Decálogo de buenas prácticas

Protección de datos personales

- Se considera dato personal cualquier información relativa a personas físicas (p.e: email, nombre, teléfono, fotografía, salud, orientación política, etc.), existiendo tres niveles de seguridad de acuerdo a su sensibilidad (básico, medio y alto). Tratamos a diario con dicho tipo de datos, y se deben procesar de formas concretas en cumplimiento de la Ley Orgánica de Protección de Datos

¿Qué puede pasar?

Incumplir la LOPD puede acarrear multas entre 900€ y 600.000€ para la empresa, además de daños a la imagen y credibilidad de las compañías. A continuación se muestran situaciones que podrían suponer incumplimientos y poner en riesgo datos personales bajo nuestra responsabilidad:

Accesos no autorizados
a los ficheros de datos

Pérdida de información
por falta de copias de seguridad

Desecho de soportes
sin eliminar la información que contienen

Transmisión de la información
sin que sea cifrada de forma segura

¿Cómo me protejo?

- Si la información debe ser transmitida, por redes o en soportes, asegúrate de que ésta se ha **cifrado adecuadamente** antes y durante el tránsito **para ficheros de nivel alto**.
- **Mantén la información a buen recaudo para evitar su pérdida**. Realiza copias de seguridad y **pruebas de restauración cada 6 meses**. En el caso de la documentación en papel es necesario almacenarla bajo llave.
- **Elimina la información cuando retires un soporte.** Es necesario hacer un borrado seguro o destruirlo. Evitarás que pueda recuperarse en caso de que caiga en manos de terceros
- **Oculta las direcciones en los envíos de correo masivos.** Además debes ofrecer un mecanismo para darse de baja de los envíos, e informar de él en todos los correos.
- Utiliza **destructoras de papel o contenedores seguros** a la hora de deshacerte de documentos confidenciales.
- **Limita el acceso** a la información solamente a quien sea estrictamente necesario. Usa **cuentas de usuario individuales** (no compartidas), **contraseñas con caducidad (al menos 1 año) y bloqueo por intentos erróneos (nivel medio)**, para evitar accesos de personas no autorizadas.
- Debe existir un **log (registro automatizado) de los accesos** para los datos de nivel alto.