

# Medidas Técnicas y Organizativas

Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, las circunstancias y los fines del tratamiento, así como la probabilidad y la gravedad variables del riesgo para los derechos y las libertades de las personas físicas, el Contratista, en su calidad de encargado del tratamiento de datos, aplicará las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluidas, entre otras, las siguientes:

## 1. Seudonimización

Seudonimización significa el tratamiento de datos personales del Cliente de tal manera que ya no puedan atribuirse a un interesado específico sin información adicional, siempre que dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas que garanticen que los datos personales no se atribuyen a una persona física identificada o identificable.

## 2. Confidencialidad

### 2.1 Control de acceso físico

El Contratista tomará las medidas adecuadas para reducir el riesgo de que personas no autorizadas accedan a los sistemas de tratamiento de datos con los que se procesan y utilizan los datos personales del Cliente. Las medidas de control de acceso pueden incluir, por ejemplo, sistemas automáticos de control de acceso, uso de tarjetas con chip y transpondedores, control de acceso mediante servicios de portero y sistemas de alarma. Los servidores, los sistemas de telecomunicaciones, la tecnología de redes y otros equipos similares pueden protegerse, por ejemplo, con armarios para servidores con cerradura. También tiene sentido controlar el acceso mediante medidas organizativas (por ejemplo, directivas de servicio que estipulen que las salas de servicio deben estar cerradas cuando los empleados estén ausentes).

#### Medidas técnicas:

- Sistema de control de acceso automático
- Tarjetas con chip / sistemas de transpondedor
- Sistema de cierre manual
- Puertas con pomos exteriores

#### Medidas organizativas:

- Regulación de las claves (entrega de claves, etc.)
- Visitantes acompañados por empleados
- Selección cuidadosa del personal de limpieza

### 2.2 Control de acceso al sistema

El Contratista tomará las medidas adecuadas para evitar que los sistemas de tratamiento de datos (ordenadores) sean utilizados por personas no autorizadas.

Para ello, el Contratista deberá tomar las siguientes precauciones:

#### Medidas técnicas:

- Inicio de sesión con nombre de usuario + contraseña
- Inicio de sesión parcial con datos biométricos

- Cifrado de teléfonos inteligentes
- Cifrado de ordenadores portátiles/tabletas
- Gestión de ordenadores portátiles
- Uso de software antivirus para servidores
- Instalación de software antivirus para clientes
- Bloqueo automático del escritorio

**Medidas organizativas:**

- Gestionar los permisos de los usuarios
- Crear perfiles de usuario
- Política de «traiga su propio dispositivo» (*Bring-Your-Own-Device*).
- Política de dispositivos móviles
- Política general de protección o seguridad de datos

**2.3 Control de acceso a los datos**

El Contratista tomará las medidas adecuadas para garantizar que las personas autorizadas a utilizar los sistemas de tratamiento de datos solo puedan acceder a los datos personales sujetos a su autorización de acceso y que los datos personales del Cliente no puedan ser leídos, copiados, modificados o eliminados sin autorización durante el tratamiento, el uso y después del almacenamiento. Para ello, el Contratista deberá tomar las siguientes precauciones:

**Medidas técnicas:**

- Borrado físico de los soportes de datos en los ordenadores portátiles antes de su reutilización.
- Registro del acceso a documentos importantes, especialmente cuando se introducen, modifican y eliminan datos.
- Destructora de archivos (nivel mínimo 3, corte transversal)

**Medidas organizativas:**

- Creación de un concepto de autorización
- Gestión de derechos por parte del administrador del sistema
- Reducción del número de administradores
- Área cerrada para documentos sensibles

**2.4 Control de separación**

El Contratista tomará las medidas adecuadas para garantizar que los datos personales del cliente recabados para diferentes fines puedan tratarse por separado. Para ello, el Contratista deberá tomar las siguientes precauciones:

**Medidas técnicas:**

- Almacenamiento por separado en sistemas o soportes de datos independientes.
- Separación de clientes basada en software

**Medidas organizativas:**

- Creación de un concepto de autorización

- Determinación de derechos en la base de datos

### **3. Integridad**

#### **3.1 Control de la transmisión**

El Contratista tomará medidas razonables para reducir el riesgo de que los datos personales del Cliente puedan ser leídos, copiados, modificados o eliminados sin autorización durante la transmisión electrónica o durante su transporte o almacenamiento en soportes de datos. Para ello, el Contratista deberá tomar las siguientes precauciones:

##### **Medidas técnicas:**

- Cifrado del correo electrónico
- Registro de los accesos y recuperaciones de documentos y datos importantes • Entrega a través de conexiones encriptadas como sftp, https
- Uso de procedimientos de firma

##### **Medidas organizativas:**

- Posibilidad de generar un resumen de las operaciones habituales de recuperación y transmisión.

#### **3.2 Control de entrada de datos**

El Contratista tomará las medidas adecuadas para garantizar que sea posible comprobar y determinar a posteriori si los datos personales del cliente han sido introducidos en los sistemas de tratamiento de datos, modificados o eliminados, y por quién. Para ello, el Contratista deberá tomar las siguientes precauciones:

##### **Medidas técnicas:**

- Posibilidad de registro técnico de la introducción, modificación y supresión de datos personales.

##### **Medidas organizativas:**

- Trazabilidad de la introducción, modificación y supresión de datos personales mediante nombres de usuario individuales.
- Conservación de los formularios desde los que se han transferido datos personales a operaciones de tratamiento automatizado.
- Cesión de derechos de introducción, modificación y supresión de datos personales sobre la base de un concepto de autorización.

### **4. Disponibilidad y capacidad de recuperación**

#### **4.1 Control de disponibilidad**

El Contratista tomará medidas razonables para garantizar que los datos personales del cliente estén protegidos contra la destrucción o pérdida accidental. Para ello, el Contratista deberá tomar las siguientes precauciones:

##### **Medidas técnicas:**

- Sistemas de detección de incendios y humo
- Selección cuidadosa del proveedor de servicios de alojamiento

##### **Medidas organizativas:**

- Control regular del proveedor de servicios de alojamiento

### **5. Procedimientos de revisión, valoración y evaluación periódicas.**

El Contratista aplicará procedimientos de revisión, valoración y evaluación periódicas de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

## **5.1 Gestión de la protección de datos**

### **Medidas técnicas:**

- Documentación central de todos los procedimientos, reglamentos y directrices en materia de protección de datos, con acceso para los empleados según se requiera o autorice
- Se lleva a cabo regularmente una revisión de la eficacia de las medidas técnicas de protección

### **Medidas organizativas:**

- El personal está formado y comprometido a respetar la confidencialidad
- Sensibilización de los empleados a través de la formación

La empresa cumple con las obligaciones de información de acuerdo con los arts. 13 y 14 del RGPD.

Existe un procedimiento formalizado para gestionar las solicitudes de información de los interesados.

## **5.2 Gestión de la respuesta a incidentes**

Apoyo a la respuesta a las brechas de la seguridad.

### **Medidas técnicas:**

- Uso de filtros de spam y actualización periódica
- Uso de antivirus y actualización periódica

### **Medidas organizativas:**

- Documentación de incidentes de seguridad e infracciones de datos
- Regulación de las responsabilidades sobre el seguimiento de los incidentes de seguridad y las infracciones de datos

## **5.3 Configuración por defecto respetuosa con la privacidad (Art. 25 (2) del RGPD); Privacidad por diseño / Privacidad por defecto**

### **Medidas técnicas:**

- No se recaban más datos personales de los que son necesarios para el propósito respectivo.