DOCUMENTO DE SEGURIDAD PARA FICHEROS DE DATOS DE CARÁCTER PERSONAL

Universidad de Jaén

Revisado:	Servicio de Información y Asuntos Generales	
	Servicio de Informática	
Versión: 1.0	**Fecha Versión:**26/03/2015	**Nº Total Páginas:** 22
Aprobado por: Consejo de Gobierno	**Fecha Aprobación:** 26/03/2015	

Contenido

1. Aprobación y entrada en vigor

Texto aprobado el día 26/03/2015 por el Consejo de Gobierno.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva versión de la misma.

2. Ámbito de aplicación y Recursos protegidos

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de la Universidad de Jaén, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en la Ley Orgánica de Protección de Datos y el Real Decreto 1720/2007, las personas que intervienen en el tratamiento y los locales en los que se ubican.
La protección de los datos de los ficheros frente a accesos no autorizados se deberá realizar mediante el control, 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 a los ficheros, deberán ser controlados por esta normativa son:

- Los centros de tratamiento y locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contengan.
- Los puestos de usuario, bien locales o remotos, desde los que se pueda tener acceso a los ficheros.
- Los servidores, si los hubiese, y el entorno de sistema operativo y de comunicaciones en el que se encuentran ubicados los ficheros.
- Los sistemas informáticos, o aplicaciones establecidos para acceder a los datos.
- Los archivadores y salas, en donde se almacenen los documentos en papel que contengan datos de carácter personal.

2. Ficheros inscritos

En el enlace indicado a continuación se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afectan de manera particular:
http://www10.ujaen.es/conocenos/servicios-unidades/servinfo/protecci%C3%B3ndedatosdecaracterpersonal/ficherosinscritos

3. Normas de Seguridad

3.1. Codificación de las normas y procedimientos de seguridad

Las normas de seguridad definidas en este documento se identifican mediante una letra que las identifica como tales, y que indica el nivel de seguridad en que es aplicable la norma:

B	Norma de seguridad de nivel básico
M	Norma de seguridad de nivel medio
A	Norma de seguridad de nivel alto

A continuación se indica el tipo de norma, en función de si afecta a la seguridad física o a la seguridad lógica:

F – Seguridad Física
L – Seguridad Lógica

El siguiente código indica a qué tipo de usuarios les afecta la norma:

R – Responsable del Fichero
S – Responsable de Seguridad
I – Administradores y Personal de Informática
T – Todo el personal

Por último se especifica un número de orden de la norma.
Los procedimientos de seguridad definidos siguen una codificación equivalente, utilizando como primera letra identificativa siempre una **P**

3.2. Normas sobre locales, puestos de usuario, sistemas y contraseñas

3.2.1. Centros de tratamiento y locales

Los locales donde se ubiquen los ordenadores así como los archivadores, armarios o demás contenedores que contienen cada uno de los conjuntos de datos de carácter personal, que en adelante llamaremos 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.

B	F	R	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.

M	F	R	2	El acceso a los locales donde se encuentre el fichero deberá estar restringido exclusivamente a los administradores del sistema que deban realizar labores de mantenimiento para las que sea imprescindible el acceso físico.

M	F	T	3	Como alternativa a la norma anterior, toda persona que tenga acceso a los locales deberá estar acompañada en todo momento por algún empleado autorizado, que supervisará su comportamiento.

En todas las salas se encuentran de manera habitual empleados autorizados de la propia entidad. Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre los centros de tratamiento y locales se encuentra en el **Procedimiento de Seguridad Física,** publicado para su lectura en Universidad Virtual.

3.2.2. Puestos de usuario

Son todos aquellos dispositivos desde los que se puede acceder a los datos del Fichero, como, por ejemplo, terminales u ordenadores personales.
Se consideran también puestos de usuario 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.

B	F	T	4	Cada puesto de usuario estará bajo la responsabilidad de una persona, manteniéndose por tanto una relación de puestos de usuario de acuerdo al **"Procedimiento de Seguridad Lógica"**. El responsable de un puesto de usuario garantizará que la información a la que accede o que muestra no pueda ser vista por personas no autorizadas. Esta precaución se extremará cuando existan visitas ajenas al departamento al que pertenece el fichero. La plantilla para construir la relación de puestos de usuario y de personal autorizado para acceder al fichero se encuentra en el **"Procedimiento de Seguridad Lógica"**.

.

B	F	T	5	La norma anterior implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de usuario deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

B	L	T	6	Queda prohibido el almacenamiento de cualquier tipo de documento con datos personales en los PC de usuario salvo usuarios autorizados. En caso de existir aplicaciones de gestión específicas para el tratamiento de Datos de Carácter Personal, el usuario deberá de almacenar y tratarlos mediante dichas aplicaciones. La revocación de esta prohibición será autorizada por el responsable del Fichero, quedando constancia de esta modificación en el Registro de Incidencias. En cualquier caso se garantizará el cumplimiento de las medidas de seguridad correspondientes en el PC de usuario, especialmente medidas de control de acceso. El procedimiento para establecer las contraseñas se especifica en el **"Procedimiento de Control de Accesos"**.

B	L	T	7	Cuando el responsable de un puesto de usuario 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. El procedimiento para establecer el protector de pantalla se especifica en el "**Procedimiento de Control de Accesos**".

B	F	T	8	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 del Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

B	L	T	9	Las conexiones a redes o sistemas exteriores de los puestos de usuario desde los que se realiza el acceso al Fichero, se ajustarán a lo definido en el "**Procedimiento de Seguridad Lógica**".

Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre los puestos de usuario se encuentra en el **"Procedimiento de Seguridad Lógica"**.

3.2.3. Entorno de Sistema Operativo y de Comunicaciones

Aunque el método establecido para acceder a los datos protegidos del Fichero es el sistema informático referenciado en el apartado 2 del presente documento, al estar el Fichero ubicado en un ordenador con un sistema operativo determinado y poder contar con unas conexiones que le comunican con otros ordenadores, es posible, para las personas que conozcan estos entornos, acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que pueda contar la aplicación.

Esta normativa debe, por tanto, regular el uso y acceso de las partes del sistema operativo, herramientas o programas de utilidad, o del entorno de comunicaciones, de forma que se impida el acceso no autorizado a los datos del Fichero.

B	L	R	10	El sistema operativo y de comunicaciones del Fichero deberá tener al menos un responsable, que como administrador deberá estar relacionado de acuerdo al **"Procedimiento de Seguridad Lógica"**. 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. La plantilla para construir la relación de personal autorizado para acceder al Fichero se encuentra en el "**Procedimiento de Seguridad Lógica**".

B	F	I	11	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.

B	L	I	12	Si la aplicación o sistema de acceso al Fichero utilizase usualmente ficheros temporales, ficheros de "logging", o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, el administrador deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.

B	L	T	13	Los usuarios eliminarán los ficheros intermedios que pudieran haber creado para desarrollar su trabajo, una vez que no sean necesarios. En ningún caso se conservarán estos ficheros durante largos periodos de tiempo. En el caso de los puestos de usuario de tipo PC, con sistema operativo Windows, se eliminarán al finalizar cada jornada laboral los ficheros del directorio temporal del sistema (comúnmente C:\WINDOWS\TEMP\). El procedimiento para realizar esta eliminación se especifica en el "**Procedimiento de Protección de la Información**".

B	L	I	14	Si el ordenador en el que está ubicado el fichero está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso al Fichero, el Administrador Responsable del Sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas. En cualquier caso, deberá identificarse de manera única a las personas acceden de forma remota.

B	L	I	15	En el caso de puestos con Sistema Operativo Windows, en ningún caso se compartirá en red el directorio del sistema, comúnmente C:\WINDOWS. Este directorio, entre otras cosas, almacena las contraseñas y el directorio para ficheros temporales. La revocación de esta prohibición será autorizada por el Responsable de Seguridad, quedando constancia de esta modificación en el Registro de Incidencias.

Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre la red se recoge en el "**Procedimiento de Seguridad Lógica**".

3.2.4. Sistema Informático o aplicaciones de acceso al Fichero

Son todos aquellos sistemas informáticos, programas o aplicaciones con las que se puede acceder a los datos del Fichero, y que son usualmente utilizados por los usuarios para acceder a ellos. Estos sistemas pueden ser aplicaciones informáticas expresamente diseñadas para acceder al Fichero, o sistemas preprogramados de uso general como aplicaciones o paquetes disponibles en el mercado informático.

B	L	R	16	Los sistemas informáticos de acceso al Fichero deberán tener su acceso restringido mediante un código de usuario y una contraseña.

B	L	R	17	Todos los usuarios autorizados para acceder al Fichero deberán tener un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

B	L	I	18	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.

M	L	I	19	En cualquier caso se controlarán los intentos de acceso fraudulento al

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

B	L	R I	20	En función de las posibilidades técnicas, se limitará el acceso de cada usuario al mínimo conjunto de recursos que necesite para desempeñar su trabajo, configurando de manera adecuada la aplicación y/o el sistema operativo.

M	L	I	21	Si durante las pruebas anteriores a la implantación o modificación de la aplicación de acceso al Fichero se utilizasen datos reales, se deberá aplicar a esos ficheros de prueba el mismo tratamiento de seguridad que se aplica al mismo Fichero.

A	L	SI	22	En los ficheros de nivel alto, se guardará en un registro de accesos la identificación del usuario, fecha y hora en la que se realizó el acceso, el fichero accedido, el tipo de acceso y si éste ha sido autorizado o denegado. En caso de haber sido autorizado se guardará información que permita identificar el registro accedido. Los datos de este registro deberán conservarse al menos durante dos años. Los mecanismos de registro de estos datos de acceso no podrán ser desactivados en ningún caso, y estarán siempre bajo control del responsable de seguridad competente.

3.2.5. Salvaguarda y protección de las contraseñas personales

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

B	L	R	23	Sólo las personas relacionadas de acuerdo al **"Procedimiento de Seguridad Lógica"** podrán tener acceso a los datos del Fichero.

B	L	R	24	La norma anterior se aplica también a los Administradores del sistema, incluyendo aquél personal técnico externo que de manera habitual pudiera

				colaborar en la administración de los sistemas.

B	L	T	25	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.

B	L	I	26	Los identificadores de usuario y las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determinan en el **"Procedimiento de Control de Accesos"**, asegurando que se mantiene la confidencialidad de ambos.

B	L	I	27	El archivo donde se almacenen las contraseñas deberá estar protegido y cifrado, y bajo la responsabilidad del Administrador del Sistema.

Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre las contraseñas se encuentra en el "**Procedimiento de Control de Accesos**".

3.3. Normas sobre gestión de incidencias

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

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

B	L	S	28	El Responsable de Seguridad del Fichero habilitará un Registro de Incidencias a disposición de todos los usuarios y administradores del Fichero con el fin de que se registre en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

B	L	T	29	Cualquier usuario que tenga conocimiento de una incidencia, es responsable del registro de la misma en el Registro de Incidencias del Fichero, entregándola por escrito al Responsable de Seguridad o al Responsable del Fichero, que serán los encargados de incorporarla al Libro.

B	L	T	30	El conocimiento de una incidencia y la falta de notificación o registro de la

				misma por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.

B	L	T	31	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 y una descripción detallada de la misma. El procedimiento y formulario para notificar una incidencia está descrito en el **"Procedimiento gestión de incidencias"**.

B	L	S	32	El Responsable de Seguridad se ocupará de gestionar cada incidencia para resolver los problemas que plantee de la mejor manera posible, en colaboración con el Responsable del Fichero. El procedimiento para gestionar una incidencia está descrito en el **"Procedimiento de gestión de incidencias"**.

Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre la gestión de incidencias se encuentra en el **"Procedimiento Gestión de Incidencias".**

3.4. Normas sobre gestión de soportes

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

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

Aunque este apartado hace referencia a los soportes informáticos, también se establecen algunas normas para el caso de los soportes no informáticos, como los documentos impresos en papel.

B	L	T	33	Los soportes (Memorias USB, DVDs, CD-ROMs...) que contengan datos de carácter personal, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación. El procedimiento para identificar estos soportes se encuentra en el **"Procedimiento de Protección de la Información"**.

M	F	T	34	Aquellos medios que sean reutilizables, y que hayan contenido copias de datos del Fichero, deberán ser borrados físicamente antes de su reutilización o destrucción, de forma que los datos que contenían no sean recuperables. El procedimiento para reutilizar o destruir estos soportes se encuentra en el **"Procedimiento de Protección de la Información"**.
M	F	T	35	Los documentos impresos con datos personales, una vez que ya no sean necesarios, se destruirán físicamente de manera que no puedan recuperarse los datos que contenían (por ejemplo mediante una trituradora de papel). En ningún caso se reutilizarán este tipo de documentos (por ejemplo, no podrán ser utilizados para imprimir por la otra cara, si estuviera en blanco).
B	F	T	36	Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso del Fichero que no estén, por tanto, relacionadas de acuerdo al **"Procedimiento de Protección de la Información"**. En caso de ser posible, se utilizará un lugar protegido frente a incendios. En ningún caso se dejarán a la vista, como por ejemplo encima de una mesa.
B	L	T	37	Todos los soportes que se utilicen se incluirán en un inventario, en el que se indique, para cada soporte, la fecha de alta y de baja, indicando en este último caso si el soporte se destruye definitivamente o se reutiliza. La plantilla para construir el libro de inventario de soportes se encuentra en el **"Procedimiento de Protección de la Información"**.
B	F	T	38	Los documentos impresos con datos personales se almacenarán de manera que se mantenga la confidencialidad de los mismos en lugares a los que no tengan acceso personas no autorizadas. En ningún caso se dejarán a la vista, como por ejemplo encima de una mesa.
B	L	R	39	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.

				El procedimiento y formulario para la salida de soportes se encuentra en el **"Procedimiento de Protección de la Información"**.

M	L	R	40	El Responsable de Seguridad del Fichero o persona en quien delegue mantendrá un "**Registro de entrada y salida de soportes**" donde se guardarán los formularios de entradas y de salidas de soportes descritos en el capítulo "Locales, sistemas de tratamiento, aplicaciones y puestos de usuario", con indicación de tipo de soporte, fecha y hora, emisor, número de soportes, tipo de información que contienen, forma de envío, destinatario, o persona responsable de la recepción que deberán estar debidamente autorizadas. El procedimiento y formulario para la entrada de soportes se encuentra en el **"Procedimiento de Protección de la Información"**.

M	L	T	41	Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

A	L	S	42	Se conservará una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente donde se encuentren los equipos informáticos que los tratan. Deberán cumplirse, en todo caso, las medidas de seguridad correspondientes al nivel de los datos contenidos en la copia.

Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre la gestión de soportes se encuentra en el "**Procedimiento de Protección de la Información**".

3.5. Normas sobre la entrada y salida de datos por red

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

M	L	R I	43	Todas las entradas y salidas de datos de carácter personal que se efectúen mediante correo electrónico se realizarán desde cuentas o direcciones de correo de la Universidad, estando prohibido el uso de cuentas personales. 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.

A	L	T	44	Cuando los datos del Fichero vayan a ser enviados por correo electrónico o por sistemas de transferencia de ficheros, a través de redes públicas o no protegidas, se recomienda que sean cifrados de forma que solo puedan ser leídos e interpretados por el destinatario. Si los datos son de nivel alto el cifrado es obligatorio.

Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre la red en el **"Procedimiento de Seguridad Lógica"**.

3.6. Normas sobre las copias de respaldo y recuperación

La seguridad de los datos personales del Fichero no sólo supone la confidencialidad de los mismos sino que también conlleva la integridad y la disponibilidad de esos datos.
Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos del Fichero.

B	L	I	45	Existirá una persona, bien sea el administrador o bien otro usuario expresamente designado, que será responsable de obtener periódicamente una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo. El procedimiento de realización de copias de seguridad se encuentra en el "**Procedimiento de Protección de la Información**".

B	L	I	46	Estas copias de seguridad deberán realizarse con una periodicidad, al menos, trimestral, salvo en el caso de que no se haya producido ninguna actualización de los datos.

M	L	I	47	Se evitará desgastar en exceso los soportes donde se realizan las copias de seguridad, rotándolos y renovándolos de forma periódica transcurridos un número determinado de grabaciones o un periodo de tiempo largo. El procedimiento para la rotación y renovación de soportes se encuentra en el "**Procedimiento de Seguridad Física**".

B	L	I	48	Los soportes destinados a copias de seguridad seguirán todas las normas definidas en el **"Procedimiento de gestión de Soportes"** (identificación, reutilización y

				eliminación, etc.).

B	L	I	49	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. El procedimiento de recuperación de datos se encuentra en el "**Procedimiento de Protección de información**".

B	L	R	50	Será necesaria la autorización por escrito del Responsable de Seguridad del Fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación. El formulario para notificar una incidencia se encuentra en el "**Procedimiento de Protección de información**".

Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre las copias de seguridad en el "**Procedimiento de Protección de información**".

3.7. Normas sobre los datos personales en soporte papel

El Real Decreto 1720/2007 regula las medidas de seguridad que es necesario implantar para asegurar la confidencialidad y la integridad de los datos personales almacenados en soporte papel (ficheros no automatizados).

Estas medidas afectan igualmente a las salas y archivadores destinadas al almacenamiento de los documentos que contengan datos personales, así como a los medios informáticos utilizados para su tratamiento, como pueden ser impresoras o fotocopiadoras.

B	L	T	51	Los documentos no automatizados que contengan datos de carácter personal, deberán almacenarse de manera que los empleados de la Universidad tendrán acceso únicamente a aquellos documentos en papel que precisen para el desarrollo de sus funciones. Deberá existir una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

B	L	T	52	Los documentos que contengan datos personales, deberán ser archivados

				de manera que se permita la correcta conservación de los documentos, la localización y consulta de la información, y que permitan la posibilidad del ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. En ningún caso se dejarán a la vista, como por ejemplo encima de una mesa.
B	F	T	53	Asimismo, los documentos deberán archivarse de modo que se permita identificar el tipo de información que contienen, debiendo estos ser etiquetados e inventariados.
B	F	T	54	Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.
B	F	T	55	Siempre que los documentos con datos personales no estén archivados, la persona que esté utilizando el documento, deberá custodiarlo y encargarse de asegurar la confidencialidad y la integridad de los datos que contiene, impidiendo el acceso a dicho documento por parte de usuarios no autorizados.
B	F	T	56	Siempre que se proceda al traslado físico de los documentos que contengan datos personales, deberán adoptarse las medidas que impidan el acceso por parte de usuarios no autorizados a la información trasladada, debiendo llevarse, además, un registro de los movimientos de los ficheros no automatizados realizados.
M	F	T	57	Los documentos impresos con datos personales, una vez que ya no sean necesarios, se destruirán físicamente de manera que no puedan recuperarse los datos que contenían (por ejemplo mediante una trituradora de papel). En ningún caso se reutilizarán este tipo de documentos (por ejemplo, no podrán ser utilizados para imprimir por la otra cara, si estuviera en blanco).
A	F	T	58	Las copias o reproducciones (fotocopias o impresos) de los documentos que contengan datos de carácter personal, sólo podrán ser realizadas

				por parte de personal autorizado, y han de ser destruidas físicamente y desechadas, una vez ya no sean útiles para la finalidad con la que fueron realizados.

A	F	T	59	Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse 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

A	F	T	60	Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos de nivel alto que puedan ser utilizados por múltiples usuarios. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

3.8. Normas sobre controles periódicos de verificación del cumplimiento

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

M	L	S I	61	El Responsable de Seguridad del Fichero comprobará, de acuerdo al procedimiento, que la lista de usuarios autorizados se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al Fichero, para lo que recabará la lista de usuarios de la aplicación y sus identificadores al Administrador o administradores del Fichero. De igual manera, comprobará que los niveles de acceso de cada usuario se corresponden con las medidas técnicas habilitadas para limitar este acceso (restricción de funciones de las aplicaciones, configuración de permisos de carpetas, etc.). También comprobará que se realizan de manera adecuada los procedimientos de gestión de usuarios y contraseñas, especialmente la renovación periódica de las contraseñas. Además de estas comprobaciones periódicas, el Administrador comunicará al Responsable de seguridad, en cuanto se produzca,

				cualquier alta o baja de usuarios con acceso autorizado al Fichero.
M	L	S I	62	Se comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo correctas que permitan la recuperación de Fichero según lo estipulado en el capítulo “Normas sobre las copias de respaldo y recuperación” de este documento.
M	L	S I	63	A su vez, y también con periodicidad al menos trimestral, los Administradores del Fichero comunicarán al Responsable de Seguridad cualquier cambio que se haya realizado en los datos técnicos de los sistemas, 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 datos en el **Anexo I** y resto de documentos.
M	L	S I	64	Será responsabilidad de los usuarios que las configuraciones hardware y software de los puestos se ajusten a lo establecido por el Responsable de Seguridad, verificando que no se hayan instalado programas sin autorización. Se hará hincapié en no instalar programas especiales como herramientas de utilidad que permitan el acceso no controlado a los ficheros de datos.
M	L	S I	65	Será responsabilidad del usuario no almacenar documentos con datos personales en los PCs que no estén autorizados. De igual manera se eliminarán los ficheros temporales, tanto en los PCs de usuario como en el servidor.
M	L	S I	66	El Responsable de seguridad, verificará, con periodicidad al menos bienal, el cumplimiento de lo previsto en los capítulos “Normas sobre la entrada y salida de datos por red” y "Normas sobre las copias de respaldo y recuperación" de este documento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.
M	L	R S	67	El Responsable de Seguridad analizará con periodicidad al menos bienal las incidencias registradas en el Registro correspondiente para, independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, adoptar las medidas correctoras que

				limiten esas incidencias en el futuro.

A	L	S	68	El Responsable de Seguridad revisará periódicamente la información de control registrada en el registro de accesos, y elaborará un informe de las revisiones realizadas y los problemas detectados.

M	L	R S	69	Al menos cada dos años, se realizará una auditoría, externa o interna, que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de Desarrollo de la LOPD (RD 1720/2007), identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoría serán analizados por el Responsable de Seguridad, quien propondrá al Responsable del Fichero las medidas correctoras correspondientes.

M	L	R S	70	Los resultados de todos estos controles periódicos, así como de las auditorías serán efectuadas y tratadas de acuerdo al **"Procedimiento de Gestión de Seguridad de la Información**".

3.9. Procedimientos de Seguridad

- Procedimiento de Control de Accesos
- Procedimiento de Seguridad Física
- Procedimiento de Seguridad Lógica
- Procedimiento de Gestión de Incidencias
- Procedimiento de Gestión de la Seguridad de la Información
- Procedimiento de Protección de la Información
- Procedimiento de Gestión de la Continuidad
- Procedimiento de Gestión de la Seguridad del desarrollo de SW
- Procedimiento de Gestión de Proveedores
- Procedimiento de Gestión de Soportes
- Procedimiento de Gestión del personal

Todos los procedimientos son accesibles a través de la Universidad Virtual.

4. Funciones y obligaciones del personal

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

R – **Responsable del Fichero:**

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

Sus principales funciones y obligaciones son:

- Implantar las medidas de seguridad establecidas en este documento.
- Garantizar la difusión de este Documento entre todo el personal que vaya a utilizar el fichero.
- Mantenerlo actualizado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo, según el Reglamento de Desarrollo de la LOPD.
- Adecuar en todo momento el contenido del mismo a las disposiciones vigentes en materia de seguridad de datos.
- Designar uno o varios responsables de seguridad.

Encargado Interno del Tratamiento:

El Responsable del Fichero delegará para el cumplimiento de sus funciones y responsabilidades en un Servicio/Unidad de la Universidad nombrado en las disposiciones de creación de los ficheros. Dicho servicio será el encargado interno del tratamiento y tomará las decisiones sobre dicho fichero (accesos autorizados, sistemas de tratamiento, flujos de información, etc.)

S – Responsable de Seguridad:

Es la persona designada por el responsable del fichero para coordinar y controlar las medidas de seguridad aplicables al fichero. Debe ser una persona con los conocimientos suficientes para llevar a cabo esa función, por tanto, debe estar al día en temas técnico-informáticos y también en temas jurídicos relativos al documento de seguridad y a la propia normativa.

Sus principales funciones y obligaciones son:

- Coordinar la puesta en marcha de las medidas establecidas en la normativa y en el documento de seguridad.
- Colaborar con el responsable del fichero en la difusión del documento de seguridad y coordinarse con éste en el cumplimiento de las medidas de seguridad.
- Habilitar el Registro de incidencias. Analizar las incidencias registradas y tomar las medidas oportunas.

I – Administradores de Sistemas y Personal de Informática: El administrador del sistema es el encargado de garantizar a los responsables y usuarios la seguridad de los datos que se procesan en la organización. Este rol puede ser desempeñado tanto por personal de la empresa como por una persona externa. Las funciones básicas del cargo de administrador de sistemas son:

- Proponer estándares y procedimientos relacionados con la seguridad.
- Desarrollar los planes de seguridad.

- Gestionar los perfiles de usuarios de los sistemas informáticos y los accesos de cada uno.
- Controlar y realizar el seguimiento de la seguridad física y lógica del entorno informático.
- Dar soporte a los usuarios en materia de seguridad.
- Evaluar los riesgos.
- Implantar equipos, dispositivos y paquetes relacionados con la seguridad física y lógica.
- Ofrecer a los usuarios finales los medios para posibilitar la actualización de los programas antivirus y canalizar las notificaciones de existencia de virus

T – Todo el personal. Usuarios: Los usuarios son todas aquellas personas que participan en alguna fase del tratamiento del Fichero. Entre sus obligaciones fundamentales se encuentran las siguientes:

- Proteger la información a la que tenga acceso en virtud de su puesto y funciones de acuerdo a lo establecido en las normas del presente Documento de Seguridad.
- No deben revelar nunca sus contraseñas ni mantenerlas escritas en lugares visibles de su puesto de trabajo.
- Son responsables ante la empresa de todas las actividades y accesos que se realicen con su código de usuario.
- Asimismo es responsable de la custodia y utilización del ordenador que le ha sido asignado.
- En el caso de las impresoras, deberá asegurarse que no quedan impresos en la bandeja de salida que contengan datos protegidos.
- Si el terminal es portátil, deberá ser guardado bajo llave o llevarlo consigo. Durante los viajes, no debe facturarse como equipaje en aeropuertos y estaciones.
- El usuario final es responsable exclusivo de la utilización del antivirus y la salvaguarda de los terminales.
- Ante cualquier incidencia, el usuario es responsable de la comunicación de la misma al Responsable de Seguridad. La falta de notificación de una incidencia conocida por un usuario, será considerada como falta contra la seguridad de los ficheros.
- Los usuarios firmarán por escrito que conocen y se comprometen a cumplir las políticas, normas, estándares y procedimientos establecidos en la empresa.

En el “Procedimiento de Control de Accesos” se detalla el registro de los nombramientos de cargos y usuarios que acceden a cada uno de los Ficheros.

Anexo I. Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición.

Las plantillas para ejercitar los derechos de acceso, rectificación, cancelación y oposición sobre los datos de carácter personal, en cumplimiento de los artículos del Título III del Real Decreto 1720/2007 de desarrollo de la LOPD, se encuentran disponibles en la página Web de la Universidad http://www10.ujaen.es/conocenos/servicios-unidades/servinfo/protecci%C3%B3ndedatosdecaracterpersonal/FormulariosDerechosARCO