DOCUMENTO DE SEGURIDAD DE:

Margarita Queijo Rodríguez

Para el cumplimiento del Reglamento General de Protección de Datos (RGPD) (UE) 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Adaptación realizada por:

Soluciones en LOPD

Versión: 1 **Fecha: 29 / 09 / 2020**

INTRODUCCIÓN

El objeto del presente documento es recoger las medidas de seguridad establecidas por el responsable del tratamiento para todo el personal con acceso a los datos de carácter personal que se mantienen automatizados, así como para los sistemas de información.

Debido a la continua evolución y cambios intrínsecos de los sistemas de información y a la propia complejidad de la organización, el documento intentará ser un marco estable, y a su vez, flexible, en lugar de una descripción estática, en cuyo caso se vería sometido a continuas actualizaciones.

El presente documento se mantendrá en todo momento actualizado por el Responsable del Tratamiento y será revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

De igual forma, el Documento de Seguridad se adecuará, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

DOCUMENTO DE SEGURIDAD

El documento deberá contener, como mínimo:
-Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
-Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar la seguridad de los datos personales.
-Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal.
-Estructura de los tratamientos de datos de carácter personal y descripción de los sistemas de información que los tratan.
-Procedimiento de notificación, gestión y respuesta ante las incidencias o violaciones de seguridad.
-Los procedimientos de realización de copias de respaldo y de recuperación de los datos.
-Las medidas que sea necesario adoptar para el transporte de soportes, así como para su destrucción y reutilización.
-Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los tratamientos que se traten en concepto de encargado y se deberá firmar un contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

INDICE GENERAL

2. Auditorías y controles periódicos realizados.
3. Registro de accesos.
4. Relación de cesionarios.
5. Derechos de los interesados: información y modelos de ejercicio de derechos

6) CLÁUSULAS

1. Trabajadores
2. Clientes
3. Email
4. C.V.
5. Acciones Comerciales
6. Videovigilancia (cartel e impreso)

7) USOS Y RECOMENDACIONES

1. Responsable
2. DPO
3. Usuarios autorizados
4. Usuarios datos NO automatizados
5. Administradores Informáticos
6. Personal de Att. al Público

8) CONTRATOS

FIN DEL DOCUMENTO

3) DOCUMENTO DE SEGURIDAD

1. Ámbito de aplicación del documento.
2. Funciones / obligaciones del personal.
3. Medidas, normas y procedimientos.
4. Violaciones de Seguridad y Gestión de Incidencias.
5. Contraseñas y copias de seguridad.
6. Gestión de soportes y documentos.
7. Tratamientos.
8. Controles periódicos / auditorías.
9. Encargados de tratamiento.

1) ÁMBITO DE APLICACIÓN DEL DOCUMENTO

Margarita Queijo Rodríguez, como consecuencia de las actividades desarrolladas dentro de su actividad, necesariamente trata información y datos de carácter personal.

Las medidas de seguridad definidas en el presente documento van encaminadas a proteger todos los datos de carácter personal sometidos a tratamiento por Margarita Queijo Rodríguez, y las aplicaciones, herramientas de actualización y consulta, y sistemas que tratan los datos de carácter personal, los equipos informáticos que las soportan, los dispositivos de archivo y los locales donde estos se ubican.

En los anexos del presente Documento se recoge:

- Información de los tratamientos llevados a cabo por el responsable y su entorno.

- Descripción de las instalaciones y estructura informática.

- Descripción de las políticas de acceso a los datos, medidas de seguridad implantadas en los sistemas y definición de los procedimientos de copias de seguridad.

Este documento ha sido elaborado bajo la responsabilidad de Margarita Queijo Rodríguez, quien, como Responsable del Tratamiento, se compromete a implantar y actualizar la normativa de Seguridad que de él se desprende. Dicha normativa será de obligado cumplimiento para todo el personal que tenga acceso a los datos de carácter personal y/o a los sistemas de información que permiten el acceso a los mismos.

Los datos de identificación del RESPONSABLE DEL TRATAMIENTO son los siguientes:

• **RAZÓN SOCIAL**: Margarita Queijo Rodríguez
• **NIF/CIF:** 33274407P
• **DOMICILIO:** C/ Real 66, 1º - 15003 - A Coruña - A CORUÑA
• **DIRECCIÓN DONDE SE REALIZAN LOS TRATAMIENTOS:** La especificada en el ANEXO D (Locales)
• **ACTIVIDAD:** Sanidad

En concreto, los tratamientos sujetos a las medidas de seguridad establecidas en este documento son los detallados en el ANEXO A.

Como recursos protegidos de la entidad se han tenido en cuenta los siguientes componentes:

• Los tratamientos
• Aplicaciones Informáticas con acceso a datos personales
• Soportes informáticos y papel
• Equipos de almacenamiento
• Equipos de tratamiento
• Comunicaciones y sistemas de acceso remoto
• Oficinas y edificios
• Sistemas de Validación
• Personas

2) FUNCIONES / OBLIGACIONES DEL PERSONAL

Todas las personas que tengan acceso a los datos personales, a través del sistema informático o a través de cualquier otro medio automatizado de acceso, están obligadas a cumplir lo establecido en este documento, y por lo tanto, sujetas a las consecuencias que puedan derivar en caso de incumplimiento. El incumplimiento de las políticas, prácticas y procedimientos de seguridad estará sujeto a una acción disciplinaria, pudiendo conllevar una acción civil y/o penal.

Sin embargo, una eventual vulneración de la normativa de seguridad por parte de algún usuario, no eximirá de responsabilidad al Responsable del Tratamiento, sin perjuicio de las acciones que pueda éste ejercitar contra dicho usuario por el incumplimiento de sus obligaciones con respecto al mismo.

Las medidas de índole organizativas afectan en primera instancia a la actividad propia de la organización y a la asignación de funciones relacionadas con la seguridad. Por tanto, el responsable del tratamiento debe asegurar la implantación de las medidas técnicas y organizativas en sus sistemas de información y delimitar el acceso a los datos de carácter personal mediante la asignación de perfiles entre su personal. Dicha división conlleva a su vez una imposición de responsabilidades directamente relacionadas con la función a desempeñar dentro de la entidad. Los perfiles son básicamente los siguientes:

• **Responsable del tratamiento:** persona física o jurídica que decide sobre la finalidad y medios del tratamiento.

• **Delegado de Protección de Datos (si procede):** persona o personas físicas, designadas por el responsable del tratamiento, con las siguientes funciones:

Informar y asesorar al responsable o encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.

Cooperar con la autoridad de control.

Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

El DPD será obligatorio en:
- Autoridades y organismos públicos.
- Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala.
- Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles.
- Los colegios profesionales y sus consejos generales.
- Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
- Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
- Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de

los usuarios del servicio.
- Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
- Los establecimientos financieros de crédito.
- Las entidades aseguradoras y reaseguradoras.
- Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
- Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
- Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.
- Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.
- Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.
- Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.
- Las empresas de seguridad privada.
- Las federaciones deportivas cuando traten datos de menores de edad.

Aunque esta figura no siempre sea obligatoria, es muy recomendable como elemento clave para garantizar el cumplimiento de las medidas de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al Responsable del Tratamiento.

Las funciones principales del DPD respecto al Documento serán:

- Coordinar la actualización del documento.
- Coordinar y controlar la implantación y aplicación de las medidas definidas en el Documento de Seguridad.
- Poner en conocimiento de los usuarios de los datos las medidas y procedimientos de seguridad que les afectan.
- Realizar controles periódicos para verificar el cumplimiento de las medidas.
- Analizar los informes de auditoría y elevar las conclusiones al responsable adecuado.

• **Administrador/es de Sistemas:** personas físicas encargadas de implantar y mantener las medidas técnicas de seguridad, una vez autorizadas por el DPD o el Responsable del Tratamiento.

• **Usuarios de los datos:** Aquellos que, en ejercicio de sus funciones contractuales, tratan datos de carácter personal bajo el criterio de "necesidad de saber" establecido por el responsable del tratamiento. Los usuarios, así como el resto de personal con acceso y tratamiento de datos de carácter personal, deberán conocer sus responsabilidades, siendo para ello necesario que se articulen mecanismos para garantizar un conocimiento comprensible de dichas normas.

En este Documento aparecen las normas que afectaran básicamente al DPD y al Administrador de Sistemas pero es muy importante que los usuarios de los datos conozcan toda la normativa que les pueda afectar. Es por ello, que junto con el Documento de Seguridad formando parte del proyecto se entrega una normativa específica para usuarios donde figuran todas las normas referentes al RGPD que afectan a todos los empleados que puedan tratar datos.

Esta normativa debe difundirse a todos los empleados ya sea entregándola en la incorporación de un empleado o publicándola en algún sitio público como la intranet o similar.

En la empresa, se procede a entregar la normativa en forma de recomendaciones a todo el personal implicado, a través del Documento (Usos y Recomendaciones) que se entregará a los diferentes perfiles de usuarios y responsables.

A los nuevos trabajadores se les haría entrega de la documentación, en el momento de la firma del contrato de trabajo.

3) MEDIDAS, NORMAS Y PROCEDIMIENTOS

En este apartado reflejamos todas las medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar y poder demostrar que el tratamiento es conforme al reglamento RGPD.

Al margen del cumplimiento de esta normativa, el Responsable del Tratamiento deberá adoptar en cada momento aquellas medidas de índole técnica y organizativa que crea necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información.

Cabe decir que, si el cumplimiento estricto de alguna de las normas expuestas supusiera un coste desproporcionado para el Responsable del Tratamiento, éste podrá modular su cumplimiento, sin que en ningún caso pueda verse afectada la protección de datos de carácter personal.

Control de Acceso a los datos personales

El control de acceso es aquella medida destinada a garantizar la identidad de cada persona que accede a los sistemas de información (identificación/autenticación), así como a asegurar que el acceso de cada usuario corresponda exclusivamente al perfil y permisos asignados por el responsable del tratamiento, con el objeto de evitar accesos no autorizados al sistema que contiene datos personales.

Exclusivamente el personal responsable de sistemas podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del tratamiento.

Las aplicaciones deberán estar hechas de tal forma que se garantice que los usuarios sólo tendrán acceso a los datos que precisen para el desarrollo de sus funciones. El administrador de sistemas establecerá mecanismos para evitar que un usuario pueda acceder a datos sin estar debidamente autorizado.

En caso de que exista personal ajeno al responsable del tratamiento que tenga acceso puntual a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal interno. Es recomendable crear cuentas de usuario específicas en los sistemas de información para este tipo de usuarios.

Identificación y autenticación

El responsable del tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

Será obligatorio establecer 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.

Si el mecanismo de autenticación se basa en contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. Estas contraseñas se deberán almacenar de forma ininteligible y tendrán que cambiarse con una periodicidad no superior al año.

Además, se establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Control de acceso físico

Las instalaciones donde se traten datos personales deberán contar con los medios mínimos de seguridad, que garanticen que los datos protegidos están a salvo de riesgos por incidencias fortuitas o intencionadas.

La estancia donde se ubiquen los servidores será objeto de especial protección, garantizándose en todo momento que están a salvo la disponibilidad, la integridad y confidencialidad de los datos.

El acceso a la ubicación donde se encuentra el Servidor, deberá estar restringido exclusivamente al personal autorizado, y a aquel que deba realizar labores de mantenimiento del mismo.

Telecomunicaciones

La transmisión de datos de carácter personal especialmente protegidos que se realicen a través de redes públicas o redes inalámbricas de comunicaciones electrónicas deberá realizarse cifrando dicha información o utilizando cualquier otro medio que garantice que la información no sea inteligible ni manipulada por terceros. Las medidas habituales consisten en la existencia de redes VPN (IPSEC o SSL) que garantizan la confidencialidad de la información transmitida normalmente mediante protocolos seguros, así como otras tecnologías para la securización de los accesos vía web a las aplicaciones de intranet o internet. Otras opciones consisten en el cifrado de origen a extremo llevado a cabo por los propios usuarios mediante el uso de software específico, certificados digitales, etc.

Puestos de trabajo

Los puestos de trabajo están bajo la responsabilidad de las personas autorizadas, que deberá garantizar que la información que puede mostrarse desde dicho puesto no podrá ser vista por personas no autorizadas. Esto implica que tanto las pantallas como las impresoras y otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

Configuración de las Aplicaciones

Los puestos de trabajo desde los que se tenga acceso a los datos personales tendrán una configuración fija en sus aplicaciones y sistemas operativos, que sólo podrá ser cambiada bajo la autorización del Administrador del sistema. Ningún usuario podrá instalar una aplicación sin autorización del Administrador del sistema, quien analizará si dicha aplicación puede perjudicar otras que traten datos de carácter personal.

Todos los ordenadores deberán tener instalados programas antivirus que deberán, asimismo, estar actualizados diariamente, para así garantizar la protección y detección inmediata de la entrada de virus informáticos en el sistema. Además, los sistemas operativos deberán mantenerse actualizados.

Medidas específicas de los soportes no automatizados:

Procedimiento de archivo

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos deberán garantizar la correcta conservación de los mismos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de los interesados.
En aquellos casos que no exista norma aplicable, el responsable del tratamiento establecerá los criterios y procedimientos de actuación que deban seguirse para el archivo.

Procedimiento para dispositivos de almacenamiento y acceso a la documentación

El responsable del tratamiento o, en su defecto, un tercero autorizado, deberá establecer mecanismos que obstaculicen la apertura de dispositivos o medios de almacenamiento. Asimismo, en caso de que la naturaleza de los mismos impida su aplicación, se deberían fijar medidas que impidan el acceso a personas no autorizadas al lugar de almacenamiento, en la medida de lo posible. Habitualmente, estos procedimientos podrán llevarse a cabo mediante la aplicación de controles de acceso físico (llaves, tarjetas de entrada, biometría, etc.).

Procedimiento de custodia de soportes

En los casos en los que la documentación no se encuentra en dispositivos debidamente protegidos sea con motivo de procesos de revisión, tramitación, previo o posterior a su archivo, el responsable a cargo de la misma deberá custodiarla impidiendo el acceso a terceros no autorizados.

Para ello, entre otras, se deberán tener en cuenta las siguientes recomendaciones:

- Se almacenará de forma protegida la información sensible en papel especialmente cuando se abandone el puesto de trabajo.
- Los puntos de correo, fotocopiadoras, escáner, etc. Deberán estar protegidos para evitar un uso no autorizado.
- Se deben recoger inmediatamente los documentos impresos o enviados a una impresora o fotocopiadora con datos de carácter personal.

Procedimiento de copia o reproducción de documentos

Para los datos especialmente protegidos, se indicarán, asimismo, las personas autorizadas para la realización de copias o reproducción de los mismos, además de garantizar la destrucción de dicha información para evitar así el acceso no autorizado o su recuperación posterior.

Para ello es fundamental dotar de dispositivos de destrucción de documentos a todas las personas con acceso a la documentación y autorizadas para ello.

Procedimiento de acceso a la documentación

Además de la obligación de restricción de accesos a la información contenida en soportes no automatizados por personal no autorizado, en el caso de acceso a la documentación con datos especialmente protegidos se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

Traslado de la documentación

Siempre que se proceda al traslado físico de la documentación con datos especialmente protegidos, deberán anotarse medidas dirigidas a impedir el acceso o manipulación de la información objeto del traslado.

4) VIOLACIONES DE LA SEGURIDAD Y GESTIÓN DE INCIDENCIAS

Artículo 33 RGPD

Notificación de una violación de la seguridad de los datos personales a la autoridad de control

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. 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.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 34 RGPD

Comunicación de una violación de la seguridad de los datos personales al interesado

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple 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 a que se refiere el apartado 1;

c) 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.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

INCIDENCIAS DE SEGURIDAD

Se considerarán como incidencias de seguridad, entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal del responsable del tratamiento.

Asimismo el responsable del tratamiento intentará contemplar el sentido más amplio del concepto de incidencia, entendiendo por tal cualquier situación que contravenga las medidas descritas en la normativa de seguridad, así como el mal funcionamiento de los medios físicos y lógicos que pueda afectar a su disponibilidad y a la seguridad de la información que gestionan.

A continuación se presenta una lista de incidencias que serán inexcusablemente registradas. Esta lista no debe entenderse como limitativa, sino que podrá ser ampliada con cualquier otro tipo de incidencias que hubieran quedado omitidas:

Incidencias que afecten a la identificación y autenticación de los usuarios:
• Pérdida de confidencialidad de contraseñas.
• Asignación o modificación de derechos sobre herramientas de control de acceso y utilidades con accesos privilegiados.
• Períodos de desactivación de las herramientas de seguridad.

Incidencias que afecten a los derechos de acceso a los datos:
• Revisión de logs sobre intentos fallidos de accesos, accesos fuera de horas de oficina, etc.
• Comunicación de los usuarios de sospechas de que alguien ha suplantado su personalidad.
• Detección de puntos de acceso desatendidos y sin protección de pantalla activada.
• Detección de contraseñas escritas en los puestos de trabajo.
• Revisión de los informes de seguridad

Incidencias que afecten a la gestión de soportes:
• Comunicación de pérdida de soportes.
• Comunicación de localización de soportes en lugares inadecuados.
• Errores de contenido en soportes recibidos.

Incidencias que afecten a los procedimientos de copias de salvaguarda y recuperación:
• Errores en los procesos de realización de copias de salvaguarda.
• Recuperaciones de datos realizadas.

Cualquier otra de las observadas como consecuencia de la ejecución de los controles definidos para garantizar el cumplimiento de lo dispuesto en el Documento de Seguridad.

La aplicación del presente Procedimiento se establece para todas las Áreas del responsable del tratamiento, empleados y colaboradores externos.

Responsabilidades

El Responsable se encargará de la redacción y mantenimiento de este procedimiento; así como de su custodia y archivo.

Todos los usuarios de la entidad deben informar de cualquier incidencia producida en materia de seguridad.

El Responsable debe ocuparse del seguimiento de las incidencias en materia de seguridad.

Los usuarios de los sistemas de información, empleados y colaboradores externos, deben participar en la implantación y seguimiento de la política de seguridad, aceptando formalmente sus obligaciones.

Comunicación de Incidencias de Seguridad por Usuarios

Cualquier usuario que tenga conocimiento directa o indirectamente de cualquier incidencia de seguridad, actual o posible, lo comunicará con la mayor brevedad tal incidencia y las acciones que se hubiesen tomado de urgencia.

En este momento se procede a incluirse en el registro y, si afecta a la seguridad de los datos de carácter personal, marcarla como tal.

Registro y Distribución de las Incidencias

Con el fin de poder mantener un registro de incidencias que permita su mantenimiento y posterior tratamiento y análisis se centralizará la recepción de las mismas en una misma persona designada por el responsable.

En el caso de incidencias sobre procesos o aplicaciones se comunicarán directamente al Responsable informático, quien se ocupará de informar al responsable sobre su resolución.

Registros

El registro de incidencias será mantenido en exclusiva por el responsable.
Se facilitará el acceso estrictamente a aquellos departamentos que lo necesiten, para su consulta o análisis encaminado al estudio de acciones a llevar a cabo para la resolución de las incidencias.

Se facilitarán los formularios necesarios para llevar a cabo el registro de las incidencias. El conocimiento y la no-notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del tratamiento por parte de ese usuario.

5) CONTRASEÑAS Y COPIAS DE SEGURIDAD

Autenticación

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. Cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible. Este sistema de autenticación debe venir acompañado por una política de restricción de accesos, esto es, que exista una política en la empresa de controlar los accesos de información únicamente en lo estrictamente necesario al puesto de trabajo concreto y a las funciones que se deben desarrollar en él, siendo consecuente, que a mayor cargo y responsabilidad, mayor será el acceso que pueda obtenerse de la información del sistema, así como la restricción de acceso a la información por áreas o departamentos.

El sistema actual utilizado por el Responsable en el tratamiento en cuanto a la autenticación de las entradas en el sistema, es el que a continuación se describe:

En cuanto a las claves de acceso, el sistema operativo requiere usuario / contraseña para iniciar la sesión, éstas son dadas por el responsable de sistemas a los usuarios.

El procedimiento que se recomienda seguir para el cambio de contraseña entre los usuarios de el responsable del tratamiento es el siguiente:

1) Siempre que sea posible el sistema ha de pedir el cambio de contraseña no permitiendo volver a usar una contraseña ya utilizada anteriormente.

2) Si el punto 1 no es posible por limitaciones del sistema el administrador de sistemas pedirá personalmente a cada usuario la nueva contraseña. El usuario deberá comunicarla al administrador en un plazo máximo de 24 horas y esta comunicación se realizará por medios que garanticen la confidencialidad de la contraseña.

3) Una vez que el administrador de sistemas disponga de todas las contraseñas, validará que no sea una contraseña ya utilizada anteriormente. El administrador de sistemas cambiará la contraseña del usuario para todas las aplicaciones que la requieran junto con la contraseña del sistema operativo y red (recursos compartidos).

4) Se verificará que el cambio de las contraseñas se ha realizado correctamente.

5) Se comunicará a los usuarios el momento del cambio y cuando pueden empezar a utilizar la nuevas contraseñas haciendo hincapié en el tema de la confidencialidad. Para llevar a cabo correctamente este procedimiento será necesario disponer de una lista/fichero protegida/o con las aplicaciones y puntos del sistema informático que requieran contraseña.

A cada usuario del sistema informático de le será asignado un nombre de usuario, que asociado a una contraseña, lo identificará dentro de los sistemas de información y permitirá el acceso a las áreas relacionadas con su actividad profesional.

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 solicitar el cambio al Responsable de Seguridad.

Cuando se incorpore un usuario nuevo el responsable de tratamiento se encargará de comunicarlo al departamento de sistemas para que se le dé de alta conforme a los permisos que le sean asignados. En esta alta se le asignará un nombre de usuario y una contraseña. No está permitida la divulgación de la clave por circunstancia alguna a otras personas integrantes de la plantilla o ajenas a la entidad.

Copias de Seguridad

La seguridad de los datos personales no sólo supone la confidencialidad de los mismos, sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos de los ficheros con datos de carácter personal.

El responsable del tratamiento se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Procedimiento de respaldo

Debe fijarse y definirse un proceso de copia total de todos los archivos del sistema a través de cualquier medio válido que asegure la recuperación. El Responsable de realizarlas es el Responsable de Copias de Seguridad o el responsable de sistemas, por un medio automatizado. Se aconseja, especialmente, la copia en disco externo para almacenarla fuera del servidor de la empresa.

Procedimiento de recuperación

Cuando se produzca una pérdida total o parcial de datos de cualquiera de los servidores se deberán tener en cuenta los siguientes puntos:

• Dejar constancia en el libro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones rellenando el formulario con todos los datos requeridos.

• La recuperación deberá realizarse partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia que permita reconstruir los datos del fichero al estado en que se encontraban antes del momento del fallo o pérdida.

Soportes para los respaldos

Los soportes de las copias de seguridad se podrán reciclar. Aún así, si alguno dejará de ser fiable para su funcionamiento, deberá ser destruido físicamente de forma que sea imposible la recuperación de los datos. Antes de reciclar cualquier soporte el personal autorizado para realizar las copias deberá verificar si es o no óptimo para su funcionamiento. Se designará por el responsable un recinto donde se guardarán los soportes de las copias de seguridad, que se mantendrá constantemente cerrado con llave y protegido.

Para datos especialmente protegidos, se aconseja conservar una copia de seguridad en un lugar diferente a aquel que se encuentren los equipos que tratan los datos o utilizar elementos que garanticen la integridad y recuperación de la información.

6) GESTIÓN DE SOPORTES Y DOCUMENTOS

Los soportes informáticos son todos aquellos medios físicos susceptibles de ser tratados en los sistemas de información, y sobre los que se pueden grabar y recuperar datos (equipos, discos, pendrives, etc.). El control de estos medios tiene una importancia fundamental, dada la facilidad para su transporte y reproducción.

Inventario

Los soportes o documentos que contengan datos de carácter personal deben estar claramente identificados con una etiqueta externa que permita identificar a través de algún identificador que tipo de datos contienen (salvo que las características físicas del soporte o documento lo impidan).

Dicho sistema debe permitir mantener un inventario de los soportes, donde se pueda registrar otra información adicional, como fecha de creación, fecha de baja, motivo de la baja, etc.

La identificación de los soportes para información especialmente sensible puede establecerse mediante una codificación que dificulte la identificación para usuarios no autorizados. Los soportes o documentos que contengan datos de carácter personal deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas.

Autorización salida o entrada de soportes

La salida de datos de carácter personal pertenecientes a los tratamientos definidos en el presente documento, sea cual sea el medio utilizado (incluye los comprendidos y/o anexos a un correo electrónico), sólo estará permitida cuando sea necesario para el desempeño de las funciones propias de la empresa, y cuando así lo autorice el Responsable del Tratamiento.

Los soportes o documentos que deban salir de las ubicaciones habituales deberán ser transportados con la debida protección frente a robos, sustracciones o accesos no autorizados, teniendo en cuenta la sensibilidad de la información. A ser posible el transporte se realizará de forma codificada o mediante otros mecanismos similares que puedan garantizar su protección durante su salida de la ubicación habitual. La tecnología de cifrado también es aplicable a los documentos como correo electrónico o equipos portátiles cuando se empleen fuera de las instalaciones.

Registro salida o entrada de soportes

La salida o entrada de soportes deberá registrarse expresamente mediante el formulario habilitado.
Este registro deberá contener el tipo de documentos o soportes, 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 o entrega.

Si la salida de dichos soportes o documentos fuera periódica como el caso de portátil, PDA, etc. podrá hacerse un registro/autorización genérico especificándolo en la hoja de registro. El movimiento de soportes entre departamentos no se considerará a estos efectos.

Reutilización o desechado de soportes

Cuando un soporte que contenga datos de carácter personal vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario en caso que no se sustituya por otro soporte destinado a la misma función.

Entrada y Salida de Datos por Red

La transmisión de datos por red, ya sea por medio de correo electrónico o mediante sistemas de transferencia de ficheros, se está convirtiendo en uno de los medios más utilizados para el envío de datos, hasta el punto de que está sustituyendo a los soportes físicos. Por ello merece un tratamiento especial ya que, por sus características, puede ser más vulnerable que los soportes físicos tradicionales.

El envío de datos de los ficheros protegidos por correo electrónico sólo se realizará cuando sea necesario para el desempeño de las funciones propias de la empresa. En todo caso, el usuario que realice o pretenda realizar el envío de los datos deberá ser un usuario autorizado para el tratamiento de esos datos.

La obligación de dicho usuario será la de asegurarse de que la entrega o envío de esa información es legítima en virtud de lo establecido en la presente normativa aplicable y en el presente Documento de Seguridad.

El envío de información entre personal interno o entre departamentos, no se considerará entrada y salida de datos a los efectos de la presente normativa.

7) TRATAMIENTOS

Registro de Actividades de Tratamiento

Cada Responsable del tratamiento y Encargado llevará un registro (Anexo A) de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

- Nombre y datos de contacto del responsable o corresponsable y del Delegado de Protección de Datos si existiese.
- Finalidades del tratamiento.
- Descripción de categorías de interesados y categorías de datos personales tratados.
- Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
- Transferencias internacionales de datos.
- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

El registro (Anexo A) constará por escrito, inclusive en formato electrónico. El responsable o el encargado del tratamiento pondrán el registro a disposición de la autoridad de control que lo solicite.

8) CONTROLES PERIÓDICOS / AUDITORÍAS

El responsable llevará a cabo controles periódicos que verifiquen el cumplimiento de las normas establecidas en el reglamento europeo y de las medidas de seguridad y organizativas descritas en el documento de seguridad, así como controlar que documentalmente las modificaciones estén actualizadas: nuevos trabajadores que firman el documento de autorización del consentimiento, contratos con los posibles nuevos encargados del tratamiento, rutinas de registros, incidencias, entradas y salidas, etc.

Periódicamente los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, a una auditoría interna o externa que verifique el cumplimiento de las normas establecidas en el reglamento europeo y en el documento de seguridad.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con objeto de verificar la adaptación, adecuación y eficacia de las mismas.

Los informes de auditoría serán analizados por el Responsable del tratamiento para que adopte las medidas correctoras adecuadas.

9) ENCARGADOS DE TRATAMIENTO

El Reglamento Europeo establece que cuando exista un tratamiento de datos por cuenta de terceros, ya sea de forma parcial o de modo exclusivo, el documento de seguridad deberá contener la identificación de dichos tratamientos, así como un contrato que regule las condiciones del encargo.

Esta exigencia se cumple a través de los modelos de contrato de encargo de tratamiento que se facilitan a través de la implantación, ya que mediante la auto cumplimentación de datos, cada uno de los contratos de encargo de tratamiento identificarán además de la empresa con la que se ha contratado los servicios que llevan implícita la comunicación y cesión de datos, es decir, la identificación del Encargo de Tratamiento, así como el resto de información a la que viene referida el artículo 28 del reglamento europeo, se señalará qué datos quedan sujetos a las cesiones o accesos de datos que deba realizar el Encargado de tratamiento para poder prestar el servicio contratado.

En un régimen diferente, ya que no se produce un tratamiento de los datos, pero para salvaguardar el posible acceso y conocimiento de datos de carácter personal titularidad del Responsable del tratamiento, encontramos terceras personas, que por la naturaleza de sus servicios (mantenimiento, mensajería y auxiliar-administrativos) tienen acceso a determinada información del centro, convirtiéndose en cesionarios de la empresa. Normalmente, son autónomos colaboradores y prestadores de algún servicio profesional que acceden a la base de datos del Responsable del Tratamiento, por lo que se hace necesario firmar el oportuno documento de acceso de datos y confidencialidad.

4) ANEXOS (MEDIDAS PROACTIVAS)

1. Anexo A
Registro de actividades de tratamiento y relación de encargados de tratamiento.
2. Anexo B
Descripción de la estructura del sistema informático.
3. Anexo C
Riesgos, Medidas de Seguridad y Políticas de Acceso.
4. Anexo D
Locales: Sede principal y delegaciones.
5. Anexo E
Nombramientos y autorizaciones:
 1. Lista de responsables.
 2. Lista de autorizaciones.
6. Anexo F
Violaciones de Seguridad y incidencias.
7. Anexo G
Procedimientos de control y seguridad:
G.1. Procedimiento de respaldo y recuperación.
G.2. Procedimiento de gestión de salida de soportes.
G.3. Procedimiento de gestión de entrada de soportes.
G.4. Autorización para el uso de ordenadores portátiles y trabajo fuera de locales.
8. Anexo H
 1. Programas y aplicaciones
 2. Equipamientos
 3. Soportes
 4. Copias

ANEXO A Registro de actividades de tratamiento

Este anexo contiene la relación de tratamientos llevados a cabo por el responsable, y además una relación de los encargados del tratamiento.

Listado de tratamientos propios

Relación de tratamientos propios del responsable Margarita Queijo Rodríguez.

Tratamiento PROPIO	Código: 1

Fecha: 05/10/2020
Nombre: Clientes/Proveedores
Encargado: Endurance International Group, Inc. (Hostgator.com)
Responsable: Margarita Queijo Rodríguez
Finalidad: Gestión administrativa y comercial de la cartera de clientes de la empresa.
Medidas técnicas: Las detalladas en el documento de seguridad.
Base legitimadora: Legitimación por consentimiento del interesado, Legitimación por ejecución de un contrato
Colectivos de interesados: Clientes y proveedores.
Categorías de datos: Datos identificativos: Nombre y Apellidos, Teléfono, CIF / NIF, Dirección Postal o Electrónica, Firma manual, manuscrita o digitalizada. Otros datos tipificados: Económicos, financieros o de seguros,
Cesiones: Bancos, cajas de ahorros y cajas rurales.Organizaciones o personas directamente relacionadas con el responsable. Administración tributaria
Duración: Finalización de la relación contractual, salvo conflicto con normativa de índole superior
Observaciones: Nivel de seguridad: No sensible

Tratamiento PROPIO	Código: 2

Fecha: 05/10/2020
Nombre: Usuarios Web
Encargado: Endurance International Group, Inc. (Hostgator.com)
Responsable: Margarita Queijo Rodríguez
Finalidad: Gestión de clientes, contable, fiscal y administrativa. Publicidad y prospección comercial
Medidas técnicas: Las detalladas en el documento de seguridad.
Base legitimadora: Legitimación por consentimiento del interesado
Colectivos de interesados: Clientes, Usuarios, Personas de contacto
Categorías de datos: Datos identificativos: Nombre y Apellidos, Dirección Postal o Electrónica, Teléfono
Duración: Finalización de la relación contractual, salvo conflicto con normativa de índole superior
Observaciones: Nivel de seguridad: No sensible

Tratamiento PROPIO	Código: 3

Fecha: 05/10/2020
Nombre: Historial Clínico
Responsable: Margarita Queijo Rodríguez
Finalidad: Gestión de historiales clínicos
Medidas técnicas: Las detalladas en el documento de seguridad.
Base legitimadora: Legitimación por consentimiento del interesado
Colectivos de interesados: Pacientes, Padres o tutores, Representante legal
Categorías de datos: Datos identificativos: Nombre y Apellidos, Dirección Postal o Electrónica, Teléfono, Nº de la Seguridad Social, CIF / NIF, Tarjeta Sanitaria, Firma manual, manuscrita o digitalizada. Otros datos tipificados: Características personales, Económicos, financieros o de seguros. Otros datos especialmente protegidos: Salud
Cesiones: Organizaciones o personas directamente relacionadas con el responsable, Organismos de la seguridad social, Entidades aseguradoras, Entidades sanitarias
Duración: Finalización de la relación contractual, salvo conflicto con normativa de índole superior
Observaciones: Nivel de seguridad: Sensible

Listado de tratamientos de terceros

No existen datos para este anexo o documento.

Relación de tratamientos por cuenta de terceros donde Margarita Queijo Rodríguez actúa como encargado.

Encargados con acceso

Listado de encargados con acceso a datos

Relación de empresas que prestan algún servicio al responsable del tratamiento, y dicho servicio implica tratamiento de datos personales.

Encargados con acceso	código: 1

Nombre del encargado: Endurance International Group, Inc. (Hostgator.com) **Nif:** 0
Dirección: Sophialaan 32, 8911 AE
Servicio que prestará el encargado: Alojamiento de la web y del correo electrónico
Descripción detallada del servicio prestado: Alojamiento de la web y del correo electrónico
Concreción de los tratamientos a realizar: Recogida, Conservación, Registro, Modificación, Comunicación
Descripción de la información que el responsable pone a disposición del encargado: Nombre y apellidos, email y datos de contacto
Datos del DPD: No se aplica
Duración del contrato: un año, renovable automáticamente siempre y cuando se mantenga vigente la relación mercantil de prestación de servicios
Fecha del contrato: 05/10/2020

Encargados sin acceso

No existen datos para este anexo o documento.

Relación de empresas que prestan algún servicio al responsable del tratamiento, y dicho servicio NO implica tratamiento de datos personales.

Responsables

No existen datos para este anexo o documento.

Relación de empresas a las cuales se les presta un servicio, y Margarita Queijo Rodríguez actúa como encargado.

ANEXO B Estructura informática

Este anexo contiene la descripción de la estructura del sistema informático, el tipo de red y el entorno de las comunicaciones.

Estructura informática	Código: 1
Página web: www.marinamelia.com **Descripción de la estructura informática:** 1 Ordenador Portátil **Esta estructura pertenece al local o locales:** Oficina 1, Oficina 2	

ANEXO H Equipamiento

Inventario de los equipos informáticos que tratan datos personales.

Características del equipos/s	Código: 1

Tipo equipo: Ordenador portátil **Cantidad:** 1
Descripción: Lenovo 110S
Nº serie o identificadores: A01
Tratamientos que realiza: Clientes/Proveedores, Usuarios Web, Historial Clínico,
Usuarios o perfiles que lo utilizan: Margarita Queijo Rodríguez,
Local donde se encuentra este equipo: Oficina 1, Oficina 2,
Sistema operativo: Windows 10 Home
Antivirus: Windows Defender
Fecha de alta: 05/10/2020 **Fecha de baja:**

ANEXO H Programas y aplicaciones

Lista de los programas Ofimáticos, Gestores de Facturación, Contabilidad, etc.. que traten datos personales.

Programa / Aplicación:	Código: 1

Nombre: Microsoft Office
Cantidad: 1
Finalidad y descripción: Ofimática
Tratamientos que realiza: Todos los tratamientos
Usuarios que lo ejecutan: Margarita Queijo Rodríguez
Equipos donde se ejecuta: Ordenador portátil (Lenovo 110S)
Registro de accesos: NO
Fecha de alta: 05/10/2020 **Fecha de baja:**

Programa / Aplicación:	Código: 2

Nombre: WhatsApp
Cantidad: 1
Finalidad y descripción: Comunicación
Tratamientos que realiza: Clientes/Proveedores,
Usuarios que lo ejecutan: Margarita Queijo Rodríguez
Equipos donde se ejecuta: Ordenador portátil (Lenovo 110S)
Registro de accesos: NO
Fecha de alta: 05/10/2020 **Fecha de baja:**

ANEXO D Locales donde se tratan datos personales

Este anexo contiene una relación de los locales donde se tratan datos personales.

Local	código: 1

Nombre del local: Oficina 1
Dirección completa del local: C/ Real 66, 1º - 15003, A Coruña
Descripción física del local: Oficina 1
Control de acceso: Personal de la empresa autorizado con llave de la entrada principal
Sistemas de seguridad:
Tratamientos: Clientes/Proveedores, Usuarios Web, Historial Clínico

Observaciones:

Local	código: 2

Nombre del local: Oficina 2
Dirección completa del local: C/Emilio González López 13-6º A, 15011, A Coruña
Descripción física del local: Domicilio particular
Control de acceso: Personal de la empresa autorizado con llave de la entrada principal
Sistemas de seguridad:
Tratamientos: Clientes/Proveedores, Usuarios Web, Historial Clínico

Observaciones:

ANEXO E Nombramientos

Este anexo contiene una relación de los diferentes responsables en materia de protección de datos, todos ellos nombrados o autorizados por el Responsable del Tratamiento: Margarita Queijo Rodríguez.

Nombramiento	código: 1

Administrador
Nombre y Apellidos: Margarita Queijo Rodríguez
Dni: 33274407P
Cargo/función en la empresa: Persona designada para conceder, alterar, o anular el acceso autorizado a los datos.
Fecha de Alta: 05/10/2020
Fecha de Baja:
Tratamientos que realiza: Clientes/Proveedores, Usuarios Web, Historial Clínico

Fdo. Responsable del tratamiento:

Fdo. Administrador:

Nombramiento	código: 2

Responsable de proteción de datos
Nombre y Apellidos: Margarita Queijo Rodríguez
Dni: 33274407P
Cargo/función en la empresa:
Fecha de Alta: 05/10/2020
Fecha de Baja:
Tratamientos que realiza: Clientes/Proveedores, Usuarios Web, Historial Clínico

Fdo. Responsable del tratamiento:

Fdo. Responsable de proteción de datos:

Nombramiento	código: 3

Responsable de copias de respaldo y recuperación
Nombre y Apellidos: Margarita Queijo Rodríguez
Dni: 33274407P
Cargo/función en la empresa:
Fecha de Alta: 05/10/2020
Fecha de Baja:
Tratamientos que realiza: Clientes/Proveedores, Usuarios Web, Historial Clínico

Fdo. Responsable del tratamiento:

Fdo. Responsable de copias de respaldo y recuperación:

Nombramiento	código: 4

Responsable de la gestión de incidencias
Nombre y Apellidos: Margarita Queijo Rodríguez
Dni: 33274407P
Cargo/función en la empresa:
Fecha de Alta: 05/10/2020
Fecha de Baja:
Tratamientos que realiza: Clientes/Proveedores, Usuarios Web, Historial Clínico

Fdo. Responsable del tratamiento:

Fdo. Responsable de la gestión de incidencias:

Nombramiento	código: 5

Responsable de atención a los afectados
Nombre y Apellidos: Margarita Queijo Rodríguez
Dni: 33274407P
Cargo/función en la empresa:
Fecha de Alta: 05/10/2020
Fecha de Baja:
Tratamientos que realiza: Clientes/Proveedores, Usuarios Web, Historial Clínico

Fdo. Responsable del tratamiento:

Fdo. Responsable de atención a los afectados:

ANEXO E Autorizaciones con acceso

Lista de usuarios con acceso a los datos.

Usuario con acceso	código: 1

Nombre y Apellidos: Margarita Queijo Rodríguez **Dni:** 33274407P
Funciones o tipo de usuario: Administradora
Tratamientos que realiza: Clientes/Proveedores, Usuarios Web, Historial Clínico
Locales donde se ubica: Oficina 1, Oficina 2
Fecha de alta: 05/10/2020 **Fecha de baja:**

ANEXO E **No existen datos para este anexo o documento.**

Lista de usuarios sin acceso a los datos.

ANEXO F Registro de violaciones de seguridad e incidencias

Registro de violaciones de seguridad y incidencias para comunicar si procede, a la autoridad de control, a los interesados o al responsable.

ANEXO F **Registro manual de violaciones de seguridad e incidencias**

Registro manual de violaciones de seguridad y incidencias para comunicar si procede, a la autoridad de control, a los interesados o al responsable.

Nº:	Fecha:

Naturaleza:
Categorías y número aproximado de interesados afectados:
Categorías y número aproximado de registros de datos personales afectados:
Nombre y los datos de contacto del DPD o de otro punto de contacto en el que pueda obtenerse más información:
Describir las posibles consecuencias de la violación de la seguridad de los datos personales:
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:
Nombre: Firma:

ANEXO G.1 Procedimiento de respaldo y recuperación

No existen datos para este anexo o documento.

Medidas proactivas — Relación de soportes

No existen datos para este anexo o documento.

MEDIDAS PROACTIVAS **Registro de copias realizadas**

En este apartado se archivan los registros de las copias de seguridad realizadas. En el caso de reutilización o eliminación de soportes grabados con datos personales se utilizará una aplicación informática para el borrado y formateo físico de los datos.

ANEXO H Registro manual de las copias realizadas

Ref. Soporte	Fecha Copia	Datos que contiene	Responsable	Resultado de la copia

ANEXO G.2 Procedimiento de gestión de salida de soportes

Cualquier salida de soportes fuera de los locales donde se tratan datos deberá ser autorizada por el responsable del tratamiento de acuerdo al documento adjunto.
El responsable del tratamiento mantendrá un Libro en el que registrará las salidas de soportes, cuyos asientos estarán constituidos por los documentos de autorización de salida debidamente cumplimentados. La persona responsable de la entrega de soportes estará debidamente autorizada por el responsable del tratamiento.

ANEXO G.2 Gestión manual de salida de soportes

Fecha y Hora de Salida:	**Referencia del soporte:**
Tipo de información que contiene:	**Tipo de soporte (documento, disco, etc..):**
Datos del destinatario:	**Cantidad de soportes incluidos en el envío:**
Medio de transporte utilizado:	**Medidas de seguridad adoptadas para su transporte:**
Responsable que autoriza la persona que realiza la entrega. **Nombre:** **Firma:**	**Persona que realiza la entrega del soporte.** **Nombre:** **Firma:**

ANEXO G.3 Procedimiento de gestión de entrada de soportes

El responsable del tratamiento mantendrá un Libro en el que registrará las entradas de soportes cuyos asientos estarán constituidos por los datos recogidos en el formulario que se adjunta.

La persona responsable de la recepción de soportes estará debidamente autorizada por el responsable del tratamiento.

ANEXO G.3 Gestión manual de entrada de soportes

Fecha y Hora de Entrada:	**Referencia del soporte:**
Ficheros que contiene:	**Tipo de soporte(documento, disco, etc..):**
Datos del emisor:	**Cantidad de soportes incluidos en el envío:**
Medio de transporte utilizado:	**Medidas de seguridad adoptadas para su transporte:**
Responsable que autoriza la persona que realiza la recepción. **Nombre:** **Firma:**	**Persona que realiza la recepción del soporte.** **Nombre:** **Firma:**

ANEXO G4 Autorización para el uso de PC portátiles

El tratamiento, acceso y transporte de datos personales en ordenadores portátiles, estará sujeto en todo caso a una autorización expresa del responsable del tratamiento o persona delegada, y sujeta a las mismas normas de seguridad que las de un puesto de trabajo fijo.

Se deberán adjuntar en este apartado las autorizaciones explícitas por parte del responsable del tratamiento o persona autorizada, para el trabajo en ordenadores portátiles fuera del local habitual, indicando la identificación de la persona autorizada, la identificación del equipo, los datos que contiene, y las medidas extraordinarias para evitar la pérdida de confidencialidad de los datos en caso de robo o, pérdida del equipo.

Se cifrarán los datos que contengan los ordenadores portátiles cuando estos se encuentren fuera de las instalaciones que están bajo el control del responsable, si esto no es posible se hará constar las medidas alternativas que se adopten.

Utilizar el siguiente formulario para ello.

ANEXO G.4 Autorización para el uso de PC portátiles

Nombre y firma persona autorizada: **Nombre y firma del responsable que autoriza:**	**Identificación del equipo:**
Tratamiento que contiene:	**Fecha autorización:** **Periodo de validez:**

Detallar las medidas extraordinarias para evitar la pérdida de confidencialidad de los datos en caso de robo o pérdida del equipo:
Se cifrarán los datos que contengan los ordenadores portátiles cuando estos se encuentren fuera de las instalaciones que están bajo el control del responsable, si esto no es posible se hará constar las medidas alternativas que se adopten. **Medidas alternativas:**

5)

Solicitudes de derechos.
Modificaciones del Documento de Seguridad.
Auditorías y controles periódicos realizados.
Registro de accesos (si existe).
Relación de cesionarios.
Recomendaciones del consultor.

REGISTRO DE MODIFICACIONES DEL DOCUMENTO DE SEGURIDAD Y ANEXOS

El responsable del tratamiento o la persona delegada, será el encargado de actualizar el documento de seguridad, los anexos y también de divulgar los cambios realizados. Cada vez que se actualice el documento de seguridad se anotará en el siguiente formulario.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los tratamientos o como consecuencia de los controles periódicos realizados. En todo caso se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

MODIFICACIONES Registro manual de Modificaciones

Lista de las modificaciones o actualizaciones realizadas en el documento de seguridad, anexos u otros documentos.

Código	Fecha	Versión	Documento o apartado modificado	Descripción de la modificación

REGISTRO DE AUDITORÍAS Y CONTROLES PERIÓDICOS

Este apartado contendrá los resultados de los controles periódicos y de las auditorías realizadas en la empresa.

Registro manual de auditorías y controles periódicos

Tipo de Control	Fecha	Documento/s Revisado/s	Resultado del Control	Persona/s o Departamentos que han intervenido

REGISTRO DE ACCESOS

El registro de accesos es una medida de control que se aconseja cunado se tratan datos especialmente protegidos. Consiste en un control y registro de los accesos a los datos por parte de los usuarios. El responsable debe realizar una revisión e informe mensual del mencionado registro. Se recomienda utilizar una aplicación informática para implantar esta medida, pues genera una gran cantidad de datos.

Documento para el Registro manual de los accesos a los tratamientos o Documentos no automatizados.

Usuario: Fecha y Hora: Tratamiento accedido: Tipo de acceso: Autorizado o Denegado: Registro accedido: Cambios realizados: Finalidad:
Usuario: Fecha y Hora: Tratamiento accedido: Tipo de acceso: Autorizado o Denegado: Registro accedido: Cambios realizados: Finalidad:
Usuario: Fecha y Hora: Tratamiento accedido: Tipo de acceso: Autorizado o Denegado: Registro accedido: Cambios realizados: Finalidad:
Usuario: Fecha y Hora: Tratamiento accedido: Tipo de acceso: Autorizado o Denegado: Registro accedido: Cambios realizados: Finalidad:
Usuario: Fecha y Hora: Tratamiento accedido: Tipo de acceso: Autorizado o Denegado: Registro accedido: Cambios realizados: Finalidad:

Hoja Nº:

Listado de cesionarios

No existen datos para este anexo o documento.

5. DERECHOS DE LOS INTERESADOS

1. Ejercicio de los derechos de los interesados (ARCO).
2. Modelos de acceso, rectificación, supresión u olvido, limitación, portabilidad, oposición y decisiones automatizadas.

DERECHOS DEL INTERESADO

Sección 1

Transparencia y modalidades

Artículo 12

Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado

1.- El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2.- El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3.- El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4.- Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

5.- La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o

b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6.- Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7.- La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá

transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8.- La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Sección 2

Información y acceso a los datos personales

Artículo 13

Información que deberá facilitarse cuando los datos personales se obtengan del interesado

1.- 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:

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

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) 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, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2.- Además de la información mencionada en el apartado 1, 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:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) 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;

c) 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 basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) 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 que no facilitar tales datos;

f) la existencia de decisiones automatizas, 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.

1. 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 a tenor del

apartado 2.

2. Las disposiciones de los apartados 1 y 2 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 14

Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado

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

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

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

d) las categorías de datos personales de que se trate;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) 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, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.

2. 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:

a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;

b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;

c) 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;

d) 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;

e) el derecho a presentar una reclamación ante una autoridad de control;

f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

g) 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.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:

a) 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;

b) 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

c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. 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 indicada en el apartado 2.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;

b) 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;

c) 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

d) 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.

Artículo 15

Derecho de acceso del interesado

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) 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;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) 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;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) 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.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

Sección 3

Rectificación y supresión

Artículo 16

Derecho de rectificación

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. 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.

Artículo 17

Derecho de supresión («el derecho al olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) 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;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) 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;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 18

Derecho a la limitación del tratamiento

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b) 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;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Artículo 19

Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Artículo 20

Derecho a la portabilidad de los datos

1. 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:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al 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.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Sección 4

Derecho de oposición y decisiones individuales automatizadas

Artículo 21

Derecho de oposición

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. 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.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

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

4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Artículo 22

Decisiones individuales automatizadas, incluida la elaboración de perfiles

1. Todo interesado tendrá 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.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas 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 la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Sección 5

Limitaciones

Artículo 23

Limitaciones

1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;

e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;

f) la protección de la independencia judicial y de los procedimientos judiciales;

g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);

i) la protección del interesado o de los derechos y libertades de otros;

j) la ejecución de demandas civiles.

2. En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:

a) la finalidad del tratamiento o de las categorías de tratamiento;

b) las categorías de datos personales de que se trate;

c) el alcance de las limitaciones establecidas;

d) las garantías para evitar accesos o transferencias ilícitos o abusivos;

e) la determinación del responsable o de categorías de responsables;

f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento;

g) los riesgos para los derechos y libertades de los interesados, y

h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.

(RGPD) MODELO DE EJERCICIO DEL DERECHO DE ACCESO

DATOS DEL RESPONSABLE DEL TRATAMIENTO
Nombre: Margarita Queijo Rodríguez
Nombre y dirección de la Oficina de acceso: Margarita Queijo Rodríguez C/ Real 66, 1º - 15003 - A Coruña - A CORUÑA

DATOS DEL SOLICITANTE:

D./Dª ....., mayor de edad, con domicilio en la C/ .....
N.º..... C.P ..... Localidad ..... Provincia .....
E-mail.....con D.N.I ....., del que acompaña fotocopia.

EXPONE:

Que por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con el artículo 15 del Reglamento General de Protección de Datos (RGPD).

SOLICITA:

1.- Que se le facilite gratuitamente el acceso a sus datos personales, en el plazo máximo de un mes a contar desde la recepción de esta solicitud. Dicho plazo podrá prorrogarse otros dos meses, informando al interesado de dicha prorroga antes de un mes, junto con los motivos del retraso.

2.- Que la información facilitada comprenda: 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, 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.

3.- Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

En _____ a _____ de _____de 20__

Firmado:

INSTRUCCIONES:
Es necesario aportar fotocopia del D.N.I. o cualquier otro medio de identificación personal válido en derecho, para que el responsable del tratamiento pueda realizar la comprobación oportuna. En caso de que se actúe a través de representación legal (menor de edad o incapacitado) deberá aportarse, además de la fotocopia del DNI, la documentación que acredite la representación legal.
La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos.

(RGPD) MODELO DE EJERCICIO DEL DERECHO DE RECTIFICACIÓN

DATOS DEL RESPONSABLE DEL TRATAMIENTO
Nombre: Margarita Queijo Rodríguez
Nombre y dirección de la Oficina de acceso: Margarita Queijo Rodríguez C/ Real 66, 1º - 15003 - A Coruña - A CORUÑA

DATOS DEL SOLICITANTE:

D./Dª ....., mayor de edad, con domicilio en la C/ .....
N.º..... C.P ..... Localidad ..... Provincia .....
E-mail.....con D.N.I ....., del que acompaña fotocopia.

EXPONE:

Que por medio del presente escrito manifiesta su deseo de ejercer su derecho de rectificación, de conformidad con el artículo 16 del Reglamento General de Protección de Datos (RGPD).

SOLICITA:

1.- Que se proceda gratuitamente a la efectiva rectificación de los datos personales inexactos que me conciernen. Y teniendo en cuenta los fines del tratamiento, que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

2.- Que el responsable responda en el plazo máximo de un mes a contar desde la recepción de esta solicitud, dicho plazo podrá prorrogarse otros dos meses, informando al interesado de dicha prorroga antes de un mes, junto con los motivos del retraso.

3.- Que el responsable del tratamiento comunique cualquier rectificación de datos personales a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

4.- Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

En _____ a _____ de _____de 20__

Firmado:

INSTRUCCIONES:
Es necesario aportar fotocopia del D.N.I. o cualquier otro medio de identificación personal válido en derecho, para que el responsable del tratamiento pueda realizar la comprobación oportuna. En caso de que se actúe a través de representación legal (menor de edad o incapacitado) deberá aportarse, además de la fotocopia del DNI, la documentación que acredite la representación legal.
La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos.

(RGPD) MODELO DE EJERCICIO DEL DERECHO DE SUPRESIÓN O DERECHO AL OLVIDO

DATOS DEL RESPONSABLE DEL TRATAMIENTO
Nombre: Margarita Queijo Rodríguez
Nombre y dirección de la Oficina de acceso: Margarita Queijo Rodríguez C/ Real 66, 1º - 15003 - A Coruña - A CORUÑA

DATOS DEL SOLICITANTE:

D./Dª ....., mayor de edad, con domicilio en la C/ .....
N.º..... C.P ..... Localidad ..... Provincia .....
E-mail.....con D.N.I ....., del que acompaña fotocopia.

EXPONE:

Que por medio del presente escrito manifiesta su deseo de ejercer su derecho de supresión o derecho al olvido, de conformidad con el artículo 17 del Reglamento General de Protección de Datos (RGPD).

SOLICITA:

1.- Que se proceda a la efectiva supresión de los datos personales que le conciernan.

2.- Que el responsable responda en el plazo máximo de un mes a contar desde la recepción de esta solicitud, dicho plazo podrá prorrogarse otros dos meses, informando al interesado de dicha prorroga antes de un mes, junto con los motivos del retraso.

3.- Que cuando se hayan hecho públicos los datos personales y esté obligado a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

4.- Que el responsable del tratamiento comunique cualquier supresión de datos personales a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

5.- Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

En _____ a _____ de _____de 20__

Firmado:

INSTRUCCIONES:
Es necesario aportar fotocopia del D.N.I. o cualquier otro medio de identificación personal válido en derecho, para que el responsable del tratamiento pueda realizar la comprobación oportuna. En caso de que se actúe a través de representación legal (menor de edad o incapacitado) deberá aportarse, además de la fotocopia del DNI, la documentación que acredite la representación legal.
La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos.

(RGPD) MODELO DE EJERCICIO DEL DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

DATOS DEL RESPONSABLE DEL TRATAMIENTO
Nombre: Margarita Queijo Rodríguez
Nombre y dirección de la Oficina de acceso: Margarita Queijo Rodríguez C/ Real 66, 1º - 15003 - A Coruña - A CORUÑA

DATOS DEL SOLICITANTE:

D./Dª ....., mayor de edad, con domicilio en la C/ .....
N.º..... C.P ..... Localidad ..... Provincia .....
E-mail.....con D.N.I ....., del que acompaña fotocopia.

EXPONE:

Que por medio del presente escrito manifiesta su deseo de ejercer su derecho a la limitación del tratamiento, de conformidad con el artículo 18 del Reglamento General de Protección de Datos (RGPD).

SOLICITA:

1.- Que se proceda a la efectiva limitación del tratamiento, en el plazo máximo de un mes a contar desde la recepción de esta solicitud, dicho plazo podrá prorrogarse otros dos meses, informando al interesado de dicha prorroga antes de un mes, junto con los motivos del retraso.

2- Que en el caso de que el interesado obtenga la limitación del tratamiento, sea informado por el responsable antes del levantamiento de dicha limitación.

3.- Que el responsable del tratamiento comunique cualquier limitación del tratamiento a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

4.- Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

En _____ a _____ de _____de 20__

Firmado:

INSTRUCCIONES:
Es necesario aportar fotocopia del D.N.I. o cualquier otro medio de identificación personal válido en derecho, para que el responsable del tratamiento pueda realizar la comprobación oportuna. En caso de que se actúe a través de representación legal (menor de edad o incapacitado) deberá aportarse, además de la fotocopia del DNI, la documentación que acredite la representación legal.
La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos.

(RGPD) MODELO DE EJERCICIO DEL DERECHO DE PORTABILIDAD DE LOS DATOS

DATOS DEL RESPONSABLE DEL TRATAMIENTO
Nombre: Margarita Queijo Rodríguez
Nombre y dirección de la Oficina de acceso: Margarita Queijo Rodríguez C/ Real 66, 1º - 15003 - A Coruña - A CORUÑA

DATOS DEL SOLICITANTE:

D./Dª ....., mayor de edad, con domicilio en la C/ .....
N.º..... C.P ..... Localidad ..... Provincia .....
E-mail.....con D.N.I ....., del que acompaña fotocopia.

EXPONE:

Que por medio del presente escrito manifiesta su deseo de ejercer su derecho a la portabilidad de los datos, de conformidad con el artículo 20 del Reglamento General de Protección de Datos (RGPD).

SOLICITA:

1.- 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 sea técnicamente posible.

2.- Que se le responda en el plazo máximo de un mes a contar desde la recepción de esta solicitud, dicho plazo podrá prorrogarse otros dos meses, informando al interesado de dicha prorroga antes de un mes, junto con los motivos del retraso.

3.- Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

En _____ a _____ de _____de 20__

Firmado:

INSTRUCCIONES:
Es necesario aportar fotocopia del D.N.I. o cualquier otro medio de identificación personal válido en derecho, para que el responsable del tratamiento pueda realizar la comprobación oportuna. En caso de que se actúe a través de representación legal (menor de edad o incapacitado) deberá aportarse, además de la fotocopia del DNI, la documentación que acredite la representación legal.
La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos.

(RGPD) MODELO DE EJERCICIO DEL DERECHO DE OPOSICIÓN

DATOS DEL RESPONSABLE DEL TRATAMIENTO
Nombre: Margarita Queijo Rodríguez
Nombre y dirección de la Oficina de acceso: Margarita Queijo Rodríguez C/ Real 66, 1º - 15003 - A Coruña - A CORUÑA

DATOS DEL SOLICITANTE:

D./Dª ....., mayor de edad, con domicilio en la C/ .....
N.º..... C.P ..... Localidad ..... Provincia .....
E-mail.....con D.N.I ....., del que acompaña fotocopia.

EXPONE:

1.- Que por medio del presente escrito manifiesta su deseo de ejercer su derecho de oposición, de conformidad con el artículo 21 del Reglamento General de Protección de Datos (RGPD).

2.- Que (describir la situación en la que se produce el tratamiento de sus datos personales y enumerar los motivos por los que se opone al mismo):

3.- Que para acreditar la situación descrita, acompaño una copia de los siguientes documentos:

SOLICITA:

1.- Que sea atendido mi ejercicio del derecho de oposición en los términos anteriormente expuestos.

2.- Que se le responda a más tardar en el momento de la primera comunicación.

3.- Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

En _____ a _____ de _____de 20__

Firmado:

INSTRUCCIONES:
Es necesario aportar fotocopia del D.N.I. o cualquier otro medio de identificación personal válido en derecho, para que el responsable del tratamiento pueda realizar la comprobación oportuna. En caso de que se actúe a través de representación legal (menor de edad o incapacitado) deberá aportarse, además de la fotocopia del DNI, la documentación que acredite la representación legal.
La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos.

(RGPD) MODELO DE EJERCICIO DEL DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES

DATOS DEL RESPONSABLE DEL TRATAMIENTO
Nombre: Margarita Queijo Rodríguez
Nombre y dirección de la Oficina de acceso: Margarita Queijo Rodríguez C/ Real 66, 1º - 15003 - A Coruña - A CORUÑA

DATOS DEL SOLICITANTE:

D./Dª ....., mayor de edad, con domicilio en la C/ .....
N.º..... C.P ..... Localidad ..... Provincia .....
E-mail.....con D.N.I ....., del que acompaña fotocopia.

EXPONE:

Que por medio del presente escrito manifiesta su deseo de ejercer su derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles, de conformidad con el artículo 22 del Reglamento General de Protección de Datos (RGPD).

SOLICITA:

1.- 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.

2.- Que se le responda en el plazo máximo de un mes a contar desde la recepción de esta solicitud, dicho plazo podrá prorrogarse otros dos meses, informando al interesado de dicha prorroga antes de un mes, junto con los motivos del retraso.

3.- Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

En _____ a _____ de _____de 20__

Firmado:

INSTRUCCIONES:
Es necesario aportar fotocopia del D.N.I. o cualquier otro medio de identificación personal válido en derecho, para que el responsable del tratamiento pueda realizar la comprobación oportuna. En caso de que se actúe a través de representación legal (menor de edad o incapacitado) deberá aportarse, además de la fotocopia del DNI, la documentación que acredite la representación legal.
La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos.

7) CLAUSULAS

Descripción de las cláusulas jurídicas.

7) USOS Y RECOMENDACIONES

Manual de usos y recomendaciones. (Para todos los usuarios con acceso a los datos)

USOS Y RECOMENDACIONES

Todas las personas que tengan acceso a los datos personales, a través del sistema informático o a través de cualquier otro medio automatizado de acceso, están obligadas a cumplir lo establecido en el Documento de Seguridad que dispone la entidad, y por lo tanto, sujetas a las consecuencias que puedan derivar en caso de incumplimiento. El incumplimiento de las políticas, prácticas y procedimientos de seguridad estará sujeto a una acción disciplinaria, pudiendo conllevar una acción civil y/o penal.

Esta normativa debe difundirse a todos los empleados para que todos los usuarios sepan a qué medidas de seguridad están sujetos en materia de Protección de Datos, asimismo, se recomienda hacer la entrega de algún modo que permita registrar el acuse de recibo por parte de los usuarios.

FUNCIONES ASIGNADAS AL RESPONSABLE DEL TRATAMIENTO

1. Elaborar e implantar la normativa de seguridad que deben adoptar los tratamientos detallados en el correspondiente ANEXO A del documento de seguridad así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

2. Crear y mantener el Registro de Actividades de Tratamiento.

3. Comprobar el cumplimiento del deber de información, con anterioridad a la recogida de datos de acuerdo con los medios que se utilicen para ello.

4. Recabar el consentimiento de los interesados, siempre que éste sea necesario para el tratamiento de sus datos.

5. Aprobar la designación y autorización de usuarios que emplean la aplicación en su labor cotidiana, asignando los accesos permitidos a cada usuario.

6. Aprobar una política que tenga por objetivo la formación adecuada del personal con los siguientes fines:
- conocimiento de las medidas de seguridad que afecten a las funciones de cada usuario.
- conocimiento de los procedimientos a seguir por el afectado para el ejercicio de sus derechos.

7. Autorizar la puesta en marcha de la explotación de los datos de carácter personal mediante una nueva aplicación informática, o la realización de mejoras sustanciales sobre la existente.

8. Autorizar la aprobación de una política para la salida de soportes informáticos que contengan datos de carácter personal fuera de los locales en los que esté ubicado el tratamiento.

9. Aprobar la corrección de los procedimientos establecidos para la asignación de contraseñas a fin de garantizar la confidencialidad de las mismas.

10. Aprobar los procedimientos de realización de copias de seguridad y de recuperación de los datos.

11. Aprobar las medidas correctoras que se deriven de la correspondiente auditoría.

12. Y, en general, cualquier obligación que se derive de la normativa que resulte de aplicación.

FUNCIONES ASIGNADAS AL RESPONSABLE DEL TRATAMIENTO, DPD O PERSONA DELEGADA

- Implantar, actualizar y supervisar, controles periódicos para verificar el cumplimiento de lo establecido en el documento de seguridad.

- Definir y documentar las funciones y obligaciones del personal.

- Adoptar las medidas necesarias para que los usuarios de su organización conozcan las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

- Establecer 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.

- En caso de autenticación con contraseñas, definir e implantar un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

- Controlar que las contraseñas se cambien periódicamente y su almacenamiento sea de forma ininteligible mientras estén vigentes.

- Establecer un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

- Establecer controles de acceso para los usuarios de tal forma que sólo tengan acceso autorizado a datos y recursos necesarios para sus funciones.

- Establecer mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

- Disponer lo necesario para que sólo el personal autorizado pueda conceder, alterar o anular el acceso autorizado, según los criterios establecidos por el responsable.

- Fijar un procedimiento de notificación y gestión de violaciones o incidencias de seguridad.

- Autorizar la salida de soportes fuera de los locales.

- Proceder a la destrucción o borrado de cualquier documento o soporte que contenga datos de carácter personal que vaya a desecharse, adoptando las medidas para impedir cualquier recuperación posterior de la información.

- Verificar periódicamente la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

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

- Someter los sistemas de información, periódicamente, a una auditoría interna o externa que verifique el cumplimiento del RGPD, procedimientos e instrucciones. El informe de auditoría dictaminará sobre la adecuación de las medidas y controles, identificará deficiencias y propondrá medidas correctoras o complementarias. Deberá incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

- Analizar el informe de auditoría y elevar las conclusiones al responsable del tratamiento para que adopte las medidas correctoras adecuadas.

- Revisar que los datos que se traten sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

- Revisar que los datos de carácter personal objeto de tratamiento no se usen para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

- Revisar que los datos de carácter personal sean exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

- Ordenar lo oportuno para que los datos de carácter personal sean suprimidos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados o cuando resultaran ser inexactos, en todo o en parte, o incompletos y revisar la correcta ejecución de esta obligación.

- Comprobar que, salvo en los supuestos en que el RGPD exceptúa esta obligación, se cuenta con el consentimiento previo del titular de los datos para su cesión.

- Comprobar que, salvo en los supuestos en que el RGPD exceptúa esta obligación, se cuenta con el consentimiento previo del titular de los datos para su tratamiento.

- Comprobar el cumplimiento del deber de información.

- Detectar los supuestos de encargados del tratamiento y comprobar la suscripción de los contratos de encargado/s del tratamiento.

- Atender las peticiones de ejercicio de los derechos de los interesados.

- Implantar (y en su caso revisar y/o modificar) el procedimiento para la atención al titular de los datos en el ejercicio de sus derechos.

- Comprobar si se producen transferencias internacionales y si estas cumplen con la normativa.

FUNCIONES ASIGNADAS A LOS USUARIOS

1. Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la organización.

2. Guardar todos los soportes físicos y/o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

3. Queda prohibido el traslado de cualquier soporte, listado o documento con datos de carácter personal en los que se almacene información titularidad de la organización fuera de los locales de la misma, sin autorización previa del Responsable de Tratamiento. En el supuesto de existir traslado o distribución de soportes y documentos se realizará cifrando dichos datos, o mediante otro mecanismo que imposibilite el acceso o manipulación de la información por terceros.

4. Ficheros de carácter temporal o copias de documentos son aquellos en los que se almacenan datos de carácter personal, generados para el cumplimiento de una necesidad determinada o trabajos temporales y auxiliares, siempre y cuando su existencia no sea superior a un mes. Estos ficheros de carácter temporal o copias de documentos deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán cumplir con las medidas de seguridad asignadas. Si, transcurrido el mes, el usuario necesita continuar utilizando la información almacenada en el fichero, deberá comunicarlo al Responsable, para adoptar las medidas oportunas sobre el mismo.

5. Únicamente las personas autorizadas en un listado de accesos podrán introducir, modificar o anular los datos contenidos en los ficheros o documentos objeto de protección. Los permisos de acceso de los usuarios son concedidos por el Responsable. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a datos personales o documentos a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del Responsable correspondiente.

6. Comunicar al Responsable, conforme al procedimiento de notificación, las violaciones o incidencias de seguridad de las que tenga conocimiento.

7. Cambiar las contraseñas a petición del sistema.

8. Cerrar o bloquear todas las sesiones al término de la jornada laboral o en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos no autorizados.

9. No copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal al ordenador personal, portátil o a cualquier otro soporte sin autorización expresa del Responsable correspondiente.

10. Guardar todos los ficheros con datos de carácter personal en la carpeta indicada por el Responsable de Seguridad correspondiente, a fin de facilitar la aplicación de las medidas de seguridad que les correspondan.

11. Los usuarios tiene prohibido el envío de información de carácter personal sensible, salvo autorización expresa del Responsable que tenga asignada esta tarea. En todo caso, este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros.

12. Los usuarios no podrán, salvo autorización expresa del Responsable que tenga asignada esta tarea, instalar cualquier tipo de programas informáticos o dispositivos ni en los servidores centrales ni en el ordenador empleado en el puesto de trabajo.

13. Queda prohibido:

a. Emplear identificadores y contraseñas de otros usuarios para acceder al sistema.

b. Intentar modificar o acceder al registro de accesos habilitado por el Responsable competente.

c. Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a datos o programas cuyo acceso no le haya sido permitido.

d. Enviar correos masivos (spam) empleando la dirección de correo electrónico corporativa.

e. Y en general, el empleo de la red corporativa, sistemas informáticos y cualquier medio puesto al alcance del usuario vulnerando el derecho de terceros, los propios de la organización, o bien para la realización de actos que pudieran ser considerados ilícitos.

14. Mantener debidamente custodiadas las llaves de acceso a la organización, a sus despachos y a los armarios, archivadores u otros elementos que contengan datos de carácter personal no automatizados, debiendo poner en conocimiento del Responsable competente cualquier hecho que pueda haber comprometido esa custodia.

15. Cerrar con llave las puertas de los despachos al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.

16. Asegurarse de que no quedan documentos impresos que contengan datos de carácter personal impresos en la bandeja de salida de la impresora.

17. Establecerse procedimientos en el copiado o reproducción de documentos, a fin de que solo puedan acceder a las copias las personas habilitadas por el Responsable correspondiente.

FUNCIONES ASIGNADAS A LOS USUARIOS DE DATOS NO AUTOMATIZADOS

1. Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la entidad.

2. Mantener debidamente custodiadas las llaves de acceso a la residencia, a sus despachos y a los armarios, archivadores u otros elementos que contengan datos no automatizados de carácter personal, debiendo poner en conocimiento del Responsable cualquier hecho que pueda haber comprometido esa custodia.

3. Cerrar con llave las puertas de los despachos al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.

4. Comunicar al Responsable, conforme al procedimiento de notificación, las violaciones o incidencias de seguridad de las que tenga conocimiento.

5. Queda prohibido el traslado de cualquier listado o documento análogo con datos de carácter personal en los que se almacene información titularidad de la entidad fuera de los locales de la misma.

6. Guardar todos los soportes físicos o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

7. Asegurarse de que no quedan documentos impresos que contengan datos protegidos impresos en la bandeja de salida de la impresora.

8. Únicamente las personas autorizadas para ello en el listado de accesos podrán introducir, modificar o anular los datos contenidos en los ficheros objeto de protección. Los permisos de acceso de los usuarios a los diferentes ficheros son concedidos por el Responsable. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del Responsable.

9. Ficheros de carácter temporal son aquellos en los que se almacenan datos de carácter personal, generados para el cumplimiento de una necesidad determinada, siempre y cuando su existencia no sea superior a un mes. Los ficheros de carácter temporal deben ser destruidos una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán contemplarse las medidas de seguridad contenidas en este documento.

FUNCIONES ASIGNADAS A LOS USUARIOS ADMINISTRADORES INFORMÁTICOS

El usuario que tiene privilegios para la administración de equipos informáticos, debe conocer las obligaciones que le corresponden como personal informático. Debido al especial acceso que tiene el personal informático se le atribuyen unas responsabilidades complementarias:

1. Guardar secreto de toda la información de carácter personal, o que afecte a ésta, de la que tenga conocimiento en el desarrollo de su de trabajo, aún después de acabada la relación con la organización.

2. Aunque debido a sus funciones disponga de un acceso privilegiado a ciertos recursos, se compromete a acceder únicamente a los datos necesarios para desarrollar sus funciones.

3. En el caso que detecten, deficiencias de seguridad en el sistema de información, lo deberán comunicar al Responsable correspondiente.

4. Colaborar con el Responsable/s en la resolución de las incidencias que se le encarguen.

5. Desempeñar sus funciones con estricta observancia de las obligaciones dispuestas por el RGPD.

FUNCIONES ASIGNADAS A LOS USUARIOS DE ATENCIÓN AL PÚBLICO

1. Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la organización.

2. Mantener en secreto sus claves de acceso al sistema, debiendo poner en conocimiento del Responsable cualquier hecho que pueda haber comprometido el secreto.

3. Las contraseñas de acceso al sistema son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida.

4. Cambiar las contraseñas a petición del sistema.

5. Cerrar o bloquear todas las sesiones al término de la jornada laboral.

6. Bloquear las sesiones en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos no autorizados.

7. Comunicar al Responsable, conforme al procedimiento de notificación, las violaciones o incidencias de seguridad de las que tenga conocimiento.

8. No copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal al propio ordenador, o a cualquier otro soporte sin autorización expresa del Responsable. Queda igualmente prohibido el traslado de cualquier soporte en los que se almacene información titularidad de la compañía fuera de los locales de la misma.

9. Guardar todos los ficheros con datos de carácter personal en la carpeta indicada por el Responsable a fin de facilitar la aplicación de las medidas de seguridad que les correspondan.

10. Guardar todos los soportes físicos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

11. Asegurarse de que no quedan documentos impresos que contengan datos protegidos impresos en la bandeja de salida de la impresora.

12. Únicamente las personas autorizadas para ello en el listado de accesos podrán introducir, modificar o anular los datos contenidos en los tratamientos objeto de protección. Los permisos de acceso de los usuarios a los diferentes ficheros son concedidos por el Responsable competente. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del Responsable.

13. Ficheros de carácter temporal son aquellos en los que se almacenan datos de carácter personal, generados para el cumplimiento de una necesidad determinada, siempre y cuando su existencia no sea superior a un mes. Los ficheros de carácter temporal deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán ser almacenados en la carpeta designada por el Responsable. Si, transcurrido el mes, el usuario necesita continuar utilizando la información almacenada en el fichero, deberá comunicarlo al Responsable, para adoptar las medidas oportunas sobre el mismo.

14. El correo electrónico es considerado por la entidad como elemento fundamental para las comunicaciones entre la organización y el resto de agentes, públicos o privados, que intervienen en las relaciones propias de la actividad desarrollada. Por ello, el correo electrónico sea cual sea la dirección asignada, se configura como una herramienta de trabajo no exclusiva, colectiva y de libre acceso, asignadas a áreas o puestos de trabajo y no a personas. Queda prohibido el uso del mismo para fines no relacionados con las funciones laborales encomendadas. El empleo del nombre o apellidos de los trabajadores o funcionarios junto al dominio de la organización en las direcciones de correo no significa la asignación por la organización de un correo personal, esto se realiza únicamente por motivos organizativos internos de asignación de áreas y puestos de trabajo. Los usuarios tienen prohibido el envío de Información de carácter personal sensible, salvo autorización expresa del Responsable. En todo caso, este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros.

15. Los usuarios no podrán, salvo autorización expresa del Responsable, instalar cualquier tipo de programas informáticos o dispositivos ni en los servidores centrales ni en el ordenador personal empleado para el desarrollo de su trabajo.

16. Conocer la existencia de derechos de los interesados (acceso, rectificación, cancelación, oposición, portabilidad, supresión y limitación), así como su procedimiento de respuesta ante el ejercicio de uno de ellos.

17. Queda prohibido:

a. Emplear identificadores y contraseñas de otros usuarios para acceder al sistema.

b. Intentar modificar o acceder al registro de accesos habilitado por el Responsable.

c. Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a datos o programas cuyo acceso no le haya sido permitido.

d. Utilizar Internet para tareas que no estén relacionadas directamente con las funciones asignadas al usuario. La organización regulará las modalidades de acceso y las restricciones o limitaciones del mismo. Queda prohibida la descarga de software o ficheros de cualquier tipo desde Internet, sin consentimiento expreso de la organización, y ello aunque resulte de un acceso consentido por motivos de trabajo.

e. Introducir contenidos en la red corporativa y/o ordenador personal que no guarden relación con la actividad y objetivos de la entidad.

f. Enviar correos masivos (spam) empleando la dirección de correo electrónico corporativa.

g. Y en general, el empleo de la red corporativa, sistemas informáticos y cualquier medio puesto al alcance del usuario vulnerando el derecho de terceros, los propios de la organización, o bien para la realización de actos que pudieran ser considerados ilícitos.

8) CONTRATOS

[Listado de Contratos de Encargados del Tratamiento. Si imprime este documento, incorpore aquí copia de los contratos firmados, así como los modelos, si lo desea]

CONTRATOS

En este apartado puede encontrar:

- Contratos de Encargados de tratamiento
- Contratos de prestación de servicios sin acceso a datos personales
- Acuerdos de cesión de datos

PRESTACIONES DE SERVICIO CON ACCESO A DATOS:

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

En este caso cuando un tercero presta servicio a Margarita Queijo Rodríguez y para ello necesita realizar un acceso a datos que están bajo la responsabilidad de Margarita Queijo Rodríguez (en adelante el Responsable del tratamiento), a este tercero con acceso a datos se le denominará como ENCARGADO DE TRATAMIENTO y se seguirá las siguientes directrices:

El Responsable del tratamiento y el Encargado de tratamiento deberán firmar un contrato para legalizar esta situación.

Estos son los contratos de Encargados de tratamiento que encontrará en este apartado con su asesoría laboral, asesoría fiscal, prevención de riesgos laborales, mantenimiento informático, etc…

PRESTACIONES DE SERVICIO SIN ACCESO A DATOS:

El Responsable del tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer de forma accidental con motivo de la prestación del servicio.

En este apartado encontrará los contratos para legitimar esta situación con su empresa de limpieza, mantenimiento de extintores, etc...

COMUNICACIÓN / CESIÓN DE DATOS:

Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

Para realizar una cesión de datos, deberá firmar el/los acuerdos de cesión de datos que encuentre en este apartado, así como obtener el consentimiento (mediante el aviso legal que encontrará en el apartado correspondiente) del titular de los datos que vayan a ser contenido de la cesión.

No será necesario ni el acuerdo de cesión de datos, ni el consentimiento del titular, siempre y cuando la cesión de datos sea obligatoria y/o esta autorizada por Ley (cesiones a: bancos y cajas de ahorro, administración tributaria, seguridad social, entidades aseguradoras, etc…).

RECOMENDACIONES:

- FIN DEL DOCUMENTO DE SEGURIDAD -
