AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MODELO DE DOCUMENTO DE SEGURIDAD

Versión 1.0
Abril 2005

INTRODUCCIÓN

El artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter personal, 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 natura*l".

El Real Decreto 994 /1999, de 11 de junio (BOE 25 de junio) aprobó el Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal (Reglamento de Seguridad). El Reglamento tiene por objeto establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

Entre estas medidas, se encuentra la elaboración e implantación de la normativa de seguridad mediante un documento de 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 Reglamento de Seguridad, la Agencia Española de Protección de Datos pone a su disposición este modelo de "Documento de Seguridad", que pretende servir de guía y facilitar el desarrollo y cumplimiento de la normativa sobre protección de datos.

AVISO IMPORTANTE:

Debe entenderse, en cualquier caso, que siempre habrá que atenerse a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal 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.

ORGANIZACIÓN DEL MODELO

El Reglamento de Seguridad no especifica si se debe 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, o un único documento por cada fichero o tratamiento. Cualquiera de las dos 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, y en la segunda se incluye un anexo por cada fichero o tratamiento, con las medidas que le afecten de forma específica.

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.

NOTA ACLARATORIA: Las medidas de seguridad de nivel básico son exigibles en todos los casos. Las medidas de nivel medio complementan a la 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.

DOCUMENTO DE SEGURIDAD DE <denominación del responsable del fichero>

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el Reglamento de Medidas de Seguridad (Real Decreto 994/1999 de 11 de Junio), 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 Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

El contenido principal de este Documento queda estructurado como sigue:

I. Ámbito de aplicación del documento.
II. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.
III. Procedimiento general de información al personal.
IV. Funciones y obligaciones del personal.
V. Procedimiento de notificación, gestión y respuestas ante las incidencias.
VI. Procedimientos de revisión.
VII. Consecuencias del incumplimiento del Documento de Seguridad.

Anexo I. Aspectos específicos relativos a los diferentes ficheros.
Anexo I a. Aspectos relativos al fichero <nombre del fichero a>
Anexo I 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.

CAPÍTULO I: 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 básico: Se aplicarán a los ficheros con datos de carácter personal.
Nivel medio: Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, (en estos dos casos, deberán ser de titularidad pública), servicios financieros y los que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia y crédito).
Nivel alto: Ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual o los recabados para fines policiales sin consentimiento (en este último caso, también deberán ser de titularidad pública).

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 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.

CAPÍTULO II: MEDIDAS, NORMAS PROCEDIMIENTOS, REGLAS Y ESTÁNDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO

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

  <Especificar las normativas de identificación y autenticación de los usuarios con acceso a los datos personales.
  Si la autenticación se realiza mediante contraseñas, detallar el procedimiento de asignación, distribución y almacenamiento e indicar la periodicidad con la que se deberán cambiar.
  También es conveniente incluir los requisitos que deben cumplir las cadenas utilizadas como contraseña >

  #nivel medio# En los ficheros <indicar los nombres de los ficheros de nivel medio y alto> la identificación de los usuarios se deberá realizar de forma inequívoca y personalizada, verificando su autorización. <cada identificación debe pertenecer a un único usuario>. Asimismo, 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.

  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, <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.>

#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>.

<Detallar aquí que personal (nombres o puestos de trabajo) tiene acceso a los locales y especificar los controles de acceso existentes. Tener previsto también los procedimientos para el acceso por personal de mantenimiento, limpieza, seguridad etc.>

#nivel alto# Registro de accesos

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 periódicamente la información de control registrada y elaborará un informe según se detalla en el Capítulo VI de este documento.

- Gestión de soportes

Los soportes que contengan datos de carácter personal deben ser etiquetados para permitir su identificación, inventariados y 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 informáticos que contengan datos de carácter personal, el procedimiento establecido para habilitar o retirar el permiso de acceso y los controles de acceso existentes. 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 soportes informáticos 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 informáticos que contengan datos de carácter personal, fuera de los locales en donde esté ubicado el sistema de información, únicamente puede 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.

#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 soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción, y en el caso de las salidas, el tipo de soporte, la fecha y hora, el destinatario, el número de soportes , el tipo de información que contienen, la forma de envío y la persona responsable de la entrega>

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

#nivel medio# Medidas adicionales para los soportes con datos de nivel medio

Los soportes correspondientes a <indicar los nombres de los ficheros de nivel medio y alto>, que vayan a ser desechados o reutilizados, deberán ser previamente <detallar procedimiento a realizar para impedir cualquier recuperación de la

información almacenada en ellos> de forma que no sea posible recuperar la información almacenada en ellos.

Si los soportes con datos de los mencionados ficheros van a salir fuera de los locales en que se encuentren ubicados, como consecuencia de operaciones de mantenimiento, se adoptarán las siguientes medidas con el fin de impedir cualquier recuperación indebida de la información almacenada en ellos <Detallar las medidas a tomar>.

#nivel alto# Distribución cifrada de soportes

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>.

- 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 deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

- Régimen de trabajo fuera de los locales de la ubicación del fichero

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado. <detallar el procedimiento de autorización>

- Ficheros temporales

Los ficheros temporales 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 una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

- Copias de seguridad

Es obligatorio realizar copias de respaldo de los ficheros automatizados que contengan datos de carácter personal. Los procedimientos establecidos para las

copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

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

#nivel medio# Las recuperaciones de datos de los ficheros <indicar los ficheros de nivel medio> deberán ser autorizadas por escrito por el responsable del fichero, según el procedimiento indicado en el Capítulo V.

#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, en el que se almacenará la copia mencionada y los procedimientos a realizar para ello>.

- #nivel medio# Responsable de seguridad

  El responsable del fichero designará a <indicar si existen uno o varios responsables de seguridad>, que con carácter general se encargará de coordinar y controlar las medidas definidas en este documento de seguridad.

  En ningún caso, la designación supone una delegación de la responsabilidad que corresponde a <denominación responsable del fichero> como responsable del fichero de acuerdo con el Reglamento de medidas de seguridad.

  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.

  <Si existiera un responsable de seguridad diferente para cada fichero, indicarlo en la parte correspondiente del Anexo I>

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

- #nivel medio# Pruebas con datos reales

  Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al fichero tratado.

- #nivel alto# Telecomunicaciones

  La transmisión de datos de carácter personal de los ficheros <indicar los ficheros de nivel alto> se realizará <especificar el procedimiento de cifrado o el mecanismo que garantice que no sean inteligibles ni manipulados por terceros. Esta información puede relacionarse con lo especificado para la salida de soportes de nivel alto. También podría ser adecuado cifrar los datos en la red local>.

CAPÍTULO III. 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 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>

CAPÍTULO IV. 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>

CAPÍTULO V. 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, la persona que realiza la notificación, a quién se comunica y los efectos que se hubieran derivado de la misma. 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.

CAPÍTULO VI 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 o en la organización del mismo. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal >

- #nivel medio# Auditoría

  < Indicar los procedimientos para realizar la auditoría interna o externa que verifique el cumplimiento del Reglamento de Seguridad según lo indicado su artículo 17, y que debe realizarse al menos cada dos años. El informe analizará la adecuación al Reglamento de las medidas y controles, identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias. Los informes de auditoría han de ser analizados por el responsable del fichero, y quedar a disposición de la Agencia Española de Protección de Datos >

- #nivel alto# Informe mensual sobre “Log 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 Reglamento de Seguridad>.

CAPÍTULO VII: 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 a. ASPECTOS RELATIVOS AL FICHERO <nombre del fichero a>

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 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>.

- 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 4 del Reglamento de Seguridad>.

- 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, ...>
    - Soporte utilizado para la recogida de datos: <papel, informático, telemático, ...>

- 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 del sistema de información: <Describir los sistemas de información automatizados o no en los que se realiza el tratamiento de los datos. En el caso de ficheros automatizados, incluir los equipos físicos>.

- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación <En el caso de sistemas automatizados. 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>

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 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 los artículos 20.1 y 20.2 del Reglamento de Seguridad.>