AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

GUÍA DE SEGURIDAD

ABRIL 2008

INDICE

I 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 Título VIII del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre (BOE 17, de 19 de enero de 2008) (RLOPD) desarrolla las medidas de seguridad en el tratamiento de datos de carácter personal. El citado Título 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.

Con el objeto de facilitar a los responsables de ficheros y a los encargados de tratamientos de datos personales la adopción de las disposiciones del RLOPD, la Agencia Española de Protección de Datos pone a su disposición este documento, en el que se recopila un cuadro resumen de las medidas de seguridad recogidas en el citado Titulo VIII, un modelo de "Documento de Seguridad", que pretende servir de guía y facilitar el desarrollo y cumplimiento de la normativa sobre protección de datos, y por último, un vademecum de comprobaciones con el objeto de facilitar la realización de la auditoria de seguridad que exige el artículo ...

AVISO IMPORTANTE:

Debe entenderse, en cualquier caso, que siempre habrá que atenerse a lo dispuesto en la LOPD, en el RLOPD, y en el resto de previsiones relativas a la protección de datos de carácter personal, y que la utilización de este modelo como guía de ayuda para desarrollar un "Documento de Seguridad" debe, en todo caso, tener en cuenta los aspectos y circunstancias aplicables en cada caso concreto, sin prejuzgar el criterio de la Agencia Española de Protección de Datos en el ejercicio de sus funciones.

I LAS MEDIDAS DE SEGURIDAD

1. APLICACIÓN DE NIVELES

Nivel alto. Ficheros o tratamientos con datos:

- de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico;
- recabados con fines policiales sin consentimiento de las personas afectadas; y
- derivados de actos de violencia de género.

Nivel medio. Ficheros o tratamientos con datos:

- relativos a la comisión de infracciones administrativas o penales;
- que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito);
- de Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias;
- de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros;
- de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias;
- de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social;
- que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas; y
- de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización [1]

Nivel básico. Cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros;
- se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero; y

[1] Para esta categoría de ficheros además deberá disponerse de un registro de accesos

- en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

2. MEDIDAS A APLICAR

A. EL DOCUMENTO DE SEGURIDAD

El documento de seguridad es un documento interno de la organización, que debe mantenerse siempre actualizado. Disponer del documento de seguridad es una obligación para todos los responsables de ficheros y, en su caso, para los encargados del tratamiento, con independencia del nivel de seguridad que sea necesario aplicar.

Los apartados mínimos que debe incluir el documento de seguridad son los siguientes:

- Ámbito de aplicación: especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares de seguridad.
- Funciones y obligaciones del personal.
- Estructura y descripción de los ficheros y sistemas de información.
- Procedimiento de notificación, gestión y respuesta ante incidencias.
- Procedimiento de copias de respaldo y recuperación de datos.
- Medidas adoptadas en el transporte, destrucción y/o reutilización de soportes y documentos.

A partir del nivel medio de medidas de seguridad, además de los apartados anteriores, deberán incluirse los siguientes:

- Identificación del responsable de seguridad
- Control periódico del cumplimiento del documento

En caso de haber contratado la prestación de servicios por terceros para determinados ficheros, en el documento de seguridad se debe hacer constar esta circunstancia, indicando una referencia al contrato y su vigencia así como los ficheros objeto de este tratamiento.
Si se ha contratado la prestación de servicios en relación con la totalidad de los ficheros y tratamientos de datos del responsable, y dichos servicios se prestan en las instalaciones del encargado del tratamiento se podrá delegar en éste la llevanza del documento de seguridad.

En el capítulo III se encuentra la guía modelo que facilita la elaboración de este documento de seguridad.

B. CUADRO RESUMEN

	NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO
RESPON-SABLE SEGURIDAD		-El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad). - El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento.	
PERSONAL	- Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas. - Definición de las funciones de control y las autorizaciones delegadas por el responsable - Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento.		
INCIDENCIAS	- Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras - Procedimiento de notificación y gestión de las incidencias.	**SOLO FICHEROS AUTOMATIZADOS** - Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente. - Autorización del responsable del fichero para la recuperación de datos.	
CONTROL DE ACCESO	- Relación actualizada de usuarios y accesos autorizados. - Control de accesos permitidos a cada usuario según las funciones asignadas. - Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. - Concesión de permisos de acceso sólo por personal autorizado. - Mismas condiciones para personal ajeno con acceso a los recursos de datos.	**SOLO FICHEROS AUTOMATIZADOS** - Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.	**SOLO FICHEROS AUTOMATIZADOS** - Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado. - Revisión mensual del registro por el responsable de seguridad - Conservación 2 años. - No es necesario este registro si el responsable del fichero es una persona física y es el único usuario **SOLO FICHEROS NO AUTOMATIZADOS** - Control de accesos autorizados - Identificación accesos para documentos accesibles por múltiples usuarios
IDENTIFICACIÓN Y AUTENTICACIÓN	**SOLO FICHEROS AUTOMATIZADOS** -Identificación y autenticación personalizada - Procedimiento de asignación y distribución de contraseñas - Almacenamiento ininteligible de las contraseñas - Periodicidad del cambio de contraseñas (>1 año)	**SOLO FICHEROS AUTOMATIZADOS** - Limite de intentos reiterados de acceso no autorizado	

	NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO
GESTIÓN DE SOPORTES	- Inventario de soportes - Identificación del tipo de información que contienen, o sistema de etiquetado - Acceso restringido al lugar de almacenamiento - Autorización de las salidas de soportes (incluidas a través de e-mail) - Medidas para el transporte y el desecho de soportes	**SOLO FICHEROS AUTOMATIZADOS** - Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizada para recepción/entrega.	**SOLO FICHEROS AUTOMATIZADOS** - Sistema de etiquetado confidencial - Cifrado de datos en la distribución de soportes. - Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas)
COPIAS DE RESPALDO	**SOLO FICHEROS AUTOMATIZADOS** - Copia de respaldo semanal - Procedimientos de generación de copias de respaldo y recuperación de datos. - Verificación semestral de los procedimientos. - Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita. - Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente.		**SOLO FICHEROS AUTOMATIZADOS** - Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
CRITERIOS DE ARCHIVO	**SOLO FICHEROS NO AUTOMATIZADOS** - El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos ARCO		
ALMACENA-MIENTO	**SOLO FICHEROS NO AUTOMATIZADOS** - Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura		**SOLO FICHEROS NO AUTOMATIZADOS** - Armarios, archivadores, … de documentos en áreas con acceso protegido con puertas con llave.
CUSTODIA SOPORTES	**SOLO FICHEROS NO AUTOMATIZADOS** - Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados		
COPIA O REPRO-DUCCIÓN			**SOLO FICHEROS NO AUTOMATIZADOS** - Sólo puede realizarse por los usuarios autorizados - Destrucción de copias desechadas

	NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO
AUDITORIA		- Al menos cada dos años, interna o externa. - Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad. - Verificación y control de la adecuación de las medidas. - Informe de detección de deficiencias y propuestas correctoras. - Análisis del responsable de seguridad y conclusiones al responsable del fichero	
TELECOMUNICACIONES			**SOLO FICHEROS AUTOMATIZADOS** - Transmisión de datos a través de redes electrónicas cifrada.
TRASLADO DOCUMENTACIÓN			**SOLO FICHEROS NO AUTOMATIZADOS** - Medidas que impidan el acceso o manipulación

- Los accesos a través de redes de telecomunicaciones deben garantizar un nivel de seguridad equivalente al de los accesos en modo local.
- La ejecución de trabajos fuera de los locales del responsable o del encargado del tratamiento debe ser previamente autorizada por el responsable del fichero, constando en el documento de seguridad, y garantizar el nivel de seguridad.
- Los ficheros temporales deberán cumplir el nivel de seguridad correspondiente y serán borrados una vez que hayan dejado de ser necesarios.
- Acceso facilitado a un encargado del tratamiento deberá constar en el documento de seguridad y deberá comprometerse al cumplimiento de las medidas de seguridad previstas.

III. GUÍA MODELO DEL DOCUMENTO DE SEGURIDAD

1. ORGANIZACIÓN DE LA GUÍA

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 ha 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.

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

M: 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 correspondiente.

NOTA ACLARATORIA: *Las medidas de seguridad de nivel básico son exigibles en todos los casos. Las medidas de nivel medio complementan a las anteriores en el caso de ficheros clasificados en este nivel, y las de nivel alto, cuando deban adoptarse, incluyen también las de nivel básico y medio.*

2. 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 organizativas 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 principal de este Documento queda estructurado como sigue:

1. Ámbito de aplicación del documento.
2. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.
3. Procedimiento general de información al personal.
4. Funciones y obligaciones del personal.
5. Procedimiento de notificación, gestión y respuestas ante las incidencias.
6. Procedimientos de revisión.
7. Consecuencias del incumplimiento del Documento de Seguridad.

Anexo I. Aspectos específicos relativos a los diferentes ficheros.

A Aspectos relativos al fichero <nombre del fichero a>

B Aspectos relativos al fichero <nombre del fichero b>

Anexo II Nombramientos

Anexo III Autorizaciones firmadas para la salida o recuperación de datos

Anexo IV Inventario de soportes <si se gestiona en papel>

Anexo V Registro de Incidencias <si se gestiona en papel>

Anexo VI Contratos o cláusulas de encargados de tratamiento <si existen, de acuerdo con lo indicado en el artículo 12 de la LOPD>.

Anexo VII Registro de entrada y salida de soportes

Este Documento deberá mantenerse permanente actualizado. Cualquier modificación relevante 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.

A. 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.

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

Nivel alto: Se aplicarán a los ficheros o tratamientos de datos:

- de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico;
- recabados con fines policiales sin consentimiento de las personas afectadas; y
- derivados de actos de violencia de género.

Nivel medio: Se aplicarán a los ficheros o tratamientos de datos:

- relativos a la comisión de infracciones administrativas o penales;
- que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito);
- de Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias;
- de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros;
- de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias;
- de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social;

- que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas;; y
- de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización.[2]

Nivel básico: Se aplicarán a cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros;
- se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero; y
- en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

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] Para esta categoría de ficheros además deberá disponerse de un registro de accesos.

B. 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 a acceder a los datos personales.

A

⇒ <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 >

A

NIVEL MEDIO En los ficheros <indicar los nombres de 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 autorizado 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 que 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 se actualizará <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.

A

NIVEL MEDIO: **Control de acceso físico**

Exclusivamente el personal que se indica a continuación, podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información correspondientes a <indicar los nombres de los ficheros de nivel medio y alto>.

NIVEL ALTO: **Registro de accesos**

A

En los accesos a los datos de los ficheros de nivel alto, < indicar los nombres 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 VI 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.

M

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; igualmente se definirá en este punto un registro de accesos general>.

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> cumplirán con 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 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 dificultan 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 <indicar medidas y procedimientos previstos> para evitar la sustracción, pérdida o acceso indebido a la información.

NIVEL MEDIO : **Registro de Entrada y Salida de Soportes**

Las salidas y entradas de soportes correspondientes a los ficheros <indicar los nombres de los ficheros de nivel medio y alto>, deberán ser 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>.

NIVEL ALTO : **Gestión y distribución de soportes**

Los soportes relacionados <indicar aquellos de nivel alto> serán identificados 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 <indicar los nombres 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>, serán utilizados 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>

M

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 deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación>

M

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> serán utilizados 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>.

M

Custodia de soportes

En tanto los documentos con datos personales no se encuentre archivada en los dispositivos de almacenamientos indicados en el punto anterior, por estar en proceso de tramitación, las personas que se encuentren al cargo de los mismos deberán custodiarlos e impedir en todo momento que pueda ser accedida por 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, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. Relacionar los accesos previstos y los ficheros a que se prevea acceder>.

A

NIVEL ALTO: Los datos personales correspondientes a los ficheros <relacionar los 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 podría ser 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 de este responsable del fichero <indicar en su caso, los distintos locales a los que se deban circunscribir dichos tratamientos, especialmente en el supuesto de que se produzcan 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 habría que indicar o para un perfil de usuarios.>

<Se debe garantizar el nivel de seguridad correspondiente al fichero tratado en dichos tratamientos.>

M

Traslado de documentación

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

Ficheros temporales

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.

M

Copia o reproducción

La realización de copias o reproducción de los documentos con datos personales sólo se podrán realizar bajo el control del siguiente personal autorizado <indicar los usuarios o perfil de los mismos habilitados para ello>

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

A

Copias de seguridad

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. Únicamente respecto 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 personales 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 <indicar 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/os 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 Reglamento de desarrollo de la LOPD.

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.

C. PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información están definidas de forma general en el Capítulo siguiente y de forma específica para cada fichero en la parte del Anexo I correspondiente.

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>

D. FUNCIONES Y OBLIGACIONES DEL PERSONAL

Funciones y obligaciones de carácter general.

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 su Capítulo V.

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>

E. PROCEDIMIENTO 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 y 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>.

NIVEL MEDIO: En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten a los ficheros <relacionar 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 por parte del responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

F. PROCEDIMIENTOS DE REVISIÓN

Revisión del documento de seguridad

< 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.
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>

NIVEL MEDIO: Auditoria

< Indicar los procedimientos para realizar la auditoria 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.

A

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 auditoria 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 auditoria 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>

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 24 del RLOPD>.

G. 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>

ANEXO I. DESCRIPCIÓN DE FICHEROS.

A. ASPECTOS RELATIVOS AL FICHERO …

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 o 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 esta 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 incluidos, con especificación de los que, por su naturaleza, afectan a la diferente calificación del 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:
    - Cesiones previstas:
    - Transferencias Internacionales: <relacionar las transferencias internacionales, especificando si ha sido necesaria la autorización del Director de la Agencia Española de Protección de Datos>
    - Procedencia de los datos: <indicar quien suministra los datos>
    - Procedimiento de recogida: <encuestas, formularios en papel, Internet, ...>
    - 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>.

- Terceros que acceden a los datos para la prestación de un servicio: <Relacionar las empresas de mantenimiento, de servicios, etc., que tienen acceso a los datos. Cuando sea necesario realizar un contrato escrito según lo

dispuesto en el artículo 12 de la LOPD, se incluirá una copia del mismo o de las cláusulas al efecto en el Anexo VI del documento>.

- Relación de actualizaciones de este Anexo: <incluyendo fecha, resumen de aspectos modificados y motivo>

B. ASPECTOS RELATIVOS AL FICHERO ...

……

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 original o copia de las autorizaciones que el responsable del fichero ha firmado para la salida de soportes que contengan datos de carácter personal, así como aquellas relativas a la ejecución de los procedimientos de recuperación de datos >

ANEXO IV INVENTARIO DE SOPORTES

<Si el inventario de soportes se gestiona de forma no automatizada recoger en este anexo la información al efecto, según lo indicado en el Capítulo II, punto “Gestión de soportes” 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 >

ANEXO V REGISTRO DE INCIDENCIAS

<SI EL REGISTRO DE INCIDENCIAS SE GESTIONA DE FORMA NO AUTOMATIZADA, RECOGER EN ESTE ANEXO LA INFORMACIÓN AL EFECTO, SEGÚN LO INDICADO EN EL CAPÍTULO V, "PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS" DE ESTE DOCUMENTO>

ANEXO VI 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 utilizara con fin distinto al que figure en dicho contrato, ni 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 esta obligado a implementar>

ANEXO VII REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

<Si el registro de entrada y salida de soportes al que se refiere el Capítulo II, punto "Gestión de soportes", y que es obligatorio a partir del nivel medio, se gestiona de forma no automatizada, recoger en este anexo la información al efecto, según lo indicado el artículo 97 del Reglamento de desarrollo de la LOPD.>

IV. RELACIÓN DE COMPROBACIONES PARA LA REALIZACIÓN DE LA AUDITORÍA DE SEGURIDAD

1. OBJETIVO

Determinar si se han establecido, si son adecuadas y si se cumplen las medidas de seguridad recogidas en el Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Su realización es obligatoria para ficheros de nivel medio y alto. Puede ser interna o externa. Debe realizarse al menos cada dos años. Excepcionalmente, si se han realizado modificaciones sustanciales en el sistema de información, deberá realizarse una auditoría para comprobar la adecuación, adaptación y eficacia de las medidas de seguridad. Esta auditoría iniciará el cómputo de dos años.

2. DETERMINACIÓN DEL ALCANCE DE LA AUDITORIA

Se debe establecer cuáles son los ficheros con datos de carácter personal objeto de la auditoría, tratamientos sobre los mismos, sistemas de tratamiento, procedimientos, etc.

3. PLANIFICACIÓN

Determinar los recursos necesarios para llevar a cabo la auditoría, las fuentes de información, la ubicación del fichero o las instalaciones, etc.

4. RECOLECCIÓN DE DATOS

- Relación de ficheros, estructura y contenido.
- Políticas de seguridad y procedimientos (registro de incidencias, copias de respaldo y recuperación, Identificación y autorización, borrado de soportes, cifrado, etc.).
- Documento de Seguridad y auditorías anteriores (si las hubiese).
- Diseño físico y lógico de los sistemas de información.
- Relación de usuarios, accesos autorizados y sus funciones.
- Inventario de soportes y registro de entrada y salida de soportes.
- Registros de acceso e informes de revisión de los mismos.
- Entrevistas a usuarios, técnicos de sistemas, responsables, etc.
- Inspección visual
- Etc.

5. EVALUACIÓN DE LAS PRUEBAS

Se relacionan a continuación algunas comprobaciones que se pueden realizar para verificar el cumplimiento de las disposiciones del Reglamento:

Sistema tratamiento	Comprobaciones a realizar	Nivel
	Aspectos Generales	
Todos	¿La clasificación del nivel de seguridad es adecuada respecto a la naturaleza de la información contenida en cada uno de los ficheros y su finalidad?	
	¿Se han creado, modificado o suprimido ficheros con datos de carácter personal desde la última auditoría?	
	ENCARGADO DE TRATAMIENTO	
Todos	¿Se realiza el tratamiento por persona distinta al responsable del fichero? ¿Se ha formalizado mediante contrato conforme lo establecido el artículo 12 de la LOPD?	
	Si la realización de este encargo se realiza en los locales del responsable ¿se ha hecho constar esta circunstancia en el Documento de Seguridad? ¿Consta por escrito en el contrato el compromiso del personal del encargado de tratamiento respecto al cumplimiento de las medidas de seguridad recogidas en el Documento de Seguridad del responsable?	
	Cuando el tratamiento se realiza mediante acceso remoto a los sistemas del responsable ¿se le ha prohibido al encargado de tratamiento la incorporación de los datos a sistemas o soportes distintos de los del responsable? ¿Se ha hecho constar tal circunstancia en el Documento de Seguridad del responsable?	
	Si la prestación se hace en locales propios del encargado de tratamiento (distintos de los del responsable) ¿ha elaborado el encargado el documento de seguridad? ¿Identifica el fichero o tratamiento y el responsable del mismo? ¿Detalla las medidas de seguridad a implementar en relación con su tratamiento?	
	PRESTACIÓN DE SERVICIO SIN ACCESO A DATOS PERSONALES	
Todos	Si el tratamiento no afecta a datos personales ¿se han adoptado las medidas necesarias para limitar el acceso del personal a los datos personales, soportes y recursos?	
	Si se trata de personal ajeno ¿recoge el contrato la prohibición expresa de acceder a los datos personales, así como la obligación de secreto respecto a los datos que hubieran podido conocer con motivo de la prestación de servicio?	
	DELEGACIÓN DE AUTORIZACIONES	
Todos	¿Se han delegado las autorizaciones que el Reglamento atribuye al responsable en otras personas? ¿Se ha hecho constar en el Documento de Seguridad las personas habilitadas para otorgar estas autorizaciones y las personas en quienes recae dicha delegación?	
	ACCESO A DATOS A TRAVÉS DE REDES	
Todos	¿Los accesos a datos mediante redes de comunicaciones garantizan un nivel de seguridad equivalente a los accesos en modo local?	
	RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO	
Todos	El almacenamiento de datos personales en dispositivos portátiles o los tratamientos fuera de los locales del responsable o del encargado ¿han sido autorizados expresamente por el responsable del fichero? ¿Consta dicha autorización en el Documento de Seguridad?	
	¿Se garantiza el nivel de seguridad correspondiente al tipo de fichero tratado?	
	FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS	
Todos	¿Cumplen el nivel de seguridad correspondiente?	
	¿Se han destruido o borrado cuando ya no han sido necesarios para los fines que motivaron su creación?	

Sistema tratamiento	Comprobaciones a realizar	Nivel
	DOCUMENTO DE SEGURIDAD	
Todos	¿Ha elaborado el responsable del fichero el Documento de Seguridad?	Básico
	¿Contiene los aspectos mínimos exigidos por el Reglamento?	
	¿Está el documento actualizado? ¿Se ha revisado cuando se han producido cambios relevantes desde la auditoria anterior?	
	¿Está su contenido adecuado a la normativa vigente en este momento en materia de seguridad de los datos de carácter personal?	
	¿Se ha indicado con qué periodicidad se deben cambiar las contraseñas?¿Es inferior o igual a un año?	
	¿Se especifica cuál es el personal autorizado para la concesión, alteración o anulación de accesos autorizados sobre datos o recursos?	
	¿Se especifica cuál es el personal autorizado para acceder a los lugares donde se almacenan los soportes informáticos?	
	Si el tratamiento se realiza por cuenta de terceros ¿se han reflejado los ficheros afectados por el encargo, con referencia expresa al contrato, así como la identificación del responsable y el periodo de vigencia?	
	¿Se ha reflejado en el Documento de Seguridad si los datos personales se incorporan y tratan exclusivamente en los sistemas del encargado?	
	¿Se ha delegado en el encargado del tratamiento la llevanza del Documento de Seguridad para los ficheros objeto del contrato? ¿Se ha reflejado esta circunstancia en el contrato?	
	¿Establece la identidad del responsable o responsables de seguridad? ¿Se especifica si la designación es única para todos los ficheros o está diferenciada según el sistema de tratamiento utilizado?	Medio
	¿Contiene los procedimientos y controles periódicos a realizar para verificar el cumplimento de lo dispuesto en el propio documento?	
	¿Especifica qué medidas hay que adoptar en caso de desechado o reutilización de soportes?	
	¿Relaciona las personas que están autorizadas a acceder físicamente a los locales donde se ubican los sistemas de información?	
	FUNCIONES Y OBLIGACIONES	
Todos	¿Están las funciones y obligaciones del personal con acceso a datos de carácter personal y los sistemas de información claramente definidos?	Básico
	¿Están documentadas y reflejadas en el documento de seguridad?	
	¿Se han definido las funciones de control o autorizaciones delegadas por el responsable del fichero?	
	¿Conoce el personal las medidas de seguridad que afectan al desarrollo de sus funciones?	
	¿Conoce las consecuencias de su incumplimiento?	
	REGISTRO DE INCIDENCIAS	
Todos	¿Existe un procedimiento de notificación y gestión de incidencias de seguridad? ¿El procedimiento está bien diseñado y es eficaz? ¿Conoce todo el personal afectado dicho procedimiento?	Básico
	¿Existe un registro de incidencias donde se reflejen todos los datos exigidos en el Reglamento? ¿Se han registrado todas las incidencias ocurridas?	
	¿Se revisa periódicamente el registro de incidencias para su análisis y adopción de medidas correctoras de las incidencias anotadas?	
Automatizado	¿Se han anotado las ejecuciones de los procedimientos de recuperación de datos realizados?	Medio
	¿Figuran en estas anotaciones los datos exigidos por el Reglamento?	
	¿Existe la autorización por escrito del responsable del fichero?	

Sistema tratamiento	Comprobaciones a realizar	Nivel
	CONTROL DE ACCESO	
Todos	¿Los accesos autorizados de los usuarios se corresponden exclusivamente a los datos y recursos que precisan para el desarrollo de sus funciones?	Básico
	¿Existen mecanismos que impidan que los usuarios accedan a datos o recursos distintos de los autorizados?	
	¿Existe una relación de usuarios? ¿Especifica qué datos y recursos tiene autorizados para cada uno de ellos? ¿Está actualizada?	
	¿La concesión, alteración o anulación de accesos autorizados sobre datos y recursos la realiza exclusivamente el personal autorizado para ello en el Documento de Seguridad?	
	¿Ha establecido el responsable del fichero los criterios conforme a los cuales se otorga la autorización de los accesos a los datos y a los recursos?	
	El personal ajeno al responsable que tiene acceso a los datos y recursos de éste ¿se encuentra sometido a las mismas condiciones y obligaciones que el personal propio?	
Automatizado	¿El acceso a los locales donde se encuentran ubicados los sistemas de información se realiza exclusivamente por el personal autorizado en el Documento de Seguridad?	Medio
No Automatizado	¿Se encuentran los archivadores u otros elementos de almacenamiento en áreas de acceso restringido dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente? ¿Están cerradas estas áreas mientras no sea preciso el acceso a los documentos incluidos en el fichero?	Alto
	Si los locales del responsable no permiten disponer de un área de acceso restringido ¿ha adoptado el responsable medidas alternativas? ¿Se ha hecho constar esta circunstancia en el Documento de Seguridad? ¿Se ha motivado adecuadamente?	
	GESTIÓN DE SOPORTES Y DOCUMENTOS	
Todos	¿Está identificado el tipo de información contenido en el soporte o documento?	Básico
	¿Existe y se mantiene un inventario de soportes?	
	¿Se almacenan los soportes o documentos en lugares de acceso restringido?	
	¿Existen mecanismos por los que solamente puedan acceder las personas autorizadas en el Documento de Seguridad? ¿Son funcionan adecuadamente estos mecanismos?	
	¿Se ha dejado constancia en el Documento de Seguridad, si fuera el caso, de la imposibilidad de cumplir con las obligaciones establecidas en el Reglamente sobre identificación, inventariado y acceso a los soportes dadas sus características físicas?	
	¿La salida de soportes y documentos fuera de los locales donde se ubica el fichero está siendo autorizada por el responsable del fichero o está debidamente autorizada en el Documento de Seguridad?	
	¿Se están tomando las medidas adecuadas en el traslado de documentación para evitar la sustracción, perdida o acceso indebido durante su transporte?	
	Cuando se desecha un soporte o documento conteniendo datos de carácter personal ¿se adoptan las medidas adecuadas para evitar el acceso a la información o su recuperación posterior cuando se procede a su destrucción o borrado? ¿Son adecuadas estas medidas?	
	¿Se dan de baja en el inventario estos soportes o documentos desechados?	
	Para los soportes con datos de carácter personal considerados especialmente sensibles por la organización ¿se utilizan sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto? ¿Son adecuados y cumplen su finalidad?	
	¿Existe un registro de entrada de soportes o documentos? ¿Y un registro de salida?	Medio
	¿Contienen estos registros de entrada y salida de soportes toda la información exigida en el Reglamento?	
	¿Las personas encargadas de la recepción y la entrega de soportes están debidamente autorizadas? ¿Consta en el Documento de Seguridad dicha autorización?	
	¿Se han anotado todas las entradas y salidas de soportes?	

Sistema tratamiento	Comprobaciones a realizar	Nivel
	Gestión de soportes y documentos (cont.)	
Automatizado	¿Se utilizan sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto? ¿Son adecuados y cumplen su finalidad?	Alto
	¿La distribución de soportes se realiza de forma cifrada, o por otro mecanismo que garantice que no sea inteligible o manipulable durante el transporte?	
	¿Se cifran los datos en los dispositivos portátiles cuando éstos salen de las instalaciones del responsable del fichero?	
	Si fuera imprescindible el tratamiento de datos en dispositivos portátiles que no permitan el cifrado de datos ¿se ha hecho constar motivadamente en el Documento de Seguridad? ¿Se han adoptado medidas para minimizar los riesgos derivados de este tratamiento en entornos desprotegidos? ¿Son adecuadas?	
No Automatizado	¿Se adoptan medidas que impidan el acceso o manipulación de la información en los casos de traslado físico de la documentación contenida en un fichero? ¿Son apropiadas estas medidas?	
	La generación de copias o reproducción de documentos ¿se realiza exclusivamente por el personal autorizado en el Documento de Seguridad?	
	¿Se destruyen las copias o reproducciones desechadas de forma que no se pueda acceder a la información contenida en las mismas?	
	IDENTIFICACIÓN Y AUTENTICACIÓN	
Automatizado	¿Existe una relación de usuarios con acceso autorizado? ¿Se mantiene actualizada?	Básico
	¿Existen procedimientos de identificación y autenticación para dicho acceso? ¿Garantiza la correcta identificación del usuario?	
	El mecanismo de acceso y verificación de autorización de los usuarios ¿les identifica de forma inequívoca y personalizada?	
	¿Existe un procedimiento de asignación, distribución y almacenamiento de contraseñas? ¿Garantiza su confidencialidad e integridad?	
	¿Se cambian las contraseñas con la periodicidad establecida en el documento de seguridad?	
	¿Se almacenan las contraseñas de forma ininteligible mientras están en vigor?	
	¿Se limita el intento reiterado de acceso no autorizado al sistema?¿Se anotan estos intentos en el registro de incidencias?	Medio
	COPIAS DE RESPALDO Y RECUPERACIÓN	
Automatizado	¿El responsable del fichero ha definido los procedimientos de realización de copias de respaldo y recuperación de los datos? ¿Es adecuada esta definición?	Básico
	¿Están reflejados estos procedimientos en el Documento de Seguridad?	
	¿Ha verificado el responsable del fichero la correcta aplicación de estos procedimientos? ¿Realiza esta verificación cada seis meses?	
	¿Garantizan los procedimientos establecidos la reconstrucción de los datos al estado en que se encontraban antes de producirse la pérdida o destrucción?	
	Si esta pérdida o destrucción afecta a ficheros parcialmente automatizados ¿se ha procedido a grabar manualmente los datos? ¿Queda constancia motivada de este hecho en el Documento de Seguridad?	
	¿Se realizan copias de respaldo al menos semanalmente? Si no es así ¿se debe a que no ha habido actualizaciones en ese periodo?	
	¿Las pruebas previas a la implantación o modificación de los sistemas de información se realizan con datos reales? En caso afirmativo, ¿se están aplicando las mismas medidas de seguridad que las que le corresponde por la naturaleza de los datos que contiene? ¿Se anota su realización en el Documento de Seguridad? ¿Se hacen copias de seguridad previas a la realización de pruebas con datos reales?	
	¿Se conserva una copia de respaldo y de los procedimientos de recuperación de datos en lugar diferente al de los equipos que los tratan?	Alto
	¿Cumple este lugar las medidas de seguridad exigidas en el Reglamento?	

Sistema tratamiento	Comprobaciones a realizar	Nivel
	REGISTRO DE ACCESOS	
Automatizado	¿Existe el registro de accesos? En caso negativo ¿concurren en el responsable alguna de las circunstancias que le eximen de este requisito? ¿Se ha hecho constar en el Documento de Seguridad?	Alto
	¿Se está recogiendo en este registro la información mínima exigida en el Reglamento?	
	¿Los mecanismos que permiten el registro de estos accesos están directamente bajo el control del responsable de seguridad?	
	¿Existe la posibilidad de desactivar estos mecanismos?	
	¿Se conservan los datos registrados por un período mínimo de dos años?	
	¿Revisa el responsable de seguridad periódicamente la información registrada?	
	¿Realiza el responsable de seguridad un informe, al menos mensualmente, con el resultado de las revisiones realizadas y los problemas detectados?	
No Automatizado	¿El acceso a la documentación se realiza exclusivamente por personal autorizado?	
	¿Existen mecanismos para identificar los accesos realizados cuando los documentos son utilizados por múltiples usuarios?	
	¿Se ha establecido un procedimiento para registrar el acceso de personas no incluidas en el caso anterior? ¿Es adecuado?	
	TELECOMUNICACIONES	
Automatizado	¿La transmisión de datos a través de redes se realiza de forma cifrada (o por cualquier otro mecanismos que garantice que la información no sea inteligible ni manipulada por terceros)? ¿Este mecanismo de cifrado es eficaz?	Alto
	AUDITORÍA	
Todos	¿Se realiza la actual auditoría en el plazo establecido desde la anterior?	Medio
	Si ha habido modificaciones sustanciales en el sistema de información ¿se ha realizado a continuación una auditoría para verificar la adaptación, adecuación y eficacia de las medidas de seguridad?	
	¿Los informes de las auditorías anteriores incluían los datos, hechos y observaciones en los que se basaban sus dictámenes?	
	¿Se han implementado las medidas correctoras propuestas por auditorías anteriores? ¿Han sido eficaces y han corregido las deficiencias encontradas?	
	CRITERIOS DE ARCHIVO	
No Automatizado	¿Existe legislación específica con criterios para el archivo de soportes o documentos? ¿Garantizan estos criterios la conservación de documentos, la localización y consulta de la información? ¿Posibilitan el ejercicio de los derechos de oposición, acceso, rectificación y cancelación?	Básico
	En caso de no existir legislación específica ¿ha establecido el responsable del fichero los criterios y procedimientos de actuación para el archivo de documentos? ¿Es adecuado este procedimiento?	
	DISPOSITIVOS DE ALMACENAMIENTO	
No Automatizado	¿Los dispositivos de almacenamiento de documentos disponen de mecanismos que obstaculicen su apertura? Si sus características físicas no permiten adoptar esta medida ¿ha adoptado el responsable medidas que impidan el acceso de personas no autorizadas?	Básico
	CUSTODIA DE SOPORTES	
No Automatizado	¿Se custodia correctamente la documentación cuando ésta no se encuentra archivada en los dispositivos de almacenamiento por estar en revisión o tramitación? ¿Se impide en todo momento que sea accedida por persona no autorizada?	Básico

6. ELABORACIÓN DEL INFORME

Debe dictaminar sobre:

- Adecuación de las medidas y controles establecidas a lo dispuesto en el Título VIII del Reglamento.
- Identificación de deficiencias y propuesta de medidas correctoras o complementarias.
- Incluirá los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.
- Será analizado por el responsable de seguridad, y elevará sus conclusiones al responsable del fichero para que adopte las medidas adecuadas.
- Deberá quedar a disposición de la Agencia Española de Protección de Datos.