# MODELO DOCUMENTO DE SEGURIDAD

***Responsable del Fichero*** .....

.....

***Nombre del Fichero*** .....

.....

***Nº de Inscripción*** .....

***Nº de la Versión*** .....

***Fecha*** .....

**ÍNDICE**

## *1. Objeto del documento*

El documento de seguridad está redactado cumpliendo lo dispuesto en el Reglamento de Medidas de Seguridad (Real Decreto 994/1999, de 11 de junio), en el que se 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 de Protección de Datos (Ley Orgánica 15/1999, de 13 de diciembre).

El fichero de datos de carácter personal . . . . . está clasificado como de nivel . . . . . .

Este documento deberá mantenerse permanentemente actualizado. Cualquier modificación relevante en los sistemas de información, 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.

## *2. Ámbito de aplicación*

El responsable del fichero . . . . . ha elaborado este documento comprometiéndose a implantarlo y actualizarlo.

Especificar la estructura de los ficheros con datos de carácter personal y la descripción de los sistemas de información que los tratan es una medida de seguridad de nivel básico. Se trata de una medida de índole técnica y organizativa necesaria para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal.

El fichero . . . . . contiene datos de carácter personal de nivel . . . . . Por tanto, se tomarán las medidas de seguridad correspondientes a este nivel.

## *3. Recursos protegidos*

Los recursos que quedan protegidos son:

- Los centros de tratamiento y locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contenga.
- Los puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso al fichero.
- Los servidores y el entorno de sistema operativo y de comunicaciones en el que se encuentra ubicado el fichero.
- Los sistemas informáticos, o aplicaciones establecidos para acceder a los datos.

El período mínimo de conservación de los datos registrados será de dos años.

## *4. Funciones y obligaciones del personal*

Las personas con acceso a los datos de carácter personal y a los sistemas de información deben tener sus funciones y obligaciones claramente definidas.

El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

El personal que tenga acceso a los datos del fichero debe conocer y respetar las medidas que afectan a las funciones que tiene encomendadas.

Si existiese alguna incidencia, el personal debe notificarla al responsable del fichero o al responsable de seguridad.

Las personas empleadas que colaboren deben guardar secreto con respecto a los datos del fichero de los que tengan conocimiento en el desarrollo de sus funciones.

## *5. Normas y procedimientos de seguridad*

- 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 de fichero o quien esté autorizado para ello)* y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado (nivel . . . . . ).

- Ficheros temporales.

  Los ficheros temporales deberán cumplir el nivel de seguridad . . . . . .

  Todo fichero temporal será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

- 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 tipo de fichero tratado (. . . . . .).

- Identificación y autenticación.

  El responsable del fichero debe encargarse de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de que se establezcan procedimientos de identificación y autenticación para dicho acceso.

  Las contraseñas han de cambiarse cada . . . . . *(indicar tiempo)*

  Mientras estén vigentes, se almacenarán de forma ininteligible.

  El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información, y la verificación de que está autorizado.

- Identificación del responsable de seguridad.

  El responsable del fichero designa a . . . . . *(nombre del responsable de seguridad)* como responsable de seguridad, durante un período de . . . . . *(indicar el tiempo de desempeño del cargo)* que se ocupará de coordinar y controlar las medidas definidas en el documento de seguridad. Esta designación no supone la delegación de la responsabilidad que corresponde al responsable del fichero.

- Control de accesos.

  El personal sólo puede acceder a los datos que sean necesarios para el desarrollo de sus funciones:

  Únicamente . . . . . *(nombre de la persona o puesto encargado de conceder, alterar o anular el acceso autorizado al sistema de información)* estará autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos.

  Únicamente . . . . . *(nombre de la persona que se encarga del alta, modificación y baja de las autorizaciones de acceso)* estará autorizado para llevar a cabo el procedimiento de alta, modificación y baja de las autorizaciones de acceso.

- Control de accesos físico.

  Únicamente . . . . . *(indicar el nombre de la persona que tenga acceso a los locales donde se encuentren los sistemas de información)* estará autorizado para acceder a los locales en los que se encuentren los sistemas de información que corresponden a . . . . . .

- Acceso a datos a través de redes de comunicaciones.

  Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de telecomunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

- Telecomunicaciones (transmisión telemática de datos).

  La transmisión de los datos del fichero a través de redes de telecomunicaciones se realizará cifrando dichos datos o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

- Registro de accesos.

  Cada acceso a los datos del fichero . . . . . (*nombre del fichero)* ha de quedar registrado, dando constancia del nombre del usuario, la fecha, la hora, el nombre del fichero, el tipo de acceso y si hay autorización o no.

  Los datos anotados en el registro de accesos serán conservados por un período de tiempo de . . . . . *(no menos de dos años).*

  La información registrada debe ser revisada de manera periódica. Esta función será desempeñada por el responsable de seguridad y la hará constar en un informe.

- Gestión de soportes.

  Los soportes deben ser etiquetados, para hacer posible su identificación, y almacenados en . . . . . *(lugar)*, lugar al que sólo podrá acceder el personal autorizado.

  Únicamente el responsable del fichero o un delegado de éste podrá autorizar la salida de datos de carácter personal en soporte informático del lugar en que estén almacenados.

  Debe constar el registro de las entradas y salidas de los soportes correspondientes al fichero.

En el caso de las entradas de soportes, se deberán cumplimentar los siguientes campos:

- Tipo de soporte
- Fecha
- Emisor
- Número de soportes
- Tipo de información que contienen
- Forma de envío
- Responsable de recepción
- Sistema informático utilizado

En el caso de las salidas de soportes:

- Tipo de soporte
- Fecha
- Hora
- Destinatario
- Número de soportes
- Tipo de información que contienen
- Forma de envío
- Responsable de la entrega
- Sistema informático utilizado

- Medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

  Aquellos soportes que vayan a ser desechados o reutilizados deberán ser . . . . . (procedimiento para impedir la recuperación de los datos) para que sea imposible la recuperación de los datos almacenados en ellos.

  Cuando se realicen operaciones de mantenimiento y los soportes salgan del local en que se encuentran, habrá que adoptar las siguientes medidas . . . . . para hacer imposible la recuperación de la información por personal no autorizado.

- Distribución de soportes.

  La distribución y salida del soporte en que está contenido el fichero . . . . . .debe llevarse a cabo mediante un procedimiento de cifrado de datos u otro mecanismo que impida que los datos sean inteligibles o manipulados mientras estén siendo transportados.

- Procedimiento de notificación, gestión y respuesta ante las incidencias.

  El procedimiento de notificación y gestión de incidencias consistente en . . . . . *(detallar el procedimiento de notificación y gestión de las posibles incidencias)* debe contener un registro en el que conste:

  - El tipo de incidencia.
  - El momento en que se ha producido.
  - La persona que realiza la notificación.
  - A quién se le comunica.
  - Los efectos que se hubieran derivado de la misma.

- El sistema informático utilizado en caso de tratarse de gestión automatizada.

- Registro de incidencias.

  En los procedimientos ejecutados para la recuperación de los datos habrá que indicar la persona que ejecutó el proceso, los datos que han sido restaurados y, en su caso, los datos que han tenido que ser grabados manualmente.

  Para ello será necesaria la autorización del responsable del fichero.

- Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

  El responsable del fichero debe verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

  Estos procedimientos deben garantizar la reconstrucción en el estado en que se encontraban los datos al tiempo de producirse la pérdida o destrucción.

  Las copias han de llevarse a cabo como mínimo una vez por semana, salvo que no se hubiera producido ningún cambio durante ese período.

- Copias de respaldo y recuperación.

  La copia de respaldo y de los procedimientos de recuperación de los datos se conservarán en . . . . . *(indicar un lugar diferente de aquél en donde se encuentren los equipos informáticos que los tratan cumpliendo en todo caso las medidas de seguridad exigidas en el Reglamento de Medidas de Seguridad)*.

- Revisión del documento de seguridad.

  El documento ha de mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización.

  Deberá, además, estar adecuado a las disposiciones legales vigentes en cada momento en materia de seguridad de los datos.

. . . . . es el encargado de la proposición de cambios, aprobación y comunicación de datos, así como de informar a los trabajadores de las modificaciones.

- Auditorías.

  Se someterán a una auditoría interna o externa los sistemas de información e instalaciones de tratamiento de datos para verificar el cumplimiento del Reglamento de Medidas de Seguridad, de los procedimientos y de las instrucciones vigentes en materia de seguridad de datos.

  Se hará una auditoría, al menos, cada dos años.

  Tras la auditoría, se redactará un informe para dictaminar sobre la adecuación de las medidas y controles, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.

  Deberá también incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

  Estos informes serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas, y quedarán a disposición de la Agencia de Protección de Datos.

## ANEXOS

1. ***Estructura del fichero***
2. ***Personal autorizado***
3. ***Funciones y obligaciones del personal***
4. ***Encargado del tratamiento***
5. ***Centros de tratamiento***
6. ***Sistema operativo y entorno de comunicaciones***
7. ***Sistema informático de acceso***
8. ***Inventario de soportes***
9. ***Procedimientos de control y seguridad***
10. ***Documentos de notificación a la AEPD***
11. ***Notificación de incidencias***
12. ***Autorizaciones***
13. ***Controles periódicos y auditorías***

## *1. Estructura del fichero*

- Responsable del fichero:

  Nombre o razón social . . . . . .
  . . . . . .
  CIF . . . . . Dirección . . . . . .
  . . . . . .
  Teléfono . . . . . Fax . . . . . .
  E-mail . . . . . .

- Servicio o unidad ante la que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición:

  Nombre o razón social . . . . . .
  . . . . . .
  CIF . . . . . Dirección . . . . . .
  . . . . . .
  Teléfono . . . . . Fax . . . . . .
  E-mail . . . . . .

- Encargado del tratamiento:

  Nombre o razón social . . . . . .
  . . . . . .
  CIF . . . . . Dirección . . . . . .
  . . . . . .
  Teléfono . . . . . Fax . . . . . .
  E-mail . . . . . .

- Fichero:

  Nombre del fichero . . . . . .
  . . . . . .
  Descripción . . . . . .
  . . . . . .
  Finalidad . . . . . .
  . . . . . .
  Identificador . . . . . .
  Ubicación . . . . . .
  . . . . . .

. . . . . .Nivel . . . . . .
Procedencia de los datos . . . . . .
. . . . . .
Procedimiento de recogida . . . . . .
. . . . . .
Cesión o comunicación de datos . . . . . .
. . . . . .
Transferencia internacional de datos . . . . . .
. . . . . .
Soporte utilizado para la recogida de datos . . . . . .
. . . . . .

Leyes aplicables al fichero . . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .

## *2. Personal autorizado*

Además de cumplimentar los campos que aparecen a continuación, habrá que adjuntar los originales, con sus respectivas copias, de los nombramientos de los perfiles incluidos en el documento.

- Responsable del fichero: decide sobre la finalidad, contenido y uso del tratamiento.

  Nombre . . . . . .
  . . . . . .
  Cargo . . . . . .
  Alta / Baja . . . . . .

- Responsable de seguridad: coordina y controla las medidas definidas.

  Nombre . . . . . .
  . . . . . .
  Cargo . . . . . .
  Alta / Baja . . . . . .

- Administradores del sistema: administra o mantiene el entorno operativo del fichero.

  Nombre . . . . . .
  . . . . . .
  Cargo . . . . . .
  Alta / Baja . . . . . .

- Usuarios del fichero: usualmente utilizan el sistema de acceso al fichero.

  Nombre . . . . . .
  . . . . . .
  Cargo . . . . . .
  Alta / Baja . . . . . .

## *3. Funciones y obligaciones del personal*

### ***Funciones***

- Responsable del fichero.

  El responsable del fichero es el encargado jurídicamente de la seguridad del fichero y de las medidas establecidas en el presente documento, implantará las medidas de seguridad establecidas en él y adoptará las medidas necesarias para que el personal afectado por este documento conozca las normas que repercutan al desarrollo de sus funciones.

  Designará al responsable de seguridad.

- Responsable de seguridad.

  Es el encargado de coordinar y controlar las medidas definidas en el presente documento.

- Personal autorizado en producción habitual.

  El acceso se limita a los siguientes perfiles

  - Usuario/Administrador del sistema.

- Operador.

- Administradores técnicos e informáticos generales que intervienen en situaciones no habituales.

  Cuando no existe un personal técnico determinado que se pueda relacionar de forma directa con un fichero o sistema informático y que acceda habitualmente al mencionado fichero o sistema.

  Siempre será posible conocer el personal que intervino con posterioridad, dejando constancia de ello, identificando al personal técnico y anotándolo en el Registro de Incidencias.

- Administradores o personal informático.

  El personal que administra el sistema de acceso al fichero se puede, a su vez, clasificar en varias categorías, que no necesariamente deberán estar presentes en todos los casos, siendo en algunas ocasiones asumidas por una misma persona. Estas categorías son:

  - Administradores (red, sistemas operativos y bases de datos). Serán los responsables de los máximos privilegios y, por tanto, del máximo riesgo de que una actuación errónea pueda afectar al sistema. Tendrán acceso al software del sistema, a las herramientas necesarias para su trabajo y a los ficheros o bases de datos necesarios para resolver los problemas que surjan.

  - Operadores (red, sistemas operativos, bases de datos y aplicación). Sus actuaciones están limitadas a la operación de los equipos y redes utilizando las herramientas de gestión disponibles. No deben, en principio, tener acceso directo a los datos del fichero, ya que su actuación no lo precisa.

  - Mantenimiento de los sistemas y aplicaciones. Personal responsable de la resolución de incidencias que puedan surgir en el entono hardware/software de los sistemas informáticos o de la propia aplicación de acceso al fichero.

  - Cualquier otro que la organización establezca.

***Obligaciones***

- Responsable del fichero.

  Está obligado a implantar las medidas de seguridad establecidas en este documento.

  El responsable del fichero deberá garantizar la difusión de este documento entre todo el personal que vaya a utilizarlo.

  Tendrá que mantenerlo actualizado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

  Será también su misión adecuar en todo momento el contenido del mismo a las disposiciones vigentes en materia de seguridad de datos.

  Forzosamente, designará uno o varios responsables de seguridad.

  - Entorno de sistema operativo y de comunicaciones.

    El responsable del fichero aprobará o designará al administrador que se responsabilizará del sistema operativo y de comunicaciones.

    En el caso más simple, como es que el fichero se encuentre ubicado en un ordenador personal y accedido mediante una aplicación local monopuesto, el administrador del sistema operativo podrá ser el mismo usuario que accede usualmente al fichero.

  - Sistema informático o aplicaciones de acceso al fichero.

    El responsable del fichero se encargará de que los sistemas informáticos de acceso al fichero tengan su acceso restringido mediante un código de usuario y una contraseña.

    Asimismo cuidará que todos los usuarios autorizados para acceder al Fichero, relacionados en el anexo 2, tengan un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

  - Salvaguarda y protección de las contraseñas personales.

Sólo las personas relacionadas en el Anexo 2, podrán tener acceso a los datos del fichero.

- Gestión de soportes.

  La salida de soportes informáticos que contengan datos del fichero fuera de los locales donde está ubicado deberá ser expresamente autorizada por el responsable del fichero.

- Entrada y salida de datos por red.

  Todas las entradas y salidas de datos del fichero que se efectúen mediante correo electrónico, se realizarán desde una única cuenta o dirección de correo controlada por un usuario especialmente autorizado por el responsable del fichero. Igualmente, si se realiza la entrada o salida de datos mediante sistemas de transferencia de ficheros por red, únicamente un usuario o administrador estará autorizado para realizar esas operaciones.

- Procedimientos de respaldo y recuperación.

  El responsable del fichero se encargará de verificar la definición y correcta aplicación de las copias de respaldo y recuperación de los datos.

  Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

- Controles periódicos de verificación del cumplimiento.

  El responsable del fichero junto con el responsable de seguridad, analizarán con periodicidad (al menos trimestralmente) las incidencias registradas en el libro correspondiente, para, independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, poner las medidas correctoras que limiten esas incidencias en el futuro.

Al menos cada dos años, se realizará una auditoría, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoría serán analizados por el responsable de seguridad, quien propondrá al responsable del fichero las medidas correctoras correspondientes.

Los resultados de todos estos controles periódicos, así como de las auditorías, serán adjuntados a este documento de seguridad.

- Responsable de seguridad.

El responsable de seguridad coordinará la puesta en marcha de las medidas de seguridad, colaborará con el responsable del fichero en la difusión del documento de seguridad y cooperará con el responsable del fichero controlando el cumplimiento de las mismas.

- Gestión de incidencias.

  El responsable de seguridad habilitará un libro de incidencias a disposición de todos los usuarios y administradores del fichero con el fin de que se registre en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

  Analizará las incidencias registradas, tomando las medidas oportunas en colaboración con el responsable del fichero.

- Controles periódicos de verificación del cumplimiento.

  El responsable de seguridad del Fichero comprobará, con cierta periodicidad (al menos trimestral), que la lista de usuarios autorizados del Anexo 2 se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al fichero, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador del fichero. Además de estas comprobaciones periódicas, el administrador comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al fichero.

Se comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación de fichero.

A su vez, al menos cada tres meses, los administradores del fichero comunicaran al responsable de seguridad cualquier cambio que se haya realizado en los datos técnicos de los anexos, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al fichero, procediendo igualmente a la actualización de los anexos.

El responsable de seguridad, verificará, al menos trimestralmente, el cumplimiento de lo previsto para las entradas y salidas de datos, sean por red o en soporte magnético.

El responsable del fichero junto con el responsable de seguridad, analizarán con periodicidad al menos trimestral las incidencias registradas en el libro correspondiente, para, independientemente de las medidas particulares que se hayan adoptado en el momento en que se produjeron, poner las medidas correctoras que limiten esas incidencias en el futuro.

Al menos cada dos años, se realizará una auditoría, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad a las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las mediadas correctoras necesarias. Los informes de auditoría serán analizados por el responsable de seguridad, quien propondrá al responsable del fichero las medidas correctoras correspondientes.

Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad sin que se deba permitir, en ningún caso la desactivación de los mismos.

El responsable de seguridad se encargará de revisar periódicamente la información de control registrada.

Los resultados de todos estos controles periódicos, así como de las auditorías, serán adjuntados a este documento de seguridad.

- Todo el personal.

  - Puestos de trabajo.

    Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.

    Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

    Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente, o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

    En el caso de las impresoras, deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

    Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero. La revocación de esta prohibición será autorizada por el responsable del fichero, quedando constancia de esta modificación en el libro de incidencias.

    Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, que sólo podrá ser cambiada bajo la autorización del responsable de seguridad o por administradores autorizados.

  - Salvaguarda y protección de las contraseñas personales.

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

- Gestión de incidencias.

  Cualquier usuario que tenga conocimiento de una incidencia es responsable de la comunicación de la misma al administrador del sistema, o, en su caso, del registro de la misma en el sistema de registro de incidencias del fichero.

  El conocimiento y la no notificación de una incidencia por parte de un usuario serán considerados como una falta contra la seguridad del fichero por parte de ese usuario.

- Gestión de soportes.

  Los soportes que contengan datos del fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, qué tipo de datos contiene, proceso que los ha originado y fecha de creación.

  Aquellos medios que sean reutilizables, y que hayan contenido copias de datos del fichero, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

  Los soportes que contengan datos del fichero deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso del fichero que no estén por tanto relacionadas en el Anexo 2.

  Cuando la salida de datos del fichero se realice por medio de correo electrónico los envíos se realizaran, siempre y únicamente, desde una dirección de correo controlada por el administrador de seguridad, dejando constancia de estos envíos en el directorio histórico de esa dirección de correo o en algún otro sistema de

registro de salidas que permita conocer en cualquier momento los envíos realizados, a quién iban dirigidos y la información enviada.

En el caso en que los datos deban ser enviados fuera del recinto físicamente protegido donde se encuentra ubicado el Fichero, bien sea mediante un soporte físico de grabación de datos, o bien sea mediante correo electrónico, deberán ser encriptados de forma que sólo puedan ser leídos e interpretados por el destinatario.

Se deberán registrar mediante correo electrónico o transferencia de datos por red, de forma que se pueda siempre identificar su origen, tipo, formato, fecha y hora del envío, y destinatario de los mismos.

- Obligaciones de los administradores y personal informático

  - Entorno de sistema operativo y de comunicaciones

    Ninguna herramienta o programa de utilidad que permita el acceso al fichero deberá ser accesible a ningún usuario o administrador no autorizado en el Anexo 2.

    En la norma anterior se incluye cualquier medio de acceso en bruto, (no elaborado o editado) a los datos del fichero, como los llamados "queries", editores universales, analizadores de ficheros, etc., que deberán estar bajo el control de los administradores autorizados relacionados en el Anexo 2.

    El administrador deberá responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo del Fichero, de forma que ninguna persona no autorizada tenga acceso a las mismas.

    Si la aplicación o sistema de acceso al fichero utilizase usualmente ficheros temporales, o cualquier otro medio en el que pudiesen ser grabados los datos protegidos, el administrador deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.

    Si el ordenador en el que está ubicado el fichero está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso al fichero, el

administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.

- Sistema Informático o aplicaciones de acceso al fichero.

  Si la aplicación informática que permite el acceso al Fichero no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.

  En cualquier caso se controlarán los intentos de acceso fraudulento al Fichero, limitando el número máximo de intentos fallidos, y, cuando sea técnicamente posible, guardando en un fichero auxiliar la fecha, hora, código y claves erróneas que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos.

  Si durante las pruebas anteriores a la implantación o modificación de la aplicación de acceso al fichero se utilizasen datos reales, se deberá aplicar a esos ficheros de prueba el mismo tratamiento de seguridad que se aplica al fichero.

- Salvaguarda y protección de las contraseñas personales.

  Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en los anexos. Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas, y será responsabilidad del administrador del sistema.

  El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

- Procedimientos de respaldo y recuperación.

  Existirá una persona, bien sea el administrador o bien otro usuario expresamente designado, que será responsable de obtener

periódicamente una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo.

Estas copias deberán realizarse con una periodicidad, al menos, semanal, salvo en el caso de que no se haya producido ninguna actualización de los datos.

En caso de fallo del sistema con pérdida total o parcial de los datos del fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban en el momento del fallo. Ese procedimiento está descrito en los anexos.

Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

- Controles periódicos de verificación del cumplimiento.

El responsable de seguridad del fichero comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados del 2B se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al fichero, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador del fichero. Además de estas comprobaciones periódicas, el administrador comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado.

Se comprobará también, al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación de fichero.

A su vez, y también con periodicidad al menos trimestral, los administradores del fichero comunicarán al responsable de

seguridad cualquier cambio que se haya realizado en los datos técnicos de los anexos, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al fichero, procediendo igualmente a la actualización de dichos anexos.

El responsable de seguridad, verificará, con periodicidad al menos trimestral, el cumplimiento de las previsiones para las entradas y salidas de datos, sean por red o en soporte magnético.

Al menos cada dos años, se realizará una auditoría, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoría serán analizados por el responsable de seguridad, quien propondrá al responsable del fichero las medidas correctoras correspondientes.

Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad sin que se deba permitir, en ningún caso, la desactivación de los mismos.

El responsable de seguridad se encargará de revisar periódicamente la información de control registrada.

Los resultados de todos estos controles periódicos, así como de las auditorías serán adjuntadas a este documento de seguridad en los anexos.

## *4. Encargado del tratamiento*

Adjuntar el contrato por el que se establece que el encargado tratará los datos conforme a las instrucciones dadas pro el responsable del fichero y no los aplicará ni destinará a un fin distinto del que se mencione en el contrato ni siquiera comunicándolo a terceras personas.

En el contrato han de venir fijadas las medidas de seguridad a que se refiere la LOPD.

## *5. Centros de tratamiento*

Este Anexo hace referencia a los locales en los que se encuentra ubicado el fichero o en los que se almacenan los soportes que lo contengan, y los puestos de trabajo desde los que se puede tener acceso al fichero.

- Locales.

  Ubicación física . . . . . .
  . . . . . .
  Tipo de acceso y control . . . . . .
  . . . . . .
  Equipamiento . . . . . .
  . . . . . .

- Puestos de trabajo.

  Relación de puestos de trabajo . . . . . .
  . . . . . .
  Descripción de los equipos . . . . . .
  . . . . . .

## *6. Sistema operativo y entorno de comunicaciones*

Este Anexo debe ser cumplimentado por el administrador del sistema . . . . . .
. . . . . .

Responsable del mantenimiento . . . . . .
. . . . . .

- Sistema operativo.

  Nombre . . . . . .
  Fabricante . . . . . .
  Versión . . . . . .
  Características . . . . . .
  . . . . . .
  Control de acceso . . . . . .
  . . . . . .
  Archivos del procedimiento de histórico de operaciones y del

procedimiento de recuperación . . . . . .
. . . . . .
. . . . . .

- Entorno de comunicaciones.

  Tipo de red local . . . . . .
  . . . . . .
  Tipo de conexión con otras redes locales o WAN . . . . . .
  . . . . . .
  ¿Se comparten recursos y archivos? . . . . . Si se responde “sí”, indicar el tipo de sistema de redes . . . . . .
  . . . . . .
  Control de acceso al fichero desde la red . . . . . .
  . . . . . .
  Sistema de cifrado para la transmisión de datos . . . . . .
  . . . . . .

## *7. Sistema informático de acceso*

El sistema informático consiste en el conjunto de programas con los que se accede al fichero, para consultarlo o actualizarlo.

- Descripción del sistema informático.

  Nombre de la aplicación . . . . . .
  . . . . . .
  Nombre del programador . . . . . .
  . . . . . .
  Fecha de programación . . . . . .
  Responsable del mantenimiento . . . . . .
  . . . . . .
  Tipo de control de acceso . . . . . .
  . . . . . .
  . . . . . .
  . . . . . *(indicar si está limitado el número de intentos fallidos de acceso y si se guarda el historial de los mismos)*.
  Tipo de procedimientos de histórico de operaciones y de recuperación *(si*

*los hay)* . . . . . .
. . . . . .

## *8. Inventarios de soportes*

La información registrada debe ser revisada de manera periódica. Esta función será desempeñada por el responsable de seguridad y la hará constar en un informe.

## *9. Procedimientos de control y seguridad*

- Procedimiento de asignación y cambio de contraseñas . . . . . .
  . . . . . .
  . . . . . .
  . . . . . .
  . . . . . .
- Procedimiento de respaldo y recuperación . . . . . .
  . . . . . .
  . . . . . .
  . . . . . .
  . . . . . .
- Procedimiento de gestión de soportes.

  Identificación de etiquetas . . . . . .
  . . . . . .
  Inventario de soportes . . . . . .
  . . . . . .
  Lugar de almacenamiento . . . . . .
  . . . . . .
  Método de borrado físico de datos . . . . . .
  . . . . . .
- Entrada y salida de datos por red

  Cuenta de correo . . . . . .
  Responsable de transferencias electrónicas . . . . . .

. . . . . .

- Procedimiento de distribución de soportes . . . . . .

- Sistema de cifrado de datos . . . . . .

## *10. Documentos de notificación a la Agencia Española de Protección de Datos*

Debe adjuntarse en este Anexo el documento de notificación a la Agencia de Protección de Datos de registro del fichero, junto con sus modificaciones, y una copia de la publicación de la disposición de creación.

## *11. Notificación de incidencias*

- Notificación de incidencias.

  Nº de orden . . . . . .
  Tipo de incidencia . . . . . .
  Fecha y hora en que se produjo . . . . . .
  Persona que la notifica . . . . . .
  Departamento . . . . . .
  Persona a quien se comunica . . . . . .
  Departamento . . . . . .
  Efectos . . . . . .

- Si hay recuperación de datos, añadir la notificación de recuperación de datos.

  Procedimientos de recuperación . . . . . .
  Persona que ejecuta la recuperación . . . . . .

. . . . . .
Datos restaurados . . . . . .
. . . . . .
. . . . . .
Datos grabados manualmente. . . . . .
. . . . . .
. . . . . .

## *12. Autorizaciones*

- Autorizaciones de salida.

  Adjuntar copias de las autorizaciones firmadas por el responsable del fichero para la salida de soportes con datos de carácter personal.

- Autorizaciones de entrada.

  Adjuntar copias de las autorizaciones firmadas por el responsable del fichero para la entrada de soportes con datos de carácter personal.

- Autorizaciones de recuperación.

  Adjuntar las copias de las autorizaciones relativas a la ejecución de procedimientos de recuperación de datos.

## *13. Controles periódicos y auditorías*

Este Anexo debe contener los resultados de los controles periódicos y de las auditorías realizadas.