

Documento de Seguridad relativo a ficheros de Datos de Carácter Personal

Fichero afectado:

N. ° Inscripción

NOMBRE DEL FICHERO

Fecha última revisión del documento	
Versión	

Índice

1. Objeto del documento	2
2. Ámbito de aplicación	3
3. Definiciones	4
4. Recursos protegidos	7
5. Funciones y obligaciones del personal	8
6. Normas y procedimientos de seguridad	9
7. Gestión de incidencias	15
8. Gestión de soportes	16
9. Procedimientos de respaldo y recuperación	17
ANEXOS	18
Anexo A. Documentos de Notificación	19
Anexo B. Descripción detallada de la estructura lógica del Fichero o la Base de Datos	21
Anexo C. Entorno Lógico del Fichero	23
Anexo D. Entorno hardware, software y de comunicaciones del fichero	26
Anexo E. Localizaciones de acceso físico a los datos	29
Anexo F. Personal autorizado para acceder al Fichero	30
Anexo G. Funciones y obligaciones del personal	31
Anexo H. Procedimiento de Notificación y Gestión de Incidencias	34
Anexo I. Procedimiento de Gestión de soportes	36
Anexo J. Procedimientos de backup y recuperación de datos	38

1. Objeto del documento

El presente documento responde a las obligaciones establecidas en los artículos 8 y 15 del *Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal* (en adelante, RMS) que obliga al establecimiento y documentación, por parte de entidades públicas y privadas, de las medidas técnicas, legales y organizativas establecidas en la normativa sobre protección de datos de carácter personal para garantizar la seguridad del entorno de tratamiento de dichos datos.

Este documento se aplica al siguiente Fichero:

.....

Figura debidamente inscrito y actualizado en el Registro General de Protección de datos de la Agencia Española de Protección de Datos (APD), según consta en el documento que se adjunta como [Anexo A](#).

Atendiendo a las condiciones descritas en el artículo 4 del RMS, el nivel de seguridad aplicable a los datos del mismo es el nivel básico, según se describen en los artículos 8 a 14 de dicha norma.

Se puede encontrar una **descripción funcional** del Fichero dividida en campos y registros, así como una descripción general de la finalidad y usos del mismo en el [Anexo B](#).

Dicha descripción especifica los datos que se recogen de los afectados y que en última instancia se almacenan en el Fichero, y por lo tanto determinan el nivel de seguridad del mismo. Cualquier **modificación** realizada sobre dicha estructura de datos deberá ser revisada y permitida por el Responsable del Fichero, ya que puede conllevar un cambio del nivel de seguridad del mismo.

2. **Ámbito de aplicación**

Este documento ha sido elaborado bajo la responsabilidad de la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo descrita en el **Apartado 1** del Documento de Notificación de Inscripción del Fichero en la Agencia de Protección de Datos adjunto en el [Anexo A](#), denominada como **Responsable del Fichero**.

Dicho Responsable del Fichero se compromete a implantar y actualizar esta Normativa de Seguridad de obligado cumplimiento para todo el personal con acceso a los datos protegidos o a los sistemas de información que permiten dicho acceso.

Todas las **personas que tengan acceso a los datos** del Fichero, bien a través del sistema informático habilitado para acceder al mismo, o bien a través de cualquier otro medio automatizado de acceso, deben someterse al cumplimiento de lo establecido en este documento, así como atenerse a las consecuencias en las que pudieran incurrir en caso de incumplimiento.

Este documento será entregado, para su conocimiento, a cada persona autorizada a acceder a los datos del Fichero, siendo requisito obligatorio para poder acceder a esos datos el devolver una **copia firmada** del mismo como prueba de su lectura, comprensión y aceptación.

3. Definiciones

A los efectos de este documento, siguiendo la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el RMS, se entiende por:

Datos de carácter personal	<i>Cualquier información concerniente a personas físicas identificadas o identificables</i>
Fichero	<i>Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso</i>
Tratamiento de datos	<i>Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias</i>
Responsable del fichero o tratamiento	<i>Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento</i>
Encargado del tratamiento	<i>La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento</i>
Responsable de Seguridad	<i>Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables</i>
Declarante	<i>Persona física que cumplimenta la solicitud de inscripción y actúa como mediador entre la Agencia y el responsable del fichero. No debe necesariamente coincidir con el responsable</i>
Afectado o interesado	<i>Persona física titular de los datos que sean objeto del tratamiento</i>
Procedimiento de	<i>Todo tratamiento de datos personales de modo que la</i>

disociación	<i>información que se obtenga no pueda asociarse a persona identificada o identificable</i>
Bloqueo de datos	<i>La identificación y reserva de los datos con el fin de impedir su tratamiento</i>
Consentimiento del interesado	<i>Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen</i>
Comunicación o cesión de datos	<i>Toda revelación de datos realizada a una persona distinta del interesado</i>
Fuentes accesibles al público	<i>Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación</i>
Identificación del afectado	<i>Cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona afectada</i>
Transferencia de datos	<i>El transporte de los datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional</i>
Sistema de Información	<i>Conjunto de ficheros automatizados, programas, sorteos y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal</i>
Usuario	<i>Sujeto o proceso autorizado para acceder a datos o recursos</i>
Recurso	<i>Cualquier parte componente de un sistema de información</i>
Accesos	<i>Autorizaciones concedidas a un usuario para la</i>

Autorizados	<i>utilización de los diversos recursos</i>
Identificación	<i>Procedimiento de reconocimiento de la entidad de un usuario</i>
Autenticación	<i>Procedimiento de comprobación de la identidad de un usuario</i>
Control de Acceso	<i>Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos</i>
Contraseña	<i>Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario</i>
Incidencia	<i>Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos</i>
Soporte	<i>Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos</i>
Copia de respaldo	<i>Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación</i>

4. Recursos protegidos

La protección de los datos del Fichero frente a accesos no autorizados se deberá realizar mediante el control, protección y monitorización 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- **Entorno Físico:** Los centros de tratamiento y locales donde se encuentren ubicados los ficheros o se almacenen los soportes físicos que los contengan, cuya descripción figura en el [Anexo D](#).
- 2- **Entorno a nivel de sistema informático:** 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 D](#).
- 3- **Entorno de nivel de aplicación:** Los servidores y el entorno de sistema operativo y de comunicaciones en el que se encuentra ubicado el Fichero y los sistemas informáticos o aplicaciones establecidos para acceder a los datos, descritos en el [Anexo C](#).

5. Funciones y obligaciones del personal

En relación a los artículos 9 y 16 del RMS, se definen varias categorías de personal que mantienen obligaciones y realizan tareas que afectan de forma directa (operación y manipulación) o indirecta (administración y gestión) a los datos contenidos en el Fichero, siendo posible la creación de nuevas figuras siempre y cuando se considere necesario.

Este documento es de obligado cumplimiento para todo el personal de la entidad, cuya relación deberá existir, ya se de forma directa o por medio de categorías. Las funciones y obligaciones del personal están descritas en el [Anexo G](#), siendo necesario un control estricto de las altas y bajas producidas en la misma.

A efectos de esta normativa, clasificamos al personal afectado por esta normativa en las siguientes categorías:

1. **Responsable del Fichero:** Es el encargado de diseñar, implantar y actualizar el Reglamento de Seguridad, de obligado cumplimiento para todo el personal. Es el último responsable de toda actividad relacionada con el Fichero.
2. **Administradores del sistema:** Se encargan de las tareas de administración y mantenimiento del entorno operativo (aplicaciones, equipos informáticos, sistemas operativos e infraestructura de comunicaciones) del Fichero.
3. **Usuarios del Fichero:** Personal que utiliza el sistema informático de acceso al Fichero como parte de sus labores diarias (manipulación de datos, entrada y/o salida de los mismos, etc...).

El presente documento impone una serie de medidas de obligado cumplimiento para todos ellos. Dicho documento se entregará bajo copia doble a cada usuario del Fichero, debiendo devolver una de las copias **firmada** al Responsable de Seguridad como prueba de aceptación de las obligaciones del mismo.

6. Normas y procedimientos de seguridad

6.1. Ejercicio y tutela de los derechos de los afectados

6.1.1. *Carácter Personal de los Derechos*

Los derechos de acceso a los ficheros automatizados, así como los de oposición, rectificación y cancelación de datos serán ejercidos por el afectado frente al responsable del fichero, sin otras limitaciones que las que prevén la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los datos de carácter personal.

Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos.

6.1.2. *Derecho de Acceso*

El derecho de acceso se ejercerá mediante petición o solicitud dirigida al Responsable del Fichero, formulada por escrito en el que conste el fichero o ficheros a consultar.

El afectado podrá optar por uno o varios de los siguientes sistemas de consulta del fichero, siempre que la configuración e implantación material del fichero lo permita:

- Escrito, copia o fotocopia remitida por correo.
- Fax.
- Certificado emitido por el encargado del fichero con el "Visto Bueno" del Responsable.

6.1.3. *Contenido de la Información*

La información, cualquiera que sea el soporte en que fuera facilitada, se dará en forma legible e inteligible; ésta comprenderá los datos de base del afectado y los resultantes de cualquier elaboración o proceso informático,

así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

6.1.4. Denegación del Acceso

Tratándose de datos de carácter personal registrados en ficheros de titularidad privada, únicamente se denegará el acceso cuando la solicitud sea formulada por persona distinta del afectado.

En caso de que el afectado sea incapaz, se entenderá capacitado para ejercer sus derechos quien presente representación legal bastante y suficiente, presentando conjuntamente con la pretensión, resolución judicial o escritura de poder representación con mención especial.

6.1.5. Derecho de Rectificación o Cancelación

Cuando el acceso al Fichero revele que los datos del afectado son inexactos o incompletos, inadecuados o excesivos, podrá solicitarse al Responsable del Fichero la rectificación o, en su caso, cancelación de los mismos. No obstante, cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo, aquellos se considerarán exactos siempre que coincidan con éste.

La rectificación o cancelación se hará efectiva siguiendo el procedimiento descrito en el anexo D. En el supuesto de que el Responsable del Fichero considere que no procede acceder a lo solicitado por el afectado, se lo comunicará motivadamente.

6.1.6. Bloqueo de los Datos

En los casos en que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el Responsable del Fichero procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización.

6.2. Centros de tratamiento y locales

Los locales donde se ubiquen los ordenadores que contienen el Fichero son objeto de especial protección para garantizar la disponibilidad y confidencialidad de los datos protegidos. En concreto, debido a que el Fichero que se encuentra ubicado en un servidor accedido a través de una red, se tienen en cuenta los siguientes criterios de seguridad en lo relativo al acceso físico a los mismos:

- 6.2.1. Los locales contarán 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 H](#).
- 6.2.2. El acceso a donde se encuentre el Fichero (en soporte informático o en papel) estará restringido exclusivamente al personal autorizado.

6.3. 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.

- 6.3.1. 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, ya sean de la propia empresa o externos como clientes que se encuentran en la oficina, operarios de servicios, etc.
- 6.3.2. 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 o supervisión por parte de las personas responsables de los puestos de trabajo.
- 6.3.3. 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.
- 6.3.4. 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 fueran 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.
- 6.3.5. Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero que no estén habilitados a través de la salida

corporativa a Internet. La revocación de esta prohibición será autorizada por el Responsable del Fichero, quedando constancia de esta modificación en el Libro de Incidencias.

- 6.3.6. 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.

6.4. 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 otro ordenador 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.

- 6.4.1. El sistema operativo y de comunicaciones del Fichero deberá tener un *Responsable de Seguridad* aunque es el *Responsable del Fichero*, en primer término quien ostenta esta responsabilidad, debido a que el nivel de los ficheros es básico y se ha tomado esta figura para centralizar los procedimientos que afectan a protección de datos de carácter personal.
- 6.4.2. En el caso más simple, como es que los Ficheros se encuentren ubicados 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.
- 6.4.3. Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado.
- 6.4.4. 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.

- 6.4.5. El *Responsable de Seguridad* deberá mantener la vigilancia 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.
- 6.4.6. Si la aplicación o sistema de acceso a los Ficheros utilizase usualmente ficheros temporales, ficheros de "logging", o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, el *Responsable de Seguridad* deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.
- 6.4.7. Si el ordenador en el que están ubicados los Ficheros 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 o quién determine el *Responsable del Fichero* deberá asegurarse de que este acceso no se permite a personas no autorizadas.

6.5. 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.

- 6.5.1. Los sistemas informáticos de acceso al Fichero deberán tener su acceso restringido mediante un código de usuario y una contraseña.
- 6.5.2. Todos los usuarios autorizados para acceder al Fichero 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.
- 6.5.3. 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.

6.6. Salvaguarda y protección de 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 *Responsable de Seguridad*, quién delegará a su criterio para subsanarla en el menor plazo de tiempo posible.

- 6.6.1. Sólo las personas relacionadas en el [Anexo F](#) podrán tener acceso a los datos del Fichero.
- 6.6.2. 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.
- 6.6.3. Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determine.
- 6.6.4. El archivo donde se almacenen las contraseñas estará protegido y bajo la responsabilidad del *Responsable de Seguridad*. En caso de que se almacenen las contraseñas en formato papel, se conservará bajo llave.

7. Gestión de incidencias

Una incidencia es cualquier circunstancia o hecho que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad del Fichero o de los datos, 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. Establecer un procedimiento de gestión de las mismas conforma un mecanismo imprescindible para la prevención de futuros fallos y la reacción precoz a posibles contingencias que afecten al Fichero.

- 7.1. Los administradores habilitarán un *Libro de Incidencias* a disposición de todos los *usuarios del Fichero* con el fin de que se registre en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.
- 7.2. 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 del Fichero*.
- 7.3. 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.
- 7.4. 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.

Como especifica el artículo 10 del Reglamento de Seguridad, se establece un procedimiento para la gestión y tratamiento de incidencias descrito en el [Anexo H](#).

8. 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 Cds, DVDs, discos duros externos, 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.

- 8.1. 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 área o departamento se trata o si es global y fecha de creación de la copia.
- 8.2. 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.
- 8.3. 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 F.
- 8.4. La salida de soportes informáticos que contengan datos del Fichero, fuera de los locales donde está ubicado el mismo, deberá ser expresamente autorizada por el Responsable del Fichero, utilizando para ello el documento adjunto en el anexo G, salvo cuando la salida obedezca a la política de seguridad de las copias conforme al procedimiento descrito en el anexo G.

Las normas establecidas para la gestión de soportes vienen definidas en extensión dentro del [Anexo I](#) de este documento.

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, como se establece en el Artículo 14 del RMS, unos procedimientos de respaldo y de recuperación que, en caso de fallo del sistema informático, garanticen en todo momento recuperar y en su caso reconstruir los datos contenidos en el Fichero.

- 9.1 Responsable de Seguridad obtendrá 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.
- 9.2 Con una periodicidad señalada en el [Anexo J](#), se hará una copia total del sistema del servidor y una prueba de recuperación de datos, a cargo del *Responsable de Seguridad*.
- 9.3 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 J](#).

ANEXOS

Anexo A. Documentos de Notificación

Este anexo está destinado a todos los documentos de carácter oficial que sean necesarios para justificar el presente Fichero ante la Agencia de Protección de Datos.

Se adjunta:

- **Copia del Documento de Notificación a la Agencia de Protección de Datos de Registro del Fichero.**
- **Contestación afirmativa de la inscripción del Fichero de la Agencia de Protección de Datos.**

En caso de que se proceda al cambio y/o supresión de la situación del Fichero será necesario modificar el Registro de la Agencia de Protección de Datos que incluya las modificaciones y se ajuste a los datos reales del fichero, quedando aquí documentado.

1. Documentos relacionados con la Agencia de Protección de Datos			
Nombre del Fichero:			
		Nº de Inscripción	
Documento	Fecha de Envío	Fecha de Recepción	Notas
Notificación a la APD de la inscripción del Fichero			
Confirmación de la APD del registro del Fichero			

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

En este Anexo se hace referencia a los usos y finalidades genéricos del Fichero, así como a la estructura lógica del Fichero.

El Fichero se encuentra en la dirección social:

La información del Fichero se encuentra tanto en soporte informático, como en papel.

Realización de pruebas con datos reales

No se realizan pruebas con datos reales pertenecientes al Fichero. No se realizan pruebas sobre el entorno operativo del Fichero, o en caso de realizarlas, se procede al empleo de datos ficticios.

Estructura lógica del Fichero

Con respecto a la estructura lógica del Fichero, en la siguiente tabla se indica de forma detallada los campos o registros de los que se compone. En este punto se trabaja únicamente sobre los tipos de datos recogidos, tratando la tipología de los mismos (es decir, indicar si son tablas, bases de datos, etc...) en el [Anexo C](#).

3. Estructura Lógica del Fichero		
Nombre del Fichero:		
	Nº de Inscripción	
Campo	Tipo de dato posible	Notas

Anexo C. Entorno Lógico del Fichero

Ubicación lógica del Fichero

En este Anexo se ofrece información detallada referente a la localización y a las aplicaciones y mecanismos empleados para acceder a los datos contenidos al Fichero. Se tratan en este punto tanto la localización lógica final del Fichero como datos referentes a la aplicación empleada para realizar el acceso a los datos del mismo.

4. Ubicación lógica del Fichero		
Nombre del Fichero:		
	Nº de Inscripción	
Nombre lógico del Fichero:		
Tipo de Fichero:		
Directorio en el que se encuentra:		
Nombre del equipo en el que se encuentra:		

Mecanismos de acceso al Fichero

En siguiente tabla se indican las características más importantes de la aplicación empleada para realizar los distintos tipos de acceso al Fichero, centrándose en las relativas al Reglamento de Seguridad.

5. Mecanismos de acceso al Fichero	
Nombre del Fichero:	
	Nº de Inscripción
Nombre de la aplicación de acceso al Fichero:	
Versión:	
Fabricante:	
Responsable del mantenimiento de la aplicación:	
Controles de autenticación existentes:	
Clases de accesos posibles (total, solo lectura, etc ...):	
Mecanismos de registro de accesos al Fichero:	
Mecanismos internos de recuperación de datos:	
Notas:	

Creación de Ficheros temporales

No se generan Ficheros temporales durante el transcurso de las actividades, o en todo caso los generan las propias aplicaciones de acceso a los datos, eliminándolos de forma automática una vez finalizadas las operaciones pertinentes mediante la eliminación de ficheros temporales del propio sistema operativo. Adicionalmente se eliminarán, con una frecuencia de al menos una vez por semana, los ficheros temporales del Sistema Operativo de forma manual. El encargado de dicha operación será el usuario de cada equipo con acceso al Fichero.

Anexo D. Entorno hardware, software y de comunicaciones del fichero

En el Anexo que se presenta a continuación se hace referencia tanto al entorno del propio equipo informático que contiene el equipo (tanto hardware como software) como a las características de la red de comunicaciones en la que se encuentra.

Entorno hardware del Fichero

Este apartado se refiere a la localización física del Fichero, así como a datos específicos del hardware en el que se contiene el mismo.

6. Entorno hardware del Fichero		
Nombre del Fichero:		
	Nº de Inscripción	
Nombre identificativo del equipo		
Tipo de procesador		
Modelo (si es posible)		
Fabricante		
Localización física		
Responsable del mantenimiento del hardware		
Medios de extracción de información (CD-ROM, cinta magnética, tarjeta de red)		
Notas adicionales		

Entorno software del Fichero

En este apartado se hace referencia al Sistema Operativo sobre el cual se produce el acceso a los datos contenidos en el Fichero.

7. Entorno software del Fichero	
Nombre del Fichero:	
	Nº de Inscripción
Nombre identificativo del equipo	
Sistema Operativo	
Versión	
Fabricante	
Responsable del mantenimiento del software	
Procedimientos de autenticación y control de acceso	
Posibilidad de establecer perfiles de acceso al Sistema Operativo	
Mecanismos de registro de accesos o logging	
Notas adicionales	

Entorno de Comunicaciones

Este apartado es de obligado cumplimiento en el caso de que el equipo en el que se encuentra contenido el Fichero esté conectado a cualquier tipo de red de telecomunicación (una red de área local o LAN, por ejemplo). Se describen las características de la red, así como las medidas de seguridad implantadas a este nivel.

8. Entorno de comunicaciones del Fichero	
Nombre del Fichero:	
	Nº de Inscripción
Tipo de red empleada	
Identificador del equipo en el sistema informático	
Responsable de la administración de la red	
Controles de acceso al Fichero desde otros equipos de la red	
Posibilidad de establecer perfiles de acceso al Fichero desde la red	
Mecanismos de registro de accesos o logging	
Conexiones a otras redes de telecomunicaciones	
Mecanismos de control y registro de accesos a dichas redes de telecomunicaciones	
Notas adicionales	

Acceso de datos a través de redes de telecomunicaciones

No existen conexiones a otras redes ajenas a la de la propia organización, no existiendo en los equipos auditados conexión a Internet.

Anexo E. Localizaciones de acceso físico a los datos

En este Anexo se hace referencia a las localizaciones en las que se encuentran ubicados los ficheros o se almacenen los soportes que los contengan, así como las medidas de seguridad establecidas según establece el art. 9 del RMS.

Será necesario completar la tabla siguiente para cada uno de los contenedores de Ficheros de los que se disponga en el sistema informático (al menos el equipo informático y la copia de seguridad).

9. Localizaciones en las que se opera o se almacena el Fichero	
Nombre del Fichero:	
	Nº de Inscripción
Dirección y/o nombre del edificio en el que se alberga el Fichero	
Localización física dentro del mismo	
Contenedor del Fichero (disco duro, cinta magnética, CDROM)	
Mecanismos de control de acceso físico al Fichero	
Medios existentes para prevenir problemas en el suministro eléctrico	
Medios existentes para prevenir incendios	
Notas adicionales	

Anexo F. Personal autorizado para acceder al Fichero

En este Anexo se compone una lista de las personas autorizadas a acceder al Fichero, junto con los permisos básicos establecidos.

10. Personal autorizado para acceder al Fichero			
Nombre del Fichero:			
		<i>Nº de Inscripción</i>	
<i>Nombre y apellidos</i>	<i>Cargo</i>	<i>Lectura</i>	<i>Total</i>

Anexo G. Funciones y obligaciones del personal

En este Anexo se detallan las funciones y obligaciones a las que está sujeto todo el personal que tenga cualquier tipo de relación con el Fichero. Se definen los deberes de las categorías definidas en el cuerpo del documento, así como se plantea la posibilidad de generar nuevas categorías en el caso de que se estime oportuno.

Obligaciones que afectan a todo el personal

Todo el personal que acceda al Fichero deberá cumplir las normas de seguridad que se definen a continuación:

- a) Facilitar los derechos de acceso, rectificación y cancelación a los interesados a petición del Responsable del Fichero, ajustándose al plazo de tiempo desde que se reciba la comunicación escrita hasta que se envíe la contestación escrita no supere los quince días.
- b) Cambiar su contraseña de acceso a los sistemas de información o solicitar el cambio a personal técnico cuando sea conocida, accidental o fraudulentamente por compañeros, colaboradores o administradores.
- c) Cambiar la contraseña con la periodicidad definida por la empresa, en principio mensualmente.
- d) No escribir, guardar referencia u otros de su contraseña de acceso al sistema de información. En caso de que así fuera, ninguna otra persona puede acceder al lugar donde se guarde bajo llave a tal efecto, excepto el interesado. La contraseña personal no se revelará nunca ni se dará a conocer a otras personas.
- e) No dejar información visible en la pantalla de su PC cuando abandone su puesto, aunque sea de manera temporal, si hay alguna persona ajena a la empresa.
- f) Destruir toda la información en soporte papel que pueda resultar delicada de manera que resulte ilegible antes del desechado.
- g) Hacer las copias de seguridad de toda la información introducida o generada por el sistema informático por asunción de la citada función o delegación del responsable de la misma debido a enfermedad o ausencia, con la periodicidad establecida; así como la información de carácter personal que pudieran guardar en sus propios discos duros, al menos con periodicidad mensual.

- h) Comunicar al *Responsable de Seguridad* los cambios que, a su criterio, debieran operarse en el Documento de Seguridad a raíz de los cambios tecnológicos o de los requerimientos legales.

Funciones y Obligaciones del Responsable del Fichero

El responsable del fichero es el encargado final de la seguridad del fichero y de las medidas establecidas en el presente documento. Sus deberes para con el mismo pueden exponerse en la lista siguiente:

- Administrar el fichero.
- Realizar el control del tratamiento, calidad y seguridad de los datos.
- Controlar la forma y requisitos para proceder a los ingresos y cancelaciones.
- Controlar los soportes de seguridad.
- Gestionar y dirigir los procedimientos de acceso, rectificación, cancelación y oposición de los afectados.
- Garantizar los bienes jurídicos y recursos protegidos
- Establecer, junto con el Responsable de Seguridad, los controles y auditorías necesarios para garantizar la adecuación y correcta aplicación de las medidas de seguridad.

Funciones y Obligaciones del Responsable de Seguridad

Es el encargado de coordinar y controlar las medidas de seguridad definidas en el presente documento, así como de actuar de enlace con el Responsable del Fichero siempre que sea oportuno.

El responsable de seguridad deberá cumplir las siguientes obligaciones:

1. Coordinar la puesta en marcha de las medidas de seguridad.
2. Controlar el cumplimiento de las mismas.
3. Colaborar con el Responsable del Fichero en la difusión del Documento de seguridad.
4. Habilitar 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, y tomar las medidas reactivas necesarias para preservar la seguridad del Fichero.
5. Analizar las incidencias registradas, tomando las medidas oportunas en colaboración con el Responsable del Fichero.

Funciones y Obligaciones de los Administradores del Entorno Operativo

Los Administradores son los encargados de la administración y mantenimientos de todo el entorno operativo (Sistemas Operativos, Redes y Comunicaciones, Bases de Datos, etc...) que permita un correcto acceso a los datos contenidos en el Fichero.

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.

Sus deberes específicos serán los siguientes:

1. Establecer los controles que permiten acceder al Fichero únicamente a las personas autorizadas en el [Anexo F](#) , ya sea en modo local o de forma remota.
2. Guardar en lugar seguro las copias de seguridad realizadas de los datos contenidos en el Fichero.
3. Establecer los oportunos mecanismos de registro para recoger información acerca de las posibles incidencias que afecten al Fichero, y analizar dicha información.
4. Cumplir de forma directa todos los procedimientos establecidos en este Documento, en especial atención a los referentes a:
 - a. Procedimientos de control de acceso y gestión de contraseñas.
 - b. Procedimientos de backup y recuperación de datos.
 - c. Procedimientos de gestión de soportes y entrada y salida de datos.

Funciones del personal informático

El personal informático o usuario del Fichero realizará las tareas de uso diario del Fichero, incluyendo la inserción, modificación o eliminación de los datos contenidos en el mismo. Sus funciones y obligaciones para con el Fichero se limitan a hacer un uso correcto del mismo de acuerdo con su el trabajo asignado.

En todo momento deberán conservar la confidencialidad de los datos contenidos en el Fichero, así como cumplir las obligaciones establecidas para todos los usuarios del Fichero en el presente Anexo.

Anexo H. Procedimiento de Notificación y Gestión de Incidencias

Todo el personal de la entidad tiene la **capacidad y obligación** de generar una incidencia que afecte al Fichero. Para ello deberá entrar en contacto con el *Responsable de Seguridad del Fichero*, o en su defecto, con el personal de administración informática de la entidad, para notificar la existencia de la incidencia e iniciar así los procedimientos de evaluación y respuesta oportunos. En cualquiera de los casos, se deberá comunicar la existencia de la incidencia al *Responsable de Seguridad* en cuanto sea posible.

El resto de incidencias quedarán registradas en un **Registro de Incidencias**, cuyo mantenimiento y custodia recaerá sobre el Responsable de Seguridad del Fichero. Se almacenarán dichas incidencias durante un **periodo no inferior a doce meses**. Puede encontrarse un modelo de Registro de Incidencias en la tabla que se presenta a continuación. En el caso de que se trate de una incidencia que provoque una **recuperación de datos**, se deberá contar con la autorización expresa y por escrito del Responsable del Fichero.

11. Ficha de registro de Incidencias			
Nombre del Fichero :			
Código de Incidencia (A rellenar por el Responsable de seguridad)			
Fecha y hora de notificación		Gravedad	MENOR . MEDIA . GRAVE .
Tipo de incidencia			
Persona comunicante		Cargo	
Persona comunicada		Cargo	
Descripción detallada de la incidencia			
Efectos que puede producir			
Acciones tomadas			
<i>(A rellenar sólo si la incidencia es de recuperación de datos)</i>			
Procedimiento realizado			
Datos Restaurados			
Datos grabados manualmente			
Persona que realiza la operación			
Firma del receptor de la notificación			
Fdo.: _____			
Firma del emisor de la notificación			
Fdo.: _____			

Anexo I. Procedimiento de Gestión de soportes

Este Anexo trata las cuestiones referentes a la gestión de los soportes físicos que contengan de forma parcial o total datos de carácter personal pertenecientes al Fichero.

Cada vez que se genere un nuevo soporte físico que contenga datos del Fichero, se deberá proceder a su etiquetado e inventariado de forma unívoca dentro del sistema mediante los siguientes datos:

- Fecha y hora de su almacenamiento.
- Ficheros de los que guarda copia de seguridad.

Se almacenarán los soportes que contengan datos del Fichero en lugares a los que únicamente tengan acceso las personas autorizadas en el [Anexo F](#). Los lugares y controles de acceso físico pertinentes para cumplir esta norma de seguridad se describen en el [Anexo E](#).

El *Responsable del Fichero* mantendrá un Registro de entradas y salidas con información acerca de todos los envíos y recepciones de soportes físicos relacionados con el Fichero. 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*.

12. Inventario de Soportes Físicos			
Nombre del Fichero:			
		Nº de Inscripción	
<i>Fecha y hora</i>	<i>Identificador</i>	<i>Contenido</i>	<i>Creación / Eliminación</i>

13. Salida de Soportes Físicos			
Nombre del Fichero:			
<i>Nº de Inscripción</i>		<i>Fecha</i>	

Soporte	
<i>Tipo de soporte y número</i>	
<i>Contenido</i>	
<i>Ficheros de donde proceden los datos</i>	
<i>Fecha y hora de salida del soporte</i>	
Finalidad y Destino	
<i>Finalidad</i>	
<i>Destino</i>	
<i>Destinatario</i>	
Forma de envío	
<i>Medio de envío</i>	
<i>Precauciones para el transporte</i>	
Autorización	
<i>Persona responsable de la entrega</i>	
<i>Persona que autoriza</i>	
<i>Cargo / Puesto</i>	
<i>Observaciones</i>	
<i>Firma</i>	

Anexo J. Procedimientos de backup y recuperación de datos

La salvaguarda de los datos de carácter personal contenidos en el Fichero constituye uno de los aspectos más importantes del Reglamento de Seguridad. Deberá rellenarse la tabla siguiente para completar todos los elementos del procedimiento de copias de seguridad seguido en la entidad.

Una vez realizada la copia de seguridad, se deberán cumplir a su vez los procedimientos de gestión de soportes físicos descritos en el [Anexo I](#).

Recuperación de datos

La realización de copias de seguridad tiene como último fin el poder proceder a la recuperación de los datos en el caso de producirse una corrupción o pérdida de los mismos. A continuación se describe el procedimiento necesario para proceder a la recuperación de los datos.

Se recuerda que cualquier recuperación de datos de un sistema deberá considerarse como incidencia, y verse reflejada en el Registro dispuesto a tal efecto. En el caso de que los datos que se restauren pertenezcan al Fichero, deberá contarse con la autorización por escrito del Responsable del Fichero.

15. Realización de copias de seguridad		
Nombre del Fichero:		
	Nº de Inscripción	
Personal encargado de la operación		
Ficheros de los que se guarda copia de seguridad		
Periodicidad de la copia		
Metodología de copia (total, incremental, diferencial)		
Medio físico de realización de la copia (local, red, etc ...)		
Medio físico en el que se guarda la copia de seguridad		
Tiempo durante el que se almacena la copia de seguridad		
Lugar al que se trasladan las copias de seguridad		
Periodicidad del traslado		

16. Procedimientos de restauración de datos		
Nombre del Fichero:		
	Nº de Inscripción	
Personal encargado de la operación		
Ficheros de los que se restauran los datos		
Metodología seguida		
Notas adicionales		