

## Anexo 2 :Protección de la informacion

### INTRODUCCIÓN:

La información de una empresa no solo incluye bienes tangibles, sino también intangibles como clientes, tarifas o reputación. Proteger esta información es vital, incluso en pequeñas empresas, ya que su pérdida puede tener consecuencias graves. Esta protección se conoce como **seguridad de la información**.

### DESCRIPCIÓN DEL PROBLEMA:

El uso de tecnología facilita el mal manejo de datos. Algunos errores comunes incluyen:

- No hacer copias de seguridad.
- Uso inadecuado de carpetas compartidas.
- Usuarios con acceso innecesario a información.
- Dispositivos portátiles sin control.
- Falta de formación del personal.
- Uso de correos y almacenamiento personal para trabajo.
- Desechar equipos sin eliminar información.

**Solución:** Implementar controles de acceso, hacer copias de seguridad, limitar el uso de apps externas, capacitar al personal y borrar correctamente los dispositivos.

### DIMENSIONES DE LA SEGURIDAD DE LA INFORMACIÓN

1. **Integridad:** La información debe ser correcta y sin alteraciones. Un error puede provocar decisiones equivocadas.
2. **Confidencialidad:** Solo debe acceder quien esté autorizado (principio del “need-to-know”).
3. **Disponibilidad:** La información debe estar accesible cuando se necesita.

Las medidas deben equilibrar estas tres dimensiones sin que una afecte negativamente a otra.

### SELECCIÓN DE SALVAGUARDAS

Para elegir medidas de protección, se debe:

- Evaluar la importancia de la información.
- Clasificar la información según sus riesgos.
- Considerar controles técnicos (firewalls), organizativos (formación) y legales.
- Evaluar el coste vs el riesgo.

### IMPORTANCIA DE LA INFORMACIÓN PARA LA EMPRESA

Según el sector, la información crítica varía:

- **Sanitario:** Datos personales de pacientes.
- **Financiero:** Operaciones y datos sensibles.
- **Industrial:** Procesos confidenciales.
- **Hostelería:** Datos de clientes y reservas.

La legislación exige proteger los datos personales, especialmente los **datos sensibles** (salud, ideología, orientación sexual, etc.) bajo principios de **responsabilidad proactiva**.

## PASOS PREVIOS A LA SELECCIÓN DE SALVAGUARDAS

Hay que:

- Revisar y clasificar la información.
- Definir niveles como:  
**Confidencial, Interna y Pública.**
- Determinar el tratamiento que requiere cada tipo.

## NATURALEZA DE LOS CONTROLES

Los controles pueden ser:

- **Técnicos:** Antivirus, copias, firewalls.
- **Organizativos:** Formación, políticas internas.
- **Físicos:** Cerraduras, salas protegidas.
- **Legales:** Cumplimiento de normativas y leyes.

## RESUMEN DE CRITERIOS DE SELECCIÓN

Hay que tener en cuenta:

- Coste económico y de implementación.
- Importancia y necesidades del sistema.
- Qué dimensión de seguridad se quiere priorizar.

## SALVAGUARDAS BÁSICAS

### Control de acceso a la información:

Aplicar el principio del **mínimo privilegio**: solo acceder a lo necesario.

### Copias de seguridad:

- Analizar qué se copia y dónde está.
  - Definir número de versiones y duración.
  - Tipos: completas, incrementales, diferenciales.
  - Hacer pruebas de restauración.
  - Cifrar la información si es confidencial.
  - Guardar copias fuera de la empresa.
- 

## CIFRADO DE INFORMACIÓN

El cifrado protege la información codificándola.

### Importante:

- Usar claves fuertes.
  - No perder la clave.
  - Cifrar especialmente si se usan dispositivos móviles o la nube.
- 

## DESECHADO Y REUTILIZACIÓN DE SOPORTES

### Antes de desechar equipos:

- Borrar de forma **segura** (no solo eliminar archivos).
  - Si es confidencial, **destruir físicamente** el soporte o usar software especializado.
  - No olvidar el papel como soporte sensible.
- 

## ALMACENAMIENTO EN LA NUBE

Ventajas: reduce costos, acceso remoto, delegar copias.

Riesgos:


- No controlar accesos ni condiciones.
- Posibles fallos o pérdidas.
- Debe haber **contratos de tratamiento de datos** si se manejan datos personales.

Evitar servicios gratuitos sin garantías.

---

## CONFIDENCIALIDAD EN LA CONTRATACIÓN DE SERVICIOS

Externalizar servicios (copias, mantenimiento, etc.) puede ser un riesgo.

 Para mitigarlo: usar **contratos de confidencialidad** que limiten el uso de datos por parte del proveedor.

