

Control Documental en la Era Digital



1 ¿Qué es el Control Documental Digital?

- Gestión organizada de la creación, almacenamiento, acceso, modificación y eliminación de documentos en formato digital.
- Permite trazabilidad, seguridad y disponibilidad de la información.
- Sustituye los procesos físicos por plataformas electrónicas seguras.

2 BENEFICIOS

- ✓ Acceso rápido y remoto.
- ✓ Reducción de costos y papel.
- ✓ Mayor eficiencia en procesos.
- ✓ Cumplimiento normativo (ISO, SG-SST, Habeas Data, etc.).
- ✓ Disminución del riesgo de pérdida de documentos.



3 Riesgos en la Era Digital

- ⚠ Ciberataques y fugas de información.
- ⚠ Pérdida de control sobre copias no autorizadas.
- ⚠ Almacenamiento inseguro en nubes no reguladas.
- ⚠ Incumplimiento de normativas de protección de datos.

4 Protección de Datos Personales en Documentos Digitales

🔒 Principios clave del Habeas Data y la normativa de protección de datos:

- Legalidad y consentimiento: uso autorizado por el titular.
- Finalidad: solo para el propósito declarado.
- Seguridad: implementar controles técnicos y organizativos.
- Acceso restringido: solo personal autorizado.
- Conservación: por el tiempo necesario y según la ley.
- Eliminación segura: destrucción digital certificada (borrado seguro)



5 Buenas Prácticas de Control Documental con Datos Personales



- Clasificar documentos según sensibilidad.
- Usar cifrado y autenticación multifactor.
- Limitar accesos por roles y responsabilidades.
- Establecer políticas de retención y eliminación.
- Capacitación a empleados sobre protección de datos.

¡VEAMOS CASOS REALES Y SUS BUENAS PRACTICAS!

📸 Caso 1: Publicación de fotos de estudiantes en redes sociales



Riesgo: Se difunden imágenes de menores sin consentimiento, lo que puede generar problemas legales y reputacionales.

Buenas prácticas:

- Obtener consentimiento expreso y documentado de padres/tutores.
- Difundir solo en canales oficiales de la institución.
- Restringir la visibilidad de publicaciones en redes.

📊 Caso 2: Almacenamiento físico y digital de actas y resoluciones izadas.

Riesgo: Extravió de actas físicas o copias digitales no controladas en USB.

Buenas prácticas:

- Implementar un Sistema de Gestión Documental (SGD) con trazabilidad.
- Digitalización segura con control de versiones.
- Bloquear dispositivos externos para evitar copias no autorizadas.
- Mantener una copia de seguridad mediante disco duro.



“No todo dato debe compartirse, pero todo dato debe protegerse.”