amenazas
3. Contraseñas seguras
4. Correo electrónico y phishing
5. Navegación segura
6. Dispositivos móviles
7. Teletrabajo
8. Redes WiFi
9. Copias de seguridad
10. Protección de datos y confidencialidad
11. Actuación ante incidentes

## 1. Introducción

La ciberseguridad es esencial para cualquier organización. Muchos incidentes y brechas de seguridad tienen su origen en errores humanos o en la falta de **formación**, por lo que la concienciación de los empleados y la aplicación de buenas prácticas resultan fundamentales para proteger la información y reducir riesgos.

## 2. Principales amenazas

Las amenazas más habituales son el phishing, ransomware, malware, robo de credenciales, fraude del CEO e ingeniería social. Estos ataques pueden provocar brechas de seguridad que afecten a los datos personales y, en determinados casos, deban notificarse a la AEPD en un plazo máximo de 72 horas.

## 3. Contraseñas seguras

**RIESGO DE BRECHA:** El uso de contraseñas débiles facilita accesos no autorizados a bases de datos, correos electrónicos y aplicaciones corporativas que contienen datos personales de clientes, empleados o proveedores. Utilice contraseñas largas, únicas y complejas. Active siempre la autenticación multifactor cuando esté disponible.

### Consejo práctico

Utilice un gestor de contraseñas corporativo, active la autenticación multifactor siempre que sea posible y evite reutilizar la misma contraseña en diferentes servicios. Una contraseña robusta es una de las medidas más eficaces para prevenir accesos no autorizados y brechas de seguridad.

## 4. Correo electrónico y phishing

**EJEMPLO REAL DE BRECHA:** El envío de documentación a un destinatario incorrecto o la apertura de un archivo malicioso puede generar una violación de seguridad de los datos personales.

### Consejo práctico

Antes de abrir un enlace, descargar un archivo adjunto o realizar una transferencia bancaria, dedique unos segundos a verificar el remitente y confirmar la solicitud por una vía alternativa (teléfono o contacto habitual). La mayoría de los ataques de phishing se aprovechan de las prisas y la falta de comprobación.

## 5. Navegación segura

**RIESGO ASOCIADO:** Acceder a páginas fraudulentas puede provocar la descarga de malware capaz de extraer información confidencial almacenada en los equipos de la empresa.

### Consejo práctico

Antes de introducir información, descargar archivos o acceder a una página web, compruebe que la dirección es legítima y comienza por "https://". Evite navegar por sitios desconocidos o acceder a enlaces recibidos por correo o mensajería sin verificar previamente su origen.

## 6. Dispositivos móviles

**RIESGO DE PÉRDIDA DE DATOS:** La pérdida o robo de un teléfono móvil corporativo sin cifrado ni bloqueo puede constituir una brecha de seguridad si contiene información de clientes o empleados.

### Consejo práctico

Active siempre el bloqueo automático del dispositivo, el cifrado de la información y la posibilidad de localización o borrado remoto. En caso de pérdida o robo, podrá minimizar el riesgo de acceso no autorizado a datos personales o información confidencial de la empresa.

## 7. Teletrabajo

**MEDIDA RECOMENDADA RGPD:** Durante el teletrabajo debe evitarse imprimir documentación con datos personales en domicilios particulares y utilizar dispositivos personales sin autorización.

### Consejo práctico

Cuando trabaje fuera de la oficina, utilice únicamente equipos y aplicaciones autorizadas por la empresa. Evite conectarse a redes WiFi-públicas y asegúrese de que nadie pueda visualizar documentación o información confidencial desde su entorno de trabajo.

## 8. Redes WiFi

**RIESGO DE INTERCEPTACIÓN:** Las redes WiFi-inseguras pueden permitir el acceso de terceros a comunicaciones que contengan datos personales o información confidencial.

### Consejo práctico

Configure la red WiFi con una contraseña robusta, cambie las credenciales predeterminadas del router y limite el acceso únicamente a personas autorizadas. Una red inalámbrica mal protegida puede facilitar el acceso de terceros a información confidencial y datos personales de la organización.

## 9. Copias de seguridad

**CONTINUIDAD DE NEGOCIO:** Las copias de seguridad permiten recuperar la disponibilidad de los datos tras un ransomware o incidente técnico, minimizando el impacto de una brecha.

### Consejo práctico

Realice copias de seguridad automáticas de forma periódica y compruebe regularmente que pueden restaurarse correctamente. Mantener una copia aislada o desconectada de la red puede ser

fundamental para recuperar la información en caso de ransomware, fallo técnico o pérdida accidental de datos.

## **10. Protección de datos y confidencialidad**

**CONCEPTO DE BRECHA DE SEGURIDAD:** Se considera brecha cualquier destrucción, pérdida, alteración, divulgación o acceso no autorizado a datos personales, ya sea accidental o intencionado.

### **Consejo práctico**

Limite el acceso a la información únicamente a las personas que realmente la necesiten para desempeñar sus funciones. Una adecuada gestión de permisos, junto con la formación del personal en materia de confidencialidad, ayuda a prevenir accesos indebidos y posibles brechas de seguridad.

## **11. Actuación ante incidentes**

**PROTOCOLO DE ACTUACIÓN:** Toda incidencia debe comunicarse inmediatamente al responsable designado para analizar si existe obligación de notificación a la AEPD y/o a los afectados.

### **Consejo práctico**

Ante cualquier incidente de seguridad, actúe con rapidez: comuníquelo inmediatamente a la persona responsable, conserve las evidencias disponibles y evite realizar acciones que puedan dificultar el análisis posterior. Una respuesta rápida puede minimizar el impacto del incidente y facilitar el cumplimiento de las obligaciones legales de notificación.