

**Documento de Seguridad para ficheros automatizados de datos de carácter personal con nivel de seguridad **alto****

**Fichero**

Nº inscripción	NOMBRE DE FICHERO	
----------------	-------------------	--

**Comunidad de Madrid**

**Consejería / Ente Público**

**Dirección General / Órgano / Organismo / Entidad**

Fecha versión del Documento de Seguridad

Versión

Sistema de Información


<b>ÍNDICE</b>	
Objeto del documento	3
Ámbito de aplicación	3
Recursos protegidos	3
Funciones y obligaciones del personal	4
Normas y procedimientos de seguridad	4
Gestión de incidencias	8
Gestión de soportes	8
Entrada /salida de datos por red y telecomunicaciones	9
Procedimientos de respaldo y recuperación	10
Controles periódicos de verificación del cumplimiento	10

<b>ANEXOS</b>	
A. Documentos de notificación y Decretos de creación de ficheros	12
B. Descripción de la estructura del Fichero o la base de datos	13
C. Descripción del Sistema informático y perfiles de usuarios	14
D. Entorno del sistema operativo y de comunicaciones	15
E. Locales y equipamientos	16
F. Personal autorizado para acceder al fichero	17
G. Procedimientos de control de accesos, respaldo y recuperación y gestión de soportes	20
H. Funciones y obligaciones del personal	26
I. Procedimientos de notificación y gestión de incidencias	33
J. Controles periódicos	35
K. Modificaciones introducidas en las revisiones de este documento	41



## 1. Objeto del documento

El presente documento responde a la obligación establecida en el artículo 8 del Real Decreto 994/1999 de 11 de Junio en el que se regulan las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

El fichero de datos: **NOMBRE DE FICHERO**, en adelante el Fichero, descrito en el documento de Notificación a la Agencia de Protección de Datos de la Comunidad de Madrid, que se adjunta en el Anexo A, se encuentra oficialmente clasificado como de nivel de seguridad **alto**, atendiendo a las condiciones descritas en el artículo 4 del Real Decreto citado, siendo por tanto aplicable a él todas las medidas de seguridad de nivel **alto** que se establecen en el Capítulo III del citado decreto.

## 2. Ámbito de aplicación

Este documento ha sido elaborado bajo la responsabilidad de la persona descrita en el apartado (1) del documento adjunto en el Anexo A, quien, como responsable del Fichero, se compromete a implantar y actualizar ésta Normativa de Seguridad de obligado cumplimiento para todo el personal con acceso a los datos protegidos o a los sistemas de información que permiten al acceso a los mismos.

Todas las personas que tengan acceso a los datos del Fichero, bien a través del sistema informático **NOMBRE DEL SISTEMA INFORMÁTICO** habilitado para acceder al mismo, o bien a través de cualquier otro medio automatizado de acceso al Fichero, se encuentran obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Una copia de este documento con la parte que le afecte será entregada, para su conocimiento, a cada persona autorizada a acceder a los datos del Fichero, siendo requisito obligatorio para poder acceder a esos datos el haber firmado la recepción del mismo.

## 3. Recursos protegidos

La protección de los datos del Fichero frente a accesos no autorizados se deberá

realizar mediante el control, a su vez, de todas las vías por las que se pueda tener acceso a dicha información.

Los recursos que, por servir de medio directo o indirecto para acceder al Fichero, deberán ser controlados por esta normativa son:

- 1- Los centros de tratamiento y locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contengan, su descripción figura en el Anexo E.
- 2- Los puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso al Fichero. La relación de esos puestos de trabajo está descrita en el Anexo E.
- 3- Los servidores, si los hubiese, y el entorno de sistema operativo y de comunicaciones en el que se encuentra ubicado el Fichero, que está descrito en el Anexo D.
- 4- Los sistemas informáticos, o aplicaciones establecidos para acceder a los datos, descritos en el Anexo C.

#### **4. Funciones y obligaciones del personal**

El personal afectado por esta normativa se clasifica en dos categorías:

1. **Administradores del sistema**, encargados de administrar o mantener el entorno operativo del Fichero. Este personal deberá estar explícitamente relacionado en el Anexo F, ya que por sus funciones pueden utilizar herramientas de administración que permitan el acceso a los datos protegidos saltándose las barreras de acceso de la Aplicación.
2. **Usuarios del Fichero**, o personal que usualmente utiliza el sistema informático de acceso al Fichero, y que también deben estar explícitamente relacionados en el Anexo F.

Además del personal anteriormente citado existirá un **Responsable de Seguridad del Fichero** cuyas funciones serán las de coordinar y controlar las medidas definidas en el documento, sirviendo al mismo tiempo de enlace con el **Responsable del Fichero**, sin que esto suponga en ningún caso una delegación de la responsabilidad que

corresponde a éste último, de acuerdo con el R.D. 994/1999 de 11 de Junio. Este documento es de obligado cumplimiento para todos ellos. Las funciones y obligaciones del personal están descritas en el Anexo H. Sin embargo, los administradores del sistema deberán además atenerse a aquellas normas, más extensas y estrictas, que se referencian en el Anexo G, y que atañen, entre otras, al tratamiento de los respaldos de seguridad, normas para el alta de usuarios y contraseñas, así como otras normas de obligado cumplimiento en la unidad administrativa a la que pertenece el Fichero.

## **5. Normas y procedimientos de seguridad**

### **5.1 Centros de tratamiento y locales**

Los locales donde se ubiquen los ordenadores que contienen el Fichero deben ser objeto de especial protección que garantice la disponibilidad y confidencialidad de los datos protegidos, especialmente en el caso de que el Fichero esté ubicado en un servidor accedido a través de una red.

5.1.1. Los locales deberán contar con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad del Fichero que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas. La descripción de esos medios se encuentra en el Anexo E.

5.1.2. El acceso a los locales donde se encuentre el fichero deberá estar restringido exclusivamente a los administradores del sistema que deban realizar labores de mantenimiento para las que sean imprescindibles el acceso físico.

### **5.2 Puestos de trabajo**

Son todos aquellos dispositivos desde los cuales se puede acceder a los datos del Fichero, como, por ejemplo, terminales u ordenadores personales.

Se consideran también puestos de trabajo aquellos terminales de administración del sistema, como, por ejemplo, las consolas de operación, donde en algunos casos también pueden aparecer los datos protegidos del Fichero.

5.2.1. Cada puesto de trabajo estará bajo la responsabilidad de una persona de las autorizadas en el Anexo F, que garantizará que la información que muestra no

pueda ser vista por personas no autorizadas.

- 5.2.2. 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.
- 5.2.3. 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.
- 5.2.4. 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.
- 5.2.5. 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.
- 5.2.6. Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser cambiada bajo la autorización del responsable de seguridad o por administradores autorizados del anexo F.

### **5.3 Entorno de Sistema Operativo y de Comunicaciones**

Aunque el método establecido para acceder a los datos protegidos del Fichero es el sistema informático referenciado en el Anexo C, al estar el fichero ubicado en un ordenador con un sistema operativo determinado y poder contar con unas conexiones que le comunican con otros ordenadores, es posible, para las personas que conozcan estos entornos, acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que pueda contar la aplicación.

Esta normativa debe, por tanto, regular el uso y acceso de las partes del sistema operativo, herramientas o programas de utilidad, o del entorno de comunicaciones, de

forma que se impida el acceso no autorizado a los datos de Fichero.

- 5.3.1. El sistema operativo y de comunicaciones del Fichero deberá tener al menos un responsable, que, como administrador deberá estar relacionado en el Anexo F.
- 5.3.2. 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.
- 5.3.3. 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 F.
- 5.3.4. En la norma anterior se incluye cualquier medio de acceso en bruto, es decir 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 F.
- 5.3.5. 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.
- 5.3.6. Si la aplicación o sistema de acceso al Fichero utilizase usualmente ficheros temporales, ficheros de "logging", o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, el administrador deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.
- 5.3.7. 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 acceso al Fichero, el administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.



## 5.4 Sistema Informático o aplicaciones de acceso al Fichero

Son todos aquellos sistemas informáticos, programas o aplicaciones con las que se puede acceder a los datos del Fichero, y que son usualmente utilizados por los usuarios para acceder a ellos.

Estos sistemas pueden ser aplicaciones informáticas expresamente diseñadas para acceder al Fichero, o sistemas preprogramados de uso general como aplicaciones o paquetes disponibles en el mercado informático.

5.4.1. Los sistemas informáticos de acceso al Fichero deberán tener su acceso restringido mediante un código de usuario y una contraseña.

5.4.2. Todos los usuarios autorizados para acceder al Fichero, relacionados en el Anexo F, deberán tener un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

5.4.3. 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.

5.4.4. 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 clave erróneas que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos.

5.4.5. 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 mismo Fichero, y se deberán relacionar esos ficheros de prueba en el Anexo B.

5.4.5 De cada acceso se guardarán, como mínimo, 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 se trata de un acceso autorizado, se guardará la clave del registro o bien la información que permita identificar el registro accedido.

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

## **5.5 Salvaguarda y protección de las contraseñas personales**

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos, y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible.

- 5.5.1. Sólo las personas relacionadas en el Anexo F podrán tener acceso a los datos del Fichero.
- 5.5.2. 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 registrarla como incidencia y proceder inmediatamente a su cambio.
- 5.5.3. Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el Anexo G.
- 5.5.4. El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

## **6. Gestión de incidencias**

Una incidencia es cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad del Fichero, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad de los datos.

El mantener un registro de las incidencias que comprometan la seguridad de un Fichero es una herramienta imprescindible para la prevención de posibles ataques a esa seguridad, así como para persecución de los responsables de los mismos.

- 6.1.1. El responsable de seguridad de Fichero habilitará un Libro de Incidencias a disposición de todos los usuarios y administradores del Fichero con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.
- 6.1.2. Cualquier usuario que tenga conocimiento de una incidencia es responsable del registro de la misma en el Libro de Incidencias del Fichero o en su caso de la comunicación por escrito al responsable de seguridad o al responsable del Fichero.

- 6.1.3. El conocimiento y la no notificación o registro de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.
- 6.1.4. La notificación o registro de una incidencia deberá constar al menos de los siguientes datos: tipo de incidencia, fecha y hora en que se produjo, persona que realiza la notificación, persona a quien se comunica, efectos que puede producir, descripción detallada de la misma. El procedimiento está descrito en el Anexo I.

## 7. Gestión de soportes

Soportes informáticos son todos aquellos medios de grabación y recuperación de datos que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación que gestiona el Fichero.

Dado que la mayor parte de los soportes que hoy en día se utilizan, como disquetes o CD-ROMs, son fácilmente transportables, reproducibles y/o copiables, es evidente la importancia que para la seguridad de los datos del Fichero tiene el control de estos medios.

- 7.1.1. 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 o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.
- 7.1.2. 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.
- 7.1.3. Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso del Fichero que no estén por tanto relacionadas en el Anexo F.
- 7.1.4. La salida de soportes informáticos que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el responsable del Fichero, utilizando para ello el documento adjunto en el anexo G.
- 7.1.5 El responsable del Fichero mantendrá un Libro de registro de entradas y salidas donde se guardarán los formularios de entradas y de salidas de soportes descritos en el anexo G, con indicación de tipo de soporte, fecha y hora, emisor, número de soportes, tipo de información que contienen, forma de envío,**

destinatario, o persona responsable de la recepción que deberán estar debidamente autorizadas.

7.1.6 Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

7.1.8 La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

## 8. Entrada/salida de datos por red y Telecomunicaciones

La transmisión de datos por red, ya sea por medio de correo electrónico o mediante sistemas de transferencia de ficheros, se está convirtiendo en uno de los medios más utilizados para el envío de datos, hasta el punto de que está sustituyendo a los soportes físicos. Por ello merecen un tratamiento especial ya que, por sus características, pueden ser más vulnerables que los soportes físicos tradicionales.

8.1.1 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.

8.1.2 Se guardarán copias de todos los correos electrónicos que involucren entradas o salidas de datos del Fichero, en directorios protegidos y bajo el control del responsable citado. Se mantendrán copias de esos correos durante al menos dos años. También se guardará durante un mínimo de dos años, en directorios protegidos, una copia de los ficheros recibidos o transmitidos por sistemas de transferencia de ficheros por red, junto con un registro de la fecha y hora en que se realizó la operación y el destino del fichero enviado.

8.1.4 Cuando los datos del Fichero vayan a ser enviados por correo electrónico o por sistemas de transferencia de ficheros, a través de redes públicas o no protegidas, se recomienda que sean encriptados de forma que solo puedan ser leídos e interpretados por el destinatario.

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

## 9. Procedimientos de respaldo y recuperación

La seguridad de los datos personales del Fichero no sólo supone la confidencialidad de los mismos sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos del Fichero.

9.1.1. 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.

9.1.2. 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.

9.1.3. 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 el Anexo G.

9.1.4 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.

9.1.5. Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en el Reglamento.

## 10. Controles periódicos de verificación del cumplimiento

La veracidad de los datos contenidos en los anexos de este documento, así como el cumplimiento de las normas que contiene deberán ser periódicamente comprobados, de forma que puedan detectarse y subsanarse anomalías.

10.1.1. El responsable de seguridad del Fichero comprobará, con una periodicidad

al menos trimestral, que la lista de usuarios autorizados del Anexo F 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 o administradores 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.

10.1.2 Se comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación de Fichero según lo estipulado en el apartado 8 de este documento.

10.1.3 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.

10.1.4 El responsable de seguridad, verificará, con periodicidad al menos trimestral, el cumplimiento de lo previsto en los apartados 7 y 8 de este documento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.

10.1.5 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 que se produjeron, adoptar las medidas correctoras que limiten esas incidencias en el futuro.

10.1.6 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.

10.1.7 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.

- 10.1.8** El responsable de seguridad se encargará de revisar periódicamente la información de control registrada y eleborará un informe de las revisiones relaizadas y los problemas detectados al menos una vez al mes.
- 10.1.9** Los resultados de todos estos controles periódicos, así como de las auditorías serán adjuntadas a este documento de seguridad en el Anexo J.

## **Anexo A.      Documentos de Notificación y Decretos**

Documento de Notificación a la Agencia de Protección de Datos de Registro del Fichero.

*Se adjuntará aquí una copia del documento de notificación de la creación, y en su caso de las posibles modificaciones del Fichero.*

*En este mismo apartado se recojerá una copia de la publicación de la disposición de creación, y si procede de las modificaciones.*



## **Anexo B.      Descripción detallada de la estructura del Fichero o la Base de Datos.**

*La descripción contendrá al menos los siguientes aspectos:*

*Ubicación física del Fichero, tipo de soporte, servidor, nombre del área o directorio etc...*

*Descripción lógica, archivos o tablas, registros o tuplas, campos o columnas, así como el formato, descripción y relaciones entre los mismos.*

*Si se realizan pruebas con datos reales , se relacionaran estos ficheros de prueba, indicando el nombre y descripción de los mismos y procedimiento previsto para el borrado físico de estos datos.*

*Gestor de base de datos, mecanismos de recuperación Y mecanismos del registro de accesos.*

## **Anexo C. Descripción del sistema informático de acceso al fichero.**

Descripción del Sistema Informático de acceso al Fichero

*El sistema informático o aplicación de acceso al fichero es el conjunto de programas, específicamente diseñados para el caso o de propósito general, con los que normalmente se accede para consultar o actualizar los dato del Fichero.*

*La descripción deberá al menos contener los siguientes datos:*

*Nombre de la aplicación*

*Si se trata de un paquete o producto estándar del mercado o de unos programas expresamente diseñados para ese propósito.*

*Quién y en que fecha se programó.*

*Responsables del mantenimiento.*

*Tipo de control de acceso si lo tiene, indicando si se limita el numero de intentos fallidos de acceso al sistema y si se guarda en un fichero auxiliar la historia de estos intentos.*

*Tipo de procedimientos de histórico de operaciones (logging) y de recuperación, si los tiene.*

## **Anexo D. Entorno de Sistema Operativo y de Comunicaciones del Fichero**

Entorno de Sistema Operativo y de Comunicaciones del Fichero  
(a ser cumplimentado por el administrador del sistema)

*Deberá contener al menos los siguientes datos y aspectos:*

### **Sistema operativo**

*Nombre y versión*

*Fabricante*

*Características generales (monopuesto, multiusuario, compartición de ficheros u otros recursos, etc..)*

*Control de acceso, características*

*Archivos de logging y procedimientos de recuperación propios del sistema.*

*Responsables del mantenimiento*

### **Entorno de comunicaciones (si lo tuviese)**

*Tipo de red local (Ethernet, otras), ámbito y extensión.*

*Si existe conexión con otras redes locales o WAN, indicar el tipo de conexión (permanente, esporádica, etc..), a través de redes públicas como Internet o con conexiones privadas etc..*

*Hay compartición de recursos y archivos ?. Si es así indicar que tipo de sistema de red es*

*utilizado, sus límites y alcance.*

*Controles de acceso desde la red al sistema del Fichero.*

### **Sistema de cifrado utilizado en la transmisión de datos**

## **Anexo E.      Locales y equipamiento**

Locales y equipamiento de los centros de tratamiento y almacenamiento de las copias de respaldo y recuperación.

### **Locales**

*Descripción de la ubicación física*

*Tipo de acceso: Se especificara el tipo de control de acceso*

*Sistemas de continuidad*

*Equipamiento; armarios ignífugos, etc*

### **Puestos de Trabajo**

*Descripción Equipos: Servidores, equipos, Impresoras*

*Relación de puestos de trabajo*

## **Anexo F. Personal autorizado para acceder al Fichero**

### **RESPONSABLE DEL FICHERO**

<b>Nombre y apellidos</b>	<b>Cargo</b>	<b>Alta</b>	<b>Baja</b>

### **RESPONSABLE DE SEGURIDAD**

<b>Nombre y apellidos</b>	<b>Cargo</b>	<b>Alta</b>	<b>Baja</b>





## **Anexo G. Procedimientos de control y seguridad**

Contendrá al menos los procedimientos siguientes :

Procedimiento de asignación y cambio de contraseñas.

Procedimiento de respaldo y recuperación.

Procedimiento de gestión de soportes:

Constará al menos de los siguientes apartados

- Identificación de etiquetas
- Inventario de soportes
- Lugar de almacenamiento
- En el caso de reutilización o eliminación de soportes grabados con datos del fichero se indicará el método utilizado para el borrado físico de estos datos.

Se adjunta impreso de inventario de soportes y formularios de inscripción para registrar en el Libro de entradas y salida de soportes.

Entrada y salida de datos por red :

Se especificará

- Cuenta de correo
- Responsable de transferencias electrónicas

Procedimiento de distribución de soportes.

Se describirá el sistema utilizado para el cifrado de datos.





## **SALIDA DE SOPORTES**

Cualquier salida de soportes fuera de los locales donde esta ubicado el fichero deberá ser autorizada por el responsable del fichero de acuerdo con el documento que se adjunta.

El responsable del fichero mantendrá un Libro en el que registrará las salidas de soportes, cuyos asientos estarán constituidos por los documentos de autorización de salida debidamente cumplimentados.

La persona responsable de la entrega de soportes estará debidamente autorizada por el responsable del fichero.

# REGISTRO Y AUTORIZACIÓN DE SALIDA DE SOPORTES

Fecha y hora de salida del soporte

SOPORTE	
Tipo de soporte y número	
Contenido	
Ficheros de donde proceden los datos	
Fecha de creación	

FINALIDAD Y DESTINO	
Finalidad	
Destino	
<b>Destinatario</b>	

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	

AUTORIZACIÓN	
<b>Persona responsable de la entrega</b>	
Persona que autoriza	
Cargo / Puesto	
Observaciones	
Firma	

## **ENTRADA DE SOPORTES**

El responsable del fichero mantendrá un Libro en el que registrará las entradas de soportes cuyos asientos estarán constituidos por los datos recogidos en el formulario que se adjunta.

La persona responsable de la recepción de soportes estará debidamente autorizada por el responsable del fichero.

## REGISTRO DE ENTRADA DE SOPORTES

Fecha y hora de entrada de soporte

SOPORTE	
Tipo de soporte y número	
Contenido	
Fecha de creación	

ORIGEN Y FINALIDAD	
Finalidad	
Origen	

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	

AUTORIZACIÓN	
Persona responsable de la recepción	
Cargo / Puesto	
Observaciones	
Firma	

## **Anexo H.      Funciones y obligaciones del personal**

### **FUNCIONES DEL 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 afecten al desarrollo de sus funciones.

Designará al responsable de seguridad que figura en el Anexo F.

### **FUNCIONES DEL RESPONSABLE DE SEGURIDAD**

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

### **CLASIFICACIÓN DEL PERSONAL DE ADMINISTRACIÓN O PERSONAL INFORMÁTICO**

Se distinguen dos situaciones diferentes, que condicionan el tipo de personal que tiene acceso al fichero en cada caso:

- Producción habitual, sin incidencias técnicas. Explotación diaria.
- Errores, cortes, incidencias técnicas de cualquier tipo que detienen la producción.

#### **PERSONAL AUTORIZADO EN PRODUCCIÓN HABITUAL**

En el primer caso, 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 a la intervención, dejando constancia de ello, identificando al personal técnico, anotándolo en le Registro de Incidencias.

### **FUNCIONES DE LOS 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 o personas. Estas categorías son:

- Administradores (Red, Sistemas operativos y Bases de Datos). Serán los responsables de los máximos privilegios y por tanto de máximo riesgo de que una actuación errónea pueda afectar al sistema. Tendrán acceso al software (programas y datos) 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 precisa de dicho acceso.
- Mantenimiento de los sistemas y aplicaciones. Personal responsable de la resolución de incidencias que puedan surgir en el entorno hardware/software de los sistemas informáticos o de la propia aplicación de acceso al Fichero.
- Cualquier otro que la organización establezca.

## **OBLIGACIONES DEL RESPONSABLE DEL FICHERO**

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 utilizar.

Deberá mantenerlo actualizado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo, según los artículos 8 y 9 de la Normativa de Seguridad.

Deberá adecuar en todo momento el contenido del mismo a las disposiciones vigentes en materia de seguridad de datos.

**Deberá designar uno o varios responsables de seguridad.**

### **Entorno de Sistema Operativo y de Comunicaciones**

- 5.3.1 El responsable del Fichero aprobará o designará al administrador que se responsabilizará del sistema operativo y de comunicaciones que deberá estar relacionado en el Anexo F.
- 5.3.2 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**

- 5.4.1 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.
- 5.4.2 Asimismo cuidará que todos los usuarios autorizados para acceder al Fichero, relacionados en el Anexo F, 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**

- 5.5.1 Sólo las personas relacionadas en el Anexo F, podrán tener acceso a los datos del Fichero.

## Gestión de soportes

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

## Entrada y salida de datos por red

- 8.1.1 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.

- 9.1.4 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

- 10.1.5 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 que se produjeron, poner las medidas correctoras que limiten esas incidencias en el futuro.
- 10.1.6 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.
- 10.1.9 Los resultados de todos estos controles periódicos, así como de las auditorías serán adjuntadas a este documento de seguridad en el Anexo J.

## OBLIGACIONES DEL 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

- 6.1.1 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 registren 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

- 10.1.1. El responsable de seguridad del Fichero comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados del Anexo F 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 o administradores 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.
- 10.1.2 Se comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación de Fichero según lo estipulado en el apartado 8 de este documento.
- 10.1.3 A su vez, y también con periodicidad al menos trimestral, 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 dichos anexos.
- 10.14 El responsable de seguridad, verificará, con periodicidad al menos trimestral, el cumplimiento de lo previsto en los apartados 7 y 8 de este documento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.
- 10.15 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 que se produjeron, poner las medidas correctoras que limiten esas incidencias en el futuro.
- 10.1.6 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.
- 10.1.7 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.
- 10.1.8 El responsable de seguridad se encargará de revisar periódicamente la información de control registrada.
- 10.1.9 Los resultados de todos estos controles periódicos, así como de las auditorías serán adjuntadas a este documento de seguridad en el Anexo J.

## OBLIGACIONES QUE AFECTAN A TODO EL PERSONAL

### Puestos de trabajo

- 5.2.1 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.
- 5.2.2 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.

- 5.2.3 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.
- 5.2.4 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.
- 5.2.5 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.
- 5.2.6 Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser cambiada bajo autorización del responsable de seguridad o por administradores autorizados del anexo F.

### **Salv guarda y protección de las contraseñas personales**

- 5.5.2 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 registrarla como incidencia y proceder a su cambio.

### **Gestión de incidencias**

- 6.1.1 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.
- 6.1.2 El conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.

### **Gestión de soportes**

- 7.1.1 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 o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.
- 7.1.2 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.
- 7.1.3 Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso del Fichero que no estén por tanto relacionadas en el Anexo F.
- 7.1.5. Cuando la salida de datos del Fichero se realice por medio de correo electrónico los envíos se realizarán, 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 quien iban dirigidos y la información enviada.

**7.1.6.** Cuando los datos del Fichero 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 solo puedan ser leídos e interpretados por el destinatario.

**7.1.8.** Se deberán registrar mediante correo electrónico o transferencia de datos por red, de forma que se pueda siempre identificar su origen, tipo de datos, 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**

5.3.3 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 F.

5.3.4 En la norma anterior se incluye cualquier medio de acceso en bruto, es decir 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 F.

5.3.5 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.

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

5.3.7 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**

5.4.3 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.

**5.4.4.** 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 clave erróneas que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos.

**5.4.5.** 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 mismo Fichero, y se deberán relacionar esos ficheros de prueba en el Anexo B.

## Salvaguarda y protección de las contraseñas personales

- 5.5.5 Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el Anexo G. Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas, y será responsabilidad del administrador del sistema.
- 5.5.6 El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

## Procedimientos de respaldo y recuperación

- 8.1.1 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.
- 8.1.2 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.
- 8.1.3 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 el Anexo G.
- 8.1.4 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

- 10.1.1. El responsable de seguridad del Fichero comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados del Anexo F 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 o administradores 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.
- 10.1.2 Se comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación de Fichero según lo estipulado en el apartado 8 de este documento.
- 10.1.3 A su vez, y también con periodicidad al menos trimestral, 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 dichos anexos.

- 10.1.4 El responsable de seguridad, verificará, con periodicidad al menos trimestral, el cumplimiento de lo previsto en los apartados 7 y 8 de este documento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.
- 10.1.6 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.
- 10.1.7 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.
- 10.1.8 El responsable de seguridad se encargará de revisar periódicamente la información de control registrada,
- 10.1.9 Los resultados de todos estos controles periódicos, así como de las auditorías serán adjuntadas a este documento de seguridad en el Anexo J.

## **Anexo I. Procedimiento de Notificación y gestión de Incidencias**

Procedimiento de Notificación y gestión de incidencias

*Se describirá el procedimiento de notificación y gestión de incidencias*

*En la notificación se hará constar :*

*Tipo de incidencia*

*Fecha y hora en que se produjo*

*Persona que realiza la notificación*

*Persona a quien se comunica*

*Efectos que puede producir la incidencia*

*Descripción detallada de la misma*

*Si se trata de una recuperación de datos se incluirá además :*

*Autorización del responsable del fichero*

*Procedimientos realizados*

*Persona que realizó el proceso*

*Datos restaurados*

*Datos grabados manualmente*

*Se adjunta el impreso de notificación manual que podrá ser utilizado para la notificación de incidencias*

Cuando ocurra una incidencia, el usuario o administrador deberá registrarla en el Libro de Incidencias o comunicarla al Responsable de seguridad para que a su vez proceda a su registro.

Se mantendrán las incidencias registradas de los 12 últimos meses.

A continuación se adjunta el impreso de notificación manual que podrá ser utilizado para la notificación de incidencias.

## Impreso de notificación de incidencias

Incidencia N°:  _____  ( Este número será rellenado por el Responsable de seguridad)	
Fecha de notificación: /_/_/___/___/	
Tipo de incidencia:	
Descripción detallada de la incidencia:	
Fecha y hora en que se produjo la incidencia:	
Persona(s) a quien(es) se comunica:	
Efectos que puede producir: (En caso de no subsanación o incluso independientemente de ella)	
<b>Recuperación de Datos :</b> ( A rellenar sólo si la incidencia es de este tipo)	
<b>Procedimiento realizado:</b>	
<b>Datos restaurados:</b>	
<b>Datos grabados manualmente:</b>	
<b>Persona que ejecutó el proceso:</b>	
<b>Firma del Responsable del fichero:</b>	
<b>Fdo:</b> _____	
Persona que realiza la comunicación: Fdo.: _____	

## **Anexo J. Controles periódicos y auditorías**

*Contendrá los resultados de los controles periódicos descritos en el apartado 10 y de las auditorías realizadas*



**Anexo K.      Modificaciones introducidas en las revisiones  
de este documento:**

<b>Versión</b>	<b>Fecha</b>	<b>Actualizaciones</b>