NOTA: Este Documento deberá mantenerse permanentemente actualizado. Cualquier modificación en los sistemas de información automatizados o no, en la organización de los mismos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal conllevará la revisión de la normativa incluida y si procede, su modificación total o parcial.

DOCUMENTO DE SEGURIDAD

VERSIÓN: V.1/17

El presente documento será de aplicación en MUGARIK GABE O.N.G.D. de acuerdo con lo establecido en la Ley Orgánica 15/1999 de Protección de datos de carácter personal y su normativa de desarrollo, en relación con el tratamiento de los datos de carácter personal y su nivel de seguridad de acuerdo con el Reglamento 1720/2007 que la desarrolla.

ÍNDICE

ANEXOS

1. DEFINICIONES:

- ***Dato de carácter Personal***: cualquier información concerniente a personas físicas identificadas o identificables.
- ***Fichero***: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
- ***Tratamiento de datos***: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
- ***Responsable del fichero o tratamiento*:** persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
- ***Afectado o interesado***: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.
- ***Procedimiento de disociación***: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
- ***Encargado del tratamiento***: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
- ***Consentimiento del interesado*:** toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
- ***Cesión o comunicación de datos*:** toda revelación de datos realizada a una persona distinta del interesado.
- ***Fuentes accesibles al público:*** aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

2. INTRODUCCIÓN:

El artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD), establece en su punto 1 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 Reglamento de desarrollo de la LOPD (RLOPD), aprobado por el Real Decreto 1720/2007, de 21 de diciembre, fue publicado en el BOE número 17, de 19 de enero de 2008. El Título VIII de este reglamento desarrolla las medidas de seguridad en el tratamiento de datos de carácter personal y 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 obligado cumplimiento para el personal con acceso a los datos de carácter personal.

Por este motivo ha sido elaborado este "documento de seguridad" por parte del responsable de los ficheros, tomando como referencia los estándares aplicados por la Agencia Española de Protección de Datos, sus resoluciones e informes jurídicos y la legislación vigente hasta la fecha de su aprobación.

3. NORMATIVA APLICABLE A ESTE DOCUMENTO

- Directiva Europea 95/46/CE sobre tratamiento de Datos Personales
- Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de carácter personal
- Real Decreto 1720/2007 de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.
- Ley 2/2011 de 5 de marzo de economía sostenible.
- Real Decreto 195/2000 por el que se establece el plazo para implantar las medidas de seguridad
- Real Decreto 156/1996 por el que se aprueba la modificación del RD 428/93 sobre el estatuto de la Agencia Española de Protección de Datos (AGPD)
- Resolución de 8 de septiembre de 2006 de la Agencia de Protección de datos por el que se corrigen errores en las resoluciones de 12 de julio de 2006, por la que se crea el Registro Telemático y se aprueban los formularios electrónicos.
- Resolución de 12 de julio de 2006 de la AGPD por la que se crea el Registro Telemático de la AGPD.
- Instrucción 1/2006, de 12 de diciembre de la AGPD sobre el tratamiento de datos con fines de vigilancia a través de sistemas de cámaras o videocámaras.
- Instrucción 1/2004 de 22 de diciembre de la AGPD sobre publicación de sus Resoluciones.
- Instrucción 1/1996 de 1 de marzo de la AGPD sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios.
- Memorias de la Agencia Española de Protección de Datos.
- Informes del gabinete jurídico de la Agencia Española de Protección de Datos.

4. ORGANIZACIÓN DEL DOCUMENTO DE SEGURIDAD

El Reglamento de Seguridad no especifica si se debe disponer de un solo documento de Seguridad que incluya todos los ficheros y tratamientos con datos personales de los que una persona física o jurídica sea responsable, o un único documento por cada fichero o tratamiento. Cualquiera de las dos opciones, la Agencia Española de Protección de datos las viene admitiendo como válidas hasta la fecha de hoy.

En este caso concreto y para hacerlo más manejable y lograr una consulta más ágil, se ha optado por un único modelo de seguridad para todos los ficheros con independencia del

nivel de seguridad aplicable y de su forma de tratamiento (automatizado, manual o mixto).

A este respecto, el documento de seguridad se organiza en dos partes: En la primera de ellas, se recogen las medidas que afectan a todos los sistemas de información de forma general de acuerdo con lo establecido en el RD 1720/2007. La segunda parte, a modo de anexos, se delimitan los procedimientos y perfiles particulares de cada fichero, junto con aquellas medidas que puedan ser exigibles al responsable del fichero de acuerdo con la legislación vigente.

Ahora bien, el Responsable del Fichero, o en su defecto, el responsable de Seguridad, podrá incorporar en los anexos cualquier otra medida que se considere oportuna para aumentar la seguridad de los tratamientos, o incluso, adoptar las medidas exigidas para un nivel de seguridad superior al que por el tipo de información les correspondería, teniendo en cuenta la infraestructura y las circunstancias particulares de la organización.

5. ÁMBITO DE APLICACIÓN DEL DOCUMENTO

El presente documento tiene como ámbito de aplicación los ficheros que contienen datos de carácter personal, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en la normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

El objeto del Documento de Seguridad es establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida o acceso no autorizado que ha de aplicarse por MUGARIK GABE O.N.G.D. de acuerdo con el RD 1720/2007.

Su uso será exclusivamente de carácter interno para la empresa y a él sólo podrán tener acceso personas autorizadas, sin perjuicio de la adopción de las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones.

Las medidas de seguridad se clasifican en tres niveles acumulativos: básico, medio y alto, en base a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integración de la información.

- **Nivel básico**: Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico, es decir, independientemente del tipo de datos a tratar (nombre, apellidos, domicilio, salud, económicos, etc.) las medidas mínimas a implantar en el fichero son calificadas de nivel básico.
- **Nivel Medio**: Deberán implantarse, además de las medidas de seguridad básicas, las medidas de nivel medio, en aquellos ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, los relativos a los servicios de información sobre solvencia patrimonial y de crédito, aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros, aquellos de los que sean responsables las Entidades Gestoras y Servicios comunes de la Seguridad Social en ejercicio de sus competencias, de igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social. También aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características de la personalidad o del comportamiento de los mismos.
- **Nivel Alto**: Ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, relacionados con la violencia de género o los

recabados para fines policiales sin consentimiento del afectado (en este último caso también deberán de ser de titularidad pública).

En cuanto al tratamiento, este puede ser:

- **Fichero Automatizado**: Todo conjunto de datos de carácter personal organizado de forma automatizada, cualquiera que fuere la forma o modalidad de creación, almacenamiento, organización y acceso.
- **Fichero Manual o No Automatizado:** Conjunto de datos personales organizados de forma no automatizada y estructurados conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.
- **Fichero Mixto:** Aquel conjunto de datos que se encuentra organizado de forma automatizada y manual, ya sea de forma total, parcial o complementaria.

Los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

FICHEROS	NIVEL DE SEGURIDAD	TRATAMIENTO	Nº DE INSCRIPCIÓN
SOCIOS	BÁSICO	MIXTO	2171540140
AGENDA Y CORREO ELECTRONICO	BÁSICO	MIXTO	2171540141
NÓMINAS-RECURSOS HUMANOS	BÁSICO	MIXTO	2171540143
FISCAL Y CONTABLE	BÁSICO	MIXTO	2171540142

NOTA: Estos ficheros ya han sido debidamente notificados e inscritos en el Registro General de Protección de Datos (art. 26 de la L.O. 15/1999). Los documentos de notificación, modificación y registro se adjuntan en el ANEXO I.

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

Todas las personas que tengan acceso a datos personales de cualquiera de los ficheros designados, bien a través del sistema informático o de cualquier otro medio, sea o no automatizado, se encuentran obligadas por ley a cumplir con lo establecido en este documento y a no revelar datos personales ni otra información confidencial a la que pudiera tener acceso como consecuencia de su puesto de trabajo. Por consiguiente, el responsable del fichero, su representante o la persona desinada a tal efecto, hará entrega de una circular o contrato para su ratificación por los empleados, que se adjunta en el apartado de empleados, en virtud del cual se pone en conocimiento de los trabajadores, sus obligaciones respecto al almacenamiento, consulta y tratamiento de datos personales, sin perjuicio de hacer entrega de una copia de este documento de seguridad o de la parte que le afecte de manera particular cuando fuera preciso. En cualquier caso, todo el personal tiene el acceso libre a este documento de seguridad para cualquier consulta y en particular al apartado relativo a FUNCIONES Y OBLIGACIONES DEL PERSONAL.

6. GUÍA DE APLICACIÓN

Tal y como se describe en el párrafo anterior, este documento de seguridad tiene una naturaleza mixta, de forma que puede abarcar varios ficheros de diferentes niveles de seguridad con el objeto de facilitar su manejo y garantizar el cumplimiento de la legislación vigente en materia de protección de datos de carácter personal.

Por este motivo, desde LEGALIDAT (Abogados & Consultores) nos esforzamos en diseñar este formato mucho más manejable, rápido e intuitivo gracias a nuestro sistema de símbolos y cuadros, en virtud de los cuales, se interrelacionan los distintos criterios que determina la LOPD y su normativa de desarrollo, encuadrando las medidas de seguridad propias de cada fichero de acuerdo con su nivel de seguridad.

NOTA: Los niveles de seguridad son correlativos, de modo que las medidas que no van precedidas de ninguno de los símbolos que se describen a continuación, se entiende que son medidas de seguridad básicas y por tanto comunes para todos los ficheros:

Nivel básico: Medidas de seguridad mínimas y comunes para todos los ficheros

Nivel medio: Medidas del Nivel básico + Medidas propias del Nivel medio

Las medidas específicas para cada uno de los ficheros se destacan por la aplicación de los siguientes símbolos:

NIVEL MEDIO: con esta marca se señalarán las medidas que sólo son obligatorias en los ficheros que tengan que adoptar un nivel de seguridad medio.

AUTOMATIZADOS: Con esta marca se señalarán las medidas específicas para aplicar exclusivamente a ficheros informatizados o automatizados.

MANUALES : Con esta marca se señalarán las medidas específicas para aplicar exclusivamente a ficheros manuales o no automatizados.

Por Ejemplo:

Si queremos conocer las medidas de seguridad aplicables a un fichero determinado, procederíamos de la siguiente manera: buscaremos en el epígrafe anterior, el nombre del fichero, su nivel de seguridad y el tipo tratamiento (por ejemplo: clientes - nivel básico- tratamiento automatizado), pues bien, las medidas aplicables para el fichero clientes, serán aquellas que no se encuentran dentro de ningún cuadro (nivel básico). Si fuera nivel medio como el fichero de empleados, se cumplirían a mayores las medidas encuadradas con el símbolo **NIVEL MEDIO.** Para terminar nos fijaremos el tipo de tratamiento, puesto que como es obvio, no es lo mismo aplicar medidas de seguridad a un dato que se encuentra dentro de un fichero en soporte papel que otro en soporte informático. En el caso de nuestro ejemplo nos limitaríamos al tratamiento ***AUTOMATIZADO***. En el supuesto de que el tratamiento fuera **mixto** se aplicaría lo dispuesto al tratamiento manual para los ficheros en soporte papel y automatizado para aquellos que se tratan de forma digitalizada.

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

A. *IDENTIFICACIÓN Y AUTENTICACIÓN*

En este apartado se tratan las medidas y normas relativas a la identificación y autenticación del personal autorizado para acceder a los datos personales, por consiguiente, el responsable del fichero garantizará la existencia de una relación actualizada de aquellos usuarios con acceso autorizado al sistema de información, de modo que los ficheros de los que son objeto dicho documento de seguridad sólo serán accesibles por las personas que se identifican en el ANEXO III (Relación de usuarios y perfiles con acceso a datos personales).

Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos y el nombre de la persona o cargo de Responsable de Seguridad que gestiona los permisos de acceso, el procedimiento de asignación, distribución y almacenamiento para garantizar la confidencialidad e integridad de las claves o contraseñas.

El acceso a datos de carácter personal por parte del personal autorizado, estará limitado exclusivamente para el desarrollo de sus funciones laborales. Por otro lado, 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, de modo que no será preciso su inclusión como personal autorizado, sin perjuicio de que en caso de acceso provisional y transitorio deba de cubrirse el Documento de acceso de personal no autorizado que se acompaña en el ANEXO III.

Existe un procedimiento de identificación autentificación y asignación de contraseñas definido en el ANEXO VII con el objeto de verificar la identidad de los usuarios, restringiendo el acceso a aquellos que no se encuentren debidamente autorizados por el responsable del fichero o por la persona designada por este para tales efecto, correspondiéndole por tanto, la potestad exclusiva para conceder, alterar o anular el acceso autorizado sobre estos datos.

AUTOMATIZADOS

NIVEL MEDIO: LIMITE DE INTENTOS FALLIDOS

En los ficheros de nivel medio y alto, se limitará a tres el número de intentos para autentificarse, evitando la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

De igual modo, se establece un CONTROL DE ACCESO FÍSICO que garantiza que exclusivamente el personal que aquí se indica tiene acceso a los locales y equipos donde se encuentran ubicados los sistemas de información correspondientes a dichos ficheros con la finalidad de desempeñar sus funciones.

Las visitas autorizadas sólo podrán acceder a los locales de tratamiento acompañadas por personal de la empresa que esté autorizado a acceder a los locales de tratamiento y se le aplicarán las mismas condiciones y seguridad que al resto de personal.

MANUALES

Para los **ficheros manuales** *el acceso a la documentación se limita exclusivamente al personal autorizado.*

B. GESTIÓN DE SOPORTES Y DOCUMENTOS

Soportes informáticos son todos aquellos medios de grabación y recuperación de datos que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación o aplicaciones que gestionan los ficheros.

Dado que la mayor parte de los soportes que se manejan hoy día (CD, DVD, pendrives, cintas o discos duros) son fácilmente transportables, reproducibles y/o copiables, es evidente la importancia que para la seguridad de los datos del Fichero tiene el control de estos medios. De acuerdo con el Art. 92 del Reglamento en concordancia con lo dispuesto en el art. 9 de la Ley Orgánica 15/1999 sobre seguridad de los datos, se establecen una serie de normas que se detallan a continuación sin perjuicio de lo reflejado en el ANEXO V al respecto.

Según lo expuesto, los soportes que contengan datos de carácter personal estarán etiquetados permitiendo identificar el tipo de información que contienen, ser inventariados y serán almacenados en un lugar de acceso restringido al que solo tendrán acceso las personas que se relacionan a continuación:

a) Responsable del fichero
b) Responsables de seguridad
c) Administradores
d) Usuarios

Los permisos de acceso a los soportes los establecerá el Responsable del Fichero, su representante o del Responsable de Seguridad en caso de estar designado. Para el caso excepcional en el cual, personal ajeno al recogido en este apartado, acceda a los ficheros o a sus equipos de tratamiento por razones de urgencia, fuerza mayor, reparaciones, sustituciones de personal, etc., se cubrirá el documento que se pone a disposición en el ANEXO III sobre el control de acceso.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos en correos electrónicos, fuera de los locales o de la organización, deberá ser autorizada por el responsable de seguridad y en su defecto por el Responsable del fichero o representante legal. Los soportes que vayan a ser desechados, deberán ser previamente destruidos de forma que no sea posible el acceso a la información contenida en ellos o su recuperación posterior. En este sentido, el artículo 92 del Reglamento no especifica las formas de destrucción de los soportes para garantizar el borrado, por ello, en LEGALIDAT (Abogados & Consultores) recomendamos destructoras de papel con capacidad para destrucción de Cd o Dvd y para los ordenadores obsoletos recomendamos la utilización de software de sanitización.

AUTOMATIZADOS

NIVEL MEDIO: REGISTRO DE ENTRADA Y SALIDA DE SOPORTES
Las salidas y entradas de soportes correspondientes a los ficheros de nivel medio y alto, serán registradas de acuerdo con los documentos de autorización relativos a la entrada y salida de soportes que se incluyen en el ANEXO V. Este Registro puede llevarse a cabo de forma informatizada, siempre y cuando queden contemplados los extremos que se detallan en dicho documento. En caso de gestión automatizada se indicará en este punto el sistema informático utilizado

MANUALES

Para los **ficheros manuales** se establecen las siguientes pautas:

CRITERIOS DE ARCHIVO: El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación y en todo caso los establecidos por el responsable del fichero, que en cualquier caso garantizarán la correcta conservación de los documentos, la localización y consulta de la información y posibilitarán el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

ALMACENAMIENTO DE LA INFORMACIÓN: Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán de disponer de mecanismos que obstaculicen su apertura, como por ejemplo archivadores metálicos con llave. Por otro lado y para salvaguardar aquellos ficheros que no se encuentren bajo llave, se ha desplazado el fichero a un despacho, de acceso limitado únicamente al personal autorizado.

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.

C. *ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES*

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

Sólo se podrán llevar a cabo aquellas conexiones autorizadas por el Responsable del Fichero, la persona que lo represente o del responsable de seguridad en los siguientes términos:

- El acceso a datos se llevará a cabo a través de programas autorizados dentro del ámbito de la empresa y se llevarán a cabo con fines estrictamente laborales y profesionales.
- El correo electrónico es corporativo y limitado exclusivamente al ámbito profesional dentro de la empresa, quedando expresamente prohibido el uso de cuentas personales, la conexión a redes externas o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero, tales como programas de intercambio de ficheros (FTP, P2P, etc.), mensajería instantánea o plataformas similares. Cuando un usuario sea dado de baja en el sistema de correo electrónico, la empresa podrá libremente decidir si elimina los mensajes y libreta de direcciones guardados en el directorio de correo electrónico de la dirección que causa baja o por el contrario se conserven conforme a la normativa vigente en materia de protección de datos. El responsable del fichero podrá realizar controles periódicos, sin previo aviso, con presencia del trabajador y un representante de los trabajadores o en su defecto con dos trabajadores más, comprobar el historial de navegación, registros de actividad, correo electrónico y aquellos controles necesarios para comprobar el uso correcto del sistema informático.
- Todas las entradas y salidas de datos del Fichero a través del correo electrónico se realizarán desde una cuenta o dirección de correo controlada por un usuario autorizado por el Responsable del Fichero, debiendo de quedar constancia del mismo mediante el correspondiente registro.
- Se guardarán copias de todos los correos electrónicos que involucren entradas o salidas de datos con carácter personal del Fichero, en directorios protegidos y durante al menos dos años.
- Se extremará la vigilancia con aquellos mensajes o correos electrónicos de cuya procedencia no exista plena seguridad o no hayan sido solicitados.
- Se evitará la descarga de ficheros y ejecutables procedentes de Internet que no ofrezcan garantías de su integridad y origen.

D. *RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO*

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero o quien ostente su representación legal y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Cuando el tratamiento de datos de carácter personal se realice en dispositivos portátiles o en locales distintos a los definidos en el ANEXO III, será necesaria la autorización expresa del Responsable del Fichero, y en todo caso se garantizará el nivel de seguridad adecuado para el tratamiento de los datos. En el ANEXO IV se acompaña un documento de autorización para el tratamiento de datos fuera de la ubicación del fichero así como la autorización de uso de portátiles fuera del lugar del trabajo.

E. *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. Si estos ficheros fuesen creados por los usuarios mediante copia, se almacenarán en un mismo repositorio, archivo o base de datos, siendo eliminados una vez a la semana.

F. *COPIAS DE SEGURIDAD*

Es obligatorio realizar copias de respaldo de los ficheros automatizados que contengan datos de carácter personal. Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

La periodicidad deberá ser al menos una vez a la semana salvo que no se hubiese producido ninguna actualización de los datos.

En el caso de los ficheros de ficheros parcialmente automatizados (tratamiento mixto) se grabarán manualmente los datos de forma que *permita dicha reconstrucción*.

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

En cuanto a las pruebas con datos reales, cuando estas se realicen con anterioridad 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.

AUTOMATIZADOS

NIVEL MEDIO: RECUPERACIÓN DE DATOS
Las recuperaciones de datos de los ficheros clientes deberán ser autorizadas de forma escrita por el responsable del fichero, según el procedimiento indicado en el ANEXO V. Asimismo la incidencia se registrará en el ANEXO VI.

8. PROCEDIMIENTO GENERAL DE 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 expresamente mediante el documento que viene acompañado con el documento de seguridad en el apartado relativo al personal, sin perjuicio de dar traslado de la parte que le corresponde respecto a las funciones y obligaciones del personal que se describe en el siguiente epígrafe.

Además de la circular arriba designada, el responsable del fichero ha firmado un acuerdo de confidencialidad con los empleados en donde se ponen de manifiesto tales extremos.

Si se estima oportuno, se publicará en el tablón de anuncios aquella información que afecte a la seguridad de la información.

9. FUNCIONES Y OBLIGACIONES DEL PERSONAL

A. FUNCIONES Y OBLIGACIONES COMUNES PARA TODO EL 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 y que se contemplan en este documento de seguridad. Esto incluye tanto al personal interno como externo, es decir, incluye aquellas personas contratadas o subcontratadas para desempeñar algunas de las funciones dentro de la organización, como son los consultores, auditores externos, gestorías, etc. En este último caso, se firmará un contrato de encargado de tratamiento para que se adjunte en el documento de seguridad, que garantice el cumplimiento de la normativa vigente en materia de protección de datos personales.

En cuanto al personal interno de esta empresa, constituye una **obligación de todo el personal notificar al *responsable del fichero o de seguridad en su caso,* 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.”

Queda terminantemente prohibida la creación de nuevos ficheros que traten datos de carácter personal, así como la cesión de los mismos sin previa autorización del Responsable del Fichero o de la persona que legalmente lo represente.

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo, garantizando en todo momento que la información no sea visible por personas no autorizadas. Por tanto, cuando el responsable de un puesto de trabajo abandone su puesto, ya sea de forma temporal o bien, por haber finalizado su jornada de trabajo, deberá cerrar con llave los archivadores, cuando se trate de ficheros manuales que se encuentren bajo su custodia o en el caso de ficheros automatizados, dejarlo en un modo que impida la visualización de los datos protegidos, como por ejemplo, salir de la sesión, bloquear el equipo o desconectarlo. En todo caso, la reanudación del trabajo implicará la introducción de la contraseña correspondiente.

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

Los ordenadores y puestos de trabajo desde los que se tiene acceso a fichero de datos de carácter personal tendrán una configuración fija en sus aplicaciones y sistemas operativos que sólo podrá ser cambiada mediante autorización del Responsable del Fichero o del

Responsable de Seguridad, prohibiéndose expresamente la instalación de software o hardware sin la correspondiente autorización del responsable de seguridad.

Si el usuario tuviera indicios de que su ordenador pudiera estar infectado de algún virus informático o software malicioso, deberá ponerlo en conocimiento del Responsable del Fichero o del Responsable de Seguridad, para que tome las medidas oportunas.

El usuario debe de asegurarse de que toda la información contenida en su ordenador no sea transferida a ningún soporte físico externo ni a ningún dispositivo conectado al ordenador, tales como pendrives, DVD,CD, USB, discos externos, etc. salvo que estos sean utilizados para la realización de copias de seguridad de acuerdo con lo establecido en el ANEXO V del Documento de Seguridad y estén debidamente registrados como tal.

Debe de asegurarse que el papel reutilizado no contiene datos de carácter personal. La documentación que se deseche deberá ser destruida a través de la destructora de papel, En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

En cuanto al uso de Internet y redes de telecomunicaciones se guardará una finalidad estrictamente laboral, resultando los usuarios responsables de las sesiones iniciadas desde sus terminales de trabajo, quedando expresamente prohibido el acceso y/o la descarga y/o el almacenamiento en cualquier soporte, de páginas o contenidos ilegales, inadecuados o que atenten contra la moral y las buenas costumbres; de los formatos de imágenes, sonidos o video; de virus y códigos maliciosos y, en general, de todo tipo de programas y documentos sin la expresa autorización del responsable de seguridad.

En ningún caso se pueden modificar las configuraciones de los navegadores del equipo, ni la activación de servidores o puertos sin autorización de responsable de seguridad o del responsable de fichero, en su caso.

La empresa se reserva el derecho a monitorizar y comprobar de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa.

En relación con el correo electrónico, los usuarios son responsables de todas las actividades realizadas con las cuentas de acceso y su respectivo buzón de correos provistos por la empresa, de modo que bajo ningún concepto permitirán la utilización de la cuenta y/o el correspondiente buzón a personas no autorizadas.

Los servicios de correo electrónico suministrados deben destinarse a uso estrictamente laboral. Excepcionalmente pueden ser usados para temas personales siempre que no interfieran con el rendimiento del propio servicio, la labor de los gestores del servicio o supongan un alto coste para la empresa, quedando prohibido la utilización, en los equipos informáticos provistos por la empresa, de buzones de correo electrónico de otros proveedores de Internet.

La entidad se reserva el derecho de revisar, sin previo aviso, los mensajes de correo electrónico de los usuarios de la red corporativa, con el fin de comprobar el cumplimiento de estas normas y actividades que puedan afectar a la entidad como responsable civil subsidiario.

Bajo ningún concepto se enviarán correos electrónicos a personas que no desean recibirlo o que incluya contenido publicitario fuera del ámbito laboral. En todo caso, los correos enviados a varios destinatarios se enviarán mediante copia oculta (CCO.)

B. FUNCIONES ESPECÍFICAS EN RAZÓN DE LA CATEGORÍA

Se definen tres categorías de personal que mantienen obligaciones y realizan tareas específicas que afectan de forma directa (operación y manipulación) o indirecta (administración y gestión) a los datos personales contenidos en los ficheros:

- **Responsable del Fichero:** Es el encargado de diseñar, implantar y actualizar el Documento de Seguridad, de obligado cumplimiento para todo el personal. Es el último responsable de toda actividad relacionada con el Fichero, correspondiendo a MUGARIK GABE O.N.G.D. dichas facultades.
- **Administradores del sistema**: Se encargan de las tareas de administración y mantenimiento del entorno operativo (aplicaciones, equipos informáticos, sistemas operativos e infraestructura de comunicaciones) del Fichero.

> **NIVEL MEDIO**:
> ***Responsable de Seguridad*:** Dentro de los administradores del sistema se deberá designar un responsable de seguridad que tendrá tareas específicas para dar cumplimiento a la LOPD.

- **Usuarios del Fichero:** Personal que utiliza el sistema informático de acceso al Fichero como parte de sus labores diarias (manipulación de datos, entrada y/o salida de los mismos, etc...).

Todo el personal de la entidad que tenga acceso al Fichero deberá estar explícitamente relacionado en una de las categorías anteriormente mencionadas. El ANEXO III guarda una lista completa de las personas o departamentos con su categoría.

Estas categorías no tienen que guardar correlación con la categoría laboral o profesional, siendo posible la creación de nuevas figuras siempre y cuando se considere necesario.

8.B.1. Usuarios del Fichero

El Personal que utiliza el fichero para el ejercicio de las funciones encomendadas por el responsable del fichero, está sometido a las funciones y obligaciones de carácter general contempladas en el epígrafe anterior relacionado con las funciones y obligaciones comunes para todo el personal.

8.B.2. Responsable del Fichero

- El responsable del fichero es el encargado jurídicamente de la seguridad del fichero y de las medidas establecidas en el presente documento, implantará las medidas de seguridad establecidas en el y adoptará las medidas de difusión necesarias para que el personal afectado por este documento conozca las normas que afecten al desarrollo de sus funciones.
- Es obligación del Responsable del Fichero notificar a la Agencia de Protección de Datos los ficheros de datos personales de la entidad y velar por el cumplimiento de todos los requisitos establecidos en la LOPD y en Reglamento de Seguridad.
- Redactar, establecer y comprobar la aplicación y el cumplimiento del documento de seguridad.
- Describir los sistemas de información que realizan el tratamiento de los datos personales de la entidad y estructura de los ficheros.

- Establecer los criterios que se deben de seguir al realizar la función de conceder, alterar o anular el acceso autorizado a los datos y recursos.
- Establecer los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
- Encargarse de coordinar y controlar las medidas definidas en el documento de seguridad.
- Adoptar las medidas correctoras adecuadas, en función del análisis de los Informes de Incidencias.
- Establecer un mecanismo que permita la identificación inequívoca y personalizada de todo aquél usuario que intente acceder al sistema y la verificación de que está autorizado
- Establecer y comprobar la aplicación de una medida que impida el intento reiterado de acceder de forma no autorizada al sistema de información.
- Velar por el cumplimiento de las normas de seguridad contenidas en el Documento de Seguridad.
- Recopilar y describir las medidas, normas, procedimientos, reglas y estándares de seguridad adoptados por la entidad.
- Determinar y describir los recursos informáticos a los que se aplica el documento de seguridad.
- Establecer y comprobar la aplicación del procedimiento de notificación, tratamiento y registro de incidencias.
- Establecer y comprobar la aplicación del procedimiento de realización de copias de respaldo y recuperación de datos y comprobar el cumplimiento de la periodicidad establecida para la realización de copias de respaldo.
- Elaborar y mantener actualizada la lista de usuarios que tengan acceso autorizado al sistema informático de la entidad, con especificación del nivel de acceso que tiene cada usuario.
- El responsable del fichero se encargará de que los sistemas informáticos de acceso al Fichero tengan su acceso restringido mediante un código de usuario y una contraseña. Asimismo cuidará que todos los usuarios autorizados para acceder al Fichero, relacionados en el Anexo III del documento de seguridad, tengan un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.
- Establecer y comprobar la aplicación del procedimiento de cambio periódico de las contraseñas de los usuarios.
- Establecer y comprobar la aplicación de un procedimiento que garantice el almacenamiento de las contraseñas vigentes de forma ininteligible.
- Establecer y comprobar la aplicación de un sistema que limite el acceso de los usuarios únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- Establecer y comprobar la aplicación de los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos distintos a los autorizados.
- Conceder, alterar o anular el acceso autorizados a los datos y recursos, de acuerdo con los criterios establecidos por el responsable del fichero.
- Establecer y comprobar la aplicación de un sistema que permita identificar, inventariar y almacenar en lugar seguro los soportes informáticos que contienen datos de carácter personal.
- Autorizar la salida de soportes informáticos que contengan datos de carácter personal.
- Velar por el cumplimiento de las normas de seguridad, comunicando al responsable del fichero las infracciones cometidas, para el establecimiento de las correspondientes sanciones.

- Establecer y comprobar la aplicación de controles periódicos para verificar el cumplimiento de lo dispuesto en el documento de seguridad.
- Autorizar por escrito la ejecución de los procedimientos de recuperación de datos.
- Comprobar que en la fase de pruebas de los sistemas de información, éstas no se efectúen con datos personales reales.
- Designará al responsable de seguridad cuando fuera preciso pudiendo designar uno o varios, dejando constancia de tal extremo en dicho documento de Seguridad.
- Deberá mantener actualizado el Documento de Seguridad siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.
- El responsable del fichero junto con el responsable de seguridad, analizarán con periodicidad al menos trimestralmente las incidencias registradas en el libro correspondiente, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, poner las medidas correctoras que limiten esas incidencias en el futuro.
- Al menos cada dos años, solicitará una auditoría que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias legales vigentes en materia de protección de datos.

8.B.3. Administradores del Sistema

- Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado en el Anexo III del documento de seguridad.
- El administrador deberá responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo del fichero, de forma que ninguna persona no autorizada tenga acceso a las mismas, salvo que dicha responsabilidad recaiga en el responsable de seguridad.
- Si la aplicación informática que permite el acceso al Fichero, no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.
- Las contraseñas se asignarán por el responsable del fichero y se cambiarán con una periodicidad máxima de **1 año**. Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas, y será responsabilidad del administrador del sistema, sin perjuicio de la responsabilidad que pueda incurrir el responsable de seguridad.
- El archivo sonde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema o del responsable de seguridad.
- Existirá una persona, bien sea el administrador o bien otro usuario expresamente designado, que será responsable de obtener periódicamente una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo.
- Estas copias deben realizarse con una periodicidad, al menos, semanal, salvo en el caso de que no se hayan producido ninguna actualización de los datos.
- En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del fichero al estado en que se encontraban en el momento del fallo tal y como se describe en este documento de seguridad. (Anexo V)

- Será necesaria la autorización del responsable del fichero o persona que legalmente le represente, para la ejecución de los procedimientos de recuperación de los datos mediante la cumplimentación y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse, incluyendo la persona que realizó el proceso, tal y como se establece en la hoja de notificación del mismo anexo.
- Se comprobará con una periodicidad al menos trimestral, que la lista de usuarios autorizados en el Anexo III se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al fichero. Además, comunicará al responsable de seguridad, cualquier alta o baja de usuarios con acceso autorizado al fichero.
- Se comprobará también, al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación de Fichero según lo estipulado en el apartado 2 de este documento de seguridad y su anexo V.
- Cuando exista un responsable de seguridad, el administrador le comunicará cualquier cambio que se haya realizado en el software o hardware, base de datos o aplicación de acceso al fichero, procediendo igualmente a la actualización de dichos anexos. En caso de no estar designado un responsable de seguridad, se procederá a dicha actualización comunicándoselo al responsable del fichero.

8.B.4. Responsable de seguridad

- El responsable de seguridad, con carácter general se encargará de coordinar y controlar las medidas definidas en este documento de seguridad.
- En cuanto a la duración de este nombramiento será por un periodo de tiempo indefinido. En cualquier momento, el responsable del fichero o la persona que legalmente lo represente, podrá nombrar a otra persona diferente para ostentar dichas funciones . No obstante, dicha designación no supone una exoneración de la responsabilidad que corresponde a MUGARIK GABE O.N.G.D. como responsable del fichero de acuerdo con el RLOPD.
- El responsable de seguridad habilitará un Libro de Incidencias a disposición de todos los usuarios y administradores del Fichero con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo, las analizará y tornará las medidas que estime oportunas en colaboración con el responsable del Fichero. (ANEXO VI del documento de seguridad)
- El responsable de seguridad del Fichero comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados del ANEXO III del documento de seguridad, se corresponde con la lista de los usuarios realmente autorizados en la aplicación de accesos al Fichero, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador o administradores del Fichero.
- Comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación de Fichero
- El responsable de seguridad actualizará el documento de seguridad ante cualquier cambio que se haya realizado en los datos técnicos de los anexos, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de dichos anexos. En todo caso se comunicará al responsable del Fichero.

NIVEL MEDIO: : RESPONSABLE DE SEGURIDAD

De acuerdo con el art. 95 del Real Decreto 1720/2007, se designa como responsable de Seguridad a PURIFICACIÓN PÉREZ ROJO

10. 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.

El procedimiento a seguir para la notificación de incidencias consistirá en notificar al responsable de seguridad o en su defecto, al responsable del fichero, de cualquier incidencia de la que se tenga noticia a la mayor brevedad posible. Para llevarlo a cabo, se deberá cubrir un modelo de comunicación de incidencias que se pondrá a disposición de todo el personal y que se acompaña en el ANEXO VI de este documento de seguridad.

Una vez cubierto, se adjuntará al Registro de Incidencias que se gestiona en el mismo Anexo, pudiendo solicitar copia o recibo de notificación de incidencia el notificante.

A. CONTENIDO DE LA NOTIFICACIÓN:

En el Registro de Incidencias deberá constar al menos, el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quien se comunica y los efectos que se hubieran derivado de la misma. En caso de ser automatizada se indicará el sistema informático usado.

AUTOMATIZADOS

NIVEL MEDIO:: PERDIDA Y RECUPERACIÓN DE DATOS

En caso de pérdida de datos existe un sistema de “Back up” definido en el ANEXO V. Cuando exista este tipo de incidencia, se *deberá registrar dicha incidencia de acuerdo con lo establecido en el ANEXO VI, incluyendo en la notificación la persona que ejecutó el proceso, los datos restaurados y, en su caso, que datos ha sido necesario grabar manualmente en el proceso de recuperación.*

NIVEL MEDIO:: AUTORIZACIONES

Para ejecutar los procedimientos de recuperación de datos en los ficheros mencionados en el párrafo anterior, será necesaria la autorización por escrito del responsable del fichero. En el ANEXO V se incluirán los documentos de autorización por parte del responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

11. NUEVOS FICHEROS

Sólo se podrán crear Ficheros que contengan datos de carácter personal cuando resulte necesario para desempeñar las actividades propias del Responsable del Fichero y siempre de acuerdo con los principios y garantías que la Ley Orgánica 15/1999 establece para el tratamiento de los datos de carácter personal.

La creación de Ficheros estará sometida a la autorización expresa del Responsable del Fichero o la persona que lo represente.

No se procederá a la creación de un fichero sin que previamente, se haya cursado la correspondiente notificación a la Agencia Española de Protección de Datos y haber obtenido su código de inscripción de su Registro general. De igual modo se procederá cuando se produzcan modificaciones en el Fichero o se proceda a la cancelación del mismo.

12. PRUEBAS CON DATOS REALES

De acuerdo con el Real Decreto 1720/2007 de Protección de Datos de Carácter personal, en el caso de que se realicen pruebas con datos reales, dichas operaciones deberán realizarse atendiendo y cumpliendo con los niveles de seguridad aquí descritos.

13. DIVULGACIÓN DEL DOCUMENTO DE SEGURIDAD

El Documento de Seguridad es de consulta pública para todo el personal de la empresa. El responsable de Seguridad se encargará de facilitar a cada usuario una copia parcial del presente documento con la parte que le afecte, en especial, la parte referida a las funciones y obligaciones del personal (Apartado 9).

El usuario no podrá acceder a los datos de carácter personal contenidos en los Ficheros hasta que se haya hecho efectiva la entrega de los correspondientes documentos y que se adjuntarán debidamente firmados por su destinatario.

14. MANTENIMIENTO DEL DOCUMENTO DE SEGURIDAD

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.

En todo caso **se realizará una revisión externa cada dos años para revisar la adecuación de las medidas de seguridad establecidas en la legislación vigente en aquella fecha.**

NIVEL MEDIO: AUDITORÍA

De acuerdo con el art. 96 y 109 del Reglamento a partir del nivel medio, se llevará a cabo una auditoría de los sistemas de información e instalaciones, que verifiquen el cumplimiento de este documento de seguridad, al menos cada dos años, emitiendo el respectivo informe de auditoría que se adjuntará al ANEXO VIII.

Dicha auditoría se llevará a cabo de forma externa por LEGALIDAT, quien analizará la adecuación legal al Reglamento de las medidas y controles, identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias.

Los informes de auditoría han de ser analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras y quedará a disposición de la Agencia Española de Protección de Datos, o en su caso de las autoridades de control de las comunidades autónomas

15. 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, constituye para el responsable del fichero una infracción sancionable según lo dispuesto por la LO 15/1999 de Protección de datos de

carácter personal, por lo que cuando dicho incumplimiento se asocie a un individuo concreto por una acción u omisión negligente o por la mera inobservancia de lo dispuesto en este documento de seguridad, podrá ser sancionado de forma interna por la empresa o persona que la represente de acuerdo con el artículo 58 del Estatuto de los trabajadores.

16. DISPOSICIÓN FINAL

El presente documento ha sido aprobado por MUGARIK GABE O.N.G.D. como responsable del Fichero o persona que lo represente, ordenando su ejecución y cumplimiento en dicha organización por todos aquellos a quienes les afecte de acuerdo con lo dispuesto en este documento de seguridad

En Bilbao, 19 de junio de 2017

ANEXO I

DOCUMENTOS DE NOTIFICACIÓN E INSCRIPCIÓN DE FICHEROS ANTE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Este anexo está destinado a todos los documentos de carácter oficial que sean necesarios para justificar el presente Fichero ante la Agencia de Protección de Datos. Cuando sea preciso, se adjuntará copia de los siguientes documentos:

- **Documento de Notificación a la Agencia de Protección de Datos de Registro del Fichero:** Dicha Notificación será generada con el software proporcionado a tal efecto por la Agencia de Protección de Datos, y será enviado tanto por vía telemática como por correo ordinario.

- **Documento de Aceptación remitido por la Agencia de Protección de Datos :** En dicho documento la Agencia de Protección de datos reconoce la inscripción del Fichero en su Registro y la convierte en efectiva.

- **Documentos de modificación o supresión:** En el caso de que se proceda al cambio de la situación del Fichero, será necesario modificar a su vez el Registro de la Agencia de Protección de Datos para que incluya las modificaciones y se ajuste a los datos reales del Fichero.

ES IMPORTANTE QUE LA DOCUMENTACIÓN QUE SE VAYA GENERANDO A ESTOS EFECTOS SE AÑADA AL FINAL DE DICHO ANEXO.

ANEXO II

ESTRUCTURA DE LOS FICHEROS

En este Anexo se hace referencia a todos los ficheros objeto de este documento de seguridad, con su respectiva descripción y aspectos generales de acuerdo con lo establecido en la legislación vigente en relación con aquellos ficheros que contengan datos de carácter personal así como los usos y finalidades del Fichero garantizando en todo momento el principio de calidad de los datos.

ANEXO III

CONTROL DE ACCESO AL FICHERO, PERFILES Y DESCRIPCIÓN DE LA UBICACIÓN DE LOS FICHEROS

- Personal autorizado para acceder al fichero
- Encargados de Tratamiento

En este Anexo se designarán los diferentes perfiles de usuario en relación con determinados empleados o departamentos concretos, quedando definidos los responsables de seguridad y encargados de tratamiento para cada uno de los Ficheros.

Asimismo, se describe la ubicación de los ficheros y del sistema de tratamiento de datos personales, así como las aplicaciones informáticas que acceden al fichero.

NOTA: En caso de acceso a los ficheros por parte de personal no autorizado, se deberá de incluirse en el “registro de acceso por personal no clasificado “que se acompaña en este ANEXO.

CD-ROM: En la carpeta tutoriales, podrá acceder a una guía que le explicará cómo crear cuentas de usuario y accesos en Windows y IOS (IMAC).

PERSONAL AUTORIZADO PARA ACCEDER A LOS FICHEROS

FICHERO: SOCIOS		
RESPONSABLE DEL FICHERO	**MUGARIK GABE O.N.G.D.**	
RESPONSABLE DE SEGURIDAD	**PURIFICACIÓN PÉREZ ROJO**	
USUARIOS		
NOMBRE	**PUESTO**	**PERMISOS**
PURIFICACIÓN PÉREZ ROJO	Administrativo	Recogida,Consulta,Grabado,Borrado,Cesión Conservación, Estructuración, Destrucción.
MARTA GONZÁLEZ IZQUIERDO	Administrativo	Recogida,Consulta,Grabado,Borrado,Cesión Estructuración, Destrucción.
SUSANA PIERA MORENO	Administrativo	Recogida,Consulta,Grabado,Borrado,Cesión Estructuración, Destrucción.
ENCARGADO DE TRATAMIENTO		
NOMBRE	**TRATAMIENTO**	**PERMISOS**
ASESORÍA BARTOLOMÉ ARISTEGUI, S.L.	Asesoría	Recogida,Consulta,Grabado,Borrado,Cesión Conservación, Estructuración, Destrucción.
MAZARREDO AUDITORES,S.L.	Auditoría Externa	Recogida,Consulta,Grabado,Borrado,Cesión Conservación, Estructuración, Destrucción.

FICHERO: EMPLEADOS Y RECURSOS HUMANOS		
RESPONSABLE DEL FICHERO	**MUGARIK GABE O.N.G.D.**	
RESPONSABLE DE SEGURIDAD	**PURIFICACIÓN PÉREZ ROJO**	
USUARIOS		
NOMBRE	**PUESTO**	**PERMISOS**
PURIFICACIÓN PÉREZ ROJO	Administrativo	Recogida,Consulta,Grabado,Borrado,Cesión Conservación, Estructuración, Destrucción.
MARTA GONZÁLEZ IZQUIERDO	Administrativo	Recogida,Consulta,Grabado,Borrado,Cesión Estructuración, Destrucción.
SUSANA PIERA MORENO	Administrativo	Recogida,Consulta,Grabado,Borrado,Cesión Estructuración, Destrucción.
ENCARGADO DE TRATAMIENTO		
NOMBRE	**TRATAMIENTO**	**PERMISOS**
ALEJANDRO PRADA MOMÁN	Asesor Legal	Recogida,Consulta,Grabado,Borrado,Cesión Conservación, Estructuración, Destrucción.
ASESORÍA BARTOLOMÉ ARISTEGUI, S.L.	Asesoría	Recogida,Consulta,Grabado,Borrado,Cesión Conservación, Estructuración, Destrucción.
IMQ PREVENCIÓN	Prevención Riesgos	Recogida,Consulta,Grabado,Borrado,Cesión Conservación, Estructuración, Destrucción.
MAZARREDO AUDITORES,S.L.	Auditoría Externa	Recogida,Consulta,Grabado,Borrado,Cesión Conservación, Estructuración, Destrucción.

FICHERO: AGENDA Y CORREO ELECTRÓNICO		
RESPONSABLE DEL FICHERO	**MUGARIK GABE O.N.G.D.**	
RESPONSABLE DE SEGURIDAD	**PURIFICACIÓN PÉREZ ROJO**	
USUARIOS		
NOMBRE	**PUESTO**	**PERMISOS**
PURIFICACIÓN PÉREZ ROJO	Administrativo	Recogida,Consulta,Grabado,Borrado,Cesión Conservación, Estructuración, Destrucción.
MARTA GONZÁLEZ IZQUIERDO	Administrativo	Recogida,Consulta,Grabado,Borrado,Cesión Estructuración, Destrucción.
SUSANA PIERA MORENO	Administrativo	Recogida,Consulta,Grabado,Borrado,Cesión Estructuración, Destrucción.
ENCARGADO DE TRATAMIENTO		
NOMBRE	**TRATAMIENTO**	**PERMISOS**

FICHERO: FISCAL Y CONTABLE		
RESPONSABLE DEL FICHERO	**MUGARIK GABE O.N.G.D.**	
RESPONSABLE DE SEGURIDAD	**PURIFICACIÓN PÉREZ ROJO**	
USUARIOS		
NOMBRE	**PUESTO**	**PERMISOS**
PURIFICACIÓN PÉREZ ROJO	Administrativo	Recogida,Consulta,Grabado,Borrado,Cesión Conservación, Estructuración, Destrucción.
MARTA GONZÁLEZ IZQUIERDO	Administrativo	Recogida,Consulta,Grabado,Borrado,Cesión Estructuración, Destrucción.
SUSANA PIERA MORENO	Administrativo	Recogida,Consulta,Grabado,Borrado,Cesión Estructuración, Destrucción.
ENCARGADO DE TRATAMIENTO		
NOMBRE	**TRATAMIENTO**	**PERMISOS**
ASESORÍA BARTOLOMÉ ARISTEGUI, S.L.	Asesoría	Recogida,Consulta,Grabado,Borrado,Cesión Conservación, Estructuración, Destrucción.
MAZARREDO AUDITORES,S.L.	Auditoría Externa	Recogida,Consulta,Grabado,Borrado,Cesión Conservación, Estructuración, Destrucción.

NOTA: En caso de acceso a los ficheros por parte de otra persona que no está incluida en este anexo, se deberá de cumplimentar el registro que se acompaña a continuación.

REGISTRO DE ACCESO A LOS FICHEROS POR PERSONAL NO CLASIFICADO

FECHA	NOMBRE y APELLIDOS	FICHERO	MOTIVO	FIRMA DEL RESPONSABLE DE SEGURIDAD

ANEXO IV

DESCRIPCIÓN DE LA UBICACIÓN DE LOS FICHEROS

- Descripción del sistema informático.
- Descripción del local o ubicación física del Fichero.
- Autorizaciones para el tratamiento fuera de la ubicación física del Fichero

En este Anexo se describe la ubicación de los ficheros y del sistema de tratamiento de datos personales, así como las aplicaciones informáticas que acceden al fichero.

DESCRIPCIÓN DE LA UBICACIÓN FÍSICA DE LOS FICHEROS

CENTRO DE PROCESAMIENTO
GPO. Vicente Garamendi nº 5. Bajo. 48006. Bilbao. (Vizcaya)
DESCRIPCIÓN DEL INMUEBLE Y PUESTOS DE TRABAJO
Lonja a pie de calle ubicada en plaza peatonal. Tiene 198m2 con 7 salas y dos baños. Los ficheros se encuentran en una sala sin acceso a personal no autorizado. Dispone de otras salas en donde no se albergan ficheros con datos personales como por ejemplo sala de reuniones y almacén.
VIDEOVIGILANCIA
No dispone de videovigilancia pero si alarma.
DELEGACIONES
1. C/ Katalina Eleizegi nº 46, bajo. Pta. 3. 20009. Donostia (Guipuzkoa) 2. Itziar casa de asociaciones, Plaza Zalburu s/n. 01003. Vitoria-Gasteiz Araba.

CONTROL DE ACCESO FÍSICO	Si, Instalaciones bajo llave
PERSONAL CON COPIAS DE LLAVES	Personal autorizado

FICHEROS CON DATOS PERSONALES (MANUAL)	
FICHERO	UBICACIÓN
FISCAL Y CONTABLE	Archivadores AZ en armarios de la oficina
EMPLEADOS	Archivadores AZ en armarios de la oficina
SOCIOS	Archivadores AZ en armarios de la oficina

DESCRIPCIÓN DE LA UBICACIÓN LÓGICA DE LOS FICHEROS

a) RELACIÓN DE APLICACIONES INFORMÁTICAS QUE ACCEDEN AL FICHERO

FICHEROS CON DATOS PERSONALES (AUTOMATIZADOS)		
FICHERO	APLICACIÓN QUE LO GESTIONA	DESCRIPCIÓN
FISCAL Y CONTABLE	Aplicaciones Ofimáticas Contaplús	Local
EMPLEADOS	Aplicaciones Ofimáticas Contaplús	Local
AGENDA Y EMAIL	Aplicaciones Ofimáticas	Local
SOCIOS	Aplicaciones Ofimáticas Contaplús	Local

b) ENTORNO DE SISTEMAS OPERATIVOS, SEGURIDAD Y REDES

Sistema Operativo	Descripción
Windows	Xp y 7
Control de Acceso	Control de acceso mediante clave. Suspensión mediante inactividad.
Sistema de Redes	Cable y WIFI
Conexiones Remotas	No
Archivos y recursos compartidos	Si
Antivirus y Firewall	Si
SAI´s	Si

c) EQUIPAMIENTO INFORMÁTICO

Nombre del Componente	Unidades	Descripción
Ordenador sobremesa	14	clónico
Ordenador portátil	4	HP, SAMSUNG, LENOVO,ACER
Servidor		
Impresora multifunción	3	2 HP deskjet Isio + Hp laserjet Pro
fotocopiadora		
Smartphone		
Destructora de papel	1	Dahle

d) PAGINA WEB

Dirección	www.mugarikgabe.org
Formulario de Contacto	Si
Existencia de Cookies	Si
Recogida curriculums	No
Venta on line	No, salvo donaciones.
Cesión de datos recopilados	No.

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS FUERA DE LA UBICACIÓN DEL FICHERO.

En Bilbao; a _____ de _____ de _____

PURIFICACIÓN PÉREZ ROJO con NIF número 14931700-P, actuando como responsable de seguridad de **MUGARIK GABE O.N.G.D.**, autoriza a D/Dª._____**,** con DNI: _____**,** para que pueda realizar el tratamiento de los datos relativos al fichero denominado_____, fuera del local en dónde se encuentra ubicado el mismo, quedando designada la siguiente dirección:

Dirección:

Como autorizado, se compromete a mantener la confidencialidad y deber de Secreto sobre los datos de carácter personal a los que tenga acceso, establecer las medidas de seguridad correspondientes de acuerdo con el RD.1720/2007 de Protección de Datos y adoptar cualquier otra medida que esta empresa considere necesaria para salvaguardar la seguridad de los datos.

Queda terminantemente prohibido el acceso a los datos por personas no autorizadas así como el uso de cualquier dato de carácter personal o información confidencial con otra finalidad que no sea la estrictamente laboral o profesional en su relación con esta empresa.

En prueba de conformidad se firma en el lugar y fecha ut supra.

Autoriza:

Fdo. PURIFICACIÓN PÉREZ ROJO

Fdo. Autorizado

AUTORIZACIÓN PARA USO DE PORTÁTILES FUERA DE LA ORGANIZACIÓN

En Bilbao; a _____ de _____ de _____

El abajo firmante **PURIFICACIÓN PÉREZ ROJO** con DNI: 14931700-P, actuando como responsable de seguridad de **MUGARIK GABE O.N.G.D.**, autoriza a D/Dª._____, con DNI: _____, al uso fuera de las instalaciones de la empresa del portátil identificado con las siguientes características:

Marca:

Modelo:

Dirección I.P.:

La autorización sólo es aplicable para el tratamiento de datos de carácter personal, relacionados con la actividad laboral llevada a cabo en la organización arriba referenciada, no debiendo ser utilizados los datos personales para una finalidad distinta a la establecida, ni ser comunicados a terceros, los cuales no hayan sido previamente autorizados. El usuario del portátil se compromete a mantener la confidencialidad y deber de Secreto sobre los datos de carácter personal a los que tenga acceso, así como establecer las medidas de seguridad correspondientes que impidan el acceso a los datos por personas no autorizadas, así como la integridad del equipo, salvo situaciones excepcionales como robo o pérdida, que inmediatamente será comunicado a PURIFICACIÓN PÉREZ ROJO.

Autoriza:

Fdo. PURIFICACIÓN PÉREZ ROJO

Fdo. Usuario

ANEXO V

PROCEDIMIENTO DE CONTROL Y GESTIÓN DE SOPORTES

Las copias de seguridad se efectúan periódicamente sobre un soporte o unidad grabable (HDD, CINTAS, CD, DVD Pendrive o similar). Contendrán una pegatina o signo distintivo en la carátula que las designe. Estas copias de seguridad deberán custodiarse en lugar diferente al del lugar de trabajo.

A excepción de las copias de seguridad que se custodien en un lugar diferente al centro de trabajo, cualquier salida de los soportes que contengan los datos fuera del local donde está ubicado el fichero, deberá ser autorizada por el responsable del fichero de acuerdo con el documento de "Salida de soportes" que se adjunta.

INVENTARIO DE SOPORTES				
SOPORTE	**IDENTIFICACIÓN**	**UBICACIÓN**	**FICHEROS**	**FECHA Y MÉTODO DE DESTRUCCIÓN**
Disco duro externo	HD1-IOMEGA	Oficina	TODOS	**Fecha:** …./……/…… **Método de Destrucción:**
Disco duro externo	HD2-B-MOVE	Oficina	TODOS	**Fecha:** …./……/…… **Método de Destrucción:**
Disco duro externo	HD3- SAMSUNG	Oficina	TODOS	**Fecha:** …./……/…… **Método de Destrucción:**
Disco duro externo	NAS- Búfalo	Oficina	TODOS	**Fecha:** …./……/…… **Método de Destrucción:**

USB Pendrive	Pen1	Oficina	TODOS	**Fecha:** …./……/…… **Método de Destrucción:**
USB Pendrive	Pen2	Oficina	TODOS	**Fecha:** …./……/…… **Método de Destrucción:**
USB Pendrive	Pen3	Oficina	TODOS	**Fecha:** …./……/…… **Método de Destrucción:**
USB Pendrive	Pen4	Oficina	TODOS	**Fecha:** …./……/…… **Método de Destrucción:**
USB Pendrive	Pen5	Oficina	TODOS	**Fecha:** …./……/…… **Método de Destrucción:**

REGISTRO DE COPIAS DE SEGURIDAD*

COPIAS DE SEGURIDAD		
PERIODICIDAD DE COPIAS	*Semanal*	*Cifrada:* NO
TIPO DE GRABACIÓN	*Incremental / Volcado de datos*	
SOFTWARE UTILIZADO	*COBIAN BACKUP*	

***En caso de que el software no tenga un registro de copias de seguridad o histórico de copias se deberá de cumplimentar el siguiente registro.**

ALTAS			**BAJAS**		
Identificación, Nombre o Nº de orden del soporte	Observaciones/ Persona que realiza la operación	Fecha	Motivo		Fecha
			Sobres-cribir (x)	Destruc - ción (x)	
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /

		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /
		/ /			/ /

AUTORIZACIÓN PARA LA RECUPERACIÓN DE DATOS

En Bilbao; a _____ de _____ de _____

El abajo firmante **PURIFICACIÓN PÉREZ ROJO** con DNI: 14931700-P, actuando como responsable de seguridad de **MUGARIK GABE O.N.G.D.**, en cumplimiento de la normativa vigente en materia de protección de datos de carácter personal, autoriza mediante el presente escrito a D/Dª._____**,** con DNI: _____**,** para que pueda utilizar la copia de seguridad realizada en el soporte_____ con fecha _____, con la finalidad de restaurar la información a la situación anterior al momento en que se ocasionó la pérdida de datos o se vieron corrompidos.

El operario se compromete a mantener la confidencialidad y deber de Secreto sobre los datos de carácter personal a los que pueda tener acceso con motivo de dicha operación, así como establecer las medidas de seguridad correspondientes que impidan el acceso a los datos por personas no autorizadas, así como la integridad del equipo.

Autoriza:

Fdo. PURIFICACIÓN PÉREZ ROJO

Fdo. Operario

PROCEDIMIENTO DE RECUPERACIÓN DE DATOS

NOMBRE DEL FICHERO	
NÚMERO DE INSCRIPCIÓN	
Nº DE PROCEDIMIENTO	
PERSONA QUE EJECUTA EL PROCESO	Fdo. _____
DATOS RESTAURADOS	
DATOS GRABADOS MANUALMENTE	
AUTORIZACIÓN DEL RESPONSABLE DEL FICHERO	Fdo. _____

AUTORIZACIÓN DE SALIDA DE SOPORTES

Por regla General está prohibida la salida de soportes informáticos con datos personales fuera de los locales de la empresa donde se ubiquen los ficheros. Sin embargo y por motivos excepcionales, cualquier salida de soportes (CDROMs, Discos duros, Cintas, pendrives o similares) fuera del local donde está ubicado el fichero deberá ser autorizada por el responsable del fichero de acuerdo con el documento que se adjunta como **"Registro y autorización de salida de soportes".**

Asimismo, los soportes informáticos que almacenen datos sensibles o ficheros de nivel alto, deberán ir encriptados para garantizar su integridad y evitar cualquier acceso, así como para aquellos en soporte papel deberán adoptarse medidas orientadas a impedir el acceso o manipulación de la información objeto de traslado, como por ejemplo maletines con llave.

AUTORIZACIÓN DE SALIDA DE SOPORTES	**FECHA:**	/ /
	HORA:	____ : ____
Identificación del soporte		
Contenido		
FINALIDAD Y DESTINO		
Finalidad		
Destino		
Destinatario		
FORMA DE ENVÍO		
Medio de envío		
Remitente		
Medidas de seguridad (para evitar substracción, pérdida o acceso indebido)		
AUTORIZACIÓN		
Persona responsable de la entrega		
Cargo/puesto		
Persona que autoriza la salida		
Observaciones		
Firma del Responsable del Fichero:		

AUTORIZACIÓN DE ENTRADA DE SOPORTES

Por regla General está prohibida la entrada de soportes informáticos con datos personales procedentes del exterior de los locales de la empresa donde se ubiquen los ficheros. Sin embargo y por motivos excepcionales, cualquier entrada de soportes (CDROMs, Discos duros,cintas, pendrives o similares) en el local donde está ubicado el fichero deberá ser autorizada por el responsable del fichero de acuerdo con el documento que se adjunta a continuación **"Registro y autorización de entrada de soportes".**

Asimismo, la entrada de soportes informáticos que almacenen datos sensibles o de ficheros de nivel alto, deberán venir encriptados para garantizar su integridad y evitar cualquier acceso.

AUTORIZACIÓN DE ENTRADA DE SOPORTES	**FECHA:**	/ /
	HORA:	____ : ____
Identificación del soporte		
Contenido		
ORIGEN Y FINALIDAD		
Origen		
Finalidad		
FORMA DE ENVÍO		
Medio de envío		
Remitente		
Medidas de seguridad (para evitar substracción, pérdida o acceso indebido)		
AUTORIZACIÓN		
Persona responsable de la recepción		
Cargo/puesto		
Observaciones		
Firma del Responsable del Fichero:		

ANEXO VI

PROCEDIMIENTO DE NOTIFICACIÓN Y GESTIÓN DE INCIDENCIAS

Se entiende por incidencia aquella anomalía que afecte o pudiera afectar a la seguridad de los datos, entendiendo como tal aquella que pueda constituir un riesgo o inseguridad para la confidencialidad e integridad del propio fichero y de los datos de carácter personal que contiene.

- En la notificación se hará constar:

- *Tipo de incidencia.*
- *Fecha y hora en que se produjo.*
- *Persona que realiza la notificación.*
- *Persona a quien se comunica.*
- *Efectos que puede producir la incidencia.*
- *Descripción detallada de la misma.*

- Si se trata de una recuperación de datos se incluirá además:

- *Autorización del responsable del fichero.*
- *Procedimientos realizados.*
- *Persona que realizó el proceso.*
- *Datos restaurados.*
- *Datos grabados manualmente.*

Cuando ocurra una incidencia, el usuario o administrador deberá registrarla en el Libro de incidencias o comunicarla al responsable de seguridad para que a su vez proceda a su registro.

Se mantendrán las incidencias registradas de los 12 últimos meses.

NOTA: A continuación se adjunta el impreso de notificación manual que podrá ser utilizado para la notificación de incidencias, cuyos modelos se pueden descargar del CD que se le entrego con el proyecto.

IMPRESO DE NOTIFICACIÓN DE INCIDENCIAS

Incidencia Nº: **Fecha: / / Hora**
Tipo de incidencia:
Ficheros afectados:
Descripción de la incidencia:
Detectada por: Fdo……
Daños o efectos causados: (sólo para los casos de no subsanación)
ACCIONES A EMPRENDER ☐ Preventiva ☐ Correctora Descripción:
CIERRE DE LAS ACCIONES **Fecha / /** **Firma responsable del fichero/ Resp. de seguridad:** Fdo……
RECUPERACIÓN DE DATOS (rellenar si la incidencia implica este procedimiento)
Si la acción a tomar implicase la recuperación de datos, ésta se realiza conforme al Procedimiento de Realización de Copias de Respaldo y Recuperación de Datos, describiendo la persona que realiza el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
Datos restaurados: **Persona que ejecutó el proceso** **Observaciones** **Firma responsable del fichero/ Resp. de seguridad:** Fdo……

Instrucciones para cumplimentar y notificar la notificación al dorso

INSTRUCCIONES PARA CUMPLIMENTAR LA NOTIFICACIÓN DE INCIDENCIAS

Fichero objeto de la incidencia: Consignar el nombre del fichero si se conoce o la descripción de los datos objeto de la incidencia. Por ej. *datos de clientes, de personal, de nóminas, etc…*

Tipo de Incidencia: Detallar, si es posible, el tipo de incidencia. Por ej. *copia no autorizada de datos, robo de contraseñas, pérdida de soportes, cesión de datos no autorizada, etc…*

Descripción detallada de la Incidencia: Describir la incidencia aportando el mayor nivel de detalle posible.

Fecha de la Incidencia: Consignar la fecha en que se produjo la incidencia o, en caso de no conocerse tal fecha, consignar la fecha en que se ha detectado la incidencia.

Hora de la Incidencia: Consignar la hora en que se produjo la incidencia o, en caso de no conocerse tal hora, consignar la hora en que se ha detectado la incidencia.

Efectos que puede producir: Detallar, si se conocen, los efectos que puede producir la incidencia sobre los datos de carácter personal.

Fecha de Notificación: Consignar la fecha en que realiza la notificación.

Persona(s) que realiza(n) la comunicación: Consignar el/los nombre(s) de la(s) persona(s) que realiza la notificación.

INSTRUCCIONES PARA REALIZAR LA NOTIFICACIÓN

Una vez cumplimentado el presente formulario con todos aquellos detalles de la incidencia que se conozcan, debe hacerse llegar al Responsable de Seguridad o Responsable del Fichero siguiendo procedimiento detallado a continuación:

Se puede imprimir el formulario en blanco y cumplimentarlo posteriormente a mano. O bien cumplimentarlo electrónicamente y posteriormente imprimir la copia ya rellenada. Posteriormente se debe tramitar el formulario cumplimentado por alguno de los siguientes medios:

- Entregar en mano al Responsable Propietario del Fichero.
- Entregar en mano al Responsable de Seguridad.
- Enviarlo por correo interno al a la atención del Responsable de Seguridad o responsable del Fichero.

INSTRUCCIONES PARA LA RECUPERACIÓN DE DATOS

Si la acción a tomar implicase la recuperación de datos, ésta se realiza conforme al Procedimiento de Realización de Copias de Respaldo y Recuperación de Datos, describiendo la persona que realiza el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

ANEXO VII

PROCEDIMIENTO DE DISTRIBUCIÓN, AUTENTICACIÓN Y ASIGNACIÓN DE CONTRASEÑAS

El art. 5.2 del Reglamento en su letra b), define en particular, en relación con el título VIII, la autenticación como el procedimiento de comprobación de la identidad de un usuario; a su vez se define en la letra h) la identificación como el procedimiento de la identidad de un usuario.

De acuerdo con lo arriba dispuesto, MUGARIK GABE O.N.G.D. lleva a cabo un mecanismo de Identificación y Autenticación relativo al acceso mediante un sistema concreto y único para cada uno de los usuarios y administradores que acceden a la información mediante nombre de usuario o identificación como empleado.

De las diversas formas de autenticación que existen, se ha determinado el uso de un **sistema basado en contraseñas o password** para acceder a los centros de tratamiento o equipos informáticos que contengan datos de carácter personal, siendo necesaria una contraseña que se asignará y distribuirá por el responsable del fichero quien podrá delegar en el responsable de seguridad dicha competencia, o por aquella persona designada para tal efecto, sin perjuicio de que el usuario pueda cambiarla con posterioridad de acuerdo con el procedimiento de distribución que se detalla a continuación.

En todos los casos, las contraseñas deberán garantizar en todo caso las siguientes pautas de seguridad:

- Utilizar contraseñas de calidad óptima, con una longitud de seis caracteres como mínimo, que sean fácilmente recordadas y estén formadas a partir de la combinación de letras y números, mayúsculas y minúsculas o incluir símbolos.
- Deberá evitarse que se designen contraseñas con nombres, fechas o parámetros asociados al usuario o deducible por un tercero, como por ejemplo nombre de mascotas, hijos, NIF, matrículas o numeraciones del tipo 123456
- Evitar palabras que se encuentren en el diccionario, puesto que los programas de revelación de claves utilizan diccionarios como base de datos.
- No utilizar la misma contraseña para distintos usos ni repetirla periódicamente.
- No se almacenarán de forma legible ni se escribirán en papeles o similares en lugares próximos a los equipos de tratamiento.

Las contraseñas **son personales, secretas e intransferibles y se cambiarán con una periodicidad máxima de UN AÑO**.

Le será requerida al usuario autorizado cada vez que acceda a los equipos informáticos, tanto al inicio de sesión como al reincorporarse al puesto de trabajo después de un periodo de tiempo sin actividad.

El procedimiento de distribución de contraseñas será el siguiente:
El Responsable del Fichero o la persona designada por este, asignará una contraseña al iniciarse la primera sesión en el sistema, se la distribuirá de forma cifrada o por cualquier medio seguro para que sea cambiada al iniciarse la primera sesión por el usuario siguiendo las pautas de seguridad descritas. El cambio de contraseñas se renovará dentro de los plazos establecidos a petición del sistema o por iniciativa del usuario.

De acuerdo con el artículo 98 del Reglamento se procurará que el acceso a los ficheros esté limitado a tres intentos fallidos para impedir la posibilidad de intentar reiteradamente el acceso a dichos ficheros.

Control de acceso mediante clave	Si
Suspensión mediante inactividad	Si
Número de caracteres	12
Tipo de caracteres	Alfanuméricos
Número de intentos fallidos	3
Periodicidad cambio claves	Anual
Archivos y aplicaciones compartidas	Si, acceso por intranet
Conexiones remotas	no

ANEXO VIII

DOCUMENTOS RELEVANTES Y RESULTADOS DE AUDITORÍAS