**Documento de Seguridad para ficheros**

**automatizados de datos de carácter personal con**

**nivel de seguridad básico**

**Ficheros**

|  |  |  |
| --- | --- | --- |
| *[N inscripción]* | *[NOMBRE DE FICHERO1]* |  |
| *[N inscripción]* | *[NOMBRE DE FICHERO2]* |  |
| *[N inscripción]* | *[NOMBRE DE FICHERO3]* |  |
| *[N inscripción]* | *[NOMBRE DE FICHEROn]* |  |

|  |  |
| --- | --- |
| Documento Seguridad elaborado por | ***[Encargado Interno del Tratamiento]*** |
| Versión |  |
| Fecha |  |

Índice

1**.** Objeto del documento

2. Ámbito de aplicación

3. Recursos protegidos

4. Funciones y obligaciones del personal

5. Medidas, normas y procedimientos, reglas y estándares

5.1 Autorización del personal que puede acceder al fichero

5.2 Procedimientos de Identificación y Autorización de usuarios

5.3 Centros de tratamiento y locales

5.4 Puestos de trabajo

5.5 Entorno del Sistema Operativo y de Comunicaciones

5.6 Sistema Informático ó aplicaciones de acceso al Fichero

5.7 Bases de datos, ficheros o archivos ofimáticos

6. Gestión de incidencias

7. Gestión de soportes

8. Entrada/salida de datos por red y telecomunicaciones

9. Procedimientos de respaldo y recuperación

10 Controles periódicos de verificación del cumplimiento

Anexos

Anexo A Documentos de Notificación, Disposiciones Generales de declaración de ficheros. Contratos de Encargados del tratamiento

Anexo B Descripción de la estructura del Fichero o Bases de Datos

Anexo C Descripción de los sistemas de información que tratan los ficheros

Anexo D Entorno del Sistema Operativo y Comunicaciones de los Ficheros

Anexo E Locales y Equipamiento

Anexo F Nombramientos y autorizaciones

Anexo G Procedimientos de control y seguridad

G.1 Procedimiento para dar de altas, baja o modificación de acceso a usuarios

G.2 Procedimiento de control de identificación y autenticación

G.3 Procedimiento de respaldo y recuperación

G.4 Procedimiento de gestión de soportes

G.5 Procedimiento de gestión de salidas de soportes

G.6 Procedimiento de gestión de entrada de soportes.

G.7 Procedimiento para la destrucción de soportes

G.8 Autorización para el uso de PC portátiles y trabajo fuera de los locales

G.9 Sistemas de cifrado de datos

Anexo H Funciones y obligaciones del personal

Anexo I Procedimiento de Notificación y gestión de incidencias

Anexo J Controles periódicos y auditorías

Anexo K Modificaciones introducidas en las revisiones de este documento

***<< Notación utilizada en este documento genérico y notas para su confección>>***

***<<***

1. ***Todos los textos en cursiva entre signos “<<” y “>>” y en color azul, como los textos de esta página, son comentarios de ayuda para la confección del documento de seguridad, y deberán ser retirados del documento y sustituidos por los textos propios correspondientes.***
2. ***Los textos entre signos “[“ y “]” son alternativas, que se indican dentro de ese campo separadas con signos “|”, o bien campos que deben ser rellenados al confeccionar el documento, personalizándolo con los datos de los ficheros.***
3. ***El documento de seguridad se aplicará a uno o varios ficheros. Si son varios los ficheros, todos deberán ser del mismo nivel de seguridad, básico, medio o alto. Cuando en el documento se referencia al fichero debe sobreentenderse que se aplica a todos los ficheros afectados por el documento.***
4. ***El responsable interno del fichero o encargado interno de tratamiento, y el responsable de seguridad deberán poseer una copia completa del documento y sus Anexos.***
5. ***Una copia del Anexo H de Funciones y obligaciones del Personal, deberá ser repartida a todos los usuarios del fichero junto con el procedimiento de Notificación de incidencias y******el procedimiento para la Destrucción de desechos informáticos. Asimismo, se facilitará a cada usuario, los procedimientos que sean necesarios para el desarrollo de sus funciones, que deberán estar recogidos en el Anexo G. >>***

**1. Objeto del documento**

***Es el objetivo de este documento, es decir incorporar las leyes establecidas sobre la LOPD en los datos.***

El presente documento responde a la obligación establecida en el artículo 88 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/19999, de 13 de diciembre, de protección de datos de carácter personal, en el que se regulan entre otras, las medidas de seguridad para los ficheros y tratamientos automatizados que contengan datos de carácter personal.

Los ficheros de datos a los que se refiere este documento que en adelante denominaremos el Fichero, descritos en el documento de Notificación a la Agencia Española de Protección de Datos, que se adjunta en el **Anexo A**, se encuentran legalmente clasificados como de nivel de seguridad **básico** atendiendo a las condiciones descritas en el artículo 81 del Real Decreto citado, siendo por tanto aplicables todas las medidas de seguridad de nivel **básico** que se establecen en el Capítulo III del Título VIII, del citado Reglamento. Y cuya declaración ha sido autorizada por la Secretaría General de la Universidad Politécnica de Valencia, que se adjunta en el **Anexo A**.

**2. Ámbito de aplicación**

***Hace referencia a las obligaciones y responsabilidades por parte de la persona encargada de mantener e implantar este documento.***

Este documento ha sido elaborado bajo la responsabilidad de la persona descrita en la portada, que, Encargado Interno del tratamiento, se compromete a implantar y actualizar ésta Normativa de Seguridad de obligado cumplimiento para todo el personal con acceso a los datos protegidos o a los sistemas de información que permiten al acceso a los mismos.

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

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

Este Documento deberá mantenerse permanentemente actualizado. Cualquier modificación relevante conllevará la revisión de la normativa incluida y, si procede, su modificación total o parcial.

**3. Recursos protegidos**

***Es el conjunto de medios a proteger, por contener los datos en el sistema de información.***

La protección de los datos del Fichero frente a accesos no autorizados se deberá realizar mediante el control, a su vez, de todas las vías por las que se pueda tener acceso a dicha información.

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

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

**4. Funciones y obligaciones del personal**

***Especifica las funciones y responsabilidades que tienen los diferentes tipos de personas***

Además del **Responsable del fichero**, el personal afectado por esta normativa se podría clasificar en algunas de las categorías siguientes:

1. **Responsable del Fichero**, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal en su artículo 3, apartado d), define al responsable del fichero o tratamiento de la siguiente forma: “Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento”. En el caso de la Universidad Politécnica de Valencia su Rector/a será el Responsable del Fichero.
2. **Responsable Interno del Fichero**, según el artículo 3. 1. y 2 del Reglamento sobre Protección de Datos de Carácter Personal de la Universidad Politécnica de Valencia, aprobado por acuerdo del Consejo de Gobierno de 11 de marzo de 2010. “1.Todos los ficheros de la Universidad Politécnica de Valencia tendrán designado un Responsable Interno del Fichero, que será el responsable de las distintas unidades de la misma, cuya responsabilidad alcanza al tratamiento de los datos de carácter personal en las áreas, servicios, centros, departamentos o institutos de que se traten.”

Se entienden por responsables de Unidades y Servicios a los Vicerrectores, Directores de los Departamentos, Directores o Decanos”.de los Centros y Directores de los Institutos. Serán los facultados para solicitar la creación, modificación o supresión de los ficheros, así como los responsables de asegurar el modo de recogida de los datos, según lo especificado en el Título I (del Reglamento), y el ejercicio de los derechos de los interesados”

1. **Encargado Interno del tratamiento,** serán designados por los Responsables Internos de los ficheros, de entre el personal adscrito a su Unidad o Servicio que supervisará la aplicación a los datos contenidos en el fichero, de las medidas especificadas en el Reglamento sobre Protección de Datos de la Universidad Politécnica de Valencia, así como la aplicación de las medidas organizativas y de seguridad plasmadas en el Documento de seguridad.
2. **Administradores del sistema**, encargados de administrar o mantener el entorno operativo del Fichero. Este personal deberá estar explícitamente relacionado en el **Anexo F**, ya que por sus funciones pueden utilizar herramientas de administración que permitan el acceso a los datos protegidos saltándose las barreras de acceso de las aplicaciones o sistemas de información.
3. **Usuarios del Fichero**, o personal que usualmente utiliza el sistema informático de acceso al Fichero, y que también deben estar explícitamente relacionados en el **Anexo F**.
4. **Otras personas** de empresas ajenas que por motivo de su desempeño profesional, puedan potencialmente tener acceso a la información de carácter personal.

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

Respecto a aquellas personas de la propia organización o de empresas ajenas, que por motivo del desempeño de sus trabajos puedan tener acceso a los datos del Fichero, aunque esos trabajos no impliquen el tratamiento de los datos, como pueden ser trabajadores de la limpieza, administración, vigilancia, etc.., el responsable del Fichero o del tratamiento deberá adoptar las medidas oportunas para limitar el acceso a los datos personales, así como notificarles la prohibición de acceso a los mismos y la obligación de secreto respecto a los datos que hubiesen podido conocer con motivo de la prestación del servicio.

El responsable del Fichero o del tratamiento podrá delegar sus funciones en otras personas designadas al efecto, pero esta delegación deberá constar expresamente en el **Anexo F** de este Documento de Seguridad, en donde se anotará el nombre de estas personas así como las funciones delegadas. En ningún caso esta designación supondrá una delegación de la responsabilidad que corresponde al responsable del Fichero o del tratamiento.

Cuando los datos personales del fichero se traten de modo exclusivo en los sistemas de un encargado externo de tratamiento, el Encargado Interno del tratamiento deberá incorporar el contrato correspondiente en el **Anexo A**. Dicho contrato tentara el contenido expresado en el Reglamento sobre Protección de Datos de Carácter Personal de la UPV (Anexo V) En caso de un tratamiento parcial de los datos el encargado de tratamiento podrá asumir la llevanza de un documento de seguridad que afecte a esos datos, quedando a cargo del Encargado Interno del Tratamiento la confección del documento para el resto de los datos, debiendo quedar debidamente concretado en el contrato.

**5. Medidas, normas, procedimientos, reglas y estándares**

***Hace referencia a la manera en que se deberán tratar los datos por parte de las personas que tienen acceso a ellos.***

El acceso a los datos del Fichero se realizará ateniéndose a las medidas, normas, procedimientos, reglas y estándares que se describen en este capítulo, y que serán de obligado cumplimientos para todo el personal que esté relacionado con el fichero, usuarios, técnicos y administradores.

La descripción detallada de algunos de los procedimientos y estándares se encuentra en los Anexos que se citan en cada apartado.

**5.1 Autorización del personal que puede acceder al fichero**

***Son las restricciones que se van a establecer, para que los usuarios solo tengan acceso a los datos que realmente necesitan acceder.***

El personal sea propio o ajeno solo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones**.** Sólo el personal expresamente autorizado por el responsable del Ficheromediante los procedimientos que se citan a continuación podrá tener acceso a los datos del Fichero.

5.1.1 En el **Anexo F** se incluirá la relación de usuarios actualizada con acceso autorizado a cada sistema de información que tenga acceso a los datos del Fichero, ó se referenciará la herramienta para poder obtenerlo puntual y/o periodicamente. Asimismo se incluirá el perfil o tipo de acceso autorizado para cada uno de ellos.

* + 1. Exclusivamente el Encargado Interno del Tratamiento o la persona autorizada por él en el **Anexo F**, podrá conceder, alterar o anular el acceso autorizado sobre datos o los recursos.

5.1.3 A partir del momento mismo del cese o cambio en el puesto de trabajo, se procederá a dar de baja el código de usuario correspondiente de forma que no sea posible acceder con el mismo a los datos del fichero.

5.1.4 El procedimiento para dar de alta, modificar o anular una autorización de acceso se especificará en el **Anexo G**.

**5.2 Procedimientos de Identificación y Autenticación de usuarios**

***Indica el sistema de autenticación que se va a seguir para asegurar que no se produzcan casos en los que no sea posible identificar quién o cuando accedió o trató los datos en algún momento.***

El responsable del Fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de cualquier usuario. Aunque ya existen procedimientos de identificación basados en certificado electrónico o incluso en datos biométricos como huellas dactilares, las contraseñas personales constituyen todavía hoy en día uno de los métodos más usados para proteger el acceso a los datos, y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible.

5.2.1. El procedimiento de asignación distribución y almacenamiento de contraseñas se encuentra descrito en el **Anexo G**.

5.2.2. 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 registrarlo como incidencia y proceder inmediatamente a su cambio.

* + 1. Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el **Anexo G**, y que en ningún caso deberá ser de más de un año. Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas, y será responsabilidad del administrador del sistema. Cada usuario deberá cambiar la contraseña inicial que se le asigne cuando haya sido necesaria la intervención de una tercera persona en dicho proceso. Las contraseñas deberán ser suficientemente complejas y difícilmente adivinables por terceros, evitando el uso del propio identificador como contraseña o palabras sencillas como “casa”, el nombre propio, etc. Para ello se seguirán las siguientes pautas en la construcción de las contraseñas establecidas en la Política de Contraseñas de la Universidad Politécnica de Valencia vigente:
    2. El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.
    3. El sistema informático de acceso al Fichero deberá estar programado para tratar los accesos mediante código y contraseña como se indica en el apartado 5.6
    4. Si es posible se habilitarán controles de acceso basados en certificados digitales electrónicos emitidos por la propia organización o por un organismo certificador oficial como la FNMT, o controles basados en el reconocimiento biométrico como huellas digitales. Aunque estos procedimientos suponen una mayor complejidad tecnológica, cada vez están más extendidos, y acabarán por sustituir a los controles de acceso por contraseña en los próximos años, dada su mayor seguridad. En caso de existir, estos controles se describirán en el **Anexo C**.

**5.3 Centros de tratamiento y locales**

***Especifica que se debe garantizar la especial protección a los dispositivos que contengan la información. (Servidores)***

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

* + 1. Los locales deberán contar con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad del Fichero que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas. La descripción de esos medios se encuentra en el **Anexo E**.
    2. Si el tratamiento de los datos el fichero se realizase en locales ajenos, debido a un contrato con un encargado externo del tratamiento (al que se le encarga mediante contrato el procesamiento total o parcial de los datos protegidos), el encargado externo del tratamiento deberá elaborar un documento de seguridad en que se describan las medidas de seguridad adoptadas para proteger el fichero, o en su defecto completar este documento de seguridad con las medidas adoptadas. En todo caso el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en el Reglamento.

**5.4 Puestos de trabajo**

***Se refiere a cualquíer dispositivo en el que se pueda acceder al sistema.***

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

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

5.4.1. Cada puesto de trabajo estará bajo la responsabilidad de una persona de las autorizadas en el **Anexo F**, que garantizará que la información que muestra no pueda ser vista por personas no autorizadas.

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

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

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

5.4.5. Queda expresamente prohibido cualquier cambio de la configuración de la conexión de los puestos de trabajo a redes o sistemas exteriores, que no esté autorizado expresamente por el Encargado Interno del Tratamiento o el Director del Centro o departamento al que pertenezca cada usuario. La revocación de esta prohibición deberá ser autorizada expresamente.

* + 1. 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 al autorización del responsable de seguridad o por administradores autorizados del **Anexo F**.

* + 1. Trabajo fuera de los locales de ubicación del Fichero. No se deberá copiar ni transportar información de los sistemas centrales en portátiles o estaciones de trabajo que se encuentren fuera de las oficinas sin la correspondiente autorización del Encargado Interno del Tratamiento. Especial consideración deberán tener los puestos de trabajo **portátiles,** como los ordenadores personales **portátiles.** Estos dispositivos **portátiles,** cuando puedan almacenar datos personales, deberán contar con una autorización especial por parte del responsable de Fichero o tratamiento, debiendo estar explícitamente autorizados en el **Anexo E** (como puestos de trabajo portátiles), y en **Anexo G** (procedimiento de autorización), especificando su usuario, tipo de datos que podrá tratar y periodo de autorización. En cualquier caso estos dispositivos deberán contar como mínimo con las mismas medidas de seguridad de los puestos de trabajo fijos, con una especial atención a los controles de acceso, que impidan acceder a los datos por parte de terceros en caso de pérdida o robo.

**5.5 Entorno de Sistema Operativo y de Comunicaciones**

***Se refiere a proteger de manera lógica el acceso a los datos, (Internet, firewall, comunicaciónes cifradas... )***

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 ordenadores, es posible, para las personas que conozcan estos entornos, acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que pueda contar la aplicación.

Esta normativa debe, por tanto, regular el uso y acceso de las partes del sistema operativo, herramientas o programas de utilidad, o del entorno de comunicaciones sean o no públicas, para impedir que personas no autorizadas con los conocimientos tecnológicos avanzados en esos entornos puedan saltarse las barreras de seguridad de la aplicación o sistema de acceso al fichero**.**

5.5.1. El sistema operativo y de comunicaciones del Fichero deberá tener al menos un responsable, que, como administrador deberá estar relacionado en el **Anexo F**.

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

5.5.3. El sistema operativo donde se ejecuta esa aplicación, deberá tener su acceso restringido mediante un código de usuario y una contraseña. Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado en el **Anexo F**.

5.5.4. En la norma anterior se incluye cualquier medio de acceso en bruto, es decir no elaborado o editado, a los datos del Fichero, como los llamados "queries", editores universales, analizadores de ficheros, etc., que deberán estar bajo el control de los administradores autorizados que se relacionan en el Anexo F.

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

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

5.5.7. Si el ordenador en el que está ubicado el fichero está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible acceso al Fichero, el administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.

**5.6 Sistema Informático o aplicaciones de acceso al Fichero**

***Se refiere a proteger todo el software que tendrá acceso a los ficheros que se quiere proteger. (Es muy parecido al punto anterior) + seguridad lógica***

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

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

5.6.1. Los sistemas informáticos de acceso al Fichero deberán tener su acceso restringido mediante un código de usuario y una contraseña o bien mediante otros sistemas como firma electrónica o controles biométricos. En el caso de acceso por contraseña todos los usuarios autorizados para acceder al Fichero, relacionados en el **Anexo F**, deberán tener un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario. El procedimiento para la gestión de códigos de usuario y contraseñas se describe en el **Anexo G**.

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

**5.7 Bases de datos, ficheros o archivos ofimáticos**

***Se derá proteger también las báses de datos ya que aunque directamente no sean información confidencial, si que contienen datos que deben ser protegidos.***

Los datos personales están ubicados físicamente en ficheros o en bases de datos, que deben ser protegidos, y estarán descritos en el **Anexo B**.

Por otra parte en la operativa diaria de tratamiento de los datos del Fichero pueden producirse copias de los datos protegidos sobre otros ficheros o archivos ofimáticos para tratamientos especiales. En estos casos deberá prestarse la adecuada protección a esos ficheros mientras existan.

5.7.1 Cuando se realicen tratamientos de datos extraídos del Fichero, con programas ofimáticos, como procesadores de texto u hojas de cálculo, deberá ser comunicarlo para su aprobación al Encargado Interno del Tratamiento para que se proceda a implantar las medidas de seguridad adecuadas.

* + 1. Ficheros Temporales. Se deberá evitar el guardar copias de los datos personales del Fichero en archivos intermedios o temporales. En el caso de que sea imprescindible realizar esas copias temporales por exigencias del tratamiento, se deberán adoptar las siguientes precauciones:
* Realizar siempre esas copias sobre un mismo directorio de nombre TEMP o similar, de forma que no queden dispersas por todo el disco del ordenador y siempre se pueda conocer donde están los datos temporales.
* Tras realizar el tratamiento para los que han sido necesarios esos datos temporales, proceder al borrado o destrucción de los mismos.
* Los ficheros temporales creados exclusivamente para la realización de trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de Medidas de Seguridad.

**6. Gestión de incidencias**

***Se deberá tener un sistema de control de incidencias de manera que se quede registrado cualquír posible problema, para poder tratarlo posteriormente.***

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

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

6.1.1. Se habilitará un registro de incidencias con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

6.1.2. Cualquier usuario que tenga conocimiento de una incidencia es responsable del registro de la misma, si el registro de incidencias está automatizado, ó de la notificación por escrito al Encargado Interno del Tratamiento ó al superior inmediato, si el registro se realiza manualmente.

6.1.3. El conocimiento y la no notificación o registro de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.

6.1.4. La notificación o registro de una incidencia deberá constar al menos de los siguientes datos: tipo de incidencia, fecha y hora en que se produjo, persona que realiza la notificación, persona a quien se comunica, efectos que puede producir, descripción detallada de la misma. El procedimiento está descrito en el **Anexo I**.

**7. Gestión de soportes**

***Se debe tener un buen sistema de copias de seguridad, y protegerlos de igual manera que los datos en sí. Ya que ellos contienen la misma información.***

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

Dado que la mayor parte de los soportes que hoy en día se utilizan, como disquetes, CD, DVD, cintas o memorias removibles de todo tipo (como memorias flash o “pendrives”), 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.

* + 1. Los soportes que contengan datos del Fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, o que tipo de datos contiene, proceso que los ha originado y fecha de creación.
    2. En el caso de que la organización lo considerase, podrán utilizarse sistemas de etiquetado en los soportes que contienen información especialmente sensible para la organización, que permitan a los usuarios identificar los citados soportes y la dificulten para el resto de las personas.
    3. En general, cualquier soporte que vaya a ser desechado, de cualquier tipo, que pueda contener datos protegidos del Fichero, ya sea papel impreso, soportes magnéticos, ópticos u otros, o los propios ordenadores obsoletos que vayan a desecharse, deberán ser tratados mediante el procedimiento de desechos informáticos descrito en el **Anexo G**, con el fin de impedir la pérdida de confidencialidad de los datos personales. 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.
    4. 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**.
    5. La salida de soportes que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el responsable del Fichero, utilizando para ello el documento adjunto en el **Anexo G**.
    6. Cuando soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros se adoptarán las medidas necesarias para impedir la sustracción, pérdida o acceso indebido a la información durante el transporte.

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

***Se deberá controlar la entrada y salida de datos de la red, y protegerlos de igual manera que los datos almacenados en local.***

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

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

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

**9. Procedimientos de respaldo y recuperación**

***Se deberá establecer un sistema de copias de seguridad y un plan de actuación en caso de pérdida de información. (Realizando simulacros de perdida/recuperación de datos)***

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

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

9.1.1. Existirá una persona, bien sea el administrador o bien otro usuario expresamente designado o autorizado, que será responsable de obtener periódicamente una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo.

* + 1. 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.
    2. En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban en el momento del fallo. Ese procedimiento está descrito en el **Anexo G**. Al menos cada seis meses el responsable del fichero deberá verificar la correcta definición y funcionamiento de los procedimientos de respaldo y recuperación.
    3. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizaran con datos reales, salvo que se aplique a esos ficheros de prueba el mismo tratamiento de seguridad que se aplica al mismo Fichero, y se deberán relacionar esos ficheros de prueba en el **Anexo B**. Si se van a realizar pruebas con datos reales, deberá realizarse previamente una copia de seguridad.

**10. Controles periódicos de verificación del cumplimiento**

***Periódicamente se deberá controlar que todos los sistemas implantados se están cumpliendo.***

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

10.1.1. El Encargado Interno del Tratamiento comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados del **Anexo F** se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al Fichero y perfiles, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador o administradores del Fichero. Además de estas comprobaciones periódicas, el administrador comunicará al Encargado Interno del Tratamiento, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al Fichero.

* + 1. Se comprobará al menos con periodicidad semestral, por los administradores, la existencia de copias de respaldo que permitan la recuperación de Fichero según lo estipulado en el apartado 9 de este documento, enviando evidencias de esta comprobación al responsable del fichero.
    2. A su vez, y también con periodicidad al menos semestral, los administradores del Fichero comunicaran al Encargado Interno del Tratamiento cualquier cambio que se haya realizado en los datos técnicos de los Anexos, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de dichos Anexos.
    3. El Encargado Interno del Tratamiento o la persona autorizada, analizara la información registrada en el registro de incidencias, tomando las medidas oportunas.

**Anexo A. Documentos de Notificación, Disposiciones Generales de declaración de ficheros y Contratos de Encargados del tratamiento**

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

*En este mismo apartado se recogerá una copia de la autorización para la declaración de la Secretaría General de la UPV, así como de la publicación de la disposición de creación, y si procede de las modificaciones.*

*Cuando exista encargado externo del tratamiento, en este Anexo se adjuntara una copia del contrato con el encargado o bien el documento acreditativo de la relación y circunstancias, indicando los ficheros, la Identificación del responsable y vigencia del encargo*>>

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

*<<Por cada uno de los ficheros afectados por este documento, se adjuntará una descripción que contendrá al menos los siguientes aspectos:*

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

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

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

*En el caso de que se realicen pruebas con datos reales será necesario, realizar previamente una copia de seguridad.*

*Gestor de base de datos:*

* *Mecanismos de recuperación*

*Se hará referencia a los tratamientos manuales, que existan*>>

**Anexo C. Descripción de los sistemas de información que tratan los ficheros.**

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

*Deberá adjuntarse aquí la descripción de los sistemas informáticos de acceso a los ficheros de este documento.*

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

* *Nombre del Sistema de información ó aplicación*
* *Si se trata de un paquete o producto estándar del mercado o de unos programas expresamente diseñados para ese propósito.*
* *Quién y en que fecha se programó.*
* *Responsables del mantenimiento.*
* *Tipo de control de acceso si lo tiene (acceso por contraseña, certificado de firma electrónica, controles biométricos, u otros),*
* *Tipo de procedimientos de histórico de operaciones (logging): y de recuperación, si los tiene.*>>

**Anexo D. Entorno de Sistema Operativo y Comunicaciones de los Ficheros**

*<<Por cada sistema operativo diferente de acceso a los ficheros, se adjuntará una descripción que deberá contener al menos los siguientes datos y aspectos:*

*Sistema operativo:*

* *Nombre y versión*
* *Fabricante*
* *Características generales (monopuesto, multiusuario, compartición de ficheros u otros recursos, etc.)*
* *Control de acceso, características*
* *Archivos de ”logging” y procedimientos de recuperación propios del sistema.*
* *Responsables del mantenimiento*

*Entorno de comunicaciones (si lo tuviese):*

* *Tipo de red local (Ethernet, otras), ámbito y extensión.*
* *Si existe conexión con otras redes locales o WAN, indicar el tipo de conexión (permanente, esporádica, etc.), a través de redes públicas como Internet o con conexiones privadas etc.*
* *Hay compartición de recursos y archivos? Si es así indicar que tipo de sistema de red es utilizado, sus límites y alcance.*
* *Controles de acceso desde la red al sistema del Fichero.>>*

**Anexo E. Locales y equipamiento**

*<<Descripción de los locales y equipamiento de los centros de tratamiento, y almacenamiento de soportes.*

*Locales*

* *Tipo de local. Dirección. Propietario*
* *Tipo de acceso*
* *Sistemas de continuidad*
* *Equipamiento; armarios ignífugos, etc.*

*Si existen varios locales y/o ficheros, se adjuntará un cuadro especificando por cada uno de los locales, los sistemas de información y ficheros afectados.*

*Puestos de Trabajo*

* *Descripción Equipos: Servidores, equipos, Impresoras*
* *Relación de puestos de trabajo>>*

**Anexo F Nombramientos y autorizaciones**

*<< En este anexo figuraran todas las personas nombradas por el responsable, indicando la responsabilidad y la fecha del nombramiento o el cese. Asimismo se incluirá las autorizaciones de accesos concedidas a los usuarios.*

***Nombramientos***

*El Encargado Interno del Tratamiento podrá realizar un nombramiento para delegar en otra persona la firma de autorizaciones, en ningún caso esta designación supone una delegación de la responsabilidad que corresponde al Responsable del fichero.*

*Cada nombramiento o autorización deberá hacer constar:*

* *El nombre de la persona autorizada.*
* *El tipo de autorización o responsabilidad*
* *La fecha de alta*
* *La fecha de baja en su caso*

*Podrá haber nombramientos, designados por el responsable del fichero para los siguientes tipos de responsabilidades,*

* *Responsables que puedan autorizar consultas, altas, bajas , modificaciones del fichero*
* *Responsables de Salida Soportes*
* *Responsables de Salida por Red*
* *Responsable de autorizar el trabajo fuera de los locales*

***Autorizaciones de accesos a Usuarios***

*Las autorizaciones de accesos de usuarios, deberán ser realizadas por el Responsable del fichero o la persona en la que delegue , constaran del nombre del usuario, el perfil y los recursos a los que se concede el acceso, así como el nombre y cargo de la persona que realiza la autorización.*

* *El nombre del Usuario o de la persona autorizada.*
* *Perfil*
* *El tipo de privilegio de acceso*
* *La fecha de alta*
* *La fecha de baja, o de modificación en su caso*
* *El nombre y cargo de la persona que realiza la autorización*

*Se incluirán estas autorizaciones o bien se referenciará la herramienta o recurso que permita obtenerlas puntual y/o periódicamente*. *>>*

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

*<<Contendrá los procedimientos y sistemas utilizados en la organización para el control de usuarios y accesos, respaldo y recuperación*

*G.1 Procedimiento para dar altas, baja o modificación de acceso a usuarios*

*G.2 Procedimiento de identificación y autenticación*

*G.3 Procedimiento de respaldo y recuperación*

*G.4 Procedimiento de gestión de soportes de respaldo*

*G.5 Procedimiento de gestión de salida de soportes*

*G.6 Procedimiento de gestión de entrada de soportes.*

*G.7 Procedimiento para la destrucción de desechos informáticos*

*G.8 Autorización para el uso de PC portátiles*

**G.1 Procedimiento para dar altas, baja o modificación de acceso a usuarios**

*<<Se especificará el procedimiento para dar de alta, baja o modificación a usuarios del fichero.*

*Cada de alta de autorización deberá estar aprobada por el Encargado Interno del Tratamiento o persona autorizada, conteniendo el nombre y datos identificativos del usuario, el fichero, los sistemas de información y/o recursos a los que accede, y el perfil de acceso (tipo de usuario)*>>

**G.2 Procedimiento de control de identificación y autenticación**

*<<.Si la autenticación se realiza mediante contraseñas, se detallará el procedimiento de asignación, distribución y almacenamiento con indicación de la periodicidad del cambio que en ningún caso podrá ser superior a un año.>>*

**G.2 Procedimiento de respaldo y recuperación.**

*<<Se detallará el procedimiento de respaldo y recuperación con al menos los siguientes datos:*

* *Frecuencia y tipo de soporte donde se realiza el respaldo.*
* *En caso de pérdida del fichero entre dos respaldos, se indicará en procedimiento para, a partir de los documentos con los que se actualiza en fichero, proceder a la recuperación del mismo hasta el mismo punto en que estaba cuando se produjo la pérdida.>>*

**G.4 Procedimiento de gestión de soportes**

*<<Constará al menos de los siguientes apartados*

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

*Si la gestión de soportes de respaldo se hace de forma automatizada se describirá simplemente el sistema utilizado*

*Podrán utilizarse sistemas de etiquetado en los soportes que contienen información especialmente sensible para la organización, que permitan a los usuarios identificar los citados soportes y la dificulten para el resto de las personas. .>>*

**G.5 Procedimiento de gestión de salida de soportes**

*<<Cualquier salida de soportes fuera de los locales donde esta ubicado el fichero deberá ser autorizada por el responsable del fichero de acuerdo con un formulario similar al documento ejemplo que se adjunta.*

|  |  |  |  |
| --- | --- | --- | --- |
| ***REGISTRO Y AUTORIZACIÓN DE SALIDA DE SOPORTES*** | | | |
| *Fecha y hora de salida del soporte* | |  | |

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

|  |  |
| --- | --- |
| ***FINALIDAD Y DESTINO*** | |
| *Finalidad* |  |
| *Destino* |  |
| *Destinatario* |  |

|  |  |
| --- | --- |
| ***FORMA DE ENVÍO*** | |
| *Medio de envío* |  |
| *Remitente* |  |
| *Precauciones para el transporte* |  |

|  |  |
| --- | --- |
| ***AUTORIZACIÓN*** | |
| *Persona responsable de la entrega* |  |
| *Persona que autoriza* |  |
| *Cargo / Puesto* |  |
| *Observaciones* |  |
| *Firma* |  |

***Entrada y salida de datos por red***

*Se especificará*

*- Cuentas de correo autorizadas para enviar.*

*- Responsable de transferencias electrónicas >>*

**G.6 Procedimiento para la destrucción de desechos informáticos**

*<<Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados. En este apartado se describirá el método empleado para la destrucción o borrado de los mismos. Como mínimo se deberá exigir el siguiente procedimiento,*

***Procedimiento para la destrucción de desechos informáticos***

*Todos los desechos informáticos de cualquier tipo que puedan contener información del Fichero, como CDs, cintas, discos removibles, listados, memorias removibles de cualquier tipo, o incluso los propios ordenadores obsoletos que contengan discos e almacenamiento, deberán ser eliminados o destruidos de acuerdo con el siguiente Procedimiento para la Destrucción de Desechos Informáticos.*

1. *Como norma general ningún desecho informático, ya sea listado u otro tipo de soporte, debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.*
2. *Aquellos informes en papel o CDs que contengan datos de carácter personal más sensible y no sean voluminosos, deberán ser destruidos en una destructora de papel si es que existe en la organización.*
3. *En caso de no existir máquina destructora de papel y CDs o en le caso de que los listados e informes sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una compañía de reciclaje que garantice mediante contrato la destrucción de los mismos.*
4. *Todos los disquetes y otros soportes removibles desechados deberán ser formateados y entregados para su reutilización al Encargado Interno del Tratamiento. En el caso de que no se vayan a reutilizar deberán ser formateados si se puede, y depositados en los Contenedores confidenciales de la organización para ser entregadas a la empresa encarga da de la destrucción de los datos.*
5. *Si se trata de ordenadores obsoletos, antes de su donación, venta o entrega a otras instituciones, deberá comunicarse al Encargado Interno del Tratamiento para que se formatee el disco duro o se pase un programa especial que elimine de forma segura todos los datos de los discos duros. Si el ordenador estuviese estropeado y no se pudiese realizar la operación de limpiado, se deberán desmontar los discos duros y depositarlos en le Contenedor de la empresa de reciclaje para su destrucción.*
6. *El Encargado Interno del Tratamiento deberá exigir a la empresa de reciclaje un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.*

*>>*

**G.7 Autorización para el uso de PC portátiles**

*<<El Reglamento establece que no se realizara trabajo fuera de los locales sin la debida autorización del responsable del fichero. Para ello no se deberá copiar ni transportar información de los sistemas centrales en portátiles o estaciones de trabajo que se encuentren fuera de las oficinas sin la correspondiente autorización del Encargado Interno del Tratamiento.*

*El tratamiento, acceso y transporte de los datos del fichero en ordenadores portátiles, estará sujeto en todo caso a una autorización expresa Encargado Interno del Tratamiento o persona delegada, y sujeta a las mismas normas de seguridad que las de un puesto de trabajo fijo.*

*Se deberán adjuntar en este apartado las autorizaciones explícitas por parte del responsable del fichero o persona autorizada, para el trabajo en ordenadores portátiles fuera del local habitual, indicando la identificación de la persona autorizada, la identificación del equipo, el fichero o los datos que contiene, y las medidas extraordinarias para evitar la pérdida de confidencialidad de los datos en caso de robo o, pérdida del equipo.*

*Se adjuntara un ejemplo del formulario de autorización.>>*

**G.8 Sistemas de cifrado de datos.**

*<<Se detallarán los sistemas utilizados para el cifrado de datos.*

*En el caso de que se traten de protocolos estándar, o programas comerciales de cifrado se especificará el nombre, fabricante y versión.>>*

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

*<<En este anexo se describen las funciones y responsabilidades de cada persona con acceso a los datos del fichero, que ya han sido citadas en el cuerpo del documento, pero agrupadas por tipo o perfil de usuario.*

*Deberá copiarse tal como está en el documento de seguridad que se reparta al personal que trabaje con el fichero. El responsable del fichero, o el responsable de seguridad si lo hubiese, o el encargado del tratamiento, podrán añadir obligaciones particulares aplicables al fichero, pero respetando todas las que aquí figuran.*

*Según se dice en el párrafo 2 del documento, una copia del mismo con las funciones específicas de cada colectivo, deberá ser repartida a todos los usuarios del fichero para su conocimiento.*

*En el caso de los usuarios sólo se deberá entregar un documento divulgativo que incluya el presente Anexo junto con el procedimiento de Notificación de incidencias y el Procedimiento para la Destrucción de desechos informáticos. Asimismo se facilitara a cada usuario los procedimientos que sean necesarios para el desarrollo de sus funciones, que deberán estar recogidos en el Anexo G. >>*

**H.1 Obligaciones que afectan a todo el Personal**

* Guardar secreto profesional y confidencialidad de la información tratada. Quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.
* La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos personales será considerado como una falta leve, grave o muy grave de conformidad con lo previsto en el artículo 44 de la LOPD, lo cual dará lugar a iniciación de actuaciones disciplinarias, si procediesen.
* Utilizar los sistemas de información, recursos técnicos así como la información personal a la que se accede, únicamente para el desarrollo y desempeño profesional que el usuario tiene asignado.
* Facilitar el derecho de acceso, rectificación y cancelación a los titulares de los datos. Para ello se informará inmediatamente al Responsable del Fichero Responsable de Seguridad o Encargado del tratamiento y se recogerá siempre en solicitud escrita.

**H.2 Funciones y obligaciones del Responsable del Fichero**

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

**H.3 Funciones y obligaciones del Responsable Interno del Fichero**

El responsable es la persona física o jurídica que tenga atribuida la competencia a la que sirva instrumentalmente los datos contenidos en el fichero. Decide sobre la finalidad, uso y contenido de los mismos.

* Decidirá sobre la finalidad, contenido y uso del tratamiento.
* Encargará la elaboración del documento de seguridad al encargado interno del tratamiento
* Deberá garantizar la difusión del cuerpo y de los Anexos de este Documento que les afecten, entre todo el personal que vaya a utilizar el fichero.
* Firmará los Acuerdos de Tratamiento de Datos Personales del Anexo V del Reglamento sobre Datos de Carácter Personal de la UPV que le remita el Encargado Interno del Tratamiento.
* Hacer efectivo el derecho de acceso rectificación o cancelación en los plazos fijados por el procedimiento recogido en el Reglamento sobre Protección de Datos de Carácter Personal de la UPV.
* Excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición.

**H.4 Funciones y obligaciones del Encargado Interno del tratamiento**

* Elaborará el documento de seguridad. En caso de que exista un encargado de tratamiento, y se realice el tratamiento del fichero fuera de los locales del responsable del fichero, la elaboración del mismo podría corresponder al encargado de tratamiento.
* Implantará y hará cumplir las medidas de seguridad establecidas en este documento.
* Deberá mantener actualizado este documento siempre que se produzcan cambios relevantes en la organización o entorno del fichero, y deberá adecuar en todo momento el contenido del mismo a las disposiciones vigentes en materia de protección de datos personales.

**Autorización del personal que puede acceder al fichero**

* Encargarse de que exista una relación actualizada de usuarios con acceso autorizado para acceder a los datos del fichero.
* Conceder, alterar o anular el acceso autorizado sobre datos o los recursos.
* Velar porque se cumpla el procedimiento para dar de alta, modificar o anular una autorización de acceso que está especificado en le **Anexo G**.

**Procedimientos de Identificación y Autenticación de usuarios**

* Velar por que se cumpla el procedimiento de asignación distribución y almacenamiento de contraseñas que se encuentra descrito en el **Anexo G**.
* Velar por que las contraseñas se asignen y se cambien mediante el mecanismo y periodicidad que se determina en el **Anexo G**.

**Entorno de Sistema Operativo y de Comunicaciones**

* Aprobar y designar al administrador que se responsabilizará del sistema operativo y de comunicaciones que deberá estar relacionado en el **Anexo F**.

**Sistema Informático o aplicaciones de acceso al Fichero**

* Velar porque 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 F**, tengan un código de usuario que sea único, y que esté asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

**Trabajo fuera de los locales de ubicación del Fichero**

* Habilitar los controles necesarios para que no se copie ni transporte información del fichero en ordenadores portátiles o estaciones de trabajo que se encuentren fuera de las oficinas sin la correspondiente autorización.
* Autorizar el trabajo con datos personales fuera de los locales En el **Anexo** G se referencia un procedimiento para el tratamiento de ficheros fuera de su ubicación, como es el caso de los ordenadores portátiles.

**Gestión de soportes**

* Autorizar la salida de soportes informáticos que contengan datos del fichero fuera de los locales indicados en el **Anexo E.**
* En cualquier caso deberá especificarse en el **Anexo** G, el procedimiento para la destrucción o almacenaje de esos soportes.

**Entrada y salida de datos por red**

* Autorizar al usuario que podrá realizar desde una única cuenta o dirección de correo las salidas de datos por correo electrónico ó trasferencias.

**Procedimientos de respaldo y recuperación**

* Se encargará de verificar la definición y correcta aplicación de las normas y periodicidad de la realización de copias de respaldo, al menos semestralmente.

**Otras obligaciones.**

* Informar al Responsable Interno del fichero de las posibles cesiones de los datos de carácter personal para que se realicen según lo recogido en el Título III del Reglamento sobre Protección de Datos de Carácter Personal de la UPV. Solicitando si lo considera oportuno el asesoramiento de la Oficina de la Secretaría General.
* Controlar las cesiones de datos de carácter personal a entidades cesionarias a través de los Acuerdos de Condiciones de Cesión de Datos del Anexo VI del Reglamento sobre Protección de Datos de Carácter Personal de la UPV.
* Informar a los afectados en el caso de que se efectúe una primera cesión de datos.

**H.5 Funciones y obligaciones de los Usuarios**

El personal autorizado a acceder a la información de carácter personal del Fichero, realizará las funciones propias de su puesto de trabajo, que se encuentran previstas en las relaciones de puestos de trabajo del Centro o Unidad Administrativa a la que pertenezca, a la correspondiente definición de funciones que se aplique a dicho personal.

Además de dichas funciones relativas al desempeño profesional asociado a su puesto laboral, todo el personal colaborará con el Responsable Interno del Fichero y Encargado Interno del Tratamiento en pro de velar por el cumplimiento de la legislación y reglamentación vigente sobre Protección de Datos de Carácter Personal.

* 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.
* Cada usuario deberá cambiar la contraseña inicial que se le asigne, en el primer acceso que realice al sistema o tras el desbloqueo de su contraseña cuando haya sido necesaria la intervención de una tercera persona en dicho proceso. Las contraseñas deberán ser suficientemente complejas y difícilmente adivinables por terceros, evitando el uso del propio identificador como contraseña o palabras sencillas, el nombre propio, fecha de nacimiento etc.
* Para ello se seguirán las pautas de la Política de Contraseñas de la Universidad Politécnica de Valencia para la elección de las contraseñas:
* Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.
* Tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.
* Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos, como por ejemplo un protector de pantalla con contraseña. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.
* En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
* Queda expresamente prohibido cualquier cambio de la configuración de la conexión de los puestos de trabajo a redes o sistemas exteriores, que no esté autorizado expresamente por el Responsable del Fichero o el Director del Centro o departamento al que pertenezca cada usuario. La revocación de esta prohibición deberá ser autorizada expresamente
* 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 al autorización de los administradores autorizados del **Anexo** **F.**
* Cuando se realicen tratamientos de datos extraídos del Fichero, con programas ofimáticos, como procesadores de texto u hojas de cálculo, deberá ser comunicarlo para su aprobación al Encargado Interno del Tratamiento para que se proceda a implantar las medidas de seguridad adecuadas. La utilización de dichos programas para el tratamiento de datos personales sin comunicarlo al Encargado Interno del Tratamiento será considerado como una falta contra la seguridad del fichero por parte de ese usuario.
* Se deberá evitar el guardar copias de los datos personales del Fichero en archivos intermedios o temporales. En el caso de que sea imprescindible realizar esas copias temporales por exigencias del tratamiento, se deberán adoptar las siguientes precauciones:
* Realizar siempre esas copias sobre un mismo directorio de nombre TEMP o similar, de forma que no queden dispersas por todo el disco del ordenador y siempre se pueda conocer donde están los datos temporales.
  + Tras realizar el tratamiento para los que han sido necesarios esos datos temporales, proceder al borrado o destrucción de los mismos.
  + Los ficheros temporales creados exclusivamente para la realización de trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de Medidas de Seguridad.
* Trabajo fuera de los locales de ubicación del fichero. No se deberá copiar ni transportar información de los sistemas centrales en portátiles o estaciones de trabajo que se encuentren fuera de las oficinas sin la correspondiente autorización del Encargado Interno del Fichero. En el **Anexo G** se referencia un procedimiento para el tratamiento de ficheros fuera de su ubicación, como es el caso de los ordenadores portátiles.
* Cualquier usuario que tenga conocimiento de una incidencia es responsable de la comunicación de la misma al Encargado Interno del Fichero o a la persona encargada de registrarla. El modelo de notificación de incidencias figura en el **Anexo I.**
* 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.
* Todos los usuarios estarán obligados a guardar el secreto profesional y el deber de custodia respecto de los datos de carácter personal a los que tengan acceso en el desempeño de su función aún después de haber abandonado la universidad.
* Cuando un usuario gestione o produzca 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, estos deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.
* Cuando se reciclen 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. Aquellos que no vayan a ser reutilizados deberán ser destruidos mediante un procedimiento especificado en el **Anexo G**.
* 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.
* 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. mediante el procedimiento descrito en el **Anexo** **G**.
* Solo se podrán realizar envíos del Fichero, por correo electrónico o transferencias electrónicas, desde una única cuenta o dirección de correo controlado por un usuario especialmente autorizado por el Encargado Interno del Tratamiento o persona autorizada tal como se describe en el **Anexo G.**

**H.6 Funciones y obligaciones de los Administradores o Personal Informático**

Es el personal que administra los sistemas informáticos del fichero. Se puede clasificar en varias categorías, que no necesariamente deberán estar presentes en todos los casos, siendo en algunas ocasiones asumidas por una misma persona o personas.

* Administradores (Red, Sistemas operativos y Bases de Datos). Serán los responsables de los máximos privilegios y por tanto de máximo riesgo de que una actuación errónea pueda afectar al sistema. Tendrán acceso al software (programas y datos) del sistema, a las herramientas necesarias para su trabajo y a los ficheros o bases de datos necesarios para resolver los problemas que surjan.
* Operadores (Red, Sistemas operativos, Bases de Datos y Aplicación). Sus actuaciones están limitadas a la operación de los equipos y redes utilizando las herramientas de gestión disponibles. No deben, en principio, tener acceso directo a los datos del Fichero, ya que su actuación no precisa de dicho acceso.
* Mantenimiento de los sistemas y aplicaciones. Personal responsable de la resolución de incidencias que puedan surgir en el entono hardware/software de los sistemas informáticos o de la propia aplicación de acceso al Fichero.
* Los administradores deberán garantizar que el sistema operativo donde se ejecuta el sistema de acceso al fichero tenga su acceso restringido mediante un código de usuario y una contraseña. Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado en el **Anexo** F.
* En la norma anterior se incluye cualquier medio de acceso en bruto, es decir no elaborado o editado, a los datos del Fichero, como los llamados "queries", editores universales, analizadores de ficheros, etc., que deberán estar bajo el control de los administradores autorizados relacionados en el **Anexo F**.
* Si la aplicación o sistema de acceso al Fichero utilizase usualmente ficheros temporales, ficheros de "logging", o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, los administradores deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.
* Si el ordenador en el que está ubicado el fichero está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso al Fichero, los administradores deberán asegurarse de que este acceso no se permite a personas no autorizadas.
* Deberá garantizar la obtención periódica de una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo.
* Estas copias deberán realizarse con una periodicidad, al menos, semanal, salvo en el caso de que no se haya producido ninguna actualización de los datos.
* En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban en el momento del fallo. Ese procedimiento está descrito en el **Anexo** **G**.
* Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizaran con datos reales, salvo que se aplique a esos ficheros de prueba el mismo tratamiento de seguridad que se aplica al mismo Fichero, y se deberán relacionar esos ficheros de prueba en el **Anexo B**. Si se realizan pruebas con datos reales será necesaria realizar previamente una copia de seguridad.
* Los administradores deberán responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo del Fichero, de forma que ninguna persona no autorizada tenga acceso a las mismas.
* Los administradores facilitarán al Encargado Interno del Tratamiento para su comprobación la lista de usuarios y sus códigos de acceso que extraerá de la aplicación o sistemas de acceso, al menos trimestralmente, además de estas comprobaciones periódicas, enviará estas listas actualizadas en cuanto se produzca un cambio en los accesos.
* Comprobarán al menos con periodicidad semestral, la existencia de copias de respaldo que permitan la recuperación de Fichero según lo estipulado en el apartado 9 de este documento, enviando evidencias de esta comprobación al responsable del Fichero.

* A su vez, y también con periodicidad al menos trimestral, los administradores del fichero comunicarán al Encargado Interno del Tratamiento cualquier cambio que se haya realizado en los datos técnicos de los **Anexos**, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de dichos **Anexos.**

**Anexo I. Notificación y Gestión de incidencias**

<< *Se describirán los procedimientos de notificación y de gestión de incidencias*

*Procedimiento de Notificación de incidencias*

*Cuando ocurra una incidencia, el usuario o el administrador, deberá registrarla en la aplicación de notificación incidencias, si existe un sistema automatizado para hacerlo, o en el caso de que el sistema de registro sea manual, deberá comunicarla al Encargado Interno del Tratamiento o al Responsable del fichero o superior inmediato, para que procedan a su registro en el Libro que habrá habilitado a tal efecto.*

*En cualquier caso una notificación de incidencia deberá hacer constar:*

*Tipo de incidencia*

*Fecha y hora en que se produjo*

*Persona que realiza la notificación*

*Persona a quien se comunica*

*Descripción detallada de la misma*

*Efectos que puede producir la incidencia, si se conocen o presumen*

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

*Procedimiento de gestión de incidencias*

*En este procedimiento se indicará quién será responsable de analizar el registro de incidencias y las medidas correctoras que se tomen en cada caso, que se registraran.*

*Se mantendrán las incidencias registradas de los 12 últimos meses.*

*>>*

**Impreso de notificación de incidencias**

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

**Anexo J. Controles periódicos y auditorías**

*<<Contendrá los resultados de los controles periódicos descritos en el apartado 10 >>*

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

|  |  |  |
| --- | --- | --- |
| **Versión** | **Fecha** | **Actualizaciones** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |