AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

GUÍA de Seguridad de Datos

Grupo 8:
José Joaquín Arias Gómez-Calcerrada
Manuel Diaz Gil
Daniel Mejías Ramírez
Jesús Rosa Bilbao

Indice

GUÍA MODELO DEL DOCUMENTO DE SEGURIDAD

INTRODUCCIÓN

El RLOPD especifica que se puede disponer de un solo documento que incluya todos los ficheros y tratamientos con datos personales de los que una persona física o jurídica sea responsable, un documento por cada fichero o tratamiento, o los que determine el responsable atendiendo a los criterios organizativos que haya establecido. Cualquiera de las opciones puede ser válida. En este caso se ha optado por el primer tipo, organizando el "documento de seguridad" en dos partes: en la primera se recogen las medidas que afectan a todos los sistemas de información de forma común con independencia del sistema de tratamiento sobre el que se organizan: informatizado, manual o mixto, y en la segunda se incluye un anexo por cada fichero o tratamiento, con las medidas que le afecten de forma concreta. Además, se han especificado aquellas medidas que afectan sólo a ficheros automatizados y las que afectan a los no automatizados de forma exclusiva.

El modelo se ha redactado con el objeto de recopilar las exigencias mínimas establecidas por el Reglamento. Es posible y recomendable incorporar 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.

Dentro del modelo se utilizarán los siguientes símbolos convencionales:
<comentario explicativo>: Entre los caracteres "<" y ">", se encuentran los comentarios aclaratorios sobre el contenido que debe tener un campo. Estos textos no deben figurar en el documento final, y deben desarrollarse para ser aplicados a cada caso concreto.

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.

NIVEL ALTO: Con esta marca se señalarán las medidas que sólo son obligatorias en los ficheros que tengan que adoptar un nivel de seguridad alto.

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.

Las medidas que no van precedidas de ninguna de estas marcas deben aplicarse con carácter general, tanto a ficheros o tratamientos automatizados como no automatizados y con independencia del nivel de seguridad.

MODELO DE DOCUMENTO DE SEGURIDAD

El presente Documento y sus Anexos, redactados en cumplimiento de 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.

El contenido de este documento queda estructurado como sigue:

- Ámbito de aplicación del documento.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.
- Información y obligaciones del personal.
- Procedimientos de notificación, gestión y respuestas ante las incidencias.

- Procedimientos de revisión.

ANEXO I. Descripción de ficheros.

ANEXO II. Nombramientos.

ANEXO III. Autorizaciones de salida o recuperación de datos.

ANEXO IV. Delegación de autorizaciones.

ANEXO V. Inventario de soportes.

ANEXO VI. Registro de Incidencias .

ANEXO VII. Encargados de tratamiento

ANEXO VIII. Registro de entrada y salida de soportes.

ANEXO IX. Medidas alternativas

1.ÁMBITO DE APLICACIÓN DEL DOCUMENTO

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de Fernando Fernández Fernández, 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 normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

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

Fichero o tratamiento	Tipo de sistema	Nivel de seguridad
Pacientes	Manual	Bajo
Nominas	Mixto	Medio
Partes (Siniestros)	Mixto	Medio
Historial Médico	Automatizado	Alto

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

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

IDENTIFICACIÓN Y AUTENTICACIÓN

Medidas y normas relativas a la identificación y autenticación del personal autorizado para acceder a los datos personales.

AUTOMATIZADOS

Se realizará mediante el uso de un usuario y contraseña, para acceder al sistema el cual contendrá todos los datos. Cada persona de la empresa tendrá un usuario y contraseña con el que tendrá acceso a unos datos u otros.

Las contraseñas se les asignaran a los usuarios, pidiendo luego un cambio al usuario de la contraseña, a ser posible cada 6 meses. Las contraseñas se generaran de manera aleatoria.

Las contraseñas deberán tener caracteres especiales, mayúsculas, minúsculas y números.

AUTOMATIZADOS

NIVEL MEDIO En los ficheros de nivel medio y alto, se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

CONTROL DE ACCESO

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados mediante los privilegios que tenga cada usuario en su login.

Exclusivamente el Juan Antonio Ramírez Peregrina 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.

Se deberá comunicar a Juan Antonio Ramírez Peregrina la autorización para acceder a los ficheros registrando este la persona que accede y cuando pidió el permiso.

Nivel medio o bajo puede acceder cualquiera que tenga autorización de Juan Antonio Ramírez Peregrina, mientras que si son de alto nivel solo se podrá acceder con la autorización y desde una terminal especifica.

En el Anexo I, se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista deberá mantenerse actualizada cada vez que se incluya un nuevo fichero que contenga datos.

De existir personal ajeno al responsable del fichero con acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

NIVEL ALTO: REGISTRO DE ACCESOS

AUTOMATIZADOS

En los accesos a los datos de los ficheros de nivel alto, se registrará por cada acceso la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. 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 5 años.

El responsable de seguridad revisará al menos una vez al mes la información de control registrada y elaborará un informe según se detalla en el capítulo de “Comprobaciones para la realización de la auditoría de seguridad” de este documento.

No será necesario el registro de accesos cuando:

- el responsable del fichero es una 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.

MANUALES

El acceso a la documentación se limita exclusivamente al personal autorizado.
Se establece el siguiente mecanismo para identificar los accesos realizados en el caso de los documentos relacionados los documentos que contengan datos del cliente, y el acceso se hará registrando la fecha y quien accede a el.

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 *<indicar el lugar de acceso restringido donde se almacenarán>*, lugar de acceso restringido al que solo tendrán acceso las personas con autorización que se relacionan a continuación: *<Especificar el personal autorizado a acceder al lugar donde se almacenan los soportes que contengan datos de carácter personal, el procedimiento establecido para habilitar o retirar el permiso de acceso. Tener en cuenta el procedimiento a seguir para casos en que personal no autorizado tenga que tener acceso a los locales por razones de urgencia o fuerza mayor>*.

Los siguientes soportes *<relacionar aquellos a que se refiere>* se exceptúan de las obligaciones indicadas en el párrafo anterior, dadas sus características físicas, que imposibilitan el cumplimiento de las mismas.

Los siguientes soportes *<indicar aquellos que contengan datos considerados especialmente sensibles y respecto de los que se haya optado por proceder del siguiente modo>* se identificarán utilizando los sistemas de etiquetado

siguientes <*especificar los criterios de etiquetado que serán comprensibles y con significado para los usuarios autorizados, permitiéndoles identificar su contenido, y que sin embargo dificultarán la identificación para el resto de personas*>.

Los soportes se almacenarán de acuerdo a las siguientes normas: <*indicar normas de etiquetado de los soportes. Especificar el procedimiento de inventariado y almacenamiento de los mismos. El inventario de soportes puede anexarse al documento o gestionarse de forma automatizada, en este último caso se indicará en este punto el sistema informático utilizado*>.

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 el responsable del fichero o aquel en que se hubiera delegado de acuerdo al siguiente procedimiento <*detallar el procedimiento a seguir para que se lleve a cabo la autorización. Tener en cuenta también los ordenadores portátiles y el resto de dispositivos móviles que puedan contener datos personales*>.

En el Anexo III se incluirán los documentos de autorización relativos a la salida de soportes que contengan datos personales.

Los soportes que vayan a ser desechados, deberán ser previamente <*detallar procedimiento a realizar para su destrucción o borrado*> de forma que no sea posible el acceso a la información contenida en ellos o su recuperación posterior.

En el traslado de la documentación se adoptarán las siguientes medidas para evitar la sustracción, pérdida o acceso indebido a la información: <*indicar las medidas y procedimientos previstos*>.

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 al siguiente procedimiento: *<Detallar el procedimiento por el que se registrarán las entradas y salidas de soportes>*.

El registro de entrada y salida de soportes se gestionará mediante *<indicar la forma en que se almacenará el registro, que puede ser manual o informático>* y en el que deberán constar *<indicar los campos del registro, que deberán ser, al menos, en el caso de las entradas, el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la recepción; y en el caso de las salidas, el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la entrega>*.

<En caso de gestión automatizada se indicará en este punto el sistema informático utilizado>.

AUTOMATIZADOS

NIVEL ALTO: GESTIÓN Y DISTRIBUCIÓN DE SOPORTES

En este caso los soportes se identificarán mediante el sistema de etiquetado *<especificar los criterios de etiquetado que resultarán comprensibles y con significado 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 *<indicar el procedimiento para cifrar los datos o, en su caso, para utilizar el mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte. Igualmente se cifrarán los datos que contengan los dispositivos portátiles cuando se encuentren fuera de las instalaciones que están bajo control del responsable>*.

Los siguientes dispositivos portátiles <*relacionar aquellos que no permitan el cifrado de los datos personales*>, debido a las razones indicadas <*motivar la necesidad de hacer uso de este tipo de dispositivos*>, se utilizarán en el tratamiento de datos personales adoptándose las medidas que a continuación se explicitan <*relacionar las medidas alternativas que tendrán en cuenta los riesgos de realizar tratamientos en entornos desprotegidos*>.

MANUALES
CRITERIOS DE ARCHIVO

El archivo de los soportes o documentos se realizará de acuerdo con los criterios <*indicar los previstos en la legislación que les afecte o en su defecto, 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*>.

MANUALES
ALMACENAMIENTO DE LA INFORMACIÓN

Los siguientes dispositivos <*relacionarlos así como aquellas de sus características que obstaculicen su apertura. Cuando sus características físicas no permitan adoptar esta medida, el responsable adoptará medidas que impidan el acceso a la información de personas no autorizadas*> se utilizarán para guardar los documentos con datos personales.

NIVEL ALTO: Los elementos de almacenamiento <*indicar tipos como armarios, archivadores u otros elementos utilizados*> respecto de los documentos con datos personales, se encuentran en <*indicar lugares físicos y protección con que cuenta el acceso a las mismas, como llaves u otros dispositivos. Además estos lugares permanecerán cerrados en tanto no sea preciso el acceso a los documentos. Si a la vista de las características de los locales no fuera posible cumplir lo anteriormente indicado, se adoptarán medidas alternativas que se reflejarán en este punto*>.

MANUALES

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.

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. Relacionar los accesos previstos y los ficheros a los que se prevea acceder>.

AUTOMATIZADOS

NIVEL ALTO: Los datos personales correspondientes a los ficheros de nivel alto, que se transmitan a través de redes públicas o inalámbricas de comunicaciones electrónicas se realizará cifrando previamente estos datos *<indicar en su caso otros mecanismos distintos del cifrado que se utilicen y que garanticen que la información no sea inteligible ni manipulada por terceros. También es adecuado cifrar los datos en red local>*.

RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO

Se pueden llevar a cabo los siguientes tratamientos de datos personales *<relacionar los ficheros a que afecten estos tratamientos>* fuera de los locales del responsable del fichero *<indicar en su caso, los distintos locales a los que deban circunscribirse, especialmente en el supuesto de que se*

realicen tratamientos por un encargado del tratamiento que se especificará>, así como mediante dispositivos portátiles. Esta autorización regirá durante <*indicar el período de validez de la misma*>.

<*Esta autorización puede realizarse para unos usuarios concretos que hay que indicar o para un perfil de usuarios*>.

<*Se debe garantizar el nivel de seguridad correspondiente*>.

MANUALES
NIVEL ALTO

TRASLADO DE DOCUMENTACIÓN

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse las siguientes medidas <*relacionar las medidas necesarias y en su caso alternativas recomendadas, orientadas a impedir el acceso o manipulación de la información objeto de traslado*>.

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.

MANUALES
NIVEL ALTO

COPIA O REPRODUCCIÓN

La realización de copias o reproducción de los documentos con datos personales sólo se podrán llevar a cabo bajo el control del siguiente personal autorizado <*indicar los usuarios o perfiles habilitados para ello*>.

Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida <*indicar los medios a utilizar o puestos a disposición de los usuarios para ello*>.

AUTOMATIZADOS

COPIAS DE RESPALDO Y RECUPERACIÓN

Se realizarán copias de respaldo, salvo que no se hubiese producido ninguna actualización de los datos, con la siguiente periodicidad <*especificarla, y en todo caso será como mínimo una vez a la semana*>.

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. En el caso de los ficheros parcialmente automatizados siguientes <*indicarlos*>, se grabarán manualmente los datos. <*Para la grabación manual indicada deberá existir documentación que permita dicha reconstrucción*>.

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.

En el Anexo I se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

NIVEL ALTO: En los ficheros de nivel alto se conservará una copia de respaldo y de los procedimientos de recuperación de los datos en <*especificar el lugar, diferente de donde se encuentran los sistemas informáticos que los tratan, y que deberá cumplir las medidas de seguridad, o utilizando elementos que garanticen la integridad y recuperación de la información de forma que sea recuperable*>.

NIVEL MEDIO: RESPONSABLE DE SEGURIDAD

Se designa como responsable de seguridad <*indicarlo/s en el caso de que se prevea que sean varios*>, que con carácter general se encargará de coordinar y controlar las medidas definidas en este documento de seguridad. <*La designación puede ser única para todos los ficheros o diferenciada según los sistemas de tratamiento, lo que se especificará en este documento, en la parte correspondiente del Anexo I*>.

En ningún caso, la designación supone una exoneración de la responsabilidad que corresponde a <*denominación responsable del fichero o del encargado del tratamiento*> como responsable del fichero de acuerdo con el RLOPD.

El responsable de seguridad desempeñará las funciones encomendadas durante el periodo de <*indicar periodo de desempeño del cargo*>. Una vez transcurrido este plazo <*denominación responsable del fichero*> podrá nombrar al mismo responsable de seguridad o a otro diferente.

En el Anexo II se encuentran las copias de los nombramientos de responsables de seguridad.

3. 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 de acuerdo con el siguiente

procedimiento: Las normas estarán recogidas en un documento, el cual se hará público a dichas personas a la hora de firmar el contrato. La aseguradora no se hará cargo de los incidentes que no estén cubiertos por el documento.

Con una frecuencia de dos veces al año, aproximadamente, se actualizará la información sobre seguridad. Esta información será remitida a los clientes mediante correo electrónico.

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 al responsable del fichero o de seguridad descritos en el anexo II 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.

Funciones y obligaciones de Jesús Rosa Bilbao:

- Es el responsable de la sala de comunicaciones.
- En caso de ausencia, se delegará la responsabilidad a Daniel Mejías Ramírez.

Funciones y obligaciones de Daniel Mejías Ramírez:

- Es el responsable del apartado de seguridad informática.
- En caso de ausencia se delegará la responsabilidad del apartado de seguridad informática a Manuel Díaz Gil.

- También se encarga de revisar el correcto funcionamiento de la autenticación para los trabajadores.

Funciones y obligaciones de Manuel Díaz Gil:

- Es el responsable de la seguridad física.
- En caso de ausencia se delegará la función de seguridad física a José Joaquín Arias Gómez-Calcerrada.
- Es el administrador de las Bases de Datos.

Funciones y obligaciones de José Joaquín Arias Gómez-Calcerrada:

- Es el administrador en el área de auditoría.
- En caso de ausencia se delegará la función de administrador en el área de auditoría a Jesús Rosa Bilbao.
- Es el encargado del desarrollo de software en el área de informática.

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.

Se delegan las siguientes autorizaciones en los usuarios relacionados con temas jurídicos bajo autorización de un juez.

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, se sancionará conforme a lo que se establezca en la normativa sancionadora de la Ley Orgánica de Protección de Datos.

4. 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 asociación.

El procedimiento a seguir para la notificación de incidencias será el siguiente: La notificación de la incidencia será emitida con la fecha de su ocurrencia (en formato HH:MM:SS), donde se indicará la persona que la formula y el área o departamento afectado. La notificación será entregada al departamento de seguridad de la empresa, el cuál la examinará y actuará en consecuencia en un período de tiempo dependiente de la complejidad de la misma. La incidencia debe ser apuntada en el instante que le llegue al departamento de seguridad. Será apuntada en el registro de incidencias de la empresa, junto con su fecha e identificador único, entre otras cosas.

El registro de incidencias se gestionará mediante forma informática automatizada, donde se almacenará la fecha de la ocurrencia de la incidencia, su identificador único (generado de forma automática a la hora de almacenar la notificación en el registro), la persona que formula la notificación y una breve descripción de la misma.

AUTOMATIZADOS

NIVEL MEDIO: En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten a los ficheros de nivel medio y alto, del modo que se indica a continuación: En primer lugar se restauran los posibles activos afectados, para más adelante poder restaurar los archivos perdidos sin que los activos ocasionen problemas. La restauración será a través de las copias de seguridad. Siempre habrá un

mínimo de dos copias de seguridad por cada grupo significativo de archivos, de dos fechas distintas y próximas. El proceso de la realización de estas copias de seguridad está automatizado, para que no haya problemas. Se registrará en el histórico de incidencias todos los cambios realizados sobre los activos dañados.

NIVEL MEDIO: 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 III se incluirán los documentos de autorización del responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

5. PROCEDIMIENTOS DE REVISIÓN

REVISIÓN 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.

Para la modificación del documento de seguridad, se aceptan propuestas de cambio. Las propuestas de cambio provendrán de cualquier departamento que para la ejecución de su actividad laboral tuviera que manipular datos de carácter personal o datos sensibles acogidos a la LOPD. A la hora de aprobar estos cambios o mejoras, se deben aceptar por el director y subdirector de Seguridad. En el caso de ser aprobados los cambios, debe ser comunicado en un escrito al departamento emisor. Se recuerda que el documento debe ser revisado con período de dos años.

NIVEL MEDIO: AUDITORÍA

Con el objeto de no vulnerar el cumplimiento del Título VIII del RLOPD referente a las medidas de seguridad según lo indicado en sus artículos 96 y 110 respecto de ficheros automatizados y no automatizados, las auditorías tendrán lugar cada dos años, dado que así se permite hacer un seguimiento de la evolución de la tecnología. Dichas auditorías serán ejecutadas por el director de Seguridad y serán internas a la entidad.

Con carácter extraordinario deberá realizarse cuando se lleven a cabo modificaciones sustanciales en el sistema de información que pueden repercutir en el cumplimiento de las medidas de seguridad implantadas, con el objeto de verificar la adaptación, la adecuación y la eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado.

El informe analizará la adecuación de las medidas y controles de la Ley y su desarrollo reglamentario, 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.

AUTOMATIZADOS

NIVEL ALTO: INFORME MENSUAL SOBRE EL REGISTRO DE ACCESOS

El primer día hábil de cada mes se hará un registro que contendrá información relacionada con la traza de accesos cursados sobre datos de nivel alto, con el objetivo de seguir de cerca toda posible actividad ilícita, como accesos no permitidos, para que no causen posibles perjuicios a los propietarios de los datos o la asociación en sí.

ANEXO I
DESCRIPCIÓN DE FICHEROS

Actualizado a: 7 de mayo de 2018.

ANEXO I a – Fichero sobre pacientes

- Nombre del fichero o tratamiento: Fichero_Pacientes.
- Unidad/es con acceso al fichero o tratamiento: Administración general.
- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos:
  - Identificador: PDQWY2093V
  - Nombre: Pacientes
  - Descripción: En este fichero se almacenan datos personales de los pacientes de nivel bajo o medio.
- Nivel de medidas de seguridad a adoptar: Bajo.

NIVEL MEDIO: RESPONSABLE DE SEGURIDAD Daniel Mejías Ramírez.

- Administrador: José Joaquín Arias Gómez-Calcerrada.
- Leyes o regulaciones aplicables que afectan al fichero o tratamiento: Aplicación de los criterios establecidos por la LOPD.

- Código Tipo Aplicable: Protección de datos de carácter personal, por la Ley Orgánica de Protección de Datos.

- Estructura del fichero principal: Entre los tipos de datos presentes en el fichero, se encuentran los datos de carácter identificativo. Estos son el nombre y apellidos, teléfono, dirección, firma, DNI/NIF, sexo, nacionalidad y número de inscripción en la seguridad social.

- Información sobre el fichero o tratamiento

    - Finalidad y usos previstos: Tratamiento de los datos de los pacientes para cálculos estadísticos con los datos permitidos por el usuario y para la gestión de los mismos.

    - Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales, y procedencia de los datos: Los pacientes.

    - Procedimiento de recogida: Aportados por el paciente a la hora contratar la aseguradora.

    - Cesiones previstas: Seguridad Social.

    - Transferencias Internacionales: No procede.

    - Sistema de tratamiento: Manual.

    - Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Los departamentos de administración de la asociación.

    - Descripción detallada de las copias de respaldo y de los procedimientos de recuperación: Se realizarán copias completas cada dos semanas, además de una copia progresiva mensual.

- Información sobre conexión con otros sistemas: La mayor parte de los datos personales con el fichero del Historial Médico, el fichero sobre partes y el fichero sobre nóminas.

- Funciones del personal con acceso a los datos personales: Administración general, departamento de seguridad y responsable de seguridad.

- Descripción de los procedimientos de control de acceso e identificación: Usuario y contraseña para la identificación y acceso.

- Relación actualizada de usuarios con acceso autorizado: Administración general, con clave AAAAAA, dado de alta el día 31/12/2008. Departamento de seguridad, con clave BBBBBB, dado de alta el día 31/12/2008. Responsable de seguridad, con clave CCCCCC, dado de alta el día 31/12/2008.

ANEXO I b – Fichero sobre nóminas

- Nombre del fichero o tratamiento: Fichero_Nominas.

- Unidad/es con acceso al fichero o tratamiento: Administración general.

- Identificador y nombre del fichero en el Registro General de Protección
de Datos de la Agencia Española de Protección de Datos:

  - Identificador: OWD3H98LAP
  - Nombre: Nóminas
  - Descripción: En este fichero se almacenan los datos relacionados con los registros financieros de los sueldos de los empleados.

- Nivel de medidas de seguridad a adoptar: Medio.

NIVEL MEDIO: RESPONSABLE DE SEGURIDAD

Daniel Mejías Ramírez.

- Administrador: Jesús Rosa Bilbao.

- Leyes o regulaciones aplicables que afectan al fichero o tratamiento: Aplicación de los criterios establecidos por la LOPD.

- Código Tipo Aplicable: Protección de datos de carácter personal, por la Ley Orgánica de Protección de Datos.

- Estructura del fichero principal: Entre los tipos de datos presentes en el fichero, se encuentran los datos de carácter identificativo. Estos son el nombre y apellidos, teléfono, dirección, firma, DNI/NIF, sexo, nacionalidad y número de inscripción en la seguridad social. Además, se encuentran datos de carácter financiero como los sueldos de dichos empleados.

- Información sobre el fichero o tratamiento

    - Finalidad y usos previstos: Gestión financiera de los datos y análisis de estos.

    - Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales, y procedencia de los datos: Los clientes.

    - Procedimiento de recogida: Aportados por el cliente a la hora contratar la aseguradora.

- Cesiones previstas: Seguridad Social e información económica.

- Transferencias Internacionales: No procede.

- Sistema de tratamiento: Mixto.

- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Los departamentos de administración de la asociación.

- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación: Se realizarán copias completas cada dos semanas, además de una copia progresiva mensual.

- Información sobre conexión con otros sistemas: La mayor parte de los datos personales con el fichero del Historial Médico, el fichero sobre partes y el fichero de pacientes.

- Funciones del personal con acceso a los datos personales: Administración general, departamento de seguridad y responsable de seguridad.

- Descripción de los procedimientos de control de acceso e identificación: Usuario y contraseña para la identificación y acceso.

- Relación actualizada de usuarios con acceso autorizado: Administración general, con clave DDDDDD, dado de alta el día 31/12/2008. Departamento de seguridad, con clave EEEEEE, dado de alta el día 31/12/2008. Responsable de seguridad, con clave FFFFFF, dado de alta el día 31/12/2008.

ANEXO I c – Fichero sobre Partes (Siniestros)

- Nombre del fichero o tratamiento: Fichero_Partes.

- Unidad/es con acceso al fichero o tratamiento: Seguridad.

- Identificador y nombre del fichero en el Registro General de Protección
  de Datos de la Agencia Española de Protección de Datos:

  - Identificador: QWDIN83NE2
  - Nombre: Partes
  - Descripción: En este fichero se almacenan los datos relacionados con los partes de los siniestros acontecidos.

- Nivel de medidas de seguridad a adoptar: Medio.

NIVEL MEDIO: RESPONSABLE DE SEGURIDAD
Daniel Mejías Ramírez.

- Administrador: Manuel Díaz Gil.

- Leyes o regulaciones aplicables que afectan al fichero o tratamiento: Aplicación de los criterios establecidos por la LOPD.

- Código Tipo Aplicable: Protección de datos de carácter personal, por la Ley Orgánica de Protección de Datos.

- Estructura del fichero principal: Entre los tipos de datos presentes en el fichero, se encuentran los datos de carácter identificativo. Estos son el nombre y apellidos, teléfono, dirección, firma, DNI/NIF, sexo, nacionalidad y número de inscripción en la seguridad social.

- Información sobre el fichero o tratamiento

  - Finalidad y usos previstos: Tratamiento y análisis de partes de siniestros para el seguimiento de las ocurrencias al cliente y posibles acuerdos con otros clientes, entre otras cosas.

  - Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales, y procedencia de los datos: Los clientes y otras fuentes suministradoras de información adicional del parte.

  - Procedimiento de recogida: Aportados por el cliente y otras fuentes tras el siniestro.

  - Cesiones previstas: Seguridad Social.

  - Transferencias Internacionales: No procede.

  - Sistema de tratamiento: Mixto.

  - Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Los departamentos de seguridad de la asociación.

  - Descripción detallada de las copias de respaldo y de los procedimientos de recuperación: Se realizarán copias completas cada dos semanas, además de una copia progresiva mensual.

  - Información sobre conexión con otros sistemas: La mayor parte de los datos personales con el fichero del Historial Médico, el fichero sobre nóminas y el fichero de pacientes.

  - Funciones del personal con acceso a los datos personales: Departamento de seguridad y responsable de seguridad.

- Descripción de los procedimientos de control de acceso e identificación: Usuario y contraseña para la identificación y acceso.

- Relación actualizada de usuarios con acceso autorizado: Departamento de seguridad, con clave GGGGGG, dado de alta el día 31/12/2008. Responsable de seguridad, con clave HHHHHH, dado de alta el día 31/12/2008.

ANEXO I d – Fichero sobre Historial Médico

- Nombre del fichero o tratamiento: Fichero_Historial_Medico.

- Unidad/es con acceso al fichero o tratamiento: Departamento de Seguridad y Área Médica.

- Identificador y nombre del fichero en el Registro General de Protección
  de Datos de la Agencia Española de Protección de Datos:

  - Identificador: IDQWH328QH
  - Nombre: Historial Médico
  - Descripción: En este fichero se almacenan los datos relacionados con el historial médico de los clientes de la asociación.

- Nivel de medidas de seguridad a adoptar: Alto.

NIVEL MEDIO: RESPONSABLE DE SEGURIDAD Daniel Mejías Ramírez.

- Administrador: José Joaquín Arias Gómez-Calcerrada.

- Leyes o regulaciones aplicables que afectan al fichero o tratamiento: Aplicación de los criterios establecidos por la LOPD y RD3/2010.

- Código Tipo Aplicable: Protección de datos de carácter personal, por la Ley Orgánica de Protección de Datos.

- Estructura del fichero principal: Entre los tipos de datos presentes en el fichero, se encuentran los datos de carácter identificativo. Estos son el nombre y apellidos, teléfono, dirección, firma, DNI/NIF, sexo, nacionalidad, posibles patologías (discapacidad, minusvalía, otros) y número de inscripción en la seguridad social. También tendrá los datos de donación (fecha de extracción).

- Información sobre el fichero o tratamiento

    - Finalidad y usos previstos: Tratamiento de los donantes de sangre y seguimiento del estado de los clientes/pacientes. También se hace un seguimiento del estado de los activos orgánicos.

    - Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales, y procedencia de los datos: Los clientes, pacientes y donantes de sangre (voluntarios).

    - Procedimiento de recogida: Aportados por el cliente y por el personal sanitario autorizado.

    - Cesiones previstas: Seguridad Social.

    - Transferencias Internacionales: No procede.

    - Sistema de tratamiento: Automatizado.

- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Los departamentos de seguridad de la asociación y los departamentos de la asociación sobre información médica.

- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación: Se realizarán copias completas cada dos semanas, además de una copia progresiva mensual.

- Información sobre conexión con otros sistemas: La mayor parte de los datos personales con el fichero de partes, el fichero sobre nóminas y el fichero de pacientes.

- Funciones del personal con acceso a los datos personales: Departamento de seguridad, responsable de seguridad y responsable del área médica.

- Descripción de los procedimientos de control de acceso e identificación: Usuario y contraseña para la identificación y acceso.

- Relación actualizada de usuarios con acceso autorizado: Departamento de seguridad, con clave IIIIII, dado de alta el día 31/12/2008. Responsable de seguridad, con clave JJJJJJ, dado de alta el día 31/12/2008.

ANEXO II
NOMBRAMIENTOS

- Responsable de seguridad: Daniel Mejías Ramírez.
- Responsable de administración en el área de auditoría: José Joaquín Arias Gómez-Calcerrada.
- Responsable de seguridad física: Manuel Díaz Gil.
- Responsable de la sala de comunicaciones: Jesús Rosa Bilbao.

ANEXO III
AUTORIZACIONES DE SALIDA O RECUPERACIÓN DE DATOS

A la hora de trasladar los documentos procedentes del Área Médica, estos deberán ser autorizados tanto por el personal responsable de seguridad como por los hospitales o centros médicos que hayan emitido esos activos, dado que es su propia información.

Para trasladar esa información se hará uso del transporte especificado en el apartado Gestión de soportes y documentos.

ANEXO IV
DELEGACIÓN DE AUTORIZACIONES

En su caso, las personas en las que el responsable del fichero ha delegado serán previamente constatadas. Para el resto del personal, podrán realizarse sustituciones a nivel interno siempre que pertenezcan al mismo departamento.

ANEXO V
INVENTARIO DE SOPORTES

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenados en las dependencias de cada departamento, constituyendo un lugar de acceso restringido al que solo tendrán acceso las personas con autorización.

Para cada soporte de información se habilitará un armario en cada oficina principal de cada dependencia. Así, cada personal tendrá acceso únicamente a los soportes relacionados con su actividad dentro de la asociación.

En cuanto a las copias de seguridad que se almacenan en soportes físicos, tendrán la siguiente nomenclatura: Código del departamento al que

pertenece, letra en función del tipo de soporte (U para memoria USB, C para CD o DVD, HD para disco duro, S para las tarjetas SD y P para los soportes físicos en papel), fecha de la copia de seguridad (dd/mm/aaaa) y nivel de sensibilidad de la información (desde A hasta C).

ANEXO VI
REGISTRO DE INCIDENCIAS

Todas las incidencias quedarán recogidas tal y como se especifica en el apartado "Procedimientos de notificación, gestión y respuestas ante las incidencias" (Punto 4) directamente de forma informática, siendo almacenadas en los servidores de la asociación.

ANEXO VII
ENCARGADOS DE TRATAMIENTO

Si terceras personas desean acceder o tratar datos de los ficheros, estas deberán seguir las instrucciones impuestas por el responsable de fichero y encargado de tratamiento.

Las terceras personas con acceso a dichos datos de ficheros deberán mantener la confidencialidad de ellos y usarlos únicamente con los fines permitidos.

ANEXO VIII
REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

Toda salida de soportes indicados en el Anexo V deberá ser registrada en el sistema informático con una serie de datos. Estos son: hora de salida, hora de llegada, datos almacenados, destinatario, medio de transporte, emisor y firma del responsable del fichero. El tiempo establecido debe cumplirse.

ANEXO IX
MEDIDAS ALTERNATIVAS

Dado que en todos los ficheros es posible adoptar las medidas exigidas por el RLOPD en relación con la identificación de los soporte, los dispositivos de almacenamiento de los documentos o los sistemas de almacenamiento de la información, no se consideran medidas alternativas.