kaiserkraft
Mini-guias

Checklist – O que fica onde?

Objetivo:
Ver rapidamente que informações pertencem ao armário para documentos, cofre ou cofre para dados, o que deve ser destruído e onde o backup digital também faz sentido.

01 Armário para documentos – Para documentos confidenciais necessários regularmente.

Conteúdos típicos:

- [ ] Documentos de pessoal como contratos de trabalho, avaliações ou baixas médicas – devem estar seguros, mas rapidamente acessíveis.
- [ ] Documentos financeiros e contabilísticos como faturas, balanços ou documentos fiscais que são processados regularmente.
- [ ] Contratos em curso com clientes, fornecedores e parceiros – o acesso deve estar claramente regulado.
- [ ] Diretrizes internas, instruções operacionais, de segurança e de trabalho, para que o dia a dia decorra sem problemas.

Regras básicas:

- [ ] Manter o armário sempre fechado; entregar chaves ou acesso apenas a pessoas autorizadas.
- [ ] Ordenar documentos por tema e arquivá-los por prazo de conservação, para evitar desordem e tempos de procura.
- [ ] Transferir regularmente documentos expirados para contentores protegidos de destruição de documentos, para minimizar riscos de proteção de dados.

02 Cofre / armário de segurança – Para conteúdos especialmente valiosos ou críticos.

Conteúdos típicos:

- [ ] Documentos originais como documentos de constituição, certidões prediais ou contratos notariais cuja perda teria consequências legais.
- [ ] Pastas de assinatura, carimbos da empresa e procurações indispensáveis à operação.
- [ ] Suportes de dados com informações sensíveis, como discos de backup, pens USB ou suportes de projeto confidenciais.
- [ ] Objetos de valor como dinheiro, vales ou hardware sensível (p. ex., tokens de acesso).

Regras básicas:

- [ ] Fixar bem o cofre e colocá-lo numa área protegida e discreta, para dificultar manipulações.
- [ ] Definir claramente os direitos de acesso; não “todos os colaboradores com chave”.
- [ ] Documentar acessos, p. ex., com registos de fecho ou listas de acesso, para manter responsabilidades rastreáveis.

03 Cofre para dados / armário ignífugo para suportes de dados – Para meios sensíveis ao calor e à humidade.

Conteúdos típicos:

- ☐ Backups de sistemas ERP, RH ou de produção, cuja recuperação é crítica em caso de emergência.
- ☐ Suportes de dados especiais como fitas, SSDs ou discos externos, particularmente sensíveis ao calor e à humidade.
- ☐ Dados de projeto arquivados, relevantes do ponto de vista legal ou operacional.

Regras básicas:

- ☐ Utilizar apenas armários testados para suportes de dados (classes de fogo e temperatura adequadas).
- ☐ Rodar backups regulares segundo um esquema fixo (diário, semanal, mensal) para evitar perda de dados.
- ☐ Identificar claramente os suportes de dados (conteúdo, data, sistema) – para recuperação rápida e visão

04 O que é destruído? – Utilizar corretamente destruidoras de papel e eliminação digital.

Documentos em papel:

- ☐ Dados pessoais (candidaturas, antigos processos de pessoal, listas salariais).
- ☐ Contratos, propostas ou cálculos desatualizados com informações confidenciais.
- ☐ Impressões com dados de acesso, estratégias internas ou informações financeiras.
- ☐ Notas, atas e versões intermédias que contêm detalhes sensíveis.

Regras básicas:

- ☐ Escolher o nível de segurança conforme a necessidade de proteção – níveis superiores para dados de RH
- ☐ Fechar contentores de recolha e esvaziá-los regularmente, para garantir uma destruição completa.

Dados digitais:

- ☐ Backups desatualizados que já não são necessários.
- ☐ Suportes de dados em fim de vida (discos avariados, pens USB, fitas).
- ☐ Dados de teste ou cópias que contêm conteúdos sensíveis.

Dica: Também no digital, os direitos de acesso devem estar claramente regulados e os processos de

05 Combinar conservação física + backup digital

Princípio básico: Informações importantes são guardadas fisicamente em segurança e protegidas digitalmente – nunca duplicadas sem controlo.

Exemplos:

- **Contratos importantes:** Original no armário para documentos ou cofre, versão digitalizada no arquivo digital à prova de auditoria.
- **Dados críticos de operação e instalações:** Versão de trabalho no sistema, backup regular em cofre para dados ou cofre.
- **Dados de pessoal e RH:** Documentos em papel no armário para documentos, dossiês digitais em sistema protegido com gestão de direitos.

Dica: Segurança física e digital complementam-se – assim evita perda de dados, roubo ou publicação acidental.

06 Breve autoteste para a empresa

- Há documentos sensíveis expostos em secretárias ou estantes?
- Armários para documentos, cofres e cofres para dados estão claramente atribuídos (quem acede a quê)?
- Existem rotinas fixas para destruição de documentos (p. ex., “ronda de eliminação” mensal)?
- Os backups estão claramente identificados e guardados fisicamente separados dos sistemas produtivos?

Se vários pontos forem respondidos com “Sim, mas…”:

- Verificar estruturas, ajustar armários e cofres e definir regras claras para conservação, destruição e backup digital.
- Uma breve formação ou lembrete aos colaboradores pode ajudar a clarificar responsabilidades e cumprir processos.