AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

GUÍA de Seguridad de Datos

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 *<nombre del responsable>*, 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:

<incluir relación de ficheros o tratamientos afectados, indicando si se trata de sistemas automatizados, manuales o mixtos, y el nivel de seguridad que les corresponde>

.....

.....

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

<Especificar las normativas de identificación y autenticación de los usuarios con acceso a los datos personales. La identificación de los usuarios se deberá realizar de forma inequívoca y personalizada, verificando su autorización (cada identificación debe pertenecer a un único usuario)>.

<Si la autenticación se realiza mediante contraseñas, detallar el procedimiento de asignación, distribución y almacenamiento que deberá garantizar su confidencialidad e integridad, e indicar la periodicidad con la que se deberán cambiar, en ningún caso superior a un año>

<También es conveniente incluir los requisitos que deben cumplir las cadenas utilizadas como contraseña>.

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 *<incluir estos mecanismos>*.

Exclusivamente el *<persona autorizada (o denominación de su puesto de*

trabajo) para conceder, alterar o anular el acceso autorizado> 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 <*nota: si la persona es diferente en función del fichero, incluir el párrafo en la parte del Anexo I correspondiente*>.

<*Especificar los procedimientos para solicitar el alta, modificación y baja de las autorizaciones de acceso a los datos, indicando qué persona (o puesto de trabajo) concreta tiene que realizar cada paso*.>

<*Incluir y detallar los controles de acceso a los sistemas de información*>

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 <*Especificar procedimiento de actualización*>.

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.

<*Indicar, si se estima oportuno, información relativa al sistema de registro de accesos. El mecanismo que permita este registro estará bajo control directo del responsable de seguridad, sin que se deba permitir, en ningún caso, la desactivación del mismo*>.

Los datos del registro de accesos se conservaran durante <*especificar periodo, que deberá ser al menos de dos años. No es preciso que estos datos*

se almacenen "on-line">.

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 <*indicar los documentos o tipos de documentos que puedan ser utilizados por múltiples usuarios, así como el mecanismo establecido para controlar estos accesos*>.

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*>.

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: *<indicar el procedimiento por el cual se informará a cada persona, en función de su perfil, de las normas que debe cumplir y de las consecuencias de no hacerlo. Puede ser conveniente incluir algún sistema de acuse de recibo de la información>*.

<Si se estima oportuna, la remisión periódica de información sobre seguridad: circulares, recordatorios, nuevas normas, indicar aquí el procedimiento y las personas autorizadas para hacerlo>.

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 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."

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 *<incluir un punto con las obligaciones detalladas de los perfiles que afectan a todos los ficheros, como por ejemplo, administradores de los sistemas, responsables de informática, responsable/s*

de seguridad si existe/n, responsables de seguridad física, etc. Es importante que se concrete la persona o cargo que corresponde a cada perfil. También deben contemplarse los procedimientos de actuación o delegación de funciones para casos de ausencia. Este apartado se propone principalmente como un recopilatorio que agrupe las medidas que en el resto del Documento se asignan a perfiles concretos>.

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 <*indicar usuarios, o perfiles y autorizaciones que el responsable del fichero delega en ellos para su ejercicio*>.

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 <*indicar la normativa sancionadora aplicable*>.

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 *<denominación del responsable del fichero>*.

El procedimiento a seguir para la notificación de incidencias será *<especificar concretamente los procedimientos de notificación y gestión de incidencias, indicando quien tiene que notificar la incidencia, a quien y de que modo, así como quien gestionará la incidencia>*.

El registro de incidencias se gestionará mediante *<indicar la forma en que se almacenará el registro, que puede ser manual o informático, y en el que deberán constar, al menos, el tipo de incidencia, el momento en que se ha producido o en su caso detectado, la persona que realiza la notificación, a quién se comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas. En caso de gestión automatizada se indicará en este punto el sistema informático utilizado>*.

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 *<detallar el procedimiento para registrar las recuperaciones de datos, que deberá incluir 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. En caso de gestión automatizada, se deberá prever la existencia de un código específico para recuperaciones de datos, en la información relativa al tipo de incidencia>*.

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.

<Especificar los procedimientos previstos para la modificación del documento de seguridad, con especificación concreta de las personas que pueden o deben proponerlos y aprobarlos, así como para la comunicación de las modificaciones al personal que pueda verse afectado>.

NIVEL MEDIO: AUDITORÍA

<Indicar los procedimientos para realizar la auditoría interna o externa que verifique 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 respectivamente, y que debe realizarse al menos cada dos años.

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

auditorÍa inicia el cómputo de dos años señalado.

El informe analizará la adecuación de las medidas y controles a 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

<*Indicar los procedimientos para realizar el informe mensual sobre el registro de accesos a los datos de nivel alto regulado por el artículo 103 del RLOPD*>.

ANEXO I
DESCRIPCIÓN DE FICHEROS

Actualizado a: <*fecha de la última actualización del anexo*>.

<*Se incluirá un anexo de este tipo por cada fichero incluido en el ámbito del documento de seguridad, podrían denominarse ANEXO I a, b, c, etc.*>.

- Nombre del fichero o tratamiento: <*rellenar con nombre del fichero*>.

- Unidad/es con acceso al fichero o tratamiento: <*especificar departamento unidad con acceso al fichero, si aporta alguna información*>.

- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos: <*rellenar los siguientes campos con los datos relativos a la inscripción del fichero en el Registro General de Protección de Datos (RPGD)*>.

    - Identificador: <*código de inscripción*>
    - Nombre: <*nombre inscrito*>
    - Descripción: <*descripción inscrita*>

- Nivel de medidas de seguridad a adoptar: <*básico, medio o alto*>.

NIVEL MEDIO: RESPONSABLE DE SEGURIDAD

<*Persona designada por el responsable del fichero al objeto de coordinar y controlar las medidas incluidas en este documento para este fichero, en el caso de que existan varios, o para todos los ficheros en el supuesto de que se trate de designación única*>.

- Administrador: <*persona designada para conceder, alterar, o anular el acceso autorizado a los datos*>.

- Leyes o regulaciones aplicables que afectan al fichero o tratamiento <*si existen*>.

- Código Tipo Aplicable: <*se indicará aquí si el fichero está incluido en el ámbito de alguno de los códigos tipo regulados por el articulo 32 de la LOPD*>.

- Estructura del fichero principal: <*incluir los tipos de datos personales contenidos en el fichero, especificando aquellos que, por su naturaleza, afectan al nivel de medidas de seguridad a adoptar, según lo indicado en el artículo 81 del Reglamento de desarrollo de la LOPD* >.

- Información sobre el fichero o tratamiento

    - Finalidad y usos previstos.

    - Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales, y procedencia de los datos: <*indicar procedencia de los datos, quién suministra los datos*>.

    - Procedimiento de recogida: <*encuestas, formularios en papel, Internet. ..*>.

    - Cesiones previstas: <*relacionar los destinatarios de los datos previstos*>.

    - Transferencias Internacionales: <*relacionar las transferencias internacionales, especificando si ha sido necesaria la autorización del Director de la Agencia*

Española de Protección de Datos>.

- Sistema de tratamiento: <*automatizado, manual o mixto*>.

- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: <*indicar la unidad y/o dirección. Deben preverse además, los procedimientos internos para responder a las solicitudes de ejercicio de derechos de los interesados*>.

- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación <*Especificar la periodicidad de las copias (que debe ser al menos semanal). Si se trata de ficheros manuales y tienen prevista alguna medida en este sentido, detallarla*>.

- Información sobre conexión con otros sistemas: <*Describir las posibles relaciones con otros ficheros del mismo responsable*>.

- Funciones del personal con acceso a los datos personales: <*Especificar las diferentes funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y sistema de información específicos de este fichero*>.

- Descripción de los procedimientos de control de acceso e identificación: <*Cuando sean específicos para el fichero*>.

- Relación actualizada de usuarios con acceso autorizado: <*Relacionar todos los usuarios que acceden al fichero, con especificación del tipo o grupo de usuarios al que pertenecen, su clave de identificación, nombre y apellidos, unidad, fecha de alta y fecha de baja*>.

<*Si la relación se mantiene de forma informatizada, indicar aquí cual es el sistema utilizado y la forma de obtener el listado. No obstante, siempre que*

sea posible, es conveniente imprimir la relación de usuarios y adjuntarla periódicamente a este Anexo>.

ANEXO II
NOMBRAMIENTOS

<*Adjuntar original o copia de los nombramientos que afecten a los diferentes perfiles incluidos en este documento, como el del responsable de seguridad*>.

ANEXO III
AUTORIZACIONES DE SALIDA O RECUPERACIÓN DE DATOS

<*Adjuntar las autorizaciones que el responsable del fichero ha firmado para la salida de soportes que contengan datos de carácter personal, incluyendo aquellas que se refieran a salidas que tengan un carácter periódico o planificado. Incluir asimismo, las autorizaciones relativas a la ejecución de los procedimientos de recuperación de datos*>.

ANEXO IV
DELEGACIÓN DE AUTORIZACIONES

En su caso, personas en las que el responsable del fichero ha delegado <*Indicar las autorizaciones, tales como: salida de dispositivos portátiles, la copia o reproducción de documentos en soporte papel,…*>.

ANEXO V
INVENTARIO DE SOPORTES

<*Si el inventario de soportes no está informatizado, recoger en este anexo la información al efecto, según lo indicado en el apartado de "Gestión de soportes y Documentos" de este documento. Los soportes deberán permitir identificar el tipo de información, que contienen, ser inventariados y*

almacenarse en un lugar con acceso restringido al personal autorizado para ello en este documento>.

<Si el inventario de soportes está informatizado, indicar la aplicación o ruta de acceso del archivo que lo contiene>.

ANEXO VI
REGISTRO DE INCIDENCIAS

<Si el registro de incidencias no está informatizado, recoger en este anexo la información al efecto, según lo indicado en el apartado de "Procedimientos de notificación, gestión y respuesta ante las incidencias" de este documento>.

<Si el registro de incidencias está informatizado, indicar la aplicación o ruta de acceso del acceso del archivo de lo contiene>.

ANEXO VII
ENCARGADOS DE TRATAMIENTO

<Cuando el acceso de un tercero a los datos del responsable del fichero sea necesario para la prestación de un servicio a este último, no se considera que exista comunicación de datos. Recoger aquí el contrato que deberá constar por escrito o de alguna otra forma que permita acreditar su celebración y contenido, y que establecerá expresamente que el encargado de tratamiento tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, y que no los comunicarán, ni siquiera para su conservación a otras personas.

El contrato estipulará las medidas de seguridad a que se refiere el artículo 9 de la LOPD que el encargado del tratamiento está obligado a implementar>.

ANEXO VIII
REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

<Si el registro de entrada y salida de soportes al que se refiere el apartado de "Gestión de soportes y documentos", y que es obligatorio a partir del nivel medio, no está informatizado, recoger en este anexo la información al efecto, según lo indicado el artículo 97 del RLOPD>.

<Si el registro de entrada y salida está informatizado, indicar la aplicación o ruta de acceso del acceso del archivo de lo contiene>.

ANEXO IX
MEDIDAS ALTERNATIVAS

<En el caso de que no sea posible adoptar las medidas exigidas por el RLOPD en relación con la identificación de los soportes, los dispositivos de almacenamiento de los documentos o los sistemas de almacenamiento de la información, indicar las causas que justifican que ello no sea posible y las medias alternativas que se han adoptado>.