# 4. Medidas, normas, procedimientos, reglas y estándares de seguridad.

## 4.1. Centros de tratamiento y locales

Los locales donde se encuentran los equipos informáticos que contienen los ficheros objeto de tratamiento, deben disponer de las medidas de seguridad mínimas al objeto de garantizar la confidencialidad de los datos de carácter personal y su disponibilidad.

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

4.1.1. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

En la relación de personal autorizado, se recogen las autorizaciones y el período de validez de las mismas.

## 4.2. Puestos de trabajo

Se considera como puestos de trabajo todo ordenador personal, terminal u otro dispositivo desde el que se pueda acceder a los datos del fichero.

Cada una de las personas autorizadas tendrá asignado un puesto de trabajo desde el que acceder a los datos del fichero. El usuario asignado al puesto de trabajo, será responsable de garantizar que la información a la que accede no podrá ser visualizada o comunicada a personas no autorizadas. Cualquier dispositivo conectado al puesto de trabajo tales como impresoras o pantallas deberán de estar ubicadas de forma que se garantice la confidencialidad de la información y que ésta no pueda ser visualizada o comunicada a personas no autorizadas

El usuario responsable del puesto de trabajo, cuando finalice su turno o cuando se ausente temporalmente, deberá dejar los equipos y dispositivos en un estado que

impida el acceso o la visualización de los datos protegidos a personas no autorizadas. Esto se podrá realizar mediante un protector de pantalla, la suspensión de la sesión de trabajo o la salida del sistema y apagado del equipo. La reanudación del trabajo implicará la desactivación de la pantalla protectora, el reinicio de la sesión o el encendido del equipo con la introducción del nombre de usuario y contraseña correspondiente en cada caso.

No deberá dejar en la impresora documentos impresos en la bandeja de salida que contengan datos de carácter personal. Si la impresora es compartida con otros usuarios no autorizados para acceder a los datos de Fichero, el responsable de cada puesto de trabajo deberá retirar los documentos conforme vayan siendo impresos.

La configuración de los puestos de trabajo desde los que se tiene acceso al fichero sólo podrá ser cambiada con la autorización del Responsable del fichero, el responsable de seguridad o el administrador del sistema designado.

### 4.3. Identificación y autenticación del personal autorizado.

El responsable del fichero o tratamiento establecerá un procedimiento que garantice la correcta identificación y autenticación de los usuarios autorizados a acceder a los sistemas de información.

Los accesos a los sistemas de información se realizarán mediante un mecanismo que permita la identificación de forma inequívoca y personalizada del usuario. Cada identificación deberá pertenecer a un único usuario.

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

#### 4.3.1. Procedimiento de asignación y cambio de contraseñas.

El responsable del fichero o tratamiento o la persona con autorización delegada del responsable del fichero o tratamiento, asignará un nombre de usuario y propondrá una contraseña para cada uno de los usuarios que, tras el primer acceso, vendrán obligados a cambiarlas.

Las contraseñas deberán constar de un mínimo de 6 dígitos y con una combinación de caracteres alfanuméricos. Se deberá evitar la utilización de nombre o cifras o su combinación que sean fácilmente deducibles.

Las contraseñas se almacenarán de forma ininteligible. El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

Las contraseñas son de carácter personal e intransferible y no serán visibles en pantalla cuando son introducidas.

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

Con una periodicidad de cada 6 meses y de forma automática, se propondrá a los usuarios, que cambien su contraseña por una nueva, volviendo a quedar almacenada de forma ininteligible.

El Responsable del Fichero o el Administrador del sistema, en su caso, podrá cambiar los requisitos de acceso, las condiciones, modos sistemas y formas de tratamiento o de lectura cuando lo crea oportuno, notificando la decisión a los usuarios y dejando constancia de tal modificación en el Documento de seguridad y en el Registro de incidencias.

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 del fichero o a la persona con autorización delegada del responsable del fichero o tratamiento y subsanada en el menor plazo de tiempo posible.

En los ficheros:

- Asociados
- Voluntarios
- Cursos de Formación para Educadores

Quedará limitada la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. Tras 3 intentos fallidos de acceso quedará bloqueada la contraseña.

### 4.4. Control de acceso lógico

El RLOPD, establece que los usuarios de los sistemas de información, tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

En el Anexo Relación de personal autorizado, se incluye una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

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 la restricción y disponibilidad de recursos en la sesión del usuario con el control de acceso lógico mediante usuario y contraseña.

Queda prohibido que un usuario acceda a recursos con derechos distintos de los que ha sido autorizado.

En el caso de personal ajeno al responsable del fichero que tenga acceso a los recursos estará sometido a las mismas condiciones y obligaciones de seguridad que el personal propio, constando en el Anexo Relación de personal autorizado.

Exclusivamente la persona con autorización delegada del responsable del fichero o tratamiento podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el Responsable del Fichero.

Para el caso de nuevas altas de accesos, se comunicará al Responsable del Fichero por la persona con autorización delegada del responsable del fichero o tratamiento, con la propuesta de acceso, código de acceso y listado de las funciones del nuevo autorizado. De todo ello se deberá dejar constancia en este Documento de Seguridad en el Anexo Relación de personal autorizado.

### 4.5. Control de acceso físico

Exclusivamente el personal autorizado en este Documento de Seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información correspondientes a los ficheros siguientes:

- Asociados
- Voluntarios
- Cursos de Formación para Educadores

El personal que tiene acceso a los lugares donde se hallan instalados los equipos físicos que dan soporte a los sistemas de información que tratan los ficheros indicados, constan relacionados en el Anexo Relación de personal autorizado como personal afecto a los citados ficheros.

Para el personal del Responsable del fichero o tratamiento, distinto de los usuarios con acceso a los sistemas de información, como pueden ser de mantenimiento, limpieza, seguridad, etc., serán autorizados por el responsable de seguridad, quien expedirá autorización o credencial que acredite su acceso autorizado.

Para el personal ajeno al responsable del fichero o tratamiento, que le preste servicios sin acceso a datos personales, en el contrato de prestación de servicios deberá constar expresamente la prohibición de acceder a los datos personales y la

obligación de secreto respecto a los datos que pueda conocer con motivo de la prestación de servicios.

### 4.6. Registro de accesos

Para aquellos ficheros que contienen datos de carácter personal especialmente protegidos, clasificados con el nivel de seguridad alto:

- Asociados

Deberá registrarse cada intento de acceso, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso fue autorizado, se guardará la información que permita identificar el registro accedido.

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

El período mínimo de conservación de los datos del registro de accesos será de dos años.

El responsable de seguridad revisará al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

Este registro de accesos no será necesario cuando concurran las siguientes circunstancias:

a) El responsable del fichero o tratamiento sea una persona física.
b) El responsable del fichero o tratamiento garantice que sólo él tiene acceso y trata los datos personales.

La concurrencia de estas dos circunstancias deben de hacerse constar expresamente en este documento de seguridad.

### 4.6. Acceso a la documentación (Registro de accesos).

Para aquellos ficheros que contienen datos de carácter personal especialmente protegidos, clasificados con el nivel de seguridad alto:

- Asociados

El acceso a la documentación se limita exclusivamente al personal autorizado que consta en el Anexo Relación de personal autorizado.

Para los documentos que puedan ser utilizados por múltiples usuarios, se

establecerán mecanismos que permitan identificar los accesos realizados.

El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en este documento de seguridad.

### 4.7. Entorno de Sistema Operativo y de Comunicaciones

Al estar el fichero ubicado en un ordenador (o con funciones de servidor) con un sistema operativo determinado y poder contar con unas conexiones que le comunican con otro 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.

El sistema operativo y de comunicaciones del Fichero debe tener al menos un responsable o administrador.

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.

Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado. Esto incluye cualquier medio de acceso en bruto no elaborado o editado a los datos del Fichero que deberán estar bajo el control del administrador autorizado.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Si el ordenador en el que se ubica 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.

### 4.8. Gestión de soportes y documentos

#### 4.8.1. Etiquetado e Inventario de soportes

Los soportes que contengan datos de carácter personal, deben ser etiquetados para permitir su identificación, conocer de qué fichero se trata y el tipo de información que contienen y la fecha de creación.

Los soportes han de ser inventariados y almacenados en FEDERACIÓ D'ESCOLTISME VALENCIÀ - Sede Principal (Calle Balmes, 17), lugar restringido al

personal autorizado para ello y que consta relacionado en el Anexo Relación de personal autorizado.

El inventario de soportes y su mantenimiento se gestiona mediante la aplicación informática de gestión de protección de datos personales de la organización y puede ser impreso en cualquier momento. El inventario deberá estar permanentemente actualizado.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

La identificación de los soportes que contengan datos de carácter personal que la organización considere especialmente sensibles se podrá realizar utilizando sistemas de etiquetado que serán comprensibles y con significado para los usuarios con acceso autorizado a los citados soportes y documentos y que dificulten la identificación para el resto de personas.

4.8.2. Salida de soportes y documentos

La salida de soportes y documentos que contengan datos de carácter personal, incluídos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento, deberá ser autorizada por el responsable del fichero o la persona con autorización delegada del responsable del fichero o tratamiento o encontrarse debidamente autorizada en el documento de seguridad.

Con respecto a los documentos también se consideran incluidos en la salidad de documentos los siguientes supuestos:

- Envío por correo electrónico en el cuerpo del mensaje o como adjuntos datos de un fichero o tratamiento.
- Los faxes cuando incorporan datos de un fichero o tratamiento.
- Cualquier otro procedimiento electrónico como ftp, descargas desde la web o carpetas compartidas, etc.

Los ordenadores portátiles y los dispositivos móviles que contengan datos personales deberán de ser sometidos al mismo procedimiento de autorización para su salida de los locales en los que está ubicado el fichero.

La autorización de salida de soportes y documentos se gestiona mediante la aplicación informática de gestión de protección de datos personales de la organización y puede ser impresa la autorización.

En el caso del correo electrónico para garantizar la trazabilidad de los datos que salen materialmente del sistema de información, puede servir como registro el

propio sistema de indexación del gestor del correo electrónico.

4.8.3. Traslado de soportes y documentación

En el traslado de la documentación se adoptarán las medidas y procedimientos apropiados para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4.8.3.1. Traslado de documentación

El traslado de la documentación de los ficheros:

- Asociados

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse las medidas apropiadas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

4.8.4. Destrucción y borrado de documentos o soportes

Los documentos y soportes que vayan a ser desechados correspondientes a los ficheros:

- Asociados
- Voluntarios
- Cursos de Formación para Educadores

Aquellos soportes que se vayan a reutilizar deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables de ningún modo. No será válido el borrado lógico o rápido que impide el acceso a la información pero no la elimina físicamente hasta que ha sobrescrito sobre la misma.

Los soportes que se vayan a eliminar deberán ser borrados físicamente antes de su eliminación, que consistirá en un proceso de destrucción mecánica del soporte, trituración o incineración.

Los documentos en formato papel que vayan a desecharse, deberá procederse a su destrucción mediante la trituradora de papel. Está prohibida la reutilización de documentos en formato papel.

Los procesos de reutilización y eliminación descritos han de ser previos a la preceptiva baja de los soportes en el inventario.

4.8.5. Registro de Entrada y Salida de soportes

Deberán ser registradas las salidas y entradas de soportes correspondientes a los

ficheros:

- Asociados
- Voluntarios
- Cursos de Formación para Educadores

El registro de entrada de soportes indicará el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

El registro de salida de soportes indicará el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

El procedimiento de registro de entradas y salidas de soportes se gestiona mediante el programa por persona autorizada y puede ser impreso o no como Anexo de este documento de seguridad.

4.8.6. Gestión y distribución de soportes

La gestión y distribución de soportes que contengan datos de carácter personal de los ficheros:

- Asociados

**La identificación** de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido y que dificulten la identificación para el resto de personas.

**La distribución** de los soportes se realizará cifrando los datos que contengan o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

**Los dispositivos portátiles** cuando se encuentren fuera de las instalaciones que están bajo control del responsable del fichero, deberán cifrar los datos que contengan.

En caso que se requiera el uso de **dispositivos portátiles que no permiten el cifrado**, debe especificar el motivo de su uso y adoptar las medidas de seguridad necesarias que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

### 4.9. Ficheros temporales o copias de trabajo de documentos

Los ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponde con arreglo a lo dispuesto en el RLOPD y lo expresado en este documento.

Los ficheros temporales o copias de documentos así creados serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

Lo anterior, incluye los ficheros temporales que utilicen y generen las aplicaciones de acceso al Fichero.

Las copias de trabajo de documentos en formato papel, deberá procederse a su destrucción mediante la trituradora de papel. Está prohibida la reutilización de documentos o copias de trabajo en formato papel.

El Responsable del Fichero o, en su caso, el responsable de seguridad, deberá asegurarse de que los ficheros temporales o copias de trabajo de documentos no son accesibles por personal no autorizado.

### 4.10. Responsable de seguridad

- Asociados
- Voluntarios
- Cursos de Formación para Educadores

El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en este documento de seguridad.

Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados.

En ningún caso esta designación supone una delegación de la responsabilidad que corresponde a FEDERACIÓ D'ESCOLTISME VALENCIÀ como responsable del fichero de acuerdo con el RLOPD.

El responsable/s de seguridad desempeñará las funciones encomendadas durante el período de vigencia que se haya asignado para el cargo. Transcurrido el plazo FEDERACIÓ D'ESCOLTISME VALENCIÀ nombrará un nuevo responsable de seguridad o lo renovará por un período igual al mismo que ha desempeñado hasta ahora.

### 4.11. Transmisión de datos por redes de Telecomunicaciones

- Asociados

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

## 4.12. Copias de seguridad

Es obligatorio establecer procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Los procedimientos para la recuperación de los datos deben garantizar en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

### 4.12.1. Procedimiento de realización de copias de respaldo.

Las copias de seguridad deben de realizarse como mínimo con una periodicidad semanal, cada viernes o último día laborable de la semana. El soporte magnético que las almacena dispondrá de toda la información del sistema.

Las copias han sido planificadas de tal manera que no habrá una intervención de ningún operador para esta rutina. La misión del operador de copias tendrá como trabajo principal:

- Comprobación de la copia semanal.
- Cambio de soporte.
- Verificación de la copia semanal.

La copia se entregará al Responsable del Fichero o persona designada por éste, quien deberá entregar la más antigua que tenga, estableciendo así un sistema de rotación de soportes.

En caso de que cualquiera de las copias no se efectuara correctamente, se debería de editar el informe que genera la aplicación de backup y proceder a repetir la copia manualmente o informar al responsable del sistema.

### 4.12.2. Recuperación de datos

Los procedimientos para la recuperación de los datos deben garantizar en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existirá un procedimiento, 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 al tiempo de producirse la pérdida o destrucción.

Únicamente respecto de los ficheros parcialmente automatizados siguientes:

- Asociados
- Voluntarios
- Personal
- Proveedores
- Cursos de Formación para Educadores

Siempre que exista documentación que permita alcanzar la recuperación de los datos al estado en que se encontraban al tiempo de producirse la pérdida o destrucción, se procederá a grabar manualmente los datos quedando constancia motivada de este hecho en el registro de incidencias.

4.12.3. Verificación de los procedimientos de copia y recuperación de datos

El responsable del fichero o la persona con autorización delegada del responsable del fichero o tratamiento, verificará cada seis meses la correcta definición, funcinamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos.

4.12.4. Pruebas con datos reales

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que previamente se haya realizado una copia de seguridad y se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

De las pruebas relizadas conforme al párrafo anterior, deberá quedar constancia en el registro de incidencias.

4.12.5. Almacenamiento de las copias de respaldo

Las copias de respaldo y recuperación se encuentran almacenadas en .

4.12.6. Copia de respaldo en lugar diferente

Exclusivamente para los ficheros de nivel alto:

- Asociados

Se conservará una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir las medidas de seguridad, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

### 4.13. Criterios de archivo

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

### 4.14. Dispositivos de almacenamientos

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

#### 4.14.1. Custodia de soportes

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento indicados en el apartado anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

#### 4.14.2. Almacenamiento de la información

Exclusivamente para los ficheros de nivel alto:

- Asociados

Los armarios, archivadores u otros elementos en los que se almacenan los ficheros no automatizados con datos de carácter personal se encuentran en FEDERACIÓ D'ESCOLTISME VALENCIÀ - Sede Principal (Calle Balmes, 17), en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de

apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, se adoptarán las medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

4.14.3. Copia o reproducción

Exclusivamente para los ficheros de nivel alto:

- Asociados

La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

Las copias o reproducciones desechadas deberán ser destruidas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Las copias o reproducciones desechadas se procederá a su destrucción mediante la trituradora de papel.

## 4.15. Procedimiento de notificación, registro, gestión y respuesta ante las incidencias

4.15.1. Definición

Según viene definido en el RLOPD, una incidencia es “cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos”, es decir, a la confidencialidad, integridad y disponibilidad de los datos del fichero. Cualquier incumplimiento de la normativa del presente Documento de Seguridad se considera una incidencia.

4.15.2. Procedimiento

Todo usuario que tenga conocimiento de una incidencia será responsable del registro de la misma en el registro de Incidencias del Fichero o en su caso de la comunicación por escrito a FEDERACIÓ D'ESCOLTISME VALENCIÀ o a la persona con autorización delegada del responsable del fichero o tratamiento.

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 o tratamiento por parte de ese usuario.

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, en su caso, detectado, la persona que realiza la notificación, persona a quien se le comunica, efectos que se hubieran derivado de las misma y las medidas correctoras aplicadas.

4.15.3. Registro de incidencias

El registro de incidencias se gestiona mediante la aplicación informática de gestión de protección de datos personales de la organización, concretamente en el módulo o apartado de “gestión de incidencias”.

4.15.4. Registro de incidencias

En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten a los ficheros:

- Asociados
- Voluntarios
- Cursos de Formación para Educadores

Cuando para la resolución de la incidencia se requiera realizar una recuperación de datos, deberá consignarse, además:

- Los procedimientos realizados de recuperación de los datos.
- La persona que ejecutó el proceso.
- Los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
- Autorización para la ejecución de los procedimientos de recuperación de los datos de FEDERACIÓ D'ESCOLTISME VALENCIÀ o de la persona con autorización delegada del responsable del fichero o tratamiento.

## 4.16. Revisión del documento de seguridad

El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

El responsable del fichero o la persona con autorización delegada del responsable

del fichero o tratamiento, junto con el responsable de seguridad, si es el caso, mantendrán un reunión con carácter ordinario cada seis meses y con carácter extraordinario cada vez que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos, con el objetivo de coordinar los cambios a introducir en el Documento de Seguridad, elevando conclusiones al responsable del fichero o tratamiento.

### 4.17. Procedimiento de control del cumplimiento

- Asociados
- Voluntarios
- Cursos de Formación para Educadores

El RLOPD dispone que deben de establecerse controles periódicos para verificar el cumplimiento de lo dispuesto en el Documento de Seguridad.

Estos controles se pueden establecer por ejemplo semestralmente. El semestre que coincida con la auditoría no se efectuará el control de cumplimiento.

- Verificar el inventario de hardware y software.
- Cumplimiento de la política general de seguridad.
- Registro de incidencias.
- Variaciones en el inventario de ficheros.
- Cumplimiento de la política de protección de datos.
- Verificar clasificación de datos.
- Comprobar configuración del sistema.
- Comprobar la relación de personal y accesos autorizados.
- Verificar procedimiento de gestión de soportes.
- Verificación procedimientos de identificación y autenticación.
- Se cumple el proceso de copias de respaldo y recuperación.
- Verificar prestaciones de servicios con acceso y sin acceso a datos.
- Verificar contratos de encargo de tratamiento.
- Verificar contratos de confidencialidad prestación servicios sin acceso a datos
- Variaciones en la legislación.

### 4.18. Auditoría

- Asociados
- Voluntarios
- Cursos de Formación para Educadores

Los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa, que verifique el cumplimiento del RLOPD.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

La ubicación del informe de auditoría quedará acompañado al Documento de Seguridad, indicando la fecha de su realización y el autor.

# 5. Funciones y obligaciones del personal.

Todas las personas que tienen acceso a los datos del Fichero se encuentran obligadas por ley a cumplir lo establecido en este documento. El personal afectado por esta normativa lo podemos clasificar como sigue:

1. **Administradores**, disponen de los máximos privilegios y están encargados de administrar o mantener el entorno operativo del Fichero.

2. **Personal Informático**, encargados de mantener los sistemas de información y resolver las incidencias en máquinas y programas.

3. **Usuario**, Todo sujeto autorizado para acceder a datos o recursos.

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información han de estar claramente definidas y documentadas. En el Anexo Relación de personal autorizado se relacionan.

## 5.1. Funciones y obligaciones con carácter general

Todo el personal interno o externo de la empresa que acceda a los datos de carácter personal, está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar al responsable del fichero o al responsable de seguridad las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en su Capítulo IV.

Todas las personas deberán guardar el debido secreto y confidencialidad de los datos personales que conozcan en el desarrollo de su trabajo.

## 5.2. Funciones y obligaciones 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. El responsable del fichero, 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.

El responsable del Fichero es FEDERACIÓ D'ESCOLTISME VALENCIÀ en la persona de Begoña Cruz González en calidad de representante legal de la empresa.

### 5.2.1. Ámbito

Decide sobre la finalidad, contenido, usos y aplicaciones del fichero: Asociados, Voluntarios, Personal, Proveedores, Cursos de Formación para Educadores y responde de su legalidad y legitimación, de acuerdo con lo dispuesto en la LOPD, en la Directiva de la C.E. 46/95, el RLOPD y las instrucciones y recomendaciones de la Agencia de Protección de Datos y normativa relacionada. Es el responsable de cumplir los requisitos exigidos en la legislación vigente para garantizar los derechos de los afectados (acceso, oposición, rectificación y cancelación). Responde frente al afectado, frente a terceros y frente a la Administración de todos los daños y perjuicios que se deriven del mal uso de los datos y de los ficheros.

El uso antirreglamentario de los ficheros o de los datos está tipificado en el artículo 44 de la LOPD. El responsable del fichero viene obligado a la asunción de las medidas de seguridad previstas en el artículo 9 del mismo cuerpo legal, desarrolladas en el RLOPD. El incumplimiento de las medidas previstas, comportará las sanciones descritas en el artículo 45 de la LOPD.

Coordinará la puesta en marcha de las medidas de seguridad y cuidará de la difusión del Documento de seguridad, controlando su cumplimiento por los usuarios.

### 5.2.2. Finalidad del Fichero

El Responsable del Fichero decide sobre la finalidad del tratamiento.

### 5.2.3. Usos del Fichero

El uso es confidencial e intransferible. Los datos en él contenidos serán utilizados por FEDERACIÓ D'ESCOLTISME VALENCIÀ, a través de su personal designado propio o externo, cumpliendo en todo momento las medidas de seguridad y los requisitos exigidos para su legitimación y legalidad en su tratamiento.

### 5.2.4. Funciones

- Decidir sobre la finalidad, contenido y uso del tratamiento.
- Autorizar:
  - La ejecución de tratamientos de datos de carácter personal fuera de los locales de la ubicación del fichero.
  - La salida de soportes informáticos que contengan datos de carácter personal fuera de los locales de la ubicación del fichero.
- Realizar el control del tratamiento, calidad y seguridad de los datos.
- Controlar la gestión de soportes informáticos que contienen datos de carácter personal.
- Gestionar y dirigir los procedimientos de acceso, rectificación, cancelación y oposición de los afectados y resolver:
  - La petición de acceso en el plazo de un mes.
  - La petición de rectificación o cancelación en el plazo de 10 días.

- Proceder al bloqueo de los datos en los casos en que, siendo procedente su cancelación, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado.
- Elaborar el Documento de Seguridad.
- Encargarse de que exista una relación actualizada de usuarios con acceso autorizado a los sistemas de información.
- Establecer los procedimientos de identificación y autenticación para dicho acceso.
- Establecer los mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
- Establecer los procedimientos de realización de copias de respaldo y recuperación de datos.
- Encargarse de forma directa o por delegación del cumplimiento efectivo de la normativa sobre Protección de Datos en la organización, garantizando la difusión y conocimiento de este Documento entre todo el personal.
- Implantar las medidas de seguridad establecidas en este documento.
- Mantener este Documento actualizado en todo momento, debiendo revisarse siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo y adecuar su contenido a las disposiciones vigentes en materia de seguridad de datos.
- Garantizar los bienes jurídicos y recursos protegidos.
- Designar a uno o varios responsables de seguridad.

### 5.2.5. Obligaciones

#### 5.2.5.1. Legalización de ficheros

Rellenar los formularios oficiales y presentarlos en el Registro General de la Agencia Española de Protección de Datos para su registro. Comprobar su inscripción y obtención del número de registros en la forma descrita en los reglamentos e instrucciones de la Agencia Española de Protección de Datos.

Proceder a la notificación en forma reglamentaria ante la Agencia de Protección de Datos de cualquier modificación en el fichero notificado así como de la cancelación de la inscripción llegado el caso.

#### 5.2.5.2. Legitimación para el tratamiento de los datos

Cumplir todos los requisitos legales y reglamentarios para **obtener el consentimiento del afectado** para que los datos puedan ser ingresados, tratados, guardados, transmitidos, manipulados, cedidos y/o cancelados por el responsable del fichero o aquel a quien se haya destinado para cada forma de tratamiento.

Velar para que la recogida de datos de carácter personal se realice cumpliendo con todos los requisitos legales, especialmente el derecho de información y la obtención del consentimiento inequívoco del afectado.

En la documentación de la aplicación de gestión de protección de datos de la organización, se incluyen diversos modelos de cláusulas, a modo de ejemplo, que deberán ser implementados en cada caso, o revisadas los que en la actualidad se están utilizando y adaptarlos a las exigencias de la LOPD.

5.2.5.3. Control de las entradas en el Fichero

Consiste en mantener el sistema de archivo de las fichas o formularios con los datos personales del afectado y su consentimiento, bajo control exclusivo del Responsable del Fichero y del Encargado del Fichero.

Sólo se incluirán en el fichero los datos obtenidos mediante las fichas o formularios que estén amparados por la firma del interesado. En la documentación de la aplicación de gestión de protección de datos de la organización vienen diversos modelos que deberán adaptarse previamente.

5.2.5.4. El mantenimiento actualizado de los datos

Los datos de carácter personal deben de estar siempre actualizados, deben ser exactos y responder con veracidad a la situación actual del afectado. Si los datos registrados son o devienen inexactos en todo o en parte, o incompletos han de ser cancelados o sustituidos de oficio por los correspondientes rectificados o completados. Tampoco han de mantenerse datos que hayan dejado de ser necesarios o pertinentes para la finalidad para la que fueron recabados.

5.2.5.5. Encargados de tratamiento externos

En el caso de que existan encargados de tratamiento externos, formalizar la relación con éstos de acuerdo con lo establecido en el Artículo 12 de la LOPD. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito.

5.2.5.6. Entorno de Sistema Operativo y de Comunicaciones

Designar al administrador que se responsabilizará del sistema operativo y de comunicaciones que deberá estar relacionado en el Anexo Relación de personal autorizado.

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.

5.2.5.7. Sistema Informático o aplicaciones de acceso al Fichero

Se encargará de que los sistemas informáticos de acceso al Fichero tengan su

acceso restringido mediante un código de usuario y una contraseña.

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

5.2.5.8. Salvaguarda y protección de las contraseñas personales

El responsable del fichero deberá mantener actualizada la relación de usuarios con acceso autorizado al sistema de información y establecer los procedimientos de identificación y autenticación para este acceso.

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

Sólo las personas relacionadas en el Anexo Relación de personal autorizado, podrán tener acceso a los datos del Fichero.

5.2.5.9. Gestión de incidencias

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 cada caso.

5.2.5.10. Gestión de soportes

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.

5.2.5.11. 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.

Autorizar por escrito la ejecución de los procedimientos de recuperación de datos, descrito en el subapartado *Recuperación de datos* del apartado 4 de este documento.

5.2.5.12. Auditoría

Someter los sistemas de información e instalaciones de tratamiento de datos a una

auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos cada **dos años**.

Atender las conclusiones que el Responsable de Seguridad le comunique con motivo del informe de auditoría y adoptar las medidas correctoras adecuadas.

Tener a disposición de la Agencia Española de Protección de Datos los informes de auditoría.

## 5.3. Funciones y obligaciones del responsable de Seguridad

- Asociados
- Voluntarios
- Cursos de Formación para Educadores

### 5.3.1. Funciones

Coordinar y controlar las medidas definidas en el Documento de Seguridad. Analizar los informes de Auditoría

Controlar los mecanismos que permiten el control de accesos.

### 5.3.2. Obligaciones

Elevar al Responsable del Fichero las conclusiones del análisis del informe de auditoría.
Obligación de guardar secreto de los datos de carácter personal que pueda conocer, así como sobre controles y aspectos sensibles de la organización y cualquier información que haya tenido acceso como Responsable de Seguridad, incluso después de haber causado baja en la entidad.
Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal.
Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.

Revisar periódicamente la información de control registrada.
Efectuar un informe mensual de las revisiones efectuadas.

## 5.4. Funciones y obligaciones que afectan a todo el personal

### 5.4.1. Con carácter general

Tratar los datos de carácter personal de conformidad con lo que se establece en la legislación vigente y en este documento de seguridad, accediendo al fichero

únicamente cuando sea necesario para el desarrollo de sus funciones.

Mantener el secreto profesional respecto de los datos de carácter personal que se encuentran en el fichero y custodiarlos. Esta obligación perdurará después de finalizar las relaciones con el responsable del fichero.

Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal.

Cumplir lo dispuesto en la normativa interna vigente en cada momento.

Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento, que podrían derivar en sanciones.

Comunicar al responsable del fichero, en el mismo día, cualquier solicitud de ejercicio por parte de los afectados de los derechos de acceso, rectificación, cancelación y oposición.

### 5.4.2. Puestos de trabajo

El usuario autorizado será el responsable de su puesto de trabajo, garantizando que la información que disponga o muestre su equipo no podrá ser accesible o visible por personas no autorizadas.

Procurará que la disposición de pantallas e impresoras u otros dispositivos de su puesto de trabajo se ubiquen de forma que garanticen la confidencialidad y no sea accesible o visible su contenido por peronas no autorizadas.

Al abandonar su puesto de trabajo, aun temporalmente, deberá dejarlo en un estado que impida el acceso o la visualización de los datos protegidos, mediante un protector de pantalla o la salida del sistema y apagado del equipo. La reanudación del trabajo implicará la desactivación de la pantalla protectora o el encendido del equipo con la introducción del nombre de usuario y contraseña correspondiente en cada caso.

No deberá dejar en la impresora documentos impresos en la bandeja de salida que contengan datos protegidos. Si la impresora es compartida con otros usuarios no autorizados para acceder a los datos de Fichero, el responsable de cada puesto de trabajo deberá retirar los documentos conforme vayan siendo impresos.

La configuración de los puestos de trabajo desde los que se tiene acceso al fichero sólo podrá ser cambiada con la autorización del Responsable del Fichero, el Responsable de Seguridad o el Administrador del sistema designado.

### 5.4.3. Salvaguarda y protección de las contraseñas personales

Todo usuario es responsable de mantener la confidencialidad de su contraseña. Si la contraseña es conocida por otra persona, el usuario, deberá registrarlo como incidencia y notificarlo al Responsable del Fichero o al Responsable de Seguridad, para proceder a su cambio.

### 5.4.4. Gestión de incidencias

El usuario que tenga conocimiento de una incidencia deberá de ponerlo en conocimiento del Responsable del Fichero o al Responsable de Seguridad y registrarla siguiendo el procedimiento establecido para el registro de incidencias.

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.

### 5.4.5. Gestión de soportes

Los soportes informáticos que contengan datos del Fichero, han de estar claramente identificados con una etiqueta externa que indique el fichero, tipo de datos y fecha de creación.

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

Los soportes que contengan datos del fichero deberán ser almacenados en lugares a los que no tengan acceso personas que no figuren relacionadas en el Anexo Relación de personal autorizado.

La salida de equipos o soportes fuera de las instalaciones requiere la autorización del Responsable del Fichero o del Responsable de Seguridad.

Seguir los procedimientos establecidos de gestión y distribución de soportes y observar las autorizaciones precisas en cada caso.

### 5.4.6. Correo electrónico

No utilizar el correo electrónico u otros medios de comunicación interna o con el exterior para transmitir mensajes que contengan o lleven adjuntos datos de carácter personal que por sus características, volumen o destinatarios puedan poner en peligro la confidencialidad o la integridad de los datos.

Atenerse a los procedimientos establecidos y observar las autorizaciones precisas.

### 5.4.7. Transferencias de ficheros

No realizar transferencias de ficheros con datos de carácter personal entre sistemas o descargas en equipos salvo en aquellos casos expresamente autorizados, y protegiendo después los contenidos para evitar la difusión o copias no autorizadas.

5.4.8. Tratamiento fuera de los locales del fichero

Proteger la confidencialidad e integridad de los datos personales de la entidad que excepcionalmente tuvieran que almacenarse o usarse fuera del lugar de trabajo: en casa del cliente, en el propio domicilio o en otras instalaciones alternativas tanto en sistemas fijos como en portátiles.

## 5.5. Funciones y obligaciones del administrador del sistema y personal informático.

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.

5.5.1. *Funciones*

**Administradores:** Tienen acceso con el máximo privilegio al software del sistema y a las herramientas necesarias para ello, así como al fichero. Resuelven las incidencias que surjan y gestionan los permisos y accesos.

**Personal Informático:** Resolver las incidencias que surjan en las redes y comunicaciones corporativas y efectuar el mantenimiento de máquinas y programas.

**Usuario:** Las labores propias del cargo de Usuario.

5.5.2. Obligaciones

5.5.2.1. Entorno de sistema operativo y de Comunicaciones

Cuidar de que ningún usuario no autorizado en el Anexo Relación de personal autorizado disponga de herramienta o programa que le permita el acceso al fichero.

Guardar en lugar protegido las copias respaldo y recuperación del Fichero, evitando el acceso a las mismas de persona no autorizada.
Asegurarse de que personal no autorizado pueda tener acceso a los datos protegidos

Impedir el acceso remoto de personas no autorizadas al equipo donde este ubicado el fichero, especialmente si se encuentra integrado en una red de comunicaciones.

5.5.2.2. Sistema Informático o aplicaciones de acceso al Fichero

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

5.5.2.3. Salvaguarda y protección de las contraseñas personales

Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el punto *Identificación y autenticación del personal autorizado* del apartado 4. Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas, y será responsabilidad del administrador del sistema.

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

5.5.2.4. Procedimientos de respaldo y recuperación

Obtener periódicamente una copia de seguridad del fichero, que garantice su reconstrucción en el estado en que se encontraba al tiempo de producirse la pérdida o destrucción.

Realizar la copia de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Comprobar y actualizar el 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.