PROTECCIÓN DE DATOS

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

ALEXANDRA ALEXANDROVA

03/04/2023

Versión: 1

Índice.

Apartados:

Anexos:

1. Datos Generales.

Datos del Responsable:

NIF/CIF: Y0565053A
Nombre o R. Social: ALEXANDRA ALEXANDROVA
Actividad: Otras actividades
Dirección Postal: CALLE VALLDIGNA, N.19, Esc.E, 9-1
Código Postal: 46730 **Localidad:** Playa de Gandia
Provincia: Valencia **País:** España
Teléfono: 644243004 **Fax:**
Correo Electrónico: svatok84@hotmail.com

Datos del Representante Legal:

NIF/CIF: Y0565053A
Nombre o R. Social: ALEXANDRAALEXANDROVA
Dirección Postal: CALLE VALLDIGNA, N.19, Esc.E, 9-1
Código Postal: 46730 **Localidad:** Playa de Gandía
Provincia: Valencia **País:** España
Teléfono: 644243004 **Fax:**
Correo Electrónico: svatok84@hotmail.com

Actividad de Tratamiento: CLIENTES POTENCIALES

Dirección de Acceso: CALLE VALLDIGNA, N.19, Esc.E, 9-1
Playa de Gandia 46730 Valencia

Responsable del Fichero: ALEXANDRA ALEXANDROVA

Dirección de correo electrónico: svatok84@hotmail.com

Finalidad y Usos:
Realización de presupuestos a posibles clientes.

Actividad de Tratamiento: CLIENTES Y/O PROVEEDORES

Dirección de Acceso: CALLE VALLDIGNA, N.19, Esc.E, 9-1
Playa de Gandia 46730 Valencia

Responsable del Fichero: ALEXANDRA ALEXANDROVA

Dirección de correo electrónico: svatok84@hotmail.com

Finalidad y Usos:
Fichero para el registro de clientes y proveedores de la empresa.

Actividad de Tratamiento: CONTACTOS AGENDA

Dirección de Acceso: CALLE VALLDIGNA, N.19, Esc.E, 9-1
Playa de Gandia 46730 Valencia

Responsable del Fichero: ALEXANDRA ALEXANDROVA

Dirección de correo electrónico: svatok84@hotmail.com

Finalidad y Usos:
Fichero donde de encuentran: nombres, telefonos y las direcciones de e-mail tanto de clientes,proveedores, posibles clientes o candidatos.

Actividad de Tratamiento: CONTACTOS WHATSAPP

Dirección de Acceso: CALLE VALLDIGNA, N.19, Esc.E, 9-1
Playa de Gandia 46730 Valencia

Responsable del Fichero: ALEXANDRA ALEXANDROVA

Dirección de correo electrónico: svatok84@hotmail.com

Finalidad y Usos:
Introduccion de clientes y/o trabajadores en un grupo de whatsapp

Actividad de Tratamiento: HISTORIAL CLÍNICO

Dirección de Acceso: CALLE VALLDIGNA, N.19, Esc.E, 9-1
Playa de Gandia 46730 Valencia

Responsable del Fichero: ALEXANDRA ALEXANDROVA

Dirección de correo electrónico: svatok84@hotmail.com

Finalidad y Usos:
Un fichero para facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud. Destinado fundamentalmente a garantizar una asistencia adecuada al paciente.

Actividad de Tratamiento: MENORES

Dirección de Acceso: CALLE VALLDIGNA, N.19, Esc.E, 9-1
Playa de Gandia 46730 Valencia

Responsable del Fichero: ALEXANDRA ALEXANDROVA

Dirección de correo electrónico: svatok84@hotmail.com

Finalidad y Usos:
Gestión de los datos de menores.

Actividad de Tratamiento: TPV

Dirección de Acceso: CALLE VALLDIGNA, N.19, Esc.E, 9-1
Playa de Gandia 46730 Valencia

Responsable del Fichero: ALEXANDRA ALEXANDROVA

Dirección de correo electrónico: svatok84@hotmail.com

Finalidad y Usos:
Fichero que tiene como finalidad el uso del TPV para el cobro mediante tarjeta tanto de crédito como de débito del establecimiento.

2. Introducción

El Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta a al tratamiento de datos personales y la libre circulación de estos datos, (en adelante, "Reglamento Europeo de Protección de Datos" o "Reglamento General de Protección de Datos") así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y Garantía de los Derechos Digitales (LOPD-GDD), disponen la obligación del Responsable de las Actividades de Tratamiento de actuar de forma proactiva y adoptar todas las medidas de índole técnica y organizativas que garanticen la seguridad de los datos de carácter personal objeto de tratamiento y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. En concreto, es el artículo 32 de este Reglamento Europeo (refrendado por el art. 28 de la LOPD) el que obliga, tanto a los responsables como, en su caso, a los encargados de tratamiento, a adoptar estas medidas de manera que sean apropiadas para garantizar un nivel de seguridad adecuado al riesgo, siempre teniendo en cuenta "el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance y el contexto y los fines de tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas".

El Reglamento Europeo de Protección de Datos define en su artículo 4 los datos personales que quedarán sujetos a protección como "toda información sobre una persona física identificada o identificable. La persona a la que se refieren estos datos es el "interesado". En relación al concepto de "persona física identificable" se define por este Reglamento como aquella persona "cuya identidad pueda determinarse, directa o indirectamente, en particular, mediante un identificador, como por ejemplo, un nombre, un número de identificación, un identificador en línea o uno o varios elementos propios de la identidad física, fisológica, genética, psíquica, económica, cultural o social de dicha persona".

Este mismo artículo 4 del Reglamento define el tratamiento de datos personales como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

En el ejercicio de la actividad del Responsable se realizan operaciones que constituyen o pueden constituir alguna de las formas de tratamiento definidas por este artículo 4 del Reglamento respecto de datos personales, por lo que se elabora el presente documento-informe referente al Registro de Actividades de Tratamiento de Datos Personales de acuerdo con la obligación impuesta por el párrafo 5, del artículo 30 del Reglamento Europeo de Protección de Datos para organizaciones que cuenten con más de 250 trabajadores o realicen tratamientos de datos que puedan constituir un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos.

3. Objeto y finalidad del documento

Este documento de Registro de Actividades de Tratamiento da cumplimiento a la obligación establecida en el artículo 30 del Reglamento Europeo de Protección de Datos y el artículo 31 de la Ley Orgánica de Protección de Datos, conteniendo, entre otros aspectos, las medidas de seguridad de carácter técnico y organizativo que debe de aplicar la Organización.

Es obligación del responsable de las actividades de tratamiento la elaboración e implantación de la normativa de seguridad prevista en este documento, que además es de obligado cumplimiento para todo el personal con acceso a los datos de carácter personal y a los sistemas de información.

Este documento deberá mantenerse en todo momento actualizado y ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del tratamiento de los datos personales.

El contenido de este documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

4. Ámbito de aplicación y recursos protegidos

El ámbito de aplicación del presente Documento de Registro de Actividades de Tratamiento comprende los ficheros que contienen datos de carácter personal que se encuentran bajo la responsabilidad de ALEXANDRA ALEXANDROVA, incluyendo los sistemas de información, soportes y equipos empleados, departamentos, compartimentos, instalaciones y personal propio o ajeno que intervienen en el tratamiento y los locales en donde se ubican.

ALEXANDRA ALEXANDROVA, como Responsable de las Actividades de Tratamiento viene obligado a elaborar, implantar y actualizar este documento de obligado cumplimiento para todo el personal con acceso a los datos protegidos o a los sistemas de información que permiten el acceso a los mismos.

Todas las personas que tienen acceso a los datos personales se encuentran obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

El artículo 32 del Reglamento Europeo de Protección de Datos prevé para responsables y encargados de tratamiento la obligación de aplicar las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad adecuado a la probabilidad mayor o menor de riesgo en el tratamiento de dichos datos, e igualmente en función de la mayor o menor gravedad de las consecuencias para los derechos y libertades de los interesados en caso de fallo de seguridad que pueda permitir el acceso de terceros a sus datos personales o una transmisión no consentida de los mismos. La Ley Orgánica de Protección de Datos también deja en manos del responsable la determinación de las medidas concretas de protección que aplicará, dentro de las previsiones generales establecidas por el Reglamento y por la propia ley.

En este sentido, algunas de las medidas que el Reglamento Europeo propone van desde la seudonimización y el cifrado de datos personales, hasta la implementación de medidas que garanticen la confidencialidad, integridad, disponibilidad, resiliencia permanente de los sistemas y servicios de tratamiento, o la capacidad de restaurar la disponibilidad y el acceso a los datos en caso de incidencia física o técnica. Igualmente se exige la implementación de sistemas de control que permitan una verificación periódica del correcto funcionamiento de todas las medidas de seguridad en funcionamiento.

Para el Reglamento, es imprescindible tener en cuenta todos estos elementos desde el diseño de la política de protección de datos del responsable.

4.1. Alcance.

El responsable de las actividades de tratamiento y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en el Reglamento Europeo 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de esos

datos, así como a la Ley Orgánica de Protección de Datos en vigor que lo desarrolla, con independencia de cuál sea su sistema de tratamiento.

4.2. Recursos protegidos.

El Reglamento en su artículo 32, número 1.g) y número 2.d) establece que en el Registro de Actividades de Tratamiento se deberá incluir, entre otros aspectos, y cuando sea posible, la especificación detallada de los recursos protegidos a los que les son de aplicación las medidas de seguridad así como una descripción de las mismas. La protección de los datos frente a accesos no autorizados se deberá realizar mediante el control, a su vez, de todas las vías por las que se pueda tener acceso a dicha información.

4.2.1. Relación de actividades de tratamiento

Las actividades de tratamiento sobre recursos que contienen datos de carácter personal sujetos a las medidas de seguridad recogidas en este documento son las siguientes:

- CLIENTES POTENCIALES - (Riesgo Bajo, Trat. Mixto)
- CLIENTES Y/O PROVEEDORES - (Riesgo Bajo, Trat. Mixto)
- CONTACTOS AGENDA - (Riesgo Bajo, Trat. Mixto)
- CONTACTOS WHATSAPP - (Riesgo Bajo, Trat. Mixto)
- HISTORIAL CLÍNICO - (Riesgo Elevado o Muy Alto, Trat. Mixto)
- MENORES - (Riesgo Bajo, Trat. Mixto)
- TPV - (Riesgo Bajo, Trat. Mixto)

En el Anexo Relación de Actividades de Tratamiento se incluye la relación de actividades de tratamiento titularidad de la Organización y en el Anexo Estructura del tratamiento o de la base de datos su descripción, estructura y demás aspectos que lo configuran.

4.2.2. Centro de tratamiento

Los locales donde residen los sistemas de información involucrados en el tratamiento están ubicados en el domicilio del responsable de las actividades de tratamiento, indicado como dirección de acceso a los datos en el apartado Datos Generales de este documento. En el Anexo Recursos Protegidos constan relacionados los puestos de trabajo, su localización y descripción.

4.2.3. Inventario de recursos informáticos

Para un correcto control de los recursos informáticos, es necesario mantener un inventario actualizado de los equipos, sus correspondientes ubicaciones y las aplicaciones utilizadas. La relación del software y hardware empleado en el tratamiento se recoge en el Anexo Recursos protegidos y la descripción de los sistemas de información se encuentra en el Anexo Configuración y descripción del sistema de información. Los soportes utilizados para el almacenamiento, tratamiento o envío de los datos de carácter personal, se gestionan mediante la aplicación

informática de gestión de protección de datos personales de la organización y se pueden consultar en cualquier momento.

El Responsable deberá mantener actualizado el inventario de recursos informáticos en todo momento.

4.3. Personal

Las medidas de seguridad contenidas en el presente Registro de Actividades de Tratamiento son de aplicación a todo el personal involucrado en el tratamiento de datos de carácter personal.

El personal de la organización que en el desarrollo de sus funciones trate o acceda a datos de carácter personal deberá observar lo prevenido en este Registro de Actividades de Tratamiento.

La relación de personal autorizado se recoge en el Anexo Relación de personal autorizado del presente documento.

5. Medidas, normas, procedimientos, reglas y estándares de seguridad

5.1. Centros de tratamiento y locales

Los locales donde se encuentran los equipos informáticos que contienen los ficheros objeto de tratamiento deben disponer de las medidas de seguridad necesarias para garantizar la confidencialidad de los datos de carácter personal y su disponibilidad.

El tratamiento de datos fuera de los locales o centros de tratamiento habituales del responsable deberá realizarse, en la medida de lo posible, con idénticas garantías y medidas de seguridad que resultan aplicables en ellos.

En este sentido, el responsable adoptará las medidas oportunas para evitar el acceso a los datos por parte de terceros o la violación de seguridad de los mismos. Como mínimo, para todos aquellos casos en que los datos se trasladen a través de dispositivos portátiles se procederá a su encriptación o a la exigencia de contraseñas personales e intransferibles para el acceso a los archivos y carpetas informáticos en que se encuentren almacenados.

En aplicación de lo previsto en el artículo 33 del Reglamento Europeo de Protección de Datos, cualquier violación de la seguridad de los datos como consecuencia de la pérdida o sustracción de los dispositivos de almacenamiento (USB, ordenador portátil, etc.), o cualquier otra incidencia sobre estos o cualquier otro dispositivo que los contenga, tanto en la sede o local habitual del responsable como en su traslado o durante su uso en otros locales que no constituyan sede o local del responsable, deberá ser comunicado a la autoridad de control a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y libertades de las personas titulares de dichos datos.

5.1.1. Régimen de trabajo fuera de los locales del responsable o del encargado del tratamiento.

Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable o del encargado del tratamiento, el responsable deberá garantizar que se siguen aplicando todas las medidas de seguridad necesarias en cada caso para salvaguardar la confidencialidad de los datos y evitar el acceso a los mismos por parte de terceros.

La encriptación de datos, la seudonimización o el acceso a través de contraseñas de acceso de diferentes niveles, diseñadas siguiendo parámetros de contraseña segura, son medidas de seguridad que se utilizarán siempre que sea posible para evitar riesgos y para limitar las consecuencias negativas provocadas por situaciones de riesgo inevitables en que los datos puedan ser objeto de acceso no permitido.

En la relación de personal autorizado, se recogen las autorizaciones y el período de validez de las mismas.

5.2. Puestos de trabajo

Se considera como puestos de trabajo todo ordenador personal, terminal u otro dispositivo desde el que se pueda acceder a los datos en las situaciones siguientes:

- Cuando los datos personales se encuentren almacenados directamente en el equipo.
- Cuando los datos personales se encuentren almacenados en el servidor y desde el equipo correspondiente al puesto de trabajo se pueda acceder al servidor y a los datos.
- Cuando los datos personales se encuentren almacenados "en la nube" y se acceda a los mismos desde el equipo mediante la utilización de claves de acceso y contraseñas seguras.

Cada una de las personas autorizadas tendrá asignado un puesto de trabajo desde el que acceder a los datos por alguna de las vías indicadas o cualquier otra. El usuario asignado al puesto de trabajo será responsable de garantizar que la información a la que accede no podrá ser visualizada o comunicada a personas no autorizadas. Cualquier dispositivo conectado al puesto de trabajo tales como impresoras o pantallas deberán de estar ubicadas de forma que se garantice la confidencialidad de la información y que ésta no pueda ser visualizada o comunicada a personas no autorizadas.

El usuario responsable del puesto de trabajo, cuando finalice su turno o cuando se ausente temporalmente, deberá dejar los equipos y dispositivos en un estado que impida el acceso o la visualización de los datos protegidos a personas no autorizadas. Esto se podrá realizar mediante un protector de pantalla, la suspensión de la sesión de trabajo o la salida del sistema y apagado del equipo. La reanudación del trabajo implicará la desactivación de la pantalla protectora, el reinicio de la sesión o el encendido del equipo con la introducción del nombre de usuario y contraseña correspondiente en cada caso.

No deberá dejar en la impresora documentos impresos en la bandeja de salida que contengan datos de carácter personal. Si la impresora es compartida con otros usuarios no autorizados para acceder a los datos, el responsable de cada puesto de trabajo deberá retirar los documentos conforme vayan siendo impresos.

La configuración de los puestos de trabajo desde los que se tiene acceso a los datos sólo podrá ser cambiada con la autorización del Responsable de las Actividades de Tratamiento, el Delegado de Protección de Datos o el administrador del sistema designado.

Para reducir los niveles de riesgo sobre los datos, estas medidas de seguridad (cierre de sesión, desconexión, ...) deberán ser aplicadas por todo el personal del responsable muy especialmente cuando el acceso a los datos se realice a través de sistemas de almacenamiento en la nube a los que se acceda mediante conexión a internet desde cualquier equipo informático portátil o fijo, que no sea titularidad del responsable, y esté ubicado fuera de sus locales, por lo que resulte más difícil

comprobar si se han producido violaciones de seguridad o si son susceptibles de producirse en el futuro.

5.3. Identificación y autenticación del personal autorizado.

El responsable de las actividades de tratamiento establecerá un procedimiento que garantice la correcta identificación y autenticación de los usuarios autorizados a acceder a los sistemas de información.

Los accesos a los sistemas de información se realizarán mediante un mecanismo que permita la identificación de forma inequívoca y personalizada del usuario. Cada identificación deberá pertenecer a un único usuario.

Todos los usuarios autorizados para acceder a los datos personales, relacionados en el Anexo Relación de personal autorizado, deberán tener un código o nombre de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

5.3.1. Procedimiento de asignación y cambio de contraseñas.

El responsable de las actividades de tratamiento o la persona con autorización delegada por el responsable asignará un nombre de usuario y propondrá una contraseña para cada uno de los usuarios que, tras el primer acceso, vendrán obligados a cambiarlas.

Las contraseñas deberán constar de un mínimo de 8 dígitos y con una combinación de caracteres alfanuméricos. Se deberá evitar la utilización de nombre o cifras o su combinación que sean fácilmente deducibles.

Las contraseñas se almacenarán de forma ininteligible. El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

Las contraseñas son de carácter personal e intransferible y no serán visibles en pantalla cuando son introducidas.

Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder inmediatamente a su cambio.

Con una periodicidad de cada 3 meses y de forma automática, se propondrá a los usuarios, que cambien su contraseña por una nueva, volviendo a quedar almacenada de forma ininteligible.

El responsable de las actividades de tratamiento o el Administrador del sistema, en su caso, podrá cambiar los requisitos de acceso, las condiciones, modos sistemas y formas de tratamiento o de lectura cuando lo crea oportuno, notificando la decisión a los usuarios y dejando constancia de tal modificación en este documento y en el Registro de incidencias.

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos, y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al responsable de las actividades de tratamiento, o a la persona con autorización delegada por el responsable, y subsanada en el menor plazo de tiempo posible.

Para las Actividades de Tratamiento:

- HISTORIAL CLÍNICO

Quedará limitada la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. Tras 3 intentos fallidos de acceso quedará bloqueada la contraseña.

5.4. Control de Acceso

5.4.1. Control de acceso lógico

Para reducir al nivel mínimo los riesgos de acceso y tratamiento no permitido de datos personales, el responsable ha establecido un sistema de acceso a datos en que los miembros de la organización tendrán acceso única y exclusivamente a aquellos datos que les resulten imprescindibles para el desarrollo de sus funciones.

En el Anexo Relación de personal autorizado, se incluye una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

Si la aplicación informática que permite el acceso a los datos personales no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante la restricción y disponibilidad de recursos en la sesión del usuario con el control de acceso lógico mediante usuario y contraseña.

Queda prohibido que un usuario acceda a recursos con derechos distintos de los que ha sido autorizado.

En el caso de personal ajeno al responsable de las actividades de tratamiento que tenga acceso a los recursos estará sometido a las mismas condiciones y obligaciones de seguridad que el personal propio, constando en el Anexo Relación de personal autorizado.

Exclusivamente la persona con autorización delegada del responsable de las actividades de tratamiento podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el Responsable.

Para el caso de nuevas altas de accesos, se comunicará al Responsable por la persona con autorización delegada del responsable de las actividades de tratamiento, con la propuesta de acceso, código de acceso y listado de las funciones

del nuevo autorizado. De todo ello se deberá dejar constancia en este Registro de Actividades de Tratamiento en el Anexo Relación de personal autorizado.

5.4.2. Control de acceso físico

Exclusivamente el personal autorizado podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información correspondientes a las actividades de tratamiento siguientes:

- HISTORIAL CLÍNICO

El personal que tiene acceso a los lugares donde se hallan instalados los equipos físicos que dan soporte a los sistemas de información que tratan los datos personales, constan relacionados en el Anexo Relación de personal autorizado como personal afecto a las citadas actividades de tratamiento.

Para el personal del responsable de las actividades de tratamiento, distinto de los usuarios con acceso a los sistemas de información, como pueden ser de mantenimiento, limpieza, seguridad, etc., serán autorizados por el responsable, quien expedirá autorización o credencial que acredite su acceso autorizado.

Para el personal ajeno al responsable de las actividades de tratamiento, que le preste servicios sin acceso a datos personales, en el contrato de prestación de servicios deberá constar expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que pueda conocer con motivo de la prestación de servicios.

5.4.2.1. Registro de accesos

Para aquellos tratamientos sobre datos de carácter personal especialmente protegidos, clasificados con riesgo elevado o muy alto:

- HISTORIAL CLÍNICO

Deberá registrarse cada intento de acceso, la identificación del usuario, la fecha y hora en que se realizó, el tratamiento accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso fue autorizado, se guardará la información que permita identificar el registro accedido.

Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable sin que se deba permitir, en ningún caso, la desactivación ni la manipulación de los mismos.

El período mínimo de conservación de los datos del registro de accesos será de dos años.

El responsable revisará al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

Este registro de accesos no será necesario cuando concurran las siguientes circunstancias:

a) Que el responsable de las actividades de tratamiento sea una persona física.
b) Que el responsable de las actividades de tratamiento garantice que sólo él tiene acceso y trata los datos personales.

La concurrencia de estas dos circunstancias debe hacerse constar expresamente en este registro de actividades de tratamiento.

5.4.2.2. Acceso a la documentación

Para aquellos tratamientos que contienen datos de carácter personal especialmente protegidos, clasificados con riesgo elevado o muy alto:

- HISTORIAL CLÍNICO

El acceso a la documentación se limita exclusivamente al personal autorizado que consta en el Anexo Relación de personal autorizado.

Para los documentos que puedan ser utilizados por múltiples usuarios, se establecerán mecanismos que permitan identificar los accesos realizados.

El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en este registro de actividades de tratamiento.

5.5. Entorno de Sistema Operativo y de Comunicaciones

Al estar los datos ubicados en un ordenador (o con funciones de servidor) con un sistema operativo determinado y poder contar con unas conexiones que le comunican con otros ordenadores, es posible, para las personas que conozcan estos entornos, acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que pueda contar la aplicación. Se trata de un riesgo de seguridad para los datos.

El sistema operativo y de comunicaciones debe tener al menos un responsable o administrador.

En el caso más simple, cuando los datos se encuentren ubicados en un ordenador personal y se acceda mediante una aplicación local monopuesto, el administrador del sistema operativo podrá ser el mismo usuario que accede usualmente a dichos datos.

Ninguna herramienta o programa de utilidad que permita el acceso a los datos deberá ser accesible a ningún usuario o administrador no autorizado. Esto incluye cualquier medio de acceso en bruto no elaborado o editado a los datos que deberán estar bajo el control del administrador autorizado.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Si el ordenador en el que se ubican los datos está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso a los datos, el administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.

5.6. Gestión de soportes y documentos

5.6.1. Etiquetado e Inventario de soportes

Los soportes que contengan datos de carácter personal deben ser etiquetados para permitir su identificación, conocer de qué actividad de tratamiento se trata y el tipo de información que contienen y la fecha de creación.

Los soportes han de ser inventariados y almacenados en el almacén o almacenes de soportes que constan relacionados en el apartado *Almacenes* del Anexo Recursos protegidos. El acceso al almacén o almacenes estará restringido al personal autorizado para ello y que consta relacionado en el Anexo Relación de personal autorizado.

El inventario de soportes y su mantenimiento se gestiona mediante la aplicación informática de gestión de protección de datos personales de la organización y puede ser impreso en cualquier momento. El inventario deberá estar permanentemente actualizado.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el registro de actividades de tratamiento.

La identificación de los soportes que contengan datos de carácter personal que la organización considere especialmente sensibles se podrá realizar utilizando sistemas de etiquetado que serán comprensibles y con significado para los usuarios con acceso autorizado a los citados soportes y documentos y que dificulten la identificación para el resto de personas.

5.6.2. Salida de soportes y documentos

Es previsible que en el proceso de tratamiento de los datos personales llevado a cabo en esta organización, se produzca la salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anexos a un correo electrónico, fuera de los locales del responsable o encargado y bajo el control del responsable de las actividades de tratamiento.

Para evitar riesgos sobre los datos deberán aplicarse las medidas de seguridad necesarias para garantizar su confidencialidad y evitar accesos no permitidos a los mismos. En este sentido, los datos se transmitirán encriptados siempre que sea

posible, o sólo podrán visualizarse mediante el acceso a través de nombre de usuario y contraseña.

En caso de producirse alguna incidencia sobre los datos el sistema debería detectarla lo antes posible para evitar el uso indebido de los mismos.

Con respecto a los documentos también se consideran incluidos en la salida de documentos los siguientes supuestos:

- Envío por correo electrónico en el cuerpo del mensaje o como adjuntos datos objeto de tratamiento.
- Los faxes cuando incorporan datos objeto de tratamiento.
- Cualquier otro procedimiento electrónico como ftp, descargas desde la web o carpetas compartidas, sistemas de almacenamiento en la nube, etc.

Como medida de seguridad preventiva, el responsable incorporará en este documento toda la información necesaria para conocer quiénes son las personas que tienen acceso a las diferentes formas de tratamiento y las medidas de seguridad que están obligadas a aplicar en cada una de ellas. En la medida de lo posible, el sistema almacenará como mínimo los últimos accesos para detectar irregularidades lo antes posible y prevenir riesgos en el acceso no autorizado a los datos así como su limitación lo antes posible en caso de producirse.

En el caso del correo electrónico para garantizar la trazabilidad de los datos que salen materialmente del sistema de información, puede servir como registro el propio sistema de indexación del gestor del correo electrónico.

5.6.3. Traslado de soportes y documentación

En el traslado de la documentación se adoptarán las medidas y procedimientos apropiados para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte. En este sentido, se utilizarán sistemas de encriptado siempre que sea posible, o como mínimo, la exigencia de contraseñas seguras para el acceso a los datos.

En el caso de la documentación, las personas encargadas de su custodia extremarán al máximo las medidas de prevención para evitar accesos no autorizados. Sólo será objeto de transporte la documentación en que figuren datos personales cuando sea imprescindible. Como medida de prevención de riesgos, y siempre que ello sea posible, se recurrirá a la seudonimización como garantía de confidencialidad de los datos durante su traslado en papel.

5.6.3.1. Traslado de documentación

El traslado de la documentación de las actividades de tratamiento:

- HISTORIAL CLÍNICO

Siempre que se proceda al traslado físico de la documentación, deberán adoptarse las medidas apropiadas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

5.6.4. Destrucción y borrado de documentos o soportes

Los documentos y soportes que vayan a ser desechados correspondientes a los tratamientos:

- CLIENTES POTENCIALES - (Riesgo Bajo, Trat. Mixto)
- CLIENTES Y/O PROVEEDORES - (Riesgo Bajo, Trat. Mixto)
- CONTACTOS AGENDA - (Riesgo Bajo, Trat. Mixto)
- CONTACTOS WHATSAPP - (Riesgo Bajo, Trat. Mixto)
- HISTORIAL CLÍNICO - (Riesgo Elevado o Muy Alto, Trat. Mixto)
- MENORES - (Riesgo Bajo, Trat. Mixto)
- TPV - (Riesgo Bajo, Trat. Mixto)

Aquellos soportes que se vayan a reutilizar deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables de ningún modo. No será válido el borrado lógico o rápido que impide el acceso a la información pero no la elimina físicamente hasta que ha sobrescrito sobre la misma.

Los soportes que se vayan a eliminar deberán ser borrados físicamente antes de su eliminación, que consistirá en un proceso de destrucción mecánica del soporte, trituración o incineración.

Los documentos en formato papel que vayan a desecharse, deberá procederse a su destrucción mediante la trituradora de papel. Está prohibida la reutilización de documentos en formato papel.

Los procesos de reutilización y eliminación descritos han de ser previos a la preceptiva baja de los soportes en el inventario.

5.6.5. Registro de Entrada y Salida de soportes

Deberán ser registradas las salidas y entradas de soportes correspondientes a las actividades de tratamiento:

- HISTORIAL CLÍNICO

El registro de entrada de soportes indicará el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

El registro de salida de soportes indicará el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

El procedimiento de registro de entradas y salidas de soportes se gestiona mediante el programa por persona autorizada y puede ser impreso o no como Anexo de este registro de actividades de tratamiento.

5.6.6. Gestión y distribución de soportes

La gestión y distribución de soportes que contengan datos de carácter personal de las actividades de tratamiento:

- HISTORIAL CLÍNICO

La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido y que dificulten la identificación para el resto de personas.

La distribución de los soportes se realizará cifrando los datos que contengan o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Los dispositivos portátiles cuando se encuentren fuera de las instalaciones que están bajo control del responsable de las actividades de tratamiento, deberán cifrar los datos que contengan.

En caso que se requiera el uso de **dispositivos portátiles que no permiten el cifrado**, debe especificar el motivo de su uso y adoptar las medidas de seguridad necesarias que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

5.7. Ficheros temporales o copias de trabajo de documentos

Los ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir igualmente con las medidas de seguridad que correspondan.

Como medida de prevención de riesgos, los ficheros temporales o copias de documentos así creados serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

Lo anterior, incluye los ficheros temporales que utilicen y generen las aplicaciones de acceso al Fichero.

Las copias de trabajo de documentos en formato papel, deberá procederse a su destrucción mediante la trituradora de papel. Está prohibida la reutilización de documentos o copias de trabajo en formato papel.

El Responsable de las Actividades de Tratamiento o, en su caso, el Delegado de Protección de Datos, deberá asegurarse de que los ficheros temporales o copias de trabajo de documentos no son accesibles por personal no autorizado.

5.8. Transmisión de datos por redes de Telecomunicaciones

- HISTORIAL CLÍNICO

La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

5.9. Copias de seguridad

Es obligatorio establecer procedimientos de actuación para la realización de copias de respaldo periódicas, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Los procedimientos para la recuperación de los datos deben garantizar en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción como vía para restaurar su disponibilidad y el acceso a los datos personales de forma rápida en caso de incidencia física o técnica, de acuerdo con los previsto en el artículo 32 del Reglamento Europeo de Protección de Datos.

5.9.1. Procedimiento de realización de copias de respaldo.

Las copias de seguridad deben de realizarse como mínimo con una periodicidad semanal, cada viernes o último día laborable de la semana. El soporte magnético que las almacena dispondrá de toda la información del sistema.

Las copias han sido planificadas de tal manera que no habrá una intervención de ningún operador para esta rutina. La misión del operador de copias tendrá como trabajo principal:

- Comprobación de la copia semanal.
- Cambio de soporte.
- Verificación de la copia semanal.

La copia se entregará al Responsable o persona designada por éste, quien deberá entregar la más antigua que tenga, estableciendo así un sistema de rotación de soportes.

En caso de que cualquiera de las copias no se efectuara correctamente, se debería de editar el informe que genera la aplicación de backup y proceder a repetir la copia manualmente o informar al responsable del sistema.

5.9.2. Recuperación de datos

Los procedimientos para la recuperación de los datos deben garantizar en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

En caso de fallo del sistema con pérdida total o parcial de los datos existirá un procedimiento, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban al tiempo de producirse la pérdida o destrucción. De esta manera se reducen los efectos negativos generados por las incidencias que puedan afectar a los datos.

Únicamente respecto de los tratamientos parcialmente automatizados siguientes:

- CLIENTES POTENCIALES
- CLIENTES Y/O PROVEEDORES
- CONTACTOS AGENDA
- CONTACTOS WHATSAPP
- HISTORIAL CLÍNICO
- MENORES
- TPV

Siempre que exista documentación que permita alcanzar la recuperación de los datos al estado en que se encontraban al tiempo de producirse la pérdida o destrucción, se procederá a grabar manualmente los datos quedando constancia motivada de este hecho en el registro de incidencias.

5.9.3. Verificación de los procedimientos de copia y recuperación de datos

El responsable o la persona con autorización delegada del responsable de las actividades de tratamiento verificará cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos.

5.9.4. Pruebas con datos reales

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten datos de carácter personal no se realizarán con datos reales, salvo que previamente se haya realizado una copia de seguridad y se aseguren las medidas de seguridad correspondientes al tratamiento realizado y se anote su realización en este registro de actividades de tratamiento.

De las pruebas realizadas conforme al párrafo anterior, deberá quedar constancia en el registro de incidencias.

5.9.5. Almacenamiento de las copias de respaldo

Las copias de respaldo y recuperación se encuentran almacenadas en el almacén o almacenes que constan relacionados en el apartado *Almacenes* del Anexo Recursos Protegidos.

Sobre estos almacenes se aplicarán las medidas de seguridad necesarias para evitar riesgos de accesos no autorizados y disminuir al mínimo las consecuencias de éstos en caso de producirse.

5.9.6. Copia de respaldo en lugar diferente

Se conservará una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir las medidas de seguridad, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

5.10. Criterios de archivo

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición.

En aquellos casos en los que no exista norma aplicable, el responsable de las actividades de tratamiento deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

5.11. Dispositivos de almacenamientos

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquellos no permitan adoptar esta medida, el responsable de las actividades de tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

5.11.1. Custodia de soportes

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento indicados en el apartado anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

5.11.2. Almacenamiento de la información

Los armarios, archivadores u otros elementos en los que se almacenan los ficheros no automatizados con datos de carácter personal se encuentran en el almacén o almacenes que constan relacionados en el apartado *Almacenes* del Anexo Recursos Protegidos, en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos.

Si, atendidas las características de los locales de que dispusiera el responsable de las actividades de tratamiento, no fuera posible cumplir lo establecido en el apartado

anterior, se adoptarán las medidas alternativas que, debidamente motivadas, se incluirán en el registro de actividades de tratamiento.

5.11.3. Copia o reproducción

La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el registro de actividades de tratamiento.

Las copias o reproducciones desechadas deberán ser destruidas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior. Se procederá a su destrucción mediante la trituradora de papel.

5.12. Procedimiento de notificación, registro, gestión y respuesta ante las incidencias

5.12.1. Definición

Una incidencia es “cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos”, es decir, a la confidencialidad, integridad y disponibilidad de los datos. Cualquier situación o hecho que pueda poner en peligro la confidencialidad o integridad de los datos durante su tratamiento o durante el almacenamiento que posibilite su tratamiento se considera una incidencia.

5.12.2. Procedimiento

Todo usuario que tenga conocimiento de una incidencia será responsable del registro de la misma en el registro de Incidencias o en su caso de la comunicación por escrito a ALEXANDRA ALEXANDROVA o a la persona con autorización delegada del responsable de las actividades de tratamiento.

El conocimiento y la no notificación o registro de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del tratamiento por parte de ese usuario.

La notificación o registro de una incidencia deberá constar al menos de los siguientes datos: tipo de incidencia, fecha y hora en que se produjo, en su caso, detectado, la persona que realiza la notificación, persona a quien se le comunica, efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Junto a esa gestión interna, y en cumplimiento de la obligación impuesta por el artículo 33 del Reglamento Europeo de Protección de Datos, en caso de violación de la seguridad de los datos personales, el responsable de tratamiento lo notificará a la autoridad de control sin dilación indebida, y siempre antes de que transcurran 72 horas de que haya tenido constancia de la misma. En caso de incumplirse este plazo, la notificación incorporará además las causas justificantes de este retraso.

El Reglamento excluye de la obligación de notificar esta violación únicamente en el caso de que sea improbable que la misma constituya un riesgo para los derechos y las libertades de las personas físicas.

Cuando el encargado de tratamiento tenga conocimiento de la existencia de violaciones de seguridad de datos personales, deberá ponerlo en conocimiento del responsable lo antes posible.

De acuerdo en el apartado 3 del artículo 33 del Reglamento Europeo, la notificación contemplada en el apartado 1 deberá, como mínimo: a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados; b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información; c) describir las posibles consecuencias de la violación de la seguridad de los datos personales; d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si además el responsable observa que esta violación de seguridad de los datos entraña un alto riesgo para los derechos y libertades de las personas físicas, deberá comunicarle a los interesados la incidencia producida lo antes posible, de manera que éstos puedan adoptar las medidas necesarias para reducir los riesgos de uso indebido o transmisión a terceros de los datos sobre los que se ha producido el acceso.

Según lo previsto en el artículo 34 del Reglamento Europeo, esta comunicación al interesado no será necesaria si concurre alguna de las condiciones siguientes: a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado; b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado; c) la comunicación suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

A pesar de que el responsable pueda considerar que no es necesaria la comunicación de la incidencia al interesado por concurrir alguna de estas condiciones, la comunicación será necesaria de acuerdo con el artículo 34.4 si así lo ordena la autoridad de protección de datos competente a la que se le ha comunicado previamente.

5.12.3. Registro de incidencias

El registro de incidencias se gestiona mediante la aplicación informática de gestión de protección de datos personales de la organización, concretamente en el módulo o apartado de "Gestión de Incidencias".

5.12.4. Registro de incidencias

En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten a los tratamientos:

- HISTORIAL CLÍNICO

Cuando para la resolución de la incidencia se requiera realizar una recuperación de datos, deberá consignarse, además:

- Los procedimientos realizados de recuperación de los datos.
- La persona que ejecutó el proceso.
- Los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
- Autorización para la ejecución de los procedimientos de recuperación de los datos de ALEXANDRA ALEXANDROVA o de la persona con autorización delegada del responsable de las actividades de tratamiento.

5.13. Revisión del documento

Este documento deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información objeto de tratamiento o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

El responsable o la persona con autorización delegada del responsable de las actividades de tratamiento, junto con el delegado de protección de datos, si es el caso, mantendrán una reunión cada vez que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información objeto de tratamiento, con el objetivo de coordinar los cambios a introducir en el Registro de Actividades de Tratamiento, elevando conclusiones al responsable de las actividades de tratamiento.

Igualmente el presente documento deberá actualizarse cada vez que se detecten nuevos riesgos en el tratamiento de los datos o se modifique su nivel de probabilidad o gravedad, de manera que se hayan de reflejar igualmente las nuevas medidas de seguridad implementadas para eliminar dichos riesgos o reducir su incidencia o consecuencias negativas sobre los derechos y libertades de los interesados.

5.14. Procedimiento de control del cumplimiento

Deben establecerse controles periódicos para verificar el cumplimiento de lo

dispuesto en el Registro de Actividades de Tratamiento.

- Verificar el inventario de hardware y software.
- Cumplimiento de la política general de seguridad.
- Registro de incidencias.
- Variaciones en el conjunto de actividades de tratamiento.
- Cumplimiento de la política de protección de datos.
- Verificar clasificación de datos.
- Comprobar configuración del sistema.
- Comprobar la relación de personal y accesos autorizados.
- Verificar procedimiento de gestión de soportes.
- Verificación procedimientos de identificación y autenticación.
- Se cumple el proceso de copias de respaldo y recuperación.
- Verificar prestaciones de servicios con acceso y sin acceso a datos.
- Verificar contratos de encargo de tratamiento.
- Verificar contratos de confidencialidad y prestación servicios sin acceso a datos.
- Variaciones en la legislación.

6. Funciones y obligaciones del personal

Todas las personas que tienen acceso a los datos se encuentran obligadas por ley a cumplir lo establecido en este documento. El personal afectado por esta normativa lo podemos clasificar como sigue:

1. **Administradores**, disponen de los máximos privilegios y están encargados de administrar o mantener el entorno operativo de los Equipos del Responsable.

2. **Personal Informático**, encargados de mantener los sistemas de información y resolver las incidencias en máquinas y programas.

3. **Usuario**, acceden a los datos a nivel de usuario.

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información han de estar claramente definidas y documentadas. En el Anexo Relación de personal autorizado se relacionan.

6.1. Funciones y obligaciones con carácter general

Todo el personal interno o externo de la empresa que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar al responsable de las actividades de tratamiento o al delegado de protección de datos las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este documento, y en concreto en su apartado Medidas, normas, procedimientos, reglas y estándares de seguridad.

Todas las personas deberán guardar el debido secreto y confidencialidad de los datos personales que conozcan en el desarrollo de su trabajo.

6.2. Funciones y obligaciones del Responsable

El responsable de las actividades de tratamiento es el encargado jurídicamente de la seguridad de los datos y de las medidas establecidas en el presente documento. El responsable implantará las medidas de seguridad establecidas en él y adoptará las medidas necesarias para que el personal afectado por este documento conozca las normas que afecten al desarrollo de sus funciones.

El responsable de las actividades de tratamiento es ALEXANDRA ALEXANDROVA en la persona de ALEXANDRAALEXANDROVA en calidad de representante legal de la empresa.

6.2.1. Ámbito

Decide sobre la finalidad, contenido, usos y aplicaciones de las actividades de tratamiento: CLIENTES POTENCIALES, CLIENTES Y/O PROVEEDORES, CONTACTOS AGENDA, CONTACTOS WHATSAPP, HISTORIAL CLÍNICO, MENORES, TPV y responde de su legalidad y legitimación, de acuerdo con lo dispuesto en el Reglamento Europeo 2016/679, relativo al tratamiento de datos personales, la Ley Orgánica de Protección de Datos, y las instrucciones y recomendaciones de la Agencia de Protección de Datos y normativa relacionada. Es el responsable de cumplir los requisitos exigidos en la legislación vigente para garantizar los derechos de los afectados (acceso, rectificación, supresión, limitación de tratamiento, portabilidad y oposición). Responde frente al afectado, frente a terceros y frente a la Administración de todos los daños y perjuicios que se deriven del mal uso de los datos.

Coordinará la puesta en marcha de las medidas de seguridad y cuidará de la difusión de las mismas entre todos los miembros de la organización, controlando su cumplimiento por los usuarios.

De acuerdo con el artículo 24 del Reglamento Europeo de Protección de Datos, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

En aplicación de las obligaciones que le impone el artículo 25 del mismo texto legal, el responsable, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, diseñará las medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, o como la minimización de datos, de manera que queden integradas las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del Reglamento y proteger los derechos de los interesados.

En concreto, también impone el Reglamento al responsable del tratamiento en ese artículo 25 la obligación de aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

6.2.2. Finalidad del Tratamiento

El Responsable de las Actividades de Tratamiento decide sobre la finalidad del tratamiento.

6.2.3. Usos de los Datos

El uso es confidencial e intransferible. Los datos en él contenidos serán utilizados por ALEXANDRA ALEXANDROVA, a través de su personal designado propio o externo, cumpliendo en todo momento las medidas de seguridad y los requisitos exigidos para su legitimación y legalidad en su tratamiento.

6.2.4. Funciones

- Decidir sobre la finalidad, contenido y uso del tratamiento.
- Diseñar e implementar las medidas técnicas y organizativas en materia de protección de datos tendentes de eliminar o reducir los riesgos de uso o acceso indebido a los mismos, así como a reducir las consecuencias negativas que puedan producirse como consecuencia de un uso o acceso indebido a los mismos.
- Realizar el control del tratamiento, calidad y seguridad de los datos.
- Controlar la gestión de soportes informáticos que contienen datos de carácter personal.
- Gestionar y dirigir los procedimientos de acceso, rectificación, supresión, limitación de tratamiento, portabilidad y oposición de los afectados y resolverlos en el plazo legalmente previsto.
- Proceder al bloqueo de los datos en los casos en que, siendo procedente su cancelación, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado.
- Elaborar el Registro de Actividades de Tratamiento.
- Encargarse de que exista una relación actualizada de usuarios con acceso autorizado a los sistemas de información.
- Establecer los procedimientos de identificación y autenticación para dicho acceso.
- Establecer los mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
- Establecer los procedimientos de realización de copias de respaldo y recuperación de datos.
- Encargarse de forma directa o por delegación del cumplimiento efectivo de la normativa sobre Protección de Datos en la organización, garantizando la difusión y conocimiento de este Documento entre todo el personal.
- Implantar las medidas de seguridad establecidas en este documento.
- Mantener este Documento actualizado en todo momento, debiendo revisarse siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo y adecuar su contenido a las disposiciones vigentes en materia de seguridad de datos.
- Garantizar los bienes jurídicos y recursos protegidos.
- Notificar a la autoridad de protección de datos competente, y en su caso, también al interesado, de las violaciones de seguridad de los datos que se hayan producido, cuando sea obligatorio de acuerdo con lo previsto por el artículo 33 del Reglamento Europeo de Protección de Datos.

6.2.5. Obligaciones

6.2.5.1. Legitimación para el tratamiento de los datos

Cumplir todos los requisitos legales y reglamentarios para **obtener el consentimiento del afectado** para que los datos puedan ser ingresados, tratados, guardados, transmitidos, manipulados, cedidos y/o cancelados por el responsable de las actividades de tratamiento o aquel a quien se haya destinado para cada forma de tratamiento.

Velar para que la recogida de datos de carácter personal se realice cumpliendo con todos los requisitos legales, especialmente el derecho de información y la obtención del consentimiento inequívoco del afectado.

6.2.5.2. Control de las entradas

Consiste en mantener el sistema de archivo de las fichas o formularios con los datos personales del afectado y su consentimiento, bajo control exclusivo del Responsable de las Actividades de Tratamiento.

Sólo se incluirán en el tratamiento los datos obtenidos mediante las fichas o formularios que estén amparados por la firma del interesado. En la documentación de la aplicación de gestión de protección de datos de la organización vienen diversos modelos que deberán adaptarse previamente.

6.2.5.3. El mantenimiento actualizado de los datos

Los datos de carácter personal deben de estar siempre actualizados, deben ser exactos y responder con veracidad a la situación actual del afectado. Si los datos registrados son o devienen inexactos en todo o en parte, o incompletos han de ser cancelados o sustituidos de oficio por los correspondientes rectificados o completados. Tampoco han de mantenerse datos que hayan dejado de ser necesarios o pertinentes para la finalidad para la que fueron recabados.

6.2.5.4. Encargados de tratamiento externos

En el caso de que existan encargados de tratamiento externos, se deberá formalizar la relación con éstos de acuerdo con lo establecido en el artículo 28 del Reglamento Europeo de Protección de Datos y en la Ley Orgánica de Protección de Datos. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito.

6.2.5.5. Entorno de Sistema Operativo y de Comunicaciones

Designar al administrador que se responsabilizará del sistema operativo y de comunicaciones que deberá estar relacionado en el Anexo Relación de personal autorizado.

En el caso más simple, como es que los datos están ubicados en un ordenador personal y accedidos mediante una aplicación local monopuesto, el administrador del sistema operativo podrá ser el mismo usuario que accede usualmente a dichos datos.

6.2.5.6. Sistema Informático o aplicaciones de acceso

Se encargará de que los sistemas informáticos de acceso a los datos personales tengan su acceso restringido mediante un código de usuario y una contraseña.

Asimismo cuidará que todos los usuarios autorizados para acceder a los datos, relacionados en el Anexo Relación de personal autorizado, tengan un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

6.2.5.7. Salvaguarda y protección de las contraseñas personales

El responsable de las actividades de tratamiento deberá mantener actualizada la relación de usuarios con acceso autorizado al sistema de información y establecer los procedimientos de identificación y autenticación para este acceso.

El responsable de las actividades de tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

Sólo las personas relacionadas en el Anexo Relación de personal autorizado podrán tener acceso a los datos.

6.2.5.8. Gestión de incidencias

Habilitará un Libro de Incidencias a disposición de todos los usuarios y administradores con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad de los datos.

Analizará las incidencias registradas, tomando las medidas oportunas en cada caso.

En caso de incidencia que pueda suponer una violación de seguridad de los datos, el responsable deberá comunicarlo a la autoridad de control a la mayor brevedad, y como máximo en el plazo de 72 horas desde que tuvo conocimiento de la misma, salvo que considere que es improbable que dicha violación de seguridad constituya un riesgo para los derechos y libertades de las personas físicas.

También se deberá notificar esta incidencia al interesado cuando sea probable que la violación de seguridad de los datos entrañe ese alto riesgo para los derechos y libertades de las personas físicas.

El responsable viene obligado a documentar cualquier violación de seguridad de los datos personales en el registro de incidencias, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.

6.2.5.9. Gestión de soportes

La salida de soportes informáticos que contengan datos personales fuera de los locales del Responsable deberá ser comunicada al Responsable de las Actividades de Tratamiento.

6.2.5.10. Procedimientos de respaldo y recuperación

El responsable de las actividades de tratamiento se encargará de verificar la definición y correcta aplicación de las copias de respaldo y recuperación de los datos.

6.3. Funciones y obligaciones que afectan a todo el personal

6.3.1. Con carácter general

Tratar los datos de carácter personal de conformidad con lo que se establece en la legislación vigente y en este Registro de Actividades de Tratamiento, accediendo a estos únicamente cuando sea necesario para el desarrollo de sus funciones.

Mantener el secreto profesional respecto de los datos de carácter personal que conozcan y custodiarlos. Esta obligación perdurará después de finalizar las relaciones con el responsable de las actividades de tratamiento.

Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal.

Cumplir lo dispuesto en la normativa interna vigente en cada momento.

Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento, que podrían derivar en sanciones.

Comunicar al responsable de las actividades de tratamiento, en el mismo día, cualquier solicitud de ejercicio por parte de los afectados de los derechos de acceso, rectificación, supresión, limitación de tratamiento, portabilidad y oposición, así como cualquier incidencia que conozca sobre la confidencialidad e integridad de los datos.

6.3.2. Puestos de trabajo

El usuario autorizado será el responsable de su puesto de trabajo, garantizando que la información que disponga o muestre su equipo no podrá ser accesible o visible por personas no autorizadas.

Procurará que la disposición de pantallas e impresoras u otros dispositivos de su puesto de trabajo se ubiquen de forma que garanticen la confidencialidad y no sea accesible o visible su contenido por personas no autorizadas.

Al abandonar su puesto de trabajo, aún temporalmente, deberá dejarlo en un estado que impida el acceso o la visualización de los datos protegidos, mediante un

protector de pantalla o la salida del sistema y apagado del equipo. La reanudación del trabajo implicará la desactivación de la pantalla protectora o el encendido del equipo con la introducción del nombre de usuario y contraseña correspondiente en cada caso.

No deberá dejar en la impresora documentos impresos en la bandeja de salida que contengan datos protegidos. Si la impresora es compartida con otros usuarios no autorizados para acceder a los datos, el responsable de cada puesto de trabajo deberá retirar los documentos conforme vayan siendo impresos.

La configuración de los puestos de trabajo desde los que se tiene acceso a los datos sólo podrá ser cambiada con la autorización del Responsable de las Actividades de Tratamiento.

6.3.3. Salvaguarda y protección de las contraseñas personales

Todo usuario es responsable de mantener la confidencialidad de su contraseña. Si la contraseña es conocida por otra persona, el usuario deberá registrarlo como incidencia y notificarlo al Responsable de las Actividades de Tratamiento, para proceder a su cambio.

6.3.4. Gestión de incidencias

El usuario que tenga conocimiento de una incidencia deberá de ponerlo en conocimiento del Responsable de las Actividades de Tratamiento y registrarla siguiendo el procedimiento establecido para el registro de incidencias.

El conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad de los Datos por parte de ese usuario.

Todos los miembros de la organización deben conocer la obligación del responsable de notificar las violaciones de seguridad de los datos a la autoridad de control, por lo que han de ser conocedores de su obligación de comunicar a la mayor brevedad al responsable de cualquier incidencia sobre los datos que llegue a su conocimiento y que pueda poner en peligro los derechos y libertades de los ciudadanos en este ámbito.

6.3.5. Gestión de soportes

Los soportes informáticos que contengan datos personales han de estar claramente identificados con una etiqueta externa que indique la actividad de tratamiento, tipo de datos y fecha de creación.

Los soportes que sean reutilizables, y que hayan contenido copias de datos personales, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

Los soportes que contengan datos personales deberán ser almacenados en lugares a los que no tengan acceso personas que no figuren relacionadas en el Anexo Relación de personal autorizado.

La salida de equipos o soportes fuera de las instalaciones requiere la autorización del Responsable de las Actividades de Tratamiento.

Seguir los procedimientos establecidos de gestión y distribución de soportes y observar las autorizaciones precisas en cada caso.

6.3.6. Correo electrónico

No utilizar el correo electrónico u otros medios de comunicación interna o con el exterior para transmitir mensajes que contengan o lleven adjuntos datos de carácter personal que por sus características, volumen o destinatarios puedan poner en peligro la confidencialidad o la integridad de los datos.

Atenerse a los procedimientos establecidos y observar las autorizaciones precisas.

6.3.7. Transferencias de datos

No realizar transferencias con datos de carácter personal entre sistemas o descargas en equipos salvo en aquellos casos expresamente autorizados, y protegiendo después los contenidos para evitar la difusión o copias no autorizadas.

6.3.8. Tratamiento fuera de los locales del responsable

Proteger la confidencialidad e integridad de los datos personales de la entidad que excepcionalmente tuvieran que almacenarse o usarse fuera del lugar de trabajo: en casa del cliente, en el propio domicilio o en otras instalaciones alternativas tanto en sistemas fijos como en portátiles.

Siempre que sea posible, se encriptarán los datos personales o se protegerán mediante contraseña segura.

6.4. Funciones y obligaciones del administrador del sistema y personal informático.

Siempre será posible conocer el personal que intervino con posterioridad a la intervención, dejando constancia de ello, identificando al personal técnico, anotándolo en el Registro de Incidencias.

6.4.1. Funciones

Administradores: Tienen acceso con el máximo privilegio al software del sistema y a las herramientas necesarias para la realización de las actividades de tratamiento. Resuelven las incidencias que surjan y gestionan l

Personal Informático: Resolver las incidencias que surjan en las redes y comunicaciones corporativas y efectuar el mantenimiento de máquinas y programas.

Usuario: Acceso a datos a nivel de usuario.

6.4.2. Obligaciones

6.4.2.1. Entorno de sistema operativo y de Comunicaciones

Cuidar de que ningún usuario no autorizado en el Anexo Relación de personal autorizado disponga de herramienta o programa que le permita el acceso a los datos.

Guardar en lugar protegido las copias respaldo y recuperación, evitando el acceso a las mismas de persona no autorizada.

Asegurarse de que personal no autorizado pueda tener acceso a los datos protegidos.

Impedir el acceso remoto de personas no autorizadas al equipo donde estén ubicados los datos, especialmente si se encuentra integrado en una red de comunicaciones.

6.4.2.2. Sistema Informático o aplicaciones de acceso a los datos

Si la aplicación informática que permite el acceso a los datos no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de código de usuario y contraseña.

6.4.2.3. Salvaguarda y protección de las contraseñas personales

Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el punto *Identificación y autenticación del personal autorizado* del Apartado Medidas, normas, procedimientos, reglas y estándares de seguridad. Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas, y será responsabilidad del administrador del sistema.

El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

6.4.2.4. Procedimientos de respaldo y recuperación

Obtener periódicamente una copia de seguridad del fichero, que garantice su reconstrucción en el estado en que se encontraba al tiempo de producirse la pérdida o destrucción.

Realizar la copia de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Comprobar y actualizar el procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos al estado en que se encontraban en el momento del fallo.

7. Principios de la Política de Protección de Datos

La implantación de la política de Protección de Datos de Carácter Personal debe de involucrar a todo el personal de la organización con acceso al Tratamiento. El Responsable de las Actividades de Tratamiento tomará las medidas oportunas para el conocimiento de todo el personal con acceso de los principios básicos que deben de regir la política de protección de datos.

7.1. Tratamiento

Los datos han de ser tratados de manera lícita, leal y transparente en relación con el interesado.

Los datos han de ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

7.2. Conservación

Los datos deben ser conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

7.3. Principio de Calidad de los Datos

Los datos que se recaban de los interesados han de ser adecuados y pertinentes y no excesivos respecto a la finalidad determinada para la que se hayan obtenido. No podrán utilizarse para finalidades distintas por las que se recogieron. Los datos deben estar almacenados de forma que permitan el ejercicio del derecho de acceso. En ningún caso se podrán utilizar para su recogida medios fraudulentos, desleales o ilícitos.

Los datos deben ser exactos y puestos al día y en caso de no ser así, deben ser cancelados o sustituidos de oficio. Los datos personales siempre deben responder con veracidad a la situación actual del afectado. Tampoco podrán mantenerse los datos personales en el fichero cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

7.4. Principio de Información

Los artículos 13 y 14 del Reglamento Europeo de Protección de Datos, y el artículo 11 de la Ley Orgánica 3/2018, de Protección de Datos, recogen este principio de acuerdo con las siguientes previsiones.

Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación, salvo que el interesado ya la tenga:

- la identidad y los datos de contacto del responsable y, en su caso, de su representante;

- los datos de contacto del delegado de protección de datos, en su caso;
- los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
- cuando el tratamiento se base en el artículo 6, apartado 1, letra f), del Reglamento, los intereses legítimos del responsable o de un tercero;
- los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
- en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión en relación a las garantías aportadas por ese territorio.

Además de esta información, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

- el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
- la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
- la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada, en los casos en que resulte aplicable;
- el derecho a presentar una reclamación ante una autoridad de control;
- si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos;
- la existencia de decisiones automatizas, incluida la elaboración de perfiles, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente.

Cuando los datos personales no se hayan obtenido del interesado, el responsable del tratamiento le facilitará la siguiente información:

- la identidad y los datos de contacto del responsable y, en su caso, de su representante;
- los datos de contacto del delegado de protección de datos, en su caso;
- los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;
- las categorías de datos personales de que se trate;

- los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
- en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, sobre las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.

Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

- el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;
- cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;
- la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
- cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;
- el derecho a presentar una reclamación ante una autoridad de control;
- la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;
- la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

El responsable del tratamiento facilitará toda esta información:

- dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;
- si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o
- si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente.

Estas previsiones de obligación de información no serán aplicables cuando y en la medida en que:

- el interesado ya disponga de la información;
- la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;
- la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o
- cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

7.5. Principio de Consentimiento

De acuerdo con el artículo 6 del Reglamento Europeo de Protección de Datos, se requerirá el consentimiento del interesado para el tratamiento de sus datos personales con uno o varios fines específicos, salvo que dicho tratamiento se fundamente en alguna otra previsión legal.

7.6. Seguridad de los datos

Los datos deben ser tratados de manera que se garantice su seguridad y queden protegidos contra el tratamiento no autorizado o ilícito, y contra su pérdida, alteración, daño accidental o tratamiento o acceso no autorizado. El responsable aplicará las medidas organizativas y técnicas necesarias para conseguir estos objetivos.

Todo el personal de la organización con funciones de acceso a los datos, deberá poner en conocimiento del responsable de las actividades de tratamiento cualquier incidencia que altere o pueda alterar el principio de seguridad de los datos, por los cauces y el procedimiento establecido en este Documento.

7.7. Deber de secreto

El responsable de las actividades de tratamiento y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos. Estas obligaciones subsistirán aún después de finalizar sus relaciones con el responsable.

7.8. Comunicación de datos

Los datos de carácter personal objeto del tratamiento no podrán ser comunicados a terceros. Sólo de forma excepcional y cuando concurran alguna de las condiciones establecidas en el Reglamento Europeo de Protección de Datos se podrá proceder a esta comunicación, que además se realizará de acuerdo con esta normativa y garantizando todas las garantías de protección de los datos comunicados durante el proceso de comunicación.

Habrán de respetarse especialmente las garantías legalmente establecidas cuando los datos se transmitan en aplicación del derecho de portabilidad ejercido por el interesado.

7.9. Acceso a los datos por cuenta de terceros

No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato.

El responsable verificará que el encargado de tratamiento aplica las medidas de seguridad técnicas y de organización necesarias para garantizar la confidencialidad y seguridad de los datos tratados entregados por el responsable.

7.10. Derechos de los afectados

El Reglamento Europeo de Protección de Datos y la Ley Orgánica 3/2018, de Protección de Datos, reconoce a los interesados los siguientes derechos sobre sus datos personales: acceso, rectificación, supresión, limitación de tratamiento, portabilidad y oposición.

El personal de la organización que tenga esta competencia asignada deberá velar por la tutela y normal ejercicio de estos derechos por parte de los afectados, poniendo en conocimiento del Responsable de las Actividades de Tratamiento o de aquél a quien éste hubiera designado, cualquier incidencia que pueda afectar al normal ejercicio y tutela de los derechos de los afectados.

La tutela de los derechos de los afectados se extiende, lógicamente, no sólo al normal ejercicio de sus derechos frente al Responsable del Tratamiento, sino en el cumplimiento de todas aquellas obligaciones que la normativa impone al Responsable y que constituyen la garantía de la preservación de los derechos de los afectados como, por ejemplo, el derecho de información previa a los afectados en la recogida de sus datos de carácter personal.

8. Ejercicio y tutela de los derechos de los afectados

La tutela de los derechos de los afectados y su ejercicio sin trabas por éstos es responsabilidad directa del Responsable, quien deberá poner los medios indispensables para la efectiva tutela de los derechos de los afectados, con independencia de sus facultades de delegación.

8.1. Ámbito

Todas las áreas, divisiones, departamentos, servicios y dependencias, todo el personal, así como empresas o entidades y profesionales externos y colaboradores están obligados a respetar los derechos de los interesados en relación a sus datos personales en la forma en que los reconoce el Reglamento Europeo y la Ley Orgánica de Protección de Datos de 2018.

8.2. Responsabilidad de medios y obligaciones

La tutela de los derechos de los afectados y su ejercicio sin trabas por éstos es responsabilidad directa del Responsable, quien deberá poner los medios indispensables para facilitarles su ejercicio.

Cuando se ejerciten estos derechos en relación al tratamiento de sus datos personales por parte del interesado, el responsable está obligado a facilitarle toda la información relativa a las actuaciones que ha llevado a cabo a partir de su solicitud, en el plazo de un mes contado a partir de la recepción de la misma. Atendiendo al número de solicitudes y la complejidad del caso, este plazo puede prorrogarse otros dos meses si se considera necesario. Esta prórroga se comunicará al interesado indicándole las causas que la justifican.

En caso de que el interesado solicite el ejercicio de estos derechos utilizando medios electrónicos, también la respuesta deberá cursarse por medios electrónicos, salvo que el interesado solicite que la respuesta se le notifique de otra manera.

En aquellos casos en que el responsable no proceda a tramitar la solicitud del interesado en ejercicio de alguno de estos derechos, el responsable deberá informarle de esta decisión lo antes posible y como máximo en un mes desde la recepción de la solicitud. En la notificación en que se informe al interesado de esta no tramitación, deberán indicarse las causas alegadas para tal inactividad así como indicarle la posibilidad de presentar una reclamación contra una autoridad de control y ejercer las acciones judiciales pertinentes.

Todos estos procesos de ejercicio de derechos serán gratuitos para el interesado, pero el responsable podrá cobrar un canon razonable por su tramitación, en función del volumen y complejidad de los trámites administrativos que requiera, e incluso negarse a tramitarla cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, circunstancias que corresponderá probar al responsable.

8.3. Actuación ante el ejercicio de un derecho por el afectado

Debe ser conocido por todo el personal de atención al público o de recepción de correo postal, telegramas, correo electrónico o cualquier otro medio de recepción de comunicaciones conocido o establecido en la organización.

8.4. Derechos

La normativa vigente en materia de protección de datos personales reconoce una serie de derechos que asisten a los afectados por cualquier tratamiento de sus datos personales, como son los derechos de acceso, rectificación, supresión, limitación de tratamiento, portabilidad y oposición.

8.5. Derechos personalísimos

Los derechos de acceso, rectificación, supresión, oposición, limitación de tratamiento y portabilidad de datos de carácter personal podrán ser ejercidos directamente por el interesado o por su representante legal o voluntario.

Corresponderá al responsable la prueba de haber atendido el ejercicio de estos derechos por parte del interesado.

El responsable deberá informar al interesado de los medios de que dispone para ejercer estos derechos, medios que deberán ser en todo caso accesibles para el interesado. De todas maneras, el derecho no puede ser denegado simplemente porque el interesado ha utilizado un medio diferente.

Estos derechos también se podrán ejercer directamente ante el encargado de tratamiento si así queda establecido en el contrato firmado con el responsable.

Son derechos independientes, de forma que el ejercicio de cualquiera de ellos no es requisito previo para el ejercicio de otro.

Es necesario que el interesado se identifique para ejercer estos derechos. En caso de que el responsable tenga dudas sobre la identidad de la persona que cursa la solicitud estará legitimado para solicitar la información adicional necesaria para confirmar la identidad del interesado.

8.6. Derecho de acceso

8.6.1. Contenido del derecho

El artículo 15 del Reglamento Europeo de Protección de Datos y el artículo 13 de la Ley Orgánica de Protección de Datos reconocen el Derecho de Acceso de los interesados.

El Derecho de Acceso es el derecho de interesado a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, el acceso a tales datos personales y a la siguiente

información:

- los fines del tratamiento;
- las categorías de datos personales de que se trate;
- los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
- de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
- la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
- el derecho a presentar una reclamación ante una autoridad de control;
- cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
- la existencia de decisiones automatizadas, incluida la elaboración de perfiles, y en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Además, en el caso de que los datos sean transferidos a otro país o a una organización internacional, el interesado tendrá derecho a la información sobre las garantías adaptadas en dicha transmisión.

8.6.2. Recepción de la solicitud

La solicitud del ejercicio del derecho de acceso por parte de un interesado deberá recibirse por un medio que garantice su identidad.

Las peticiones podrán recibirse por:

- Correo postal ordinario, certificado, burofax, telegramas o por mensajero.
- Correo electrónico.
- En el servicio de atención al cliente si está establecido
- Fax llamando posteriormente para confirmar la recepción.
- Personalmente con la presentación de su Documento Nacional de Identidad o cualquier otro medio válido en derecho.
- Cualquier otro que permita acreditar el envío y la recepción de la solicitud.

8.6.3. Atención de la solicitud

Cuando se ejercite el Derecho de Acceso por parte del interesado, el responsable está obligado a facilitarle toda la información relativa a las actuaciones que ha llevado a cabo a partir de su solicitud, en el plazo de un mes contado a partir de la recepción de la misma. Atendiendo al número de solicitudes y la complejidad del caso, este plazo puede prorrogarse otros dos meses si se considera necesario. Esta prórroga se comunicará al interesado indicándole las causas que la justifican.

En caso de que el interesado solicite el ejercicio de este derecho utilizando medios electrónicos, también la respuesta deberá cursarse por medios electrónicos, salvo

que el interesado solicite que la respuesta se le notifique de otra manera.

En aquellos casos en que el responsable no proceda a tramitar la solicitud del interesado en ejercicio de alguno de estos derechos, el responsable deberá informarle de esta decisión lo antes posible y como máximo en un mes desde la recepción de la solicitud. En la notificación en que se informe al interesado de esta no tramitación, deberán indicarse las causas alegadas para tal inactividad así como indicarle la posibilidad de presentar una reclamación contra una autoridad de control y ejercer las acciones judiciales pertinentes.

8.6.4. Contenido de la respuesta

Para dar cumplimiento al derecho de acceso ejercido por el interesado, el responsable estará obligado a facilitar una copia de los datos personales objeto de tratamiento. En caso de que el interesado solicite copias adicionales, el responsable está facultado para exigirle el pago de un canon que cubra los gastos administrativos generados.

De acuerdo con el artículo 13 de la Ley española de protección de datos vigente, el derecho de acceso se entenderá cumplido también cuando el responsable facilite al interesado algún sistema de acceso a los datos que sea remoto, directo y seguro con el que se facilite el acceso del interesado a todos los datos. De optar el responsable por esta vía de respuesta al ejercicio del derecho, la mera comunicación al interesado del modo en que podrá acceder a los datos por esta vía será suficiente para considerar atendido el derecho de acceso ejercido.

En caso de que la solicitud del derecho de acceso se formule por medios electrónicos, también la información se le facilitará por vía electrónica de uso común, salvo que el interesado haya solicitado que se le facilite por otra vía distinta.

8.6.5. Denegación del acceso

Se considerará que el ejercicio del derecho es repetitivo y permite el cobro de un canon o la desatención de la solicitud cuando se ejercite en más de una ocasión durante el plazo de seis meses, salvo que dicho ejercicio repetitivo tenga una causa legítima.

No es posible denegar el derecho de acceso fuera de los casos previstos legalmente.

8.7. Derecho de rectificación

8.7.1. Contenido del derecho

De acuerdo con el artículo 16 del Reglamento Europeo de Protección de Datos, el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de sus datos personales inexactos.

Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

8.7.2. Recepción de la solicitud

La solicitud del ejercicio del derecho de rectificación y cancelación por parte de un interesado deberá recibirse por un medio que garantice su identidad.

La solicitud deberá acompañar cuando sea preciso la documentación justificativa de la inexactitud o el carácter incompleto de los datos a que concierne el ejercicio del derecho.

Las peticiones podrán recibirse por:

- Correo postal ordinario, certificado, burofax, telegramas o por mensajero.
- Correo electrónico.
- En el servicio de atención al cliente si está establecido.
- Fax llamando posteriormente para confirmar la recepción.
- Personalmente con la presentación de su Documento Nacional de Identidad o cualquier otro medio válido en derecho.
- Cualquier otro que permita acreditar el envío y la recepción de la solicitud.

8.7.3. Atención de la solicitud

Cuando se ejercite el derecho de rectificación en relación al tratamiento de sus datos personales por parte del interesado, el responsable está obligado a facilitarle toda la información relativa a las actuaciones que ha llevado a cabo a partir de su solicitud, en el plazo de un mes contado a partir de la recepción de la misma. Atendiendo al número de solicitudes y la complejidad del caso, este plazo puede prorrogarse otros dos meses si se considera necesario. Esta prórroga se comunicará al interesado indicándole las causas que la justifican.

En caso de que el interesado solicite el ejercicio de estos derechos utilizando medios electrónicos, también la respuesta deberá cursarse por medios electrónicos, salvo que el interesado solicite que la respuesta se le notifique de otra manera.

En aquellos casos en que el responsable no proceda a tramitar la solicitud del interesado en ejercicio de alguno de estos derechos, el responsable deberá informarle de esta decisión lo antes posible y como máximo en un mes desde la

recepción de la solicitud. En la notificación en que se informe al interesado de esta no tramitación, deberán indicarse las causas alegadas para tal inactividad así como indicarle la posibilidad de presentar una reclamación contra una autoridad de control y ejercer las acciones judiciales pertinentes.

8.7.4. Denegación de la rectificación

La rectificación sólo podrá denegarse cuando concurra alguna circunstancia prevista legalmente.

8.8. Derecho de supresión (derecho al olvido)

8.8.1. Contenido del derecho

De acuerdo con la previsión del artículo 17 del Reglamento Europeo de Protección de Datos y del artículo 15 de la Ley Orgánica de Protección de Datos, el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de sus datos personales cuando concurra alguna de las circunstancias siguientes:

- los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
- el interesado retire el consentimiento en que se basaba el tratamiento y éste no pueda legitimarse en ningún otro fundamento jurídico;
- el interesado se oponga al tratamiento a través del ejercicio del derecho de oposición y no prevalezcan otros motivos legítimos para el tratamiento;
- los datos personales hayan sido tratados ilícitamente;
- los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
- los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

El ejercicio de este derecho también puede implicar que, cuando el responsable haya hecho públicos los datos personales y ahora esté obligado a suprimirlos, teniendo en cuenta la tecnología disponible y el coste de su aplicación, ese mismo responsable adoptará las medidas razonables, incluidas medidas técnicas, con el objetivo de informar a los responsables que estén tratando los datos personales del interesado, del ejercicio por parte de éste del derecho de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

8.8.2. Recepción de la solicitud

La solicitud del ejercicio del derecho de supresión por parte de un interesado deberá recibirse por un medio que garantice su identidad.

Las peticiones podrán recibirse por:

- Correo postal ordinario, certificado, telegramas o por mensajero.
- Correo electrónico.
- En el servicio de atención al cliente si está establecido.

- Fax llamando posteriormente para confirmar la recepción.
- Personalmente con la presentación de su Documento Nacional de Identidad o cualquier otro medio válido en derecho.
- Cualquier otro que permita acreditar el envío y la recepción de la solicitud.

8.8.3. Atención de la solicitud

Cuando se ejercite el derecho de supresión en relación al tratamiento de sus datos personales por parte del interesado, el responsable está obligado a facilitarle toda la información relativa a las actuaciones que ha llevado a cabo a partir de su solicitud, en el plazo de un mes contado a partir de la recepción de la misma. Atendiendo al número de solicitudes y la complejidad del caso, este plazo puede prorrogarse otros dos meses si se considera necesario. Esta prórroga se comunicará al interesado indicándole las causas que la justifican.

En caso de que el interesado solicite el ejercicio de este derecho utilizando medios electrónicos, también la respuesta deberá cursarse por medios electrónicos, salvo que el interesado solicite que la respuesta se le notifique de otra manera.

En aquellos casos en que el responsable no proceda a tramitar la solicitud del interesado en ejercicio de alguno de estos derechos, el responsable deberá informarle de esta decisión lo antes posible y como máximo en un mes desde la recepción de la solicitud. En la notificación en que se informe al interesado de esta no tramitación, deberán indicarse las causas alegadas para tal inactividad así como indicarle la posibilidad de presentar una reclamación contra una autoridad de control y ejercer las acciones judiciales pertinentes.

Si el ejercicio del derecho de supresión proviene del ejercicio del derecho de oposición, entonces el responsable podrá conservar los datos identificativos del interesado que considere necesarios, a efectos de impedir tratamientos futuros para fines de mercadotecnia directa.

8.8.4. Cesiones previas

El ejercicio de este derecho también puede implicar que, cuando el responsable haya hecho públicos los datos personales y ahora esté obligado a suprimirlos, teniendo en cuenta la tecnología disponible y el coste de su aplicación, ese mismo responsable adoptará las medidas razonables, incluidas medidas técnicas, con el objetivo de informar a los responsables que estén tratando los datos personales del interesado, del ejercicio por parte de éste del derecho de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

8.8.5. Denegación de la supresión

El derecho de supresión será denegado y los datos no se suprimirán ni se trasladará el ejercicio del derecho a otros responsables que los hayan incorporado tras hacerlos públicos el responsable principal, cuando concurra alguna de las siguientes circunstancias contempladas por el artículo 17.3 del Reglamento Europeo de Protección de Datos y el tratamiento de los datos sea necesario:

- para ejercer el derecho a la libertad de expresión e información;
- para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;
- por razones de interés público en el ámbito de la salud pública;
- con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, cuando la supresión de los datos pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o
- para la formulación, el ejercicio o la defensa de reclamaciones.

8.9. Derecho de oposición

8.9.1. Contenido del derecho

De acuerdo con la previsión del artículo 21 del Reglamento Europeo de Protección de Datos y del artículo 18 de la Ley Orgánica de Protección de Datos, el interesado puede oponerse al tratamiento de sus datos con ciertas finalidades, incluida la elaboración de perfiles, especialmente cuando el tratamiento de los datos tenga por objeto la mercadotecnia directa.

8.9.2. Recepción de la solicitud

El interesado podrá ejercer su derecho a oponerse por las vías establecidas por el responsable, que deberán ser sencillas y asequibles, y también por medios automatizados que apliquen especificaciones técnicas.

Las peticiones podrán recibirse por:

- Correo postal ordinario, certificado, telegramas o por mensajero.
- Correo electrónico.
- En el servicio de atención al cliente si está establecido.
- Fax llamando posteriormente para confirmar la recepción.
- Personalmente con la presentación de su Documento Nacional de Identidad o cualquier otro medio válido en derecho.
- Cualquier otro que permita acreditar el envío y la recepción de la solicitud.

8.9.3. Atención de la solicitud y supuestos de denegación de la misma

El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

En el supuesto de que los datos personales se traten con fines de investigación

científica o histórica o fines estadísticos la oposición al tratamiento de sus datos podrá ejercitarse, salvo que este tratamiento sea necesario para el cumplimiento de una misión realizada por razones de interés público, en este caso la solicitud podrá denegarse.

8.10. Derecho a no ser objeto de decisiones individualizadas

8.10.1. Contenido del derecho

De acuerdo con la previsión del artículo 22 del Reglamento Europeo de Protección de Datos y el artículo 18 de la Ley Orgánica de Protección de Datos de 2018, el interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

8.10.2. Recepción de la solicitud

El interesado podrá ejercer su derecho a oponerse por las vías establecidas por el responsable, que deberán ser sencillas y asequibles, y también por medios automatizados que apliquen especificaciones técnicas.

Las peticiones podrán recibirse por:

- Correo postal ordinario, certificado, telegramas o por mensajero.
- Correo electrónico.
- En el servicio de atención al cliente si está establecido.
- Fax llamando posteriormente para confirmar la recepción.
- Personalmente con la presentación de su Documento Nacional de Identidad o cualquier otro medio válido en derecho.
- Cualquier otro que permita acreditar el envío y la recepción de la solicitud.

8.10.3. Atención de la solicitud

El responsable del tratamiento dejará de utilizar los datos para la toma de decisiones basadas en su tratamiento automatizado, incluida la elaboración de perfiles.

8.10.4. Denegación de la solicitud

De acuerdo con lo previsto por el Reglamento General de Protección de Datos, el ejercicio de este derecho por parte del interesado podrá denegarse en tres casos:

- cuando esté autorizada a favor del responsable por el Derecho de la Unión o de los Estados miembros siempre que se cumpla con las correspondientes garantías para salvaguardar los derechos y libertades y los intereses legítimos del interesado,
- cuando esa decisión automatizada sea necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
- cuando el tratamiento se base en el consentimiento explícito del interesado.

En estos dos últimos casos, el responsable estará obligado a adoptar las medidas necesarias para salvaguardar los derechos y libertades y los intereses legítimos del

interesado, como mínimo, el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar su decisión.

Aquellas decisiones en que concurra alguna de estas circunstancias en que se admita la denegación del derecho al interesado no podrán basarse en las categorías especiales de datos contempladas por el artículo 9 del Reglamento: datos que revelen el origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos orientados a identificar de manera unívoca a una persona física, datos relativos a la salud y datos relativos a la vida sexual o a la orientación sexual de una persona física.

El tratamiento para la toma de decisiones individualizadas, incluida la elaboración de perfiles, sobre este tipo especial de datos solo será posible cuando dicho tratamiento se base en el consentimiento explícito del interesado (siempre que sea posible de acuerdo con el derecho de la Unión o sus Estados) o sea necesario en atención a un interés público esencial, y además se hayan tomado medidas especiales para salvaguardar los derechos de los interesados.

8.11. Derecho de limitación del tratamiento

8.11.1. Contenido del derecho

De acuerdo con el artículo 18 del Reglamento Europeo de Protección de Datos y el artículo 16 de la Ley Orgánica de Protección de Datos de 2018, el interesado puede ejercer ante el responsable el derecho a limitar el tratamiento de sus datos personales en los siguientes supuestos:

- en caso de impugnación por parte del interesado de la exactitud de sus datos personales: durante el plazo necesario para que el responsable pueda verificar la exactitud de los mismos;
- en caso de que el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
- en caso de que el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado sí que los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
- en caso de que el interesado haya ejercido su derecho de oposición al tratamiento, la limitación se mantendrá mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

En todos estos casos, mientras los datos están sometidos a este régimen especial de limitación de tratamiento, sólo se podrán tratar, salvo para su conservación, cuando exista consentimiento del interesado, o para la formulación o en el proceso de reclamaciones, o con el objetivo de la protección de los derechos de otra persona, o por razones de interés público.

8.11.2. Recepción de la solicitud y atención del derecho

El interesado podrá ejercer su derecho a oponerse por las vías establecidas por el responsable, que deberán ser sencillas y asequibles, y también por medios

automatizados que apliquen especificaciones técnicas.

Las peticiones podrán recibirse por:
- Correo postal ordinario, certificado, telegramas o por mensajero.
- Correo electrónico.
- En el servicio de atención al cliente si está establecido.
- Fax llamando posteriormente para confirmar la recepción.
- Personalmente con la presentación de su Documento Nacional de Identidad o cualquier otro medio válido en derecho.
- Cualquier otro que permita acreditar el envío y la recepción de la solicitud.

Una vez ejercido el derecho de limitación de tratamiento, el responsable deberá informar al interesado antes del levantamiento de tal limitación.

El responsable deberá comunicar el ejercicio de este derecho a la limitación del tratamiento a cada uno de los destinatarios a los que se hayan comunicado datos personales, siempre que sea posible y no requiera un esfuerzo desproporcionado.

El hecho de que el tratamiento de los datos esté limitado debe hacerse constar expresamente en el sistema para evitar tratamientos excesivos.

8.11.3. Denegación de la solicitud

Sólo se podrá denegar el ejercicio de este derecho con base en alguna previsión legal.

8.12. Derecho a la portabilidad de los datos

8.12.1. Contenido del derecho

De acuerdo con el artículo 20 del Reglamento Europeo de Protección de Datos y el artículo 17 de la Ley Orgánica de Protección de Datos de 2018, el interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando el tratamiento esté basado en el consentimiento del interesado o sea necesario para la ejecución de un contrato y el tratamiento se efectúe por medios automatizados.

Cuando sea técnicamente posible, el interesado que ejerza este derecho también podrá solicitar que los datos personales se transmitan directamente de responsable a responsable.

8.12.2. Recepción de la solicitud y atención del derecho

Ejercido el derecho por el interesado, el responsable le deberá informar de las actuaciones llevadas a cabo para cumplirlo.

8.12.3. Denegación de la solicitud

El derecho a la portabilidad no se aplicará en caso de tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

El ejercicio de este derecho no podrá afectar negativamente a los derechos y libertades de otros.

8.13. Encargado de derechos de los afectados

El Responsable de las Actividades de Tratamiento o aquél a quien designe con autorización delegada como responsable o encargado de la atención a los afectados deberán velar por el exacto cumplimiento del procedimiento establecido y ofrecer al interesado, dentro de los plazos arriba descritos, la respuesta al ejercicio de sus legítimos derechos.

9. Definiciones

Para comprender y actualizar correctamente el presente Informe referente al Registro de las actividades de tratamiento, puede resultar útil el listado de definiciones que incorpora el Reglamento Europeo de Protección de Datos en su artículo 4:

- **«Datos Personales»:** toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

- **«Tratamiento»:** cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

- **«Limitación del Tratamiento»:** el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

- **«Elaboración de Perfiles»:** toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

- **«Seudonimización»:** el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

- **«Fichero» o «actividad de tratamiento»:** todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

- **«Responsable del Tratamiento» o «Responsable»:** la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

- **«Encargado del Tratamiento» o «Encargado»:** la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

- **«Destinatario»:** la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

- **«Tercero»:** persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

- **«Consentimiento del Interesado»:** toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

- **«Violación de la Seguridad de los Datos Personales»:** toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

- **«Datos Genéticos»:** datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

- **«Datos Biométricos»:** datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

- **«Datos Relativos a la Salud»:** datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

- **«Establecimiento Principal»:** a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal; b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de

tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento.

- **«Representante»:** persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento.

- **«Empresa»:** persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica.

- **«Grupo Empresarial»:** grupo constituido por una empresa que ejerce el control y sus empresas controladas.

- **«Normas Corporativas Vinculantes»:** las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.

- **«Autoridad de Control»:** la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51.

- **«Autoridad de Control Interesada»:** la autoridad de control a la que afecta el tratamiento de datos personales debido a que:

  a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;

  b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o

  c) se ha presentado una reclamación ante esa autoridad de control.

- **«Tratamiento Transfronterizo»:** a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro.

- **«Objeción Pertinente y Motivada»:** la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la

importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión.

– **«Servicio de la Sociedad de la Información»:** todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo.

– **«Organización Internacional»:** una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

Anexo A. Relación de Actividades de Tratamiento.

Nombre de la Actividad de Tratamiento	Nivel de Riesgo	Sistema de Tratamiento
CLIENTES POTENCIALES	Bajo	Mixto
CLIENTES Y/O PROVEEDORES	Bajo	Mixto
CONTACTOS AGENDA	Bajo	Mixto
CONTACTOS WHATSAPP	Bajo	Mixto
HISTORIAL CLÍNICO	Elevado o Muy Alto	Mixto
MENORES	Bajo	Mixto
TPV	Bajo	Mixto

Anexo B. Estructura del fichero o la base de datos.

Fichero: CLIENTES POTENCIALES

UBICACIÓN

Nombre: ALEXANDRA ALEXANDROVA - Sede Principal **NIF/CIF:** Y0565053A

Dirección: CALLE VALLDIGNA, N.19, Esc.E, 9-1

Localidad: Playa de Gandia **Código postal:** 46730

Provincia: Valencia **País:** España

Teléfono: 644243004 **Fax:** **E-mail:** svatok84@hotmail.com

SISTEMA DE TRATAMIENTO

Tipo de Sistema de Tratamiento
- Mixto

ESTRUCTURA

Datos de carácter identificativo
- DNI / NIF
- Nombre y apellidos
- Firma manual

Otros Datos Tipificados
- Características personales
- Información comercial

FINALIDAD

Descripción detallada de la finalidad y usos previstos:
Realización de presupuestos a posibles clientes.

Finalidades
- Gestión de clientes, contable, fiscal y administrativa
- Publicidad y prospección comercial

ORIGEN Y PROCEDENCIA DE LOS DATOS

Procedencia de los datos
- El propio interesado o su representante legal

Colectivos o Categorías de interesados
- Clientes y usuarios
- Personas de contacto

CONSERVACIÓN DE LOS DATOS

Plazo de conservación previsto para los datos personales recogidos en esta actividad de tratamiento: El mínimo imprescindible

Fichero: CLIENTES Y/O PROVEEDORES

UBICACIÓN

Nombre: ALEXANDRA ALEXANDROVA - Sede Principal **NIF/CIF:** Y0565053A

Dirección: CALLE VALLDIGNA, N.19, Esc.E, 9-1

Localidad: Playa de Gandia **Código postal:** 46730

Provincia: Valencia **País:** España

Teléfono: 644243004 **Fax:** **E-mail:** svatok84@hotmail.com

SISTEMA DE TRATAMIENTO

Tipo de Sistema de Tratamiento
- Mixto

ESTRUCTURA

Datos de carácter identificativo
- DNI / NIF
- Nombre y apellidos
- Dirección (postal, electrónica)
- Teléfono
- Firma manual

Otros Datos Tipificados
- Características personales
- Información comercial
- Económicos, financieros y de seguros
- Transacciones de bienes y servicios

FINALIDAD

Descripción detallada de la finalidad y usos previstos:
Fichero para el registro de clientes y proveedores de la empresa.

Finalidades
- Gestión de clientes, contable, fiscal y administrativa

ORIGEN Y PROCEDENCIA DE LOS DATOS

Procedencia de los datos
- El propio interesado o su representante legal

Colectivos o Categorías de interesados
- Clientes y usuarios
- Proveedores
- Personas de contacto

CONSERVACIÓN DE LOS DATOS

Plazo de conservación previsto para los datos personales recogidos en esta actividad de tratamiento: El mínimo imprescindible

CESIÓN O COMUNICACIÓN DE DATOS

Categorías de Destinatarios de Cesiones
- Organizaciones o personas directamente relacionadas con el responsable
- Organismos de la seguridad social
- Otros órganos de la administración pública

- Bancos, cajas de ahorros y cajas rurales
- Administración pública con competencia en la materia

Fichero: CONTACTOS AGENDA

UBICACIÓN

Nombre: ALEXANDRA ALEXANDROVA - Sede Principal **NIF/CIF:** Y0565053A

Dirección: CALLE VALLDIGNA, N.19, Esc.E, 9-1

Localidad: Playa de Gandia **Código postal:** 46730

Provincia: Valencia **País:** España

Teléfono: 644243004 **Fax:** **E-mail:** svatok84@hotmail.com

SISTEMA DE TRATAMIENTO

Tipo de Sistema de Tratamiento
- Mixto

ESTRUCTURA

Datos de carácter identificativo
- Nombre y apellidos
- Dirección (postal, electrónica)
- Teléfono

Otros Datos Tipificados
- Características personales

FINALIDAD

Descripción detallada de la finalidad y usos previstos:
Fichero donde de encuentran: nombres, telefonos y las direcciones de e-mail tanto de clientes,proveedores, posibles clientes o candidatos.

Finalidades
- Gestión de clientes, contable, fiscal y administrativa
- Recursos humanos
- Gestión de nóminas
- Publicidad y prospección comercial
- Otras finalidades

ORIGEN Y PROCEDENCIA DE LOS DATOS

Procedencia de los datos
- El propio interesado o su representante legal
- Fuentes accesibles al público
- Registros públicos

Colectivos o Categorías de interesados
- Empleados
- Clientes y usuarios
- Proveedores
- Personas de contacto
- Solicitantes

CONSERVACIÓN DE LOS DATOS

Plazo de conservación previsto para los datos personales recogidos en esta actividad de tratamiento: El mínimo imprescindible

CESIÓN O COMUNICACIÓN DE DATOS

Categorías de Destinatarios de Cesiones

- Organizaciones o personas directamente relacionadas con el responsable

Fichero: CONTACTOS WHATSAPP

UBICACIÓN

Nombre: ALEXANDRA ALEXANDROVA - Sede Principal **NIF/CIF:** Y0565053A

Dirección: CALLE VALLDIGNA, N.19, Esc.E, 9-1

Localidad: Playa de Gandia **Código postal:** 46730

Provincia: Valencia **País:** España

Teléfono: 644243004 **Fax:** **E-mail:** svatok84@hotmail.com

SISTEMA DE TRATAMIENTO

Tipo de Sistema de Tratamiento
- Mixto

ESTRUCTURA

Datos de carácter identificativo
- Nombre y apellidos
- Teléfono

Otros Datos Tipificados
- Características personales

FINALIDAD

Descripción detallada de la finalidad y usos previstos:
Introduccion de clientes y/o trabajadores en un grupo de whatsapp

Finalidades
- Gestión de clientes, contable, fiscal y administrativa
- Publicidad y prospección comercial
- Otras finalidades

ORIGEN Y PROCEDENCIA DE LOS DATOS

Procedencia de los datos
- El propio interesado o su representante legal

Colectivos o Categorías de interesados
- Clientes y usuarios
- Personas de contacto

CONSERVACIÓN DE LOS DATOS

Plazo de conservación previsto para los datos personales recogidos en esta actividad de tratamiento: No especificado

CESIÓN O COMUNICACIÓN DE DATOS

Categorías de Destinatarios de Cesiones
- Prestaciones de servicios de telecomunicaciones

Fichero: HISTORIAL CLÍNICO

UBICACIÓN

Nombre: ALEXANDRA ALEXANDROVA - Sede Principal **NIF/CIF:** Y0565053A

Dirección: CALLE VALLDIGNA, N.19, Esc.E, 9-1

Localidad: Playa de Gandia **Código postal:** 46730

Provincia: Valencia **País:** España

Teléfono: 644243004 **Fax:** **E-mail:** svatok84@hotmail.com

SISTEMA DE TRATAMIENTO

Tipo de Sistema de Tratamiento
- Mixto

ESTRUCTURA

Categorías Especiales de Datos
- Salud

Datos de carácter identificativo
- DNI / NIF
- Nº SS / Mutualidad
- Nombre y apellidos
- Tarjeta Sanitaria
- Dirección (postal, electrónica)
- Teléfono
- Firma manual

Otros Datos Tipificados
- Características personales
- Circunstancias sociales

FINALIDAD

Descripción detallada de la finalidad y usos previstos:
Un fichero para facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud. Destinado fundamentalmente a garantizar una asistencia adecuada al paciente.

Finalidades
- Gestión de clientes, contable, fiscal y administrativa
- Gestión y control sanitario
- Historial clínico
- Otras finalidades

ORIGEN Y PROCEDENCIA DE LOS DATOS

Procedencia de los datos
- El propio interesado o su representante legal

Colectivos o Categorías de interesados
- Clientes y usuarios
- Pacientes

CONSERVACIÓN DE LOS DATOS

Plazo de conservación previsto para los datos personales recogidos en esta actividad de tratamiento: El mínimo imprescindible

CESIÓN O COMUNICACIÓN DE DATOS

Categorías de Destinatarios de Cesiones

- Organizaciones o personas directamente relacionadas con el responsable
- Organismos de la seguridad social
- Entidades sanitarias

Fichero: MENORES

UBICACIÓN

Nombre: ALEXANDRA ALEXANDROVA - Sede Principal **NIF/CIF:** Y0565053A

Dirección: CALLE VALLDIGNA, N.19, Esc.E, 9-1

Localidad: Playa de Gandia **Código postal:** 46730

Provincia: Valencia **País:** España

Teléfono: 644243004 **Fax:** **E-mail:** svatok84@hotmail.com

SISTEMA DE TRATAMIENTO

Tipo de Sistema de Tratamiento
- Mixto

ESTRUCTURA

Datos de carácter identificativo
- DNI / NIF
- Nombre y apellidos
- Tarjeta Sanitaria
- Dirección (postal, electrónica)
- Teléfono
- Firma manual

Otros Datos Tipificados
- Características personales
- Circunstancias sociales

FINALIDAD

Descripción detallada de la finalidad y usos previstos:
Gestión de los datos de menores.

Finalidades
- Gestión de actividades asociativas, culturales, recreativas, deportivas y sociales
- Otras finalidades

ORIGEN Y PROCEDENCIA DE LOS DATOS

Procedencia de los datos
- El propio interesado o su representante legal

Colectivos o Categorías de interesados
- Asociados o miembros
- Padres o tutores
- Representante legal

CONSERVACIÓN DE LOS DATOS

Plazo de conservación previsto para los datos personales recogidos en esta actividad de tratamiento: No especificado

CESIÓN O COMUNICACIÓN DE DATOS

Categorías de Destinatarios de Cesiones
- Organizaciones o personas directamente relacionadas con el responsable
- Asociaciones y organizaciones sin ánimo de lucro

Fichero: TPV

UBICACIÓN

Nombre: ALEXANDRA ALEXANDROVA - Sede Principal **NIF/CIF:** Y0565053A

Dirección: CALLE VALLDIGNA, N.19, Esc.E, 9-1

Localidad: Playa de Gandia **Código postal:** 46730

Provincia: Valencia **País:** España

Teléfono: 644243004 **Fax:** **E-mail:** svatok84@hotmail.com

SISTEMA DE TRATAMIENTO

Tipo de Sistema de Tratamiento
- Mixto

ESTRUCTURA

Datos de carácter identificativo
- Nombre y apellidos
- Firma electrónica

Otros Datos Tipificados
- Económicos, financieros y de seguros
- Transacciones de bienes y servicios

FINALIDAD

Descripción detallada de la finalidad y usos previstos:
Fichero que tiene como finalidad el uso del TPV para el cobro mediante tarjeta tanto de crédito como de débito del establecimiento.

Finalidades
- Gestión de clientes, contable, fiscal y administrativa

ORIGEN Y PROCEDENCIA DE LOS DATOS

Procedencia de los datos
- El propio interesado o su representante legal

Colectivos o Categorías de interesados
- Clientes y usuarios

CONSERVACIÓN DE LOS DATOS

Plazo de conservación previsto para los datos personales recogidos en esta actividad de tratamiento: No especificado

CESIÓN O COMUNICACIÓN DE DATOS

Categorías de Destinatarios de Cesiones
- Organizaciones o personas directamente relacionadas con el responsable
- Bancos, cajas de ahorros y cajas rurales

Anexo C. Recursos Protegidos.

LOCALES

Nombre: ALEXANDRA ALEXANDROVA - Sede Principal

Dirección: CALLE VALLDIGNA, N.19, Esc.E, 9-1

Localidad: Playa de Gandia

Código Postal: 46730 **Provincia:** Valencia

Teléfono: 644243004 **Fax:** **País:** España

E-Mail: svatok84@hotmail.com

Descripción: Sede del Responsable

ALMACENES

Nombre: ALEXANDRA ALEXANDROVA - Sede Principal

Dirección: CALLE VALLDIGNA, N.19, Esc.E, 9-1 (Playa de Gandia 46730, Valencia)

Tipo de Almacén:

- Almacén de Soportes
- Almacén de Copias de Respaldo
- Almacén de Documentos

Notas:

INVENTARIO DE EQUIPOS

Código: SMP001	**Tipo de Hardware:** Smartphone	
S.O.: ANDROID	**Descripción:**	
Fabricante: SAMSUNG	**Modelo:** S21 ULTRA	**Fecha:**
Uso:		
Dispositivo Portátil: Si		
Sistema de Cifrado:		
Sistema de Etiquetado:		

INVENTARIO DE SOFTWARE

Aplicación	Versión	Fabricante	Fecha
ANDROID			

PUESTOS DE TRABAJO

DIRECCION (ALEXANDRA ALEXANDROVA - Sede Principal)			
Personal: – ALEXANDRA ALEXANDROVA (MEDICO-GERENTE)			
Hardware			
Smartphone SMP001	SAMSUNG S21 ULTRA		ANDROID
Software			
ANDROID			
Ficheros Tratados			
– CLIENTES POTENCIALES – CLIENTES Y/O PROVEEDORES – CONTACTOS AGENDA – CONTACTOS WHATSAPP – HISTORIAL CLÍNICO – MENORES – TPV			

Anexo D. Configuración y descripción del sistema de información.

DESCRIPCIÓN DEL SISTEMA DE INFORMACIÓN

El Sistema de información está compuesto por:

Anexo E. Relación de Personal Autorizado.

Nombre: ALEXANDRA ALEXANDROVA	**NIF:** Y0565053A	**Alta:**
Cargo: MEDICO-GERENTE	**Dep.:** DIRECCION	**Baja:**
E-mail:	**Existe Cláusula Confidencialidad:** No	
Perfil:		
Función:		
Fichero: CLIENTES POTENCIALES	**Cargo:** Encargado de la Actividad de Tratamiento	
Permisos: Recogida, Consulta, Modificación, Borrado, Copia, Adjuntos email **Accesos:** Acceso Físico a Ficheros, Acceso al Almacén de Soportes, Acceso al Almacén de Documentos		
Fichero: CLIENTES Y/O PROVEEDORES	**Cargo:** Encargado de la Actividad de Tratamiento	
Permisos: Recogida, Consulta, Modificación, Borrado, Copia, Adjuntos email **Accesos:** Acceso Físico a Ficheros, Acceso al Almacén de Soportes, Acceso al Almacén de Documentos		
Fichero: CONTACTOS AGENDA	**Cargo:** Encargado de la Actividad de Tratamiento	
Permisos: Recogida, Consulta, Modificación, Borrado, Copia, Adjuntos email **Accesos:** Acceso Físico a Ficheros, Acceso al Almacén de Soportes, Acceso al Almacén de Documentos		
Fichero: CONTACTOS WHATSAPP	**Cargo:** Encargado de la Actividad de Tratamiento	
Permisos: Recogida, Consulta, Modificación, Borrado, Copia, Adjuntos email **Accesos:** Acceso Físico a Ficheros, Acceso al Almacén de Soportes, Acceso al Almacén de Documentos		
Fichero: HISTORIAL CLÍNICO	**Cargo:** Encargado de la Actividad de Tratamiento	
Permisos: Recogida, Consulta, Modificación, Borrado, Copia, Adjuntos email **Accesos:** Acceso Físico a Ficheros, Acceso al Almacén de Soportes, Acceso al Almacén de Documentos		
Fichero: MENORES	**Cargo:** Encargado de la Actividad de Tratamiento	
Permisos: Recogida, Consulta, Modificación, Borrado, Copia, Adjuntos email **Accesos:** Acceso Físico a Ficheros, Acceso al Almacén de Soportes, Acceso al Almacén de Documentos		
Fichero: TPV	**Cargo:** Encargado de la Actividad de Tratamiento	
Permisos: Recogida, Consulta, Modificación, Borrado, Copia, Adjuntos email **Accesos:** Acceso Físico a Ficheros, Acceso al Almacén de Soportes, Acceso al Almacén de Documentos		

Colaboradores y Empresas Externas:

Nombre: DATA PROTECT PLUS S.L **NIF/CIF:** B42577791
Actividad: Otras actividades
Dirección: CALLE BAUTISTA BERTOMEU SOBER, N.5, 1-31
Localidad: TORREVIEJA **Código Postal:** 03183
Prov.: Alicante **Tel.:** 965038463 **Fax:** **País:** España
E-mail: info@dataprotectplus.com
Tiene acceso a datos personales: Si
Existe Contrato: Contrato de tratamiento por cuenta de terceros
Notas:

Anexo F. Formulario de Gestión de Soportes.

FORMULARIO DE ENTRADA DE SOPORTES

Datos del soporte:

Código del soporte:

Tipo de soporte:

Fecha de Copia:

Contenido:

Datos de Entrada:

Responsable de recepción:

Fecha y hora:

Periodicidad:

Número de soportes:

Forma de envío:

Emisor:

Empresa:

Persona:

Motivo:

FORMULARIO DE SALIDA DE SOPORTES

Datos del soporte:

Código del soporte: Tipo de soporte:

Descripción:

Fecha de Copia:

Contenido:

Datos de salida:

Responsable de entrega:

Fecha y hora:

Periodicidad:

Forma de envío:

Remitente:

Precauciones para el transporte:

Destinatario:

Empresa:

Persona:

Motivo:

Autorización:

Salida autorizada por:

Observaciones:

Anexo G. Formulario de Gestión de Incidencias.

FORMULARIO DE INCIDENCIAS

Fecha y hora en que se produjo la incidencia:

Tipo de Incidencia:

Fecha de Notificación:

Notificada por:

Notificada a:

Ficheros a los que afecta:

Descripción detallada de la incidencia:

Efectos que puede producir la incidencia:

Medidas correctoras:

Entorno al que afecta la incidencia:

¿Supone pérdida de datos?:

Procedimientos realizados para la recuperación de datos

Proceso ejecutado por:

Procedimiento realizado:

Datos restaurados:

Datos recuperados manualmente: