kaiserkraft
Miniguías

Checklist – ¿Qué va dónde?

Objetivo:
Ver de un vistazo qué información va en el armario para documentos, la caja fuerte o la caja fuerte para datos, qué debe destruirse y dónde conviene una copia digital.

01 Armario para documentos – Para documentos confidenciales que se necesitan con

Contenidos típicos:

- [ ] Documentos de personal como contratos de trabajo, evaluaciones o bajas médicas: deben estar seguros, pero accesibles rápidamente.
- [ ] Documentos financieros y contables como facturas, balances o documentos fiscales que se procesan regularmente.
- [ ] Contratos vigentes con clientes, proveedores y socios: el acceso debe estar claramente regulado.
- [ ] Directrices internas, instrucciones operativas, de seguridad y de trabajo, para que el día a día funcione sin problemas.

Reglas básicas:

- [ ] Mantener siempre cerrado el armario; entregar llaves o acceso solo a personas autorizadas.
- [ ] Ordenar los documentos por tema y archivarlos según el plazo de conservación para evitar desorden y tiempos de búsqueda.
- [ ] Trasladar regularmente los documentos vencidos a contenedores protegidos para destrucción de documentos, para minimizar riesgos de protección de datos.

02 Caja fuerte / armario de seguridad – Para contenidos especialmente valiosos o críticos.

Contenidos típicos:

- [ ] Documentos originales como escrituras de constitución, extractos registrales o contratos notariales cuya pérdida tendría consecuencias legales.
- [ ] Carpetas de firma, sellos de empresa y poderes imprescindibles para la actividad.
- [ ] Soportes de datos con información sensible, como discos de copia de seguridad, memorias USB o soportes de proyecto confidenciales.
- [ ] Objetos de valor como efectivo, vales o hardware sensible (p. ej., tokens de acceso).

Reglas básicas:

- [ ] Anclar firmemente la caja fuerte y colocarla en una zona protegida y discreta para dificultar manipulaciones.
- [ ] Definir claramente los derechos de acceso; no “todo el personal con llave”.
- [ ] Documentar accesos, p. ej. mediante registros de cierre o listas de acceso, para mantener trazables las responsabilidades.

03 Caja fuerte para datos / armario ignífugo para soportes de datos – Para medios sensibles al calor y la humedad.

Contenidos típicos:

- ☐ Copias de seguridad de sistemas ERP, RR. HH. o producción cuya recuperación sea crítica en caso de
- ☐ Soportes de datos especiales como cintas, SSD o discos externos, especialmente sensibles al calor y la humedad.
- ☐ Datos de proyecto archivados, relevantes desde el punto de vista legal u operativo.

Reglas básicas:

- ☐ Utilizar solo armarios certificados para soportes de datos (clases de fuego y temperatura adaptadas).
- ☐ Rotar copias de seguridad regulares según un esquema fijo (diario, semanal, mensual) para evitar pérdida de datos.
- ☐ Etiquetar claramente los soportes de datos (contenido, fecha, sistema) – para recuperación rápida y visión

04 ¿Qué se destruye? – Utilizar correctamente destructoras de documentos y borrado digital.

Documentos en papel:

- ☐ Datos personales (solicitudes, expedientes antiguos de personal, listas salariales).
- ☐ Contratos, ofertas o cálculos obsoletos con información confidencial.
- ☐ Impresiones con datos de acceso, estrategias internas o información financiera.
- ☐ Notas, actas y versiones intermedias que contienen detalles sensibles.

Reglas básicas:

- ☐ Elegir el nivel de seguridad según la necesidad de protección – niveles superiores para datos de RR. HH. y
- ☐ Cerrar los contenedores de recogida y vaciarlos regularmente para garantizar una destrucción completa.

Datos digitales:

- ☐ Copias de seguridad obsoletas que ya no se necesitan.
- ☐ Soportes de datos al final de su vida útil (discos defectuosos, memorias USB, cintas).
- ☐ Datos de prueba o copias que contienen contenidos sensibles.

Consejo: También en digital, los derechos de acceso deben estar claramente regulados y los procesos de

05 Combinar conservación física + copia de seguridad digital

Principio básico: La información importante se conserva físicamente de forma segura y se protege digitalmente – nunca duplicada sin control.

Ejemplos:

- **Contratos importantes:** Original en el armario para documentos o caja fuerte, versión escaneada en el archi vo digital con garantía de auditoría.
- **Datos críticos de operación e instalaciones:** Versión de trabajo en el sistema, copia de seguridad regular en caja fuerte para datos o caja fuerte.
- **Datos de personal y RR. HH.:** Documentos en papel en el armario para documentos, expedientes digitales en sistema protegido con gestión de derechos.

Consejo: La seguridad física y digital se complementan – así evita pérdida de datos, robo o publicación accidental.

06

Breve autocomprobación para la empresa

- ¿Hay documentos sensibles a la vista sobre escritorios o estanterías?
- ¿Armarios para documentos, cajas fuertes y cajas fuertes para datos están claramente asignados (quién accede a qué)?
- ¿Existen rutinas fijas para destruir documentos (p. ej., “ronda de borrado” mensual)?
- ¿Las copias de seguridad están bien etiquetadas y guardadas físicamente separadas de los sistemas productivos?

Si varios puntos se responden con “Sí, pero…”:

- Revisar estructuras, adaptar armarios y cajas fuertes y definir reglas claras para conservación, destrucción y copia de seguridad digital.
- Una breve formación o un recordatorio para el personal puede ayudar a aclarar responsabilidades y cumplir procesos.