<%EMPRESA%>

FECHA ÚLTIMA ACTUALIZACIÓN: <%FECHA_SALIDA%>

Índice

1. INTRODUCCIÓN.
2. DEFINICIONES.
3. ÁMBITO DE APLICACIÓN DEL DOCUMENTO
4. MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO
5. INFORMACIÓN Y OBLIGACIONES DEL PERSONAL
6. PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS
7. PROCEDIMIENTOS DE REVISIÓN
8. VIDEOVIGILANCIA

Anexos

I. DESCRIPCIÓN DE FICHEROS
II. COMUNICACIÓN A TRABAJADORES SOBRE EL PROCESO DE IMPLANTACIÓN DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS
III. CONTRATO PARA EL ENCARGADO DE TRATAMIENTO
IV. CLAUSULAS PARA LA DOCUMENTACIÓN DE LA ORGANIZACIÓN
V. CARTA PARA EL EJERCICIO DERECHOS TITULAR DATOS
VI. REGISTRO DE INCIDENCIAS
VII. NOMBRAMIENTO DEL RESPONSABLE DE SEGURIDAD
VIII. INVENTARIO DE SOPORTES
IX. POLÍTICA DE PRIVACIDAD

1. INTRODUCCIÓN

Según el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter personal, establece que “el responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural”.

El Real Decreto 1720/2007, aprobó el Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal (Reglamento de Seguridad). El Reglamento tiene por objeto establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

Entre estas medidas, se encuentra la elaboración e implantación de la normativa de seguridad mediante un documento de seguridad, de obligado cumplimiento para el personal con acceso a los datos de carácter personal.

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el RD 1720/2007 y LOPD, recogen las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la LOPD.

Además, se ha elaborado éste documento de seguridad según el Reglamento 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. De este modo, se pretende que con éste Reglamento se unifique la legislación en cuanto a protección de datos en toda Europa, debido a que el flujo de datos personales cada vez es más importante.

Por tanto, el presente documento y sus anexos, redactados en cumplimiento con lo dispuesto en el RLOPD recogen las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la LOPD.

2. DEFINICIONES

- Datos personales: toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad puede determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo, un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
- Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- Limitación del tratamiento: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.
- Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consiste en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.
- Seudonimización: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.
- Fichero: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.
- Responsable del tratamiento o responsable: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la unión o de los estados miembros determina los fines y medios del tratamiento, el

responsable del tratamiento o los criterios específicos para su nombramiento podrán establecerlos el derecho de la unión o los estados miembros.
- Encargado del tratamiento o encargado: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
- Destinatario: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el arco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.
- Tercero: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.
- Consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
- Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
- Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.
- Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.
- Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.
- Establecimiento principal:
    - En lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal.
    - En lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la unión o, si careciera de esta, el establecimiento del encargado en la unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente reglamento.
- Representante: persona física o jurídica establecida en la unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo del artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente reglamento.
- Empresa: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica.
- Grupo empresarial: grupo constituido por una empresa que ejerce el control y sus empresas controladas.
- Normas corporativas vinculantes: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.
- Autoridad de control: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51.
- Autoridad de control interesada: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:
    - El responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control.
    - Los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento.
    - Se ha presentado un reclamación ante esa autoridad de control.
- Tratamiento transfronterizos:
    - El tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro.
    - El tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro.
- Objeción pertinente y motivada: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertados fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión.
- Organización internacional: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países en virtud de tal acuerdo.

3. ÁMBITO DE APLICACIÓN DEL DOCUMENTO

El presente documento será de aplicación a las actividades de tratamiento de datos de carácter personal que se hallan bajo la responsabilidad de <%EMPRESA%>, incluyendo los sistemas de información y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

En concreto, las actividades de tratamiento sujetas a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad, son los siguientes:

- <%TEXTO 1%>
- <%TEXTO 2%>
- <%TEXTO 3%>
- <%TEXTO 4%>
- <%TEXTO 5%>
- <%TEXTO 6%>

En el Anexo I se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afecten de manera particular.

4. MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO

IDENTIFICACIÓN Y AUTENTICACIÓN.

El procedimiento utilizado para la identificación y autentificación de los usuarios cuando intentan acceder al sistema, la red o las aplicaciones, está basado en la combinación de un código de identificación de <%TEXTO 7%>.

Actualmente, existe SERVIDORES <%TEXTO 9%> y/o DISCO_DURO al que acceden los usuarios, protegido contra el acceso.

Las labores de mantenimiento y averías, son realizadas por <%TEXTO 10%>.

Se realizan copias de seguridad diariamente.

<%TEXTO 13%>

<%TEXTO 15%>

<%TEXTO 17%>

<%PROTOCOLO%>

<%TEXTO 18%>

Control de acceso

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. La organización establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. Para ello, solo dirección o la persona autorizada, dispondrá de la llave de acceso al archivo, donde se encuentran físicamente los ficheros con datos de carácter personal.

Exclusivamente la Dirección está autorizado para conceder, alterar o anular el acceso sobre los datos y los recursos, conforme a los criterios establecidos por el responsable del fichero, mediante comunicación directa o vía email por parte de los empleados de la organización. Así como nombrar al Responsable de la Seguridad en el anexo VII. En el Anexo I, se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. De existir personal ajeno al responsable del fichero con acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad.

Si el acceso fue autorizado, se almacenará también la información que permita identificar el registro accedido. Los datos del registro de accesos se conservaran durante dos años.

No será necesario el registro de accesos cuando:

- El responsable del fichero es una única persona física.
- El responsable del fichero garantice que sólo él tiene acceso y trata los datos personales, y se haga constar en el documento de seguridad.

<%TEXTO 19%>

Gestión de soportes y documentos

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y serán almacenados en <%LUGAR%> y >%LUGAR2%> lugar de acceso restringido al que solo tendrán acceso las personas con autorización, previamente otorgada vía email o de forma directa por el Gerente y/o Responsable de seguridad de la organización.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos en correos electrónicos, fuera de los locales bajo el control del responsable del tratamiento, deberá ser autorizada por Responsable de seguridad.

Los soportes y documentos que vayan a ser desechados, deberán ser previamente borrados o destruidos de forma que no sea posible el acceso a la información contenida en ellos o su recuperación posterior.

Para el traslado de la documentación se adoptarán las siguientes medidas para evitar la sustracción, pérdida o acceso indebido a la información:

- <%SOBRES_CERRADOS%>

REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

Las salidas y entradas de soportes correspondientes a los ficheros de nivel medio/alto, serán registradas de acuerdo al siguiente procedimiento:

- Mediante documento escrito donde se identifica a la persona que accede a la documentación, hora y fecha, tipo de documentos, uso, cantidad de documentos, forma de envío, destinatarios si procede, soporte.
- <%TEXTO 21%>
- <%GESTION_AUTOMATIZADO%>

GESTIÓN Y DISTRIBUCIÓN DE SOPORTES

En este caso los soportes se identificarán mediante sistema de etiquetado, siendo los criterios de etiquetado comprensibles y con sentido para los usuarios con acceso autorizados, permitiéndoles identificar su contenido y dificultando la identificación para el resto de personas.

La distribución y salida de soportes que contengan datos de carácter personal de los ficheros de nivel alto se realizará Mediante cifrado en el caso de la información electrónica.

CRITERIOS DE ARCHIVO

El archivo de los soportes o documentos se realizará de acuerdo con los criterios de fechas de elaboración de las mismas, identificadas por el nombre, donde se archiva por fecha de llegada.

ALMACENAMIENTO DE LA INFORMACIÓN

Los dispositivos que almacenan datos personales se encuentran almacenados en <%LUGAR%> mediante la siguiente medida de seguridad:

- <%BAJO_LLAVE%>

Las carpetas físicas se encuentran almacenadas <%LUGAR_2%>, mediante las siguientes medidas de seguridad:

- <%BAJO_LLAVE_2%>

CUSTODIA DE SOPORTES

En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamiento indicados en el punto anterior, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso a personas no autorizadas.

FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

COPIAS DE RESPALDO Y RECUPERACIÓN

Se dispone de un sistema donde <%DIARIAMENTE%> se realiza una copia de seguridad de los datos locales custodiado por un Responsable de los Ficheros.

Las copias desechadas deberán ser destruidas contenida imposibilitando el posterior acceso a la información.

El responsable del fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos reales previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

RESPONSABLE DE SEGURIDAD

Se designa como responsable de seguridad a <%FULANO%>, que con carácter general se encargará de coordinar y controlar las medidas definidas en este documento de seguridad.

En ningún caso, la designación supone una exoneración de la responsabilidad que corresponde a <%EMPRESA%> como responsable del fichero de acuerdo con el RLOPD.

5. INFORMACIÓN Y OBLIGACIONES DEL PERSONAL

INFORMACIÓN AL PERSONAL

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas mediante la distribución de una circular por parte de Dirección vía email o de forma directa.

Cuando se estime oportuno, Dirección colgará en un lugar visible la circular de Obligaciones de los empleados en Materia de Protección de Datos (Anexo II), para que sea recordado por todos los empleados.

FUNCIONES Y OBLIGACIONES DEL PERSONAL

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla. Constituye una obligación del personal notificar a <%FULANO%>, las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en el apartado de "Procedimientos de notificación, gestión y respuesta ante las incidencias."

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

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los soportes que los contengan, o a los recursos del sistema de información.

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 de aquellos datos que hubiera podido conocer durante la prestación del servicio. Todo ello se formalizará en un contrato que figura en el anexo III.

CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado y de las derivadas de la LOPD, se sancionara conforme al artículo 44 de la Ley Orgánica de Protección de Datos, que establece que:

Son infracciones leves:

1. No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo.
2. No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.

3. El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.
4. La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el artículo 12 de esta Ley.

Son infracciones graves:

1. El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
2. La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley.
3. Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentara se determinen.
4. Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo
5. El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado.
6. La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave.

Son infracciones muy graves:

1. La recogida de datos en forma engañosa o fraudulenta.
2. No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello.
3. La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria.

En caso de infracciones leves se impondrán las siguientes sanciones:

1. Las infracciones leves serán sancionadas mediante empleo y sueldo.
2. Las infracciones graves serán sancionadas con 3 días de empleo y sueldo.
3. Las infracciones muy graves serán sancionadas 5 días de empleo y sueldo.

PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS

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 de la empresa.

Todo el personal puede detectar la existencia de una incidencia. De igual manera, éstas pueden ser detectadas por terceros (clientes, proveedores, partes interesadas…) Dirección, será la encargada de realizar seguimiento a todas aquellas incidencias detectadas y garantizar que se determinan las acciones necesarias para su resolución.

Todo el personal de hará el máximo esfuerzo en la identificación de las posibles incidencias antes de que el usuario se vea afectado.

Ejemplos de tipos de incidencias en materia de protección de datos:

Incidencias que afectan a la identificación y autentificación de los usuarios:

- Perdida de confidencialidad de contraseñas.
- Periodos de desactivación de las herramientas de seguridad.

Incidencias que afecten a los derechos de acceso a los datos:

- Comunicación de usuarios que sospechan que alguien ha suplantado su identidad.
- Detección de contraseñas escritas en el lugar de trabajo.
- Puertas no cerradas correctamente.
- Detección de puntos de acceso desatendidos y sin protección de pantalla activada.

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 seguridad y recuperación:

- Errores en los procesos de realización de las copias de seguridad.
- Recuperaciones de datos realizados.
- Violación del mecanismo de cierre o guarda de los ficheros no automatizados.

NOTIFICACIÓN DE LAS VIOLACIONES DE SEGURIDAD.

Tenemos que tener en cuenta, que con el nuevo RGPD, aparte de anotar las Incidencias en el Registro de Incidencias, se deben comunicar las violaciones de seguridad a la AEPD en un máximo de 72 horas.

Una brecha de seguridad es “toda violación que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos”.

Asimismo el Reglamento General de Protección de Datos enuncia en los artículos 33 y 34 que las brechas de seguridad deben ser notificadas a la autoridad de control cuando la misma constituya un riesgo para los derechos y las libertades de las personas físicas.

Las brechas de seguridad ante las que nos podemos encontrar, son las siguientes:

- Modificación, sin permiso del administrador, de una base de datos.
- Pérdida parcial o total de una base de datos.
- Destrucción de las copias de seguridad.
- Envío de datos personales por error.

Cómo debe gestionar <%NOMBRE - EMPRESA%> la brecha de seguridad:

1. Registrar la incidencia detectada.
   Para ello, el responsable del tratamiento debe llevar a cabo un registro (Anexo VI) en el cual se recojan el lugar, día y hora de detección de la violación de seguridad, así como también los sistemas, datos y equipos que se han visto afectados. Una vez resuelta la brecha, se deberá también registrar la solución al problema.
   Si la empresa cuenta con Delegado de Protección de Datos, será éste el encargado de esta obligación.
2. Averiguar si supone un riesgo para los afectados.
   Para ello, se dispone de una serie de criterios y ejemplos, los cuales se encuentran recogidos en el considerando 75 del RGPD y son los siguientes:

   - Que pueda provocar daños y perjuicios físicos, materiales o inmateriales:
     - Problemas de discriminación.
     - Usurpación de identidad o fraude.
     - Pérdidas financieras.
     - Daño para la reputación.
     - Pérdida de confidencialidad de datos sujetos al secreto profesional.
     - Reversión no autorizada de la seudonimización o cualquier otro prejuicio económico o social significativo.
   - Que se pueda privar a los interesados de sus derechos y libertados o se les impida ejercer el control sobre sus datos personales ya que los datos personales tratados revelen:
     - El origen étnico o racial.
     - Las opiniones políticas.
     - La religión o creencias filosóficas.
     - La militancia en sindicatos.
     - El tratamiento de datos genéticos.
     - Datos relativos a la salud o datos sobre la vida sexual.
     - Relativos a las condenas e infracciones penales o medidas de seguridad conexas.
   - En los casos en los que se evalúen aspectos personales:
     - En particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo.
     - Situación económica.
     - Datos de salud.
     - Preferencias o intereses personales.
     - Fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales.
   - En los datos en los que se traten datos personales de personas vulnerables, en particular niños.

3. Notificar a la autoridad de control.
   La autoridad competente para recibir las notificaciones de las brechas de seguridad, será la autoridad de control nacional de protección de datos, Agencia Española de Protección de Datos.
   La comunicación se debe realizar en un máximo de 72 horas.

   En caso de que la empresa disponga de Delegado de Protección de Datos, será éste el encargado de realizar la notificación.

   La notificación ha de incluir un contenido mínimo:

   - La naturaleza de la violación, categorías de datos y de interesados afectados.
   - Medidas impuestas por el responsable para resolver esa quiebra.
   - Si procede, las medidas adoptadas para reducir los posibles efectos negativos sobre los interesados.

4. Informar a las personas afectadas.
   Es de obligado cumplimiento informar a las personas afectadas, excepto, en los siguientes casos:

   - El responsable hubiera adoptado medidas técnicas u organizativas apropiadas antes de la violación de seguridad, en particular para las medidas que hagan ininteligibles los datos para terceros, como sería el cifrado.
   - Cuando el responsable haya tomado con posterioridad a la quiebra medidas técnicas que aseguren que ya no hay posibilidad de que el alto riesgo se materialice.
   - Cuando la notificación implique un esfuerzo desproporcionado, debido en estos casos reemplazarse por medidas alternativas como puede ser una comunicación pública.

6. PROCEDIMIENTOS DE REVISIÓN

REVISIÓN DEL DOCUMENTO DE SEGURIDAD

La dirección se asegurará que 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 ficheros 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.

El Documento de Seguridad deberá auditarse cada año, siendo obligatoria su auditoria cada dos años.

El Responsable de seguridad, deberá revisarlo cada seis meses y actualizarlo si es necesario.

ANEXO I - ACTIVIDADES DE TRATAMIENTO

ANEXO II - COMUNICACIÓN A TRABAJADORES SOBRE EL PROCESO DE IMPLANTACIÓN DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

ANEXO III - CONTRATO CON TERCEROS DE LA PRESTACIÓN DE SERVICIOS CON ACCESO A DATOS PERSONALES

CONTRATO DE SERVICIOS PARA EL TRATAMIENTO DE FICHEROS DE DATOS PERSONALES POR CUENTA DE TERCEROS.

AVISO: En su contrato con la empresa que le presta el servicio con acceso a datos personales deberá incluir las siguientes cláusulas contractuales:

1. Objeto del encargo del tratamiento
Mediante las presentes cláusulas, se habilita a _____, con dirección en _____ y NIF _____ como encargado del tratamiento, para tratar por cuenta de <%EMPRESA%>, en calidad de responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio que en adelante se especifican.

El tratamiento consistirá en _____-.

2. Identificación de la información afectada
Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad <%ZAMAKOA-S.A%> como responsable del tratamiento, pone a disposición de la entidad _____- la información disponible en los equipos informáticos que dan soporte a los tratamientos de datos realizados por el responsable.

3. Duración
El presente acuerdo tiene una duración de <%DURACION_ACUERDO%>, renovable.
Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable los datos personales, y suprimir cualquier copia que mantenga en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

4. Obligaciones del encargado del tratamiento
El encargado del tratamiento y todo su personal se obliga a:

- Utilizar los datos personales a los que tenga acceso sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.
- Llevar, por escrito, un registro de todas las categorías de actividades de tratamien-to efectuadas por cuenta del responsable, que contenga:
    1. El nombre y los datos de contacto del encargado o encargados y de cada res-ponsable por cuenta del cual actúe el encargado y, en su caso, del representan-te del responsable o del encargado y del delegado de protección de datos.
    2. Las categorías de tratamientos efectuados por cuenta del responsable.
    3. Una descripción general de las medidas técnicas y organizativas de seguridad apropiadas que esté aplicando.
- No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles. Si el encargado quiere subcontratar tiene que informar al responsable y solicitar su autorización previa.
- Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.
- Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.
- Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
- Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos, el encargado informará inmediatamente al responsable.
Notificación de violaciones de la seguridad de los datos:
El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida y a través de la dirección de correo electrónico que le indique el responsable, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

Se facilitará, como mínimo, la información siguiente:

1. Descripción de 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.
2. Datos de la persona de contacto para obtener más información.
3. Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales. Descripción de las medidas adoptadas o propuestas 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 es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

_____, a petición del responsable, comunicará en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.

La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, incluir los elementos que en cada caso señale el responsable, como mínimo:

1. La naturaleza de la violación de datos.
2. Datos del punto de contacto del responsable o del encargado donde se pueda obtener más información.
3. Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
4. 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.

1. Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

2. Implantar las medidas de seguridad técnicas y organizativas necesarias para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento
3. Auxiliar al responsable de tratamiento a implantar las medidas de seguridad necesarias para:
    a. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
    b. Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
    c. Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

Destino de los datos
El responsable del tratamiento no conservará datos de carácter personal relativos a los tratamientos del encargado salvo que sea estrictamente necesario para la prestación del servicio, y solo durante el tiempo estrictamente necesario para su prestación.

En Devolver al responsable del tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación.

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado.

No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación. caso de conservar datos de carácter personal.

5. Obligaciones del responsable del tratamiento
Corresponde al responsable del tratamiento:

- Facilitar al encargado el acceso a los equipos o datos necesarios a fin de prestar el servicio contratado.
- Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.
- Supervisar el tratamiento.

ANEXO IV - CLAUSULAS PARA LA DOCUMENTACIÓN DE LA ORGANIZACIÓN

CLAUSULAS PARA CLIENTES

Responsable: Identidad: <%EMPRESA%> - CIF: <%CIF%>, Dir. postal: <%DIRECCION%>, Correo elect: <%EMAIL%>.

“En nombre de la empresa tratamos la información que nos facilita con el fin de prestarles el servicio solicitado, realizar la facturación del mismo. Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante los años necesarios para cumplir con las obligaciones legales. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener confirmación sobre si en EMPRESA estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos, solicitar su supresión cuando los datos ya no sean necesarios, solicitar su limitación del tratamiento y la portabilidad de los datos.
Asimismo solicito su autorización para ofrecerle productos y servicios relacionados con los solicitados y fidelizarle como cliente.”

SI

NO

Nombre y apellidos:

Fdo.:

CLAUSULAS CORREOS ELECTRONICOS

"Este mensaje va dirigido, de manera exclusiva, a su destinatario y contiene información confidencial cuya divulgación no está permitida por la ley. En caso de haber recibido este mensaje por error, le rogamos que, de forma inmediata, nos lo comunique mediante correo electrónico y proceda a su eliminación, así como a la de cualquier documento adjunto al mismo.

Sus datos figuran en un fichero propiedad de <%EMPRESA%>. Puede ejercitar gratuitamente los derechos de acceso, rectificación, cancelación, oposición, portabilidad, limitación del tratamiento, dirigiéndose a <%EMPRESA%>, en <%DIRECCION%> o contactando con nosoros mediante correo electrónico a <%EMAIL%> y a presentar reclamación ante la AEPD, (art. 13 del Reglamento) Europeo de PD".

CLAUSULA PARA CANDIDATOS

Responsable: Identidad: <%EMPRESA%> - CIF: <%CIF%>, Dir. postal: <%DIRECCION%>, Correo elect: <%EMAIL%>.

“En nombre de la empresa tratamos la información que nos facilita con el fin de mantenerle informado de las distintas vacantes a un puesto de trabajo que se produzcan en nuestra organización. Los datos proporcionados se conservarán hasta la adjudicación de un puesto de trabajo o hasta que usted ejerza su derecho de cancelación por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos, solicitar su supresión cuando los datos ya no sean necesarios, solicitar su limitación del tratamiento y la portabilidad de los datos. Los datos no se cederán a terceros.”

CLAUSULA PARA FUTUROS CLIENTES

Responsable: Identidad: <%EMPRESA%> - CIF: <%CIF%>, Dir. postal: <%DIRECCION%>, Correo elect: <%EMAIL%>.

“En nombre de la empresa tratamos la información que nos facilita con el fin de enviarle publicidad relacionada con nuestros productos y servicios por cualquier medio (postal, email o teléfono) e invitarle a eventos organizados por la empresa. Los datos proporcionados se conservarán mientras no solicite el cese de la actividad. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener

confirmación sobre si en pepe estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos, solicitar su supresión cuando los datos ya no sean necesarios, solicitar su limitación del tratamiento y la portabilidad de los datos".

CLAUSULA PARA PROVEEDORES

Responsable: Identidad: <%EMPRESA%> - CIF: <%CIF%>, Dir. postal: <%DIRECCION%>, Correo elect: <%EMAIL%>.

"En nombre de la empresa tratamos la información que nos facilita con el fin de realizar pedido y facturar los servicios. Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante los años necesarios para cumplir con las obligaciones legales. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener confirmación sobre si en ZAMAKOA S.A estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos, solicitar su supresión cuando los datos ya no sean necesarios, solicitar su limitación del tratamiento y la portabilidad de los datos".

Nombre y apellidos:

Fdo.:

ANEXO V - CARTA PARA EL EJERCICIO DERECHOS TITULAR DATOS

A. EJERCICIO DEL DERECHO DE ACCESO

Petición de información sobre los datos personales incluidos en un fichero.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO EMPRESA.
DIRECCION.

DATOS DEL SOLICITANTE
D./Dª_____, mayor de edad, con domicilio en la C/_____, nº____, Localidad _____, Provincia _____, C.P. _____ y con D.N.I. _____, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con los artículos 15 de la Ley Orgánica 15/1999, y los artículos 27, 28, 29 y 30 del RD 1720/2007 y el articulo 15 del Reglamento General de protección de datos.

SOLICITA. -

1. Que se le facilite gratuitamente el acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de acceso se entenderá denegada. En este caso se interpondrá la oportuna reclamación ante la Agencia de Protección de Datos para iniciar el procedimiento de tutela de derechos, en virtud del artículo 18 de la Ley Orgánica y 28 del Real Decreto.
2. Que si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección arriba indicada en el plazo de diez días desde la resolución estimatoria de la solicitud de acceso.
3. Que esta información comprenda de modo legible e inteligible los datos de base que sobre mi persona están incluidos en sus ficheros, y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En _____, a _____ de _____de 20___ .

B. EJERCICIO DE LOS DERECHOS DE RECTIFICACIÓN

Petición de corrección de datos personales inexactos o incorrectos objeto de tratamiento, incluidos en un fichero.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO EMPRESA.
DIRECCION.

DATOS DEL SOLICITANTE
D./Dª_____, mayor de edad, con domicilio en la C/_____, nº____, Localidad _____, Provincia _____, C.P. _____ y con D.N.I. _____, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de rectificación, de conformidad con el artículo 16 de la Ley Orgánica 15/1999, y los artículos 31, 32 y 33 del RD 1720/2007 y el articulo 16 del Reglamento General de protección de datos.

SOLICITA. -

1. Que se proceda gratuitamente a la efectiva corrección en el plazo de diez días desde la recepción de esta solicitud, de los datos inexactos relativos a mi persona que se encuentren en sus ficheros.
2. Los datos que hay que rectificar se enumeran en la hoja anexa, haciendo referencia a los documentos que se acompañan a esta solicitud y que acreditan, en caso de ser necesario, la veracidad de los nuevos datos.
3. Que me comuniquen de forma escrita a la dirección arriba indicada, la rectificación de los datos una vez realizada.
4. Que, en el caso de que el responsable del fichero considere que la rectificación o la cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

En _____, a _____ de _____de 20___ .

C. EJERCICIO DEL DERECHOS DE CANCELACIÓN

Petición de supresión de datos personales objeto de tratamientos incluidos en un fichero.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

EMPRESA:
DIRECCION:

DATOS DEL SOLICITANTE
D./Dª_____, mayor de edad, con domicilio en la C/_____, nº____, Localidad _____, Provincia _____, C.P. _____ y con D.N.I. _____, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de cancelación, de conformidad con el artículo 16 de la Ley Orgánica 15/1999, y los artículos 31, 32 y 33 del Real Decreto RD 1720/2007 y el articulo 17 del Reglamento General de protección de datos.

SOLICITA. -

1. Que se proceda a la efectiva supresión en el plazo de diez días desde la recepción de esta solicitud, de los datos relativos a mi persona que se encuentren en sus ficheros y que se enumeran en el anexo, al no existir vinculación jurídica o disposición legal que justifique su mantenimiento, como se acredita en los documentos aportados.
2. Que me comuniquen de forma escrita a la dirección arriba indicada la cancelación de los datos una vez realizada.
3. Que, en el caso de que el responsable del fichero considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley Orgánica.

En _____, a _____ de _____de 20___ .

D. EJERCICIO DEL DERECHO DE OPOSICIÓN

Petición de oposición de datos personales objeto de tratamientos incluidos en un fichero.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

EMPRESA:
DIRECCION:

DATOS DEL SOLICITANTE
D./Dª_____, mayor de edad, con domicilio en la C/_____, nº____, Localidad _____, Provincia _____, C.P. _____ y con D.N.I. _____, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de oposición, de conformidad con el artículo 16 de la Ley Orgánica 15/1999, y los artículos 34, 35 y 36 del RD 1720/2007 y el articulo 21 del Reglamento General de protección de datos.

SOLICITA. -

1. Que en el plazo de diez días desde la recepción de esta solicitud, se proceda a la efectiva oposición de cualesquiera datos relativos a mi persona que se encuentren en sus ficheros, en los términos previstos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y me lo comuniquen de forma escrita a la dirección arriba indicada.
2. Que, en el caso de que el responsable del fichero considere que dicha oposición no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

En _____, a _____ de _____de 20___ .

E. EJERCICIO DEL DERECHOS DE LIMITACIÓN DEL TRATAMIENTO

Petición de limitación del tratamiento de datos personales objeto de tratamientos incluidos en un fichero.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

EMPRESA:
DIRECCION:

DATOS DEL SOLICITANTE
D./Dª_____, mayor de edad, con domicilio en la C/_____, nº____, Localidad _____, Provincia _____, C.P. _____ y con D.N.I. _____, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de cancelación, de conformidad con el artículo 16 de la Ley Orgánica 15/1999, y los artículos 31, 32 y 33 del Real Decreto RD 1720/2007 y el articulo 18 del Reglamento General de protección de datos.

SOLICITA. -

1. Que se proceda a la efectiva limitación del tratamiento en el plazo de diez días desde la recepción de esta solicitud, de los datos relativos a mi persona que se encuentren en sus ficheros y que se enumeran en el anexo, realizando solo tratamiento de conservación y 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.
2. Que me comuniquen de forma escrita a la dirección arriba indicada la limitación de los datos una vez realizada.
3. Que, en el caso de que el responsable del fichero considere que dicha limitación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley Orgánica.

En _____, a _____ de _____de 20___ .

F. EJERCICIO DEL DERECHOS DE PORTABILIDAD

Petición de portabilidad de datos personales de tratamientos incluidos en un fichero.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

EMPRESA:
DIRECCION:

DATOS DEL SOLICITANTE
D./Dª_____, mayor de edad, con domicilio en la C/_____, nº____, Localidad _____, Provincia _____, C.P. _____ y con D.N.I. _____, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de cancelación, de conformidad con el artículo 16 de la Ley Orgánica 15/1999, y los artículos 31, 32 y 33 del Real Decreto RD 1720/2007 y el articulo 20 del Reglamento General de protección de datos.

SOLICITA. -

1. Que se proceda a la efectiva portabilidad en el plazo de diez días desde la recepción de esta solicitud, de los datos relativos a mi persona que se encuentren en sus ficheros y que se enumeran en el anexo, trasmitiendo estos a _____, situada en _____-.
2. Que, en el caso de que el responsable del fichero considere que dicha portabilidad no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley Orgánica.

En _____, a _____ de _____de 20___ .

ANEXO VI - REGISTRO DE INCIDENCIAS

Núm. Incidencia	
Fecha notificación	
Hora notificación	
Notificación dirigida a:	
Datos Incidencia	
Tipo incidencia	
Fecha incidencia	
Hora incidencia	
Persona que detecto incidencia:	
Descripción detallada de la incidencia.	**Efectos probable de la incidencia y acciones emprendidas.**

Núm. Incidencia
Fecha notificación
Hora notificación
Notificación dirigida a:
Datos Incidencia
Tipo incidencia
Fecha incidencia
Hora incidencia
Persona que detecto incidencia:

Descripción detallada de la incidencia.	**efectos probable de la incidencia y acciones emprendidas.**

Núm. Incidencia
Fecha notificación
Hora notificación
Notificación dirigida a:
Datos Incidencia
Tipo incidencia
Fecha incidencia
Hora incidencia
Persona que detecto incidencia:

Descripción detallada de la incidencia.	**efectos probable de la incidencia y acciones emprendidas.**

ANEXO VII - NOMBRAMIENTO DEL RESPONSABLE DE SEGURIDAD

<%EMPRESA%>, situada en <%DIRECCION%>, con CIF <%CIF%>, designa a _____, con DNI _____. como Responsable de Seguridad para todos los ficheros referenciados en el presente Documento de Seguridad.

Con carácter general se encargará de coordinar y controlar las medidas estipuladas en este documento.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde a los Responsables de Ficheros y a los Encargados de Tratamiento.

En _____, a _____ de _____de 20___ .

Firmado:

ANEXO VIII - POLÍTICA GENERAL DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

ENTIDAD: <%EMPRESA%>
FECHA: <%FECHA%>

<%EMPRESA%> ha adoptado las medidas y niveles de seguridad de protección de los datos personales, exigidos por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y sus Reglamentos de desarrollo. Los datos personales recabados por nuestra organización se incorporan a varios ficheros ubicados en las Oficinas de <%EMPRESA%>

Nuestra política, en relación con la protección de datos de carácter personal expresada en este documento, se constituye en un marco cuyos pilares fundamentales son:

1.- Derechos de las personas en relación con los datos de carácter personal.

El cliente, el proveedor, el trabajador de la entidad y cualquier persona afectada pueden ejercitar sus derechos de acceso, rectificación, cancelación y oposición con arreglo a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa aplicable al efecto, mediante carta dirigida a nuestra dirección: <%EMPRESA%>, <%DIRECCION%> o mediante cualquier otro medio que permita reconocer la identidad del afectado y que ejercite cualquiera de los anteriores derechos.

2.- Recogida de datos e información.

La recogida de datos de carácter personal se realizará única y exclusivamente para los fines previstos en actividades directamente relacionadas con el objeto social y fines de la entidad y utilizando métodos que hayan sido aprobados en cada momento por el Responsable de los Ficheros.

3.- Tratamiento y consentimiento.

Se informará a las personas de las que se requieran datos de carácter personal de la existencia de los derechos que les asisten y se obtendrá su consentimiento por los métodos aprobados y en los términos que requiere la legislación aplicable.

4.- Transmisiones, Confidencialidad y Deber de Secreto.

Todas las comunicaciones referidas a datos de carácter personal entre <%EMPRESA%> y los interesados y cualquier otra entidad o persona que intervenga en el tratamiento, serán consideradas confidenciales.

Todos los intervinientes en el tratamiento dejaran evidencia de su compromiso de confidencialidad.

5.- Cesión de información personal a terceros.

<%EMPRESA%> no vende, cede, arrienda ni transmite de modo alguno información o datos de carácter personal de sus Clientes / Usuarios a terceros.

Los cambios que afecten al tratamiento de datos personales se comunicarán también a los interesados por los medios más adecuados en cada caso.

6.- Responsabilidad, cooperación y participación.

<%EMPRESA%> y en su nombre el Responsable de los Ficheros, se reconoce como máxima y última responsable de la correcta definición, aplicación, actualización y perfeccionamiento de esta Política. Por consiguiente y dado que esta tarea no puede ser realizada únicamente por personal directivo, solicito el compromiso y la participación activa de todo el personal de la entidad.

Fdo:

El Responsable de los Ficheros

ANEXO IX - REGISTRO DE ENTRADA Y SALIDA DE SOPORTES CON PERSONAL AUTORIZADO PARA LA RECEPCIÓN Y SALIDA DE LOS SOPORTES

Registro de Soportes

Entradas / Salidas

Entradas/Salidas Fecha y Hora Soporte Fichero. Nombres Uso Forma de envío Destinatario

Fdo.: Responsable de los Ficheros