

## POLÍTICA DE SEGURIDAD del personal

### POLÍTICA DE SEGURIDAD DEL PERSONAL PARA EL TRATAMIENTO DE DATOS PERSONALES

#### 1.- ÁMBITO DE APLICACIÓN

El Responsable del tratamiento está comprometido en implantar una cultura de privacidad en la organización, por lo que necesita que las personas autorizadas a tratar datos personales estén informadas del tratamiento de datos y se responsabilicen del mismo.

A toda persona autorizada para tratar datos personales se le exige que lea, comprenda, cumpla y haga cumplir esta Política de seguridad para proteger los datos que forman parte del tratamiento que se le ha encomendado.

Esta Política de seguridad establece las obligaciones y procedimientos que tiene que seguir el personal de la organización, tanto propio como externo, que trata datos personales en el desarrollo de su actividad, y se basa en lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril de 2016 (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD).

En este sentido, para velar y hacer cumplir esta Política, la organización ha designado un Responsable de seguridad que estará a disposición de todo el personal y se encargará de coordinar, controlar, desarrollar y verificar el cumplimiento de las citadas normativas.

#### 2.- CONCEPTOS BÁSICOS

Para proporcionar una mejor comprensión de la protección de datos, definimos los principales conceptos básicos:

##### Estructura del tratamiento:

- **Datos personales:** Información relativa a una persona física por la cual pueda determinarse su identidad.
- **Tratamiento:** Cualquier operación realizada sobre datos personales: obtención, acceso, intervención, transmisión, conservación y supresión.
- **Interesado:** Persona física sometida al tratamiento de sus datos personales.
- **Fichero:** Conjunto estructurado de datos personales susceptibles de tratamiento para un fin determinado.
- **Responsable del tratamiento:** Organización que determina los fines y los medios del tratamiento.
- **Personal autorizado:** Persona autorizada por el Responsable para realizar un tratamiento de datos mediante un compromiso de confidencialidad.

##### Categorías de datos:

- **Básicos:** Datos que no correspondan a categorías Penales o Especiales, por ejemplo:

nombre, dirección, e-mail, teléfono, edad, sexo, firma, imagen, aficiones, patrimonio, datos bancarios, información académica, profesional, social, comercial, financiera, etc.

- **Penales:** Datos relativos a la comisión de infracciones administrativas o penales, o datos que puedan ofrecer una definición de características de personalidad, etc.
- **Especiales:** Datos relativos al origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos o biométricos que permitan la identificación unívoca de una persona, datos relativos a la salud o a la vida y orientación sexuales.

### 3.- PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Los principios fundamentales para realizar un tratamiento de datos son:

- **Licitud:** lealtad y transparencia con el interesado.
- **Limitación de los fines:** tratados para fines determinados.
- **Minimización de los datos:** solo se deben obtener los datos necesarios para alcanzar los fines.
- **Exactitud:** actualizados.
- **Limitación del plazo de conservación:** guardados durante no más tiempo del necesario para conseguir los fines.
- **Integridad y confidencialidad:** aplicación de medidas de seguridad para la protección de los datos en todas las fases del tratamiento.
- **Responsabilidad proactiva:** se debe poder demostrar el cumplimiento de todos los principios de protección de datos.

#### Consentimiento para realizar un tratamiento de datos

- Para tratar datos deberemos obtener el consentimiento explícito del interesado y guardar el documento probatorio que lo acredite.
- Cuando obtengamos los datos de terceros, deberemos asegurarnos de que la comunicación sea lícita y guardar el documento probatorio que lo acredite.
- No es necesario obtener el consentimiento del interesado cuando el tratamiento se base en una obligación legal (por ejemplo, para emitir una factura).

#### Información del tratamiento al interesado

Deberemos facilitar la siguiente información al interesado:

- La identidad y los datos de contacto del Responsable del tratamiento
- Los fines del tratamiento.
- La base jurídica del tratamiento.
- El plazo de conservación de los datos o los criterios que lo determinen.
- Los derechos que asisten al interesado.
- Y si existen:
  - Los destinatarios o categorías de destinatarios de los datos.
  - La transmisión de datos a países u organizaciones establecidas fuera de la UE.

## Responsabilidad del tratamiento

El tratamiento de datos se podrá realizar por organizaciones externas siempre y cuando exista una autorización expresa del Responsable y se haya suscrito un contrato para realizar dicho tratamiento conforme a la legislación vigente. Para conocer qué empresas o terceros están autorizados a la cesión de datos, deben dirigirse al Responsable de seguridad.

Las organizaciones externas pueden ser:

- **Encargados del tratamiento:** Organización que trata datos personales por cuenta del Responsable.
- **Destinatarios de datos:** Organización distinta del Encargado, que recibe una comunicación de datos personales del Responsable.

## Medidas de seguridad

La organización ha implementado medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado a los riesgos que pueda tener el tratamiento a consecuencia de la destrucción accidental o ilícita de datos, la pérdida, alteración o comunicación no autorizada y el acceso a los datos cuando son transmitidos, conservados u objeto de algún otro tipo de tratamiento.

El personal deberá velar por la seguridad de los datos tratados por la organización y comunicará al Responsable cualquier operación de tratamiento que pueda suponer un riesgo que afecte la protección de datos o los intereses y libertades de los interesados.

Cualquier diseño de una nueva operación de tratamiento o actualización de una operación existente deberá garantizar antes de su implantación, la protección de datos personales y el ejercicio de los derechos de los interesados en todas las fases del tratamiento: obtención, acceso, intervención, transmisión, conservación y supresión.

## 4 - FUNCIONES Y OBLIGACIONES DEL PERSONAL

El personal deberá actuar en todo momento conforme a las instrucciones detalladas en el acuerdo de confidencialidad suscrito con la organización y las establecidas en esta Política de seguridad. Para ello se establecen las siguientes medidas de protección de datos que el personal está obligado a cumplir expresamente:

### Organización de la información

Se deberán clasificar los datos de manera que se puedan ejercer los derechos de los interesados: acceso, rectificación, supresión y portabilidad de los datos y limitación u oposición al tratamiento.

## **Conservación de los datos**

Se deberán conservar los datos en el mobiliario y departamento destinados a tal fin. Para tratamientos automatizados se guardarán los archivos en los soportes, carpetas o directorio de red indicados por el Responsable de seguridad.

No está permitido conservar datos en el escritorio físico o digital. Solo se permite su tratamiento temporal en dicho escritorio para realizar las operaciones que lo precisen debiendo conservarse en el lugar apropiado al término de la jornada laboral.

## **Acceso a la información**

Se deberán aplicar los mecanismos de acceso restringido a la información que haya implementado la organización, y salvaguardar las claves de acceso de toda divulgación o comunicación a otras personas.

Cada persona solo está autorizada a acceder a los recursos que sean necesarios para el desarrollo y cumplimiento de sus funciones.

Se restringirá el acceso a los equipos informáticos mediante procedimientos que puedan identificar y autenticar la persona que accede a los mismos. Los nombres de usuario y contraseña tendrán la consideración de datos personales intransferibles.

## **Procesamiento de datos**

Los soportes documentales e informáticos deberán estar dispuestos de tal forma que no sean accesibles a personas no autorizadas.

Si una persona abandona su puesto de trabajo temporalmente, deberá ocultar los documentos y bloquear el ordenador, de modo que se impida la visualización de la información con la que estaba trabajando.

Cuando se utilicen impresoras o fotocopiadoras, después de la impresión de trabajos con información de carácter personal, se debe recoger de manera inmediata, o imprimir de forma bloqueada, asegurándose de no dejar documentos impresos en la bandeja de salida.

## **Transporte de soportes**

El transporte de soportes que contengan datos personales deberá realizarse únicamente por personal autorizado o empresas externas contratadas para tal fin por el Responsable del tratamiento.

## **Eliminación de documentos**

Cualquier documento físico o soporte digital que quiera ser eliminado y que incluya datos personales, debe ser destruido con la destructora o retirado por una empresa homologada de destrucción de documentos.

## **Copia de seguridad y recuperación de datos**

El personal deberá almacenar toda la información tratada en el directorio de red correspondiente indicado por el Responsable de seguridad, lo que permitirá que a esta información se le apliquen las medidas de seguridad existentes y que se someta a los procedimientos de copias de seguridad aplicados por la organización.

### **Protección de datos**

Se deberán aplicar las medidas de protección de datos establecidas por la organización relativas a la seguridad del tratamiento como pueden ser la seudonimización o cifrado de datos o advertencias de intrusión como antivirus, *antispam*, etc.

### **Gestión de incidencias**

Se considera una incidencia cualquier violación de la seguridad que ocasione la destrucción accidental o ilícita, pérdida, alteración, o el acceso o comunicación no autorizados de datos personales.

El personal tiene la obligación de notificar sin demora injustificada, cualquier incidencia de la que tenga conocimiento al Responsable de seguridad para su conocimiento y para la aplicación de medidas correctivas para remediar y mitigar los efectos que hubiera podido ocasionar. La persona que notifica la incidencia deberá documentarla con una descripción detallada de la misma y la fecha y hora en que se ha producido o se ha tenido conocimiento de ella.

El conocimiento y no notificación de una incidencia por parte del personal se considerará una falta contra la seguridad de los datos y podrá suponer el inicio de acciones legales, así como la reclamación de las indemnizaciones, sanciones y daños o perjuicios que el Responsable se vea obligado a atender a consecuencia de dicho incumplimiento.