Complejo Hospitalario de Palencia

Sacyl

Complejo Asistencial de Palencia

Documento de Seguridad

13 de diciembre de 2005

HOJA DE CONTROL DE DOCUMENTO

DOCUMENTO / ARCHIVO

Título: **Documento de Seguridad del Complejo Asistencial de Palencia**	Nombre Archivo**: Documento de Seguridad de Complejo Asistencial de Palencia.doc**
Fecha de Creación: **16/06/2005**	Soporte lógico**: MS-Word**
Versión**: 1**	

ACTUALIZACIONES

Versión	Fecha	Autor	Modificaciones
1	**16/06/2005**	Complejo Asistencial de Palencia	No existen cambios por ser la primera versión

INDICE

1 INTRODUCCIÓN

Los Sistemas de Información del Sacyl constituyen un elemento básico de gestión en el Sistema Sanitario de la Comunidad Autónoma de Castilla y León que debe ser objeto de una especial protección, teniendo en cuenta el tratamiento, automatizado o no, que se realiza de los datos relativos a la salud.

En concreto, la legislación aplicable actualmente es:

- ✓ La Ley Orgánica de Protección de Datos de Carácter Personal 15/1999, aprobada el 13 diciembre de 1999 y publicada en el B.O.E. el 14 de diciembre de 1999 (LOPD).
- ✓ El Real Decreto 994/1999, de 11 de junio de 1999, que recoge el Reglamento de Medidas de Seguridad de los Ficheros Automatizados de Datos de Carácter Personal aprobado el 11 de junio de 1999 y publicado en el B.O.E. de 25 de junio.

Las funciones que se puedan realizar a través de los Sistemas Informáticos y Asistenciales del Complejo Asistencial de Palencia, deben atender por un lado a facilitar las tareas propias de gestión y asistencia, y por otro, a que la información que se utiliza cumpla con los principios de confidencialidad, integridad y disponibilidad, que tanto la ley como los derechos individuales de las personas exigen.

Para dar cumplimiento a las exigencias de las leyes vigentes y a las recomendaciones de la Agencia Española de Protección de Datos, y adecuar de forma gradual y precisa los Sistemas de Información a las obligaciones que establece la citada Ley Orgánica, se elabora el presente Documento de Seguridad.

2 OBJETIVO DEL DOCUMENTO DE SEGURIDAD

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

Los ficheros de Carácter Personal existentes en esta Dirección, están descritos en el **ANEXO B. Relación de Ficheros**, donde se indica el Nivel de Seguridad exigible a cada uno de ellos.

Éste documento pretende ser una guía práctica y sencilla que permita al personal del Complejo Asistencial de Palencia, observar la legalidad en el tratamiento de los datos personales sin modificar en exceso los actuales procedimientos de actuación, pero garantizando la seguridad de esos datos frente a posibles pérdidas, alteraciones, modificaciones, o accesos no autorizados. En este sentido, recoge todas las medidas y procedimientos establecidos para garantizar la seguridad en el tratamiento de los Datos Personales, como prevé la mencionada Ley 15/99 de Protección de Datos de Carácter personal y el Reglamento de Medidas de Seguridad sobre datos aprobado por R.D. 994/99.

3 ÁMBITO DE APLICACIÓN

El alcance para la aplicación de las medidas de seguridad, que se definen en el presente Documento de Seguridad, es para todos aquellos recursos, que tal y como establece el Reglamento de Medidas de Seguridad en el artículo 1 “Ámbito de aplicación y fines”, han de ser objeto de protección al formar parte de los sistemas, recursos o soportes de los Datos de Carácter Personal, relativos a los Sistemas de Información de esta Institución.

Los Sistemas de Información del Complejo Asistencial de Palencia están formados por el conjunto de datos, procedimientos y tratamientos, automatizados o no, relativos a los empleados de ésta Institución y a las personas que acudan o hayan de ser tratadas en la misma.

Las presentes instrucciones son de aplicación en:

- ✓ Los órganos, centros y unidades del Complejo Asistencial de Palencia, tanto en los equipos de proceso de datos como en los locales donde se procesen, se utilicen, depositen o almacenen datos de carácter personal. Concretándose en las personas que intervengan en el uso, tratamiento o manipulación de la información y los datos.
- ✓ Los sistemas y equipos instalados en este centro, cualquiera que sea la forma tecnológica de creación y de almacenamiento de los datos existente o futura.
- ✓ Los ordenadores u otros dispositivos portátiles de almacenamiento o proceso de datos, en cuanto a su uso con datos relativos a Usuarios del Sistema Sanitario.
- ✓ Las redes de comunicaciones de datos, ya sean externas o locales y sus sistemas de interconexión.
- ✓ Las bases de datos, los ficheros, las aplicaciones y programas informáticos u ofimáticos para el mantenimiento y explotación de las mismas.
- ✓ Los servicios de tratamiento o archivo, automatizado o no, de Datos de Carácter Personal relativos a éste centro, que presten las empresas externas mediante contratación con esta Institución o sus órganos superiores.

4 ACTUALIZACIONES

Este Documento deberá ser actualizado[1] convenientemente cuando se produzcan modificaciones en los procedimientos y mecanismos de seguridad de acuerdo con las nuevas necesidades del Complejo Asistencial de Palencia o con cambios en la normativa sobre Protección de Datos.

El Responsable del Fichero puede delegar en el Responsable de Seguridad la función de mantenimiento del Documento de Seguridad, y la responsabilidad de que la documentación incluida en el mismo esté convenientemente actualizada.

Este Documento de Seguridad corresponde a la 1ª versión del mismo, tal y como se indica en la hoja de control del documento.

[1] Tal y como indica el Artículo 8-3 del RD 994/99.

5 NIVELES DE SEGURIDAD

El Documento de Seguridad otorga una especial relevancia a la política de seguridad definida por la organización para los Ficheros que contienen Datos de Carácter Personal, estableciendo para cada uno de los niveles de protección un conjunto de medidas mínimas a aplicar.

El Reglamento de Medidas de Seguridad establece tres niveles de seguridad:

- ✓ **Básico:** todos los Ficheros que contengan Datos de Carácter Personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.
- ✓ **Medio:** los Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos Ficheros cuyo funcionamiento se rija por el artículo 7 de la Ley Orgánica 15/99 y disposiciones concordantes del Reglamente de Seguridad (R.D. 994/99), deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.
- ✓ **Alto:** los Ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.

En el **ANEXO B. Relación de Ficheros**, se identifica la relación de los niveles de seguridad de cada uno de los Ficheros de Carácter Personal existentes en el Complejo Asistencial de Palencia.

6 RESPONSABLES DE LA SEGURIDAD DE LA INFORMACIÓN

A continuación se definen y especifican las personas que, con relación a los Ficheros de Datos de Carácter Personal del Complejo Asistencial de Palencia, automatizados o no, tienen las siguientes responsabilidades que asignan la Ley 15/1999 de Protección de datos de carácter Personal y el Reglamento de Medidas de Seguridad sobre datos aprobado por R.D. 994/1999:

- ✓ Responsable del Fichero[2]: **Director Gerente del Complejo Asistencial de Palencia.**
- ✓ Encargado del Tratamiento: **Responsable de los Sistemas de Información del Complejo Asistencial de Palencia.**
- ✓ Responsable de Seguridad: **Jefe del Servicio de Informática del Complejo Asistencial de Palencia.**
- ✓ Usuarios: **Los que utilicen el Sistema de Información del Complejo Asistencial de Palencia.**

7 FUNCIONES Y OBLIGACIONES DEL PERSONAL

Se distinguen dos funciones especiales dentro del personal: el **Responsable del Fichero** y el **Responsables de Seguridad**, siendo este último el encargado de controlar y coordinar las medidas definidas en este Documento, mientras que el Responsable del Fichero es el responsable jurídico de la seguridad de los Ficheros, así como de la implantación de las medidas orientadas a obtener esta seguridad. Debe, además, encargarse de que el personal afectado conozca las partes de este Documento que afecten a sus funciones y obligaciones.

El desempeño de las labores del Responsable de Seguridad no implica una delegación de la responsabilidad del Responsable del Fichero.

Aparte del Encargado del tratamiento, algunos Usuarios pueden estar realizando labores de explotación de los Datos de Carácter Personal o bien tratarse de personal técnico ejerciendo sus funciones de administrador o encargado del mantenimiento. En este caso siempre se dejará constancia en el registro de incidencias de la identificación de cada técnico que intervino en cada incidencia.

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

[2] Artículo 3. d). Responsable del Fichero o tratamiento: persona física o jurídica de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento

- ✓ **Administradores del sistema**, encargados de administrar o mantener el entorno operativo del Fichero. Este personal deberá estar explícitamente relacionados en el ***ANEXO H. Personal Autorizado para Acceder al Fichero***, ya que por sus funciones pueden utilizar herramientas de administración que permitan el acceso a los datos protegidos saltándose las barreras de acceso de la Aplicación.

- ✓ **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 H. Personal Autorizado para Acceder al Fichero.***

Este Documento de Seguridad es de obligado cumplimiento para todos ellos. Las funciones y obligaciones del personal están descritas en el ***ANEXO J. Funciones y Obligaciones del Personal.***

Los administradores del sistema deberán además atenerse a aquellas normas, más extensas y estrictas, que se referencian también en el Anexo anterior, 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.

8 RECURSOS PROTEGIDOS

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

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

- ✓ 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. Locales.**

- ✓ 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 F. Equipamiento.***

- ✓ Los servidores, y el entorno de sistema operativo y de comunicaciones en el que se encuentra ubicado el Fichero, que está descrito en el ***ANEXO D. Entorno del Sistema Operativo y de Comunicaciones.***
- ✓ Los sistemas informáticos, o aplicaciones establecidos para acceder a los datos están descritos en el ***ANEXO C. Descripción del Sistema Operativo y de Comunicaciones.***

9 NORMAS Y PROCEDIMIENTOS DE SEGURIDAD

9.1 CENTROS DE TRATAMIENTO Y LOCALES

Los locales donde se ubiquen los ordenadores que contienen los Datos de Carácter Personal deben ser objeto de especial protección que garantice la disponibilidad y confidencialidad de los datos protegidos, especialmente en el caso de que los datos estén ubicados en un Servidor accedido a través de una red.

- ✓ Los locales deberán contar con los medios de seguridad que eviten los riesgos de indisponibilidad de los datos que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas.
- ✓ El acceso a los locales deberá estar restringido exclusivamente a los Administradores del Sistema que deban realizar labores de mantenimiento para las que sea imprescindibles el acceso físico.
- ✓ Se establecerán controles para el acceso del personal a salas de ordenadores, salas de terminales, locales donde se almacenen o archiven Datos de Carácter Personal y almacenes de copia de seguridad.
- ✓ Los locales donde se ubiquen o archiven Datos de Carácter Personal o copias de seguridad deben estar, al menos, cerrados con llave en ausencia de personal autorizado.
- ✓ En los casos en los que el equipo esté ubicado en una zona en contacto con el público, nunca se dejará el equipo operativo sin la presencia de un Usuario autorizado.
- ✓ Se establecerán las normas oportunas para el acceso de empresas de servicios contratadas por la Institución.

La descripción de los centros de tratamiento y locales donde se encuentran ubicados los Ficheros o se almacenan los soportes que los contengan figuran en el ***ANEXO E. Locales***.

9.2 ENTORNO DEL SISTEMA OPERATIVO Y DE COMUNICACIONES

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

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

- ✓ El sistema operativo y de comunicaciones del Fichero deberá tener al menos un responsable, que, como administrador deberá estar relacionado en el ***ANEXO H. Personal Autorizado para Acceder al Fichero.***
- ✓ 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 anterior.
- ✓ 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 anterior.
- ✓ 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.
- ✓ 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.

- ✓ Los servidores tendrán deshabilitados todos los servicios que no sean imprescindibles para el funcionamiento correcto de las aplicaciones.
- ✓ Si el ordenador/servidor 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 éste acceso no se permite a personas no autorizadas.

La descripción de los Servidores y el entorno de Sistema Operativo y de comunicaciones en el que se encuentran ubicados los datos de Carácter Personal, están descritos en los Anexos: ***ANEXO D. Entorno del Sistema Operativo y de Comunicaciones*** y en el ***ANEXO F Equipamiento.***

9.2.1 Disponibilidad

Los equipos que soporten determinados procesos, cuya interrupción accidental pueda provocar la alteración o pérdida de Datos de Carácter Personal o documentos administrativos, deben estar protegidos contra fallos de suministro eléctrico mediante sistemas de alimentación ininterrumpida.

Los equipos que soporten procesos especialmente críticos deben ser equipos de alta disponibilidad, que posean mecanismos tolerantes a fallos.

Los equipos deben mantenerse de acuerdo con las especificaciones de los suministradores o fabricantes.

Las áreas físicas donde se encuentren situados los equipos deben encontrarse convenientemente aseguradas frente a riesgos derivados de accesos indeseados así como ante amenazas del entorno, tales como fuegos, humos, agua, ...

9.3 APLICACIONES CON ACCESO A DATOS PERSONALES

Son todos aquellos Sistemas Informáticos, programas o aplicaciones con las que se puede acceder a los datos y que son normalmente utilizados por los Usuarios para acceder y actualizar los datos.

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

Estos sistemas y/o sus usuarios deberán cumplir de forma general, al menos, los siguientes requerimientos:

- ✓ Los Sistemas Informáticos de acceso a los datos deberán tener su acceso restringido mediante un código de Usuario y una Contraseña.
- ✓ Todos los Usuarios de estas aplicaciones deben estar autorizados para acceder a los datos y 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.
- ✓ Si la Aplicación informática que permite el acceso al Fichero no cuenta con un control de acceso, deberá ser el Sistema Operativo el que impida el acceso no autorizado, mediante el control de los citados códigos de Usuario y contraseñas.

Estos sistemas y/o sus usuarios deberán cumplir de forma específica, según el nivel de sensibilidad de la información contenida, los siguientes requerimientos:

- ✓ **Nivel Medio:** En cualquier caso se controlarán los intentos de acceso fraudulento, limitando el número máximo de intentos fallidos, y cuando sea técnicamente posible, guardando en un Fichero auxiliar la fecha, hora, código y clave errónea que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de accesos fraudulentos. Si durante las pruebas anteriores a la implantación o modificación de la Aplicación se utilizasen datos reales, se deberá aplicar a esos datos de prueba el mismo tratamiento de seguridad que se aplica a los originales.
- ✓ **Nivel Alto:** De cada acceso se guardarán, como mínimo, la identificación del Usuario, la fecha y hora en que se realizó, el Fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Si se trata de un acceso autorizado, se guardará la clave del registro o bien la información que permita identificar el registro accedido, el período mínimo de conservación de los datos registrados será de dos años.

La descripción de las aplicaciones con acceso a datos personales, está descrita en el ***ANEXO C. Descripción del Sistema Informático de Acceso al Fichero.***

9.3.1 Trazabilidad

Las aplicaciones deben estar dotadas de pistas de auditorías, que deberán registrar el código de usuario, fecha, hora y proceso mediante el que se ha realizado un alta, modificación, baja o consulta de cualquier información de carácter personal de nivel 3, tal y como recoge en el Artículo 24 del Real Decreto 994/1999 de 11 de Junio en el que se regulan las medidas de seguridad de los ficheros automatizados que contengan Datos de Carácter Personal.

9.4 PUESTOS DE TRABAJO

Puestos de trabajo son todos aquellos dispositivos desde los cuales se puede acceder a los datos del Fichero, como, por ejemplo, consolas de administración, terminales, ordenadores personales de sobremesa y portátiles, e impresoras.

- ✓ Cada puesto de trabajo estará bajo la responsabilidad de una persona de las autorizadas en el ***ANEXO H. Personal Autorizado para Acceder al Fichero***, que garantizará que la información que muestra no pueda ser vista por personas no autorizadas.
- ✓ Tanto las pantallas como las impresoras u otro tipo de dispositivos deberán estar ubicados en lugares que garanticen esa confidencialidad y en lugares no visibles al público.
- ✓ Cuando el responsable de un puesto de trabajo lo abandone temporalmente o 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.
- ✓ En el caso de las impresoras, deberá asegurarse de que no quedan documentos impresos que contengan datos protegidos. Si las impresoras son compartidas con Usuarios no autorizados, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
- ✓ Queda expresamente prohibida la conexión vía MODEM a redes o sistemas exteriores a los puestos de trabajo desde los que se pueda realizar acceso a los datos. La revocación de

esta prohibición será autorizada por el responsable de los datos, quedando constancia de esta modificación en el Libro de Incidencias.

- ✓ Los usuarios no deben incorporar programas en sus puestos de trabajo, respetando la configuración de aplicaciones ofimáticas, antivirus, etc., establecidos como corporativos manteniendo una configuración fija en sus Sistemas Operativos que sólo podrá ser cambiada bajo la autorización del Responsable de Seguridad.

- ✓ Los usuarios no deben mantener ningún dato de carácter personal en sus estaciones de trabajo (fija o portátil). En el caso de que existan usuarios con información de Carácter Personal almacenada en sus ordenadores, deberán comunicarlo inmediatamente al Responsable de Seguridad, **quedando terminantemente prohibido, el almacenamiento "particular" de éste tipo de datos.**

La relación de los puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso al Fichero está descrita en el ***ANEXO F. Equipamiento.***

9.5 PERSONAL AUTORIZADO

Se deberá asignar a cada Usuario el nivel de acceso restringido a los datos que sean necesarios e imprescindibles para su labor profesional, mediante una contraseña de uso y conocimiento exclusivo del Usuario, que deberá cambiarse periódicamente. Se deberán crear Usuarios y contraseñas individuales, nunca genéricas[3].

Se deberán crear una relación de Usuarios, en la que figure la identidad del Usuario, su identificativo, los accesos a locales, servidores, equipos y aplicaciones autorizadas y los motivos de autorización. Se adoptarán las medidas necesarias para mantener actualizada ésta relación de Usuarios.

Se deberán realizar Auditorias en todos los Sistemas de las operaciones realizadas por cada Usuario, de forma periódica, con el objetivo de cumplir las normas de seguridad y control de datos, el resultado de las Auditorias realizadas deberán incluirse en el ***ANEXO O. Controles Periódicos y Auditorias.***

[3] Una cuenta común (utilizada por múltiples usuarios), disminuye o elimina completamente la capacidad de auditar, ya que impide la identificación única por usuario en sistema.

El inventario del personal con acceso a los Datos de Carácter Personal se encuentra descrito en el ***ANEXO H. Personal Autorizado para acceder al Fichero.***

9.6 ARCHIVOS NO AUTOMATIZADOS

La ley de Protección de Datos de Carácter Personal tiene ámbito de aplicación sobre cualquier tipo de Fichero de datos de Carácter Personal con independencia de cual sea su soporte físico y los tipos de tratamientos que se realicen (Ley 15/99, Art. 1 y 2).

Los Archivos no automatizados son conjuntos de datos organizados de carácter personal cuyo soporte físico es un soporte "no informático". Por lo tanto, será cualquier Fichero "manual" o cualquier Fichero en un soporte convencional. Dichos Ficheros o Archivos no automatizados, se considerarán igualmente "recursos a proteger".

Se deberá elaborar una relación de los Archivos y/o Ficheros no automatizados existentes. Dicha relación especificará: objetivo o función del Fichero, localización física, o ámbitos en el caso de estar distribuido, Servicio o Unidad que realiza los tratamientos y responsable de dicho Servicio o Unidad, estará identificado en el ***ANEXO M. Relación Archivos y Ficheros no Automatizados.***

Se deberá poner especial cuidado en todos aquellos Ficheros que la ley considera como "especialmente sensibles":

- ✓ **Expedientes de Personal:** Informes reservados, nóminas, incapacidad temporal, comunicaciones, afiliación sindical, productividad, sentencias judiciales, etc.
- ✓ **Historias Clínicas manuales:** Informes o estudios, pruebas radiográficas, analíticas, electros, pruebas anatomopatológicas, etc.
- ✓ Otros estudios, pruebas o documentos con información "sensible" que se encuentren en Servicios de Urgencias, Servicios de Admisión, Áreas de Hospitalización, Áreas de Consultas, Áreas Quirúrgicas, Servicios Centrales, Laboratorios, etc.

En los lugares donde se encuentren Archivos y/o Ficheros no automatizados de carácter personal se deberán adoptar las medidas de seguridad necesarias para garantizar la confidencialidad de dichos datos, y se deberán extremar las medidas en aquellos recintos o dependencias donde exista tránsito de público.

Cada Usuario será responsable de garantizar la confidencialidad de la información que extraiga del Archivo hasta su retorno a dicho Archivo, poniendo especial cuidado en aquellos puestos de trabajo con atención al público o con tránsito de personal ajeno a la Institución.

Se deberán poner especial cuidado en el desecho, destrucción o cancelación de soportes no automatizados, que contengan información de nivel alto.

9.7 SALVAGUARDA Y PROTECCIÓN DE CONTRASEÑAS PERSONALES

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

- ✓ Sólo podrán tener acceso a los datos del Fichero las personas relacionadas en el ***ANEXO H. Personal Autorizado para Acceder al Fichero***.
- ✓ 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 registrarse como incidencia y proceder inmediatamente a su cambio.
- ✓ Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el ***ANEXO I. Control y Seguridad.***
- ✓ El archivo donde se almacenen las contraseñas, en caso de ser almacenadas en algún tipo de soporte, deberá estar protegido y bajo la responsabilidad del administrador del sistema.

10 GESTION DE INCIDENCIAS

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

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

- ✓ Existirá un Libro de Incidencias a disposición de todos los usuarios y administradores del Fichero con el fin de que se registren en él, cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.
- ✓ Cualquier usuario que tenga conocimiento de una incidencia es responsable del registro de la misma en el Libro de Incidencias del Fichero o en su caso de la comunicación por escrito al responsable de seguridad o al responsable del Fichero.
- ✓ 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.
- ✓ 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 registro de incidencias está descrito en el ***Procedimiento de Notificación y Gestión de Incidencias***

11 GESTION DE SOPORTES

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

Dado que la mayor parte de los soportes que hoy en día se utilizan, como disquetes o CD-ROMs, “pen drives”, 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:

- ✓ Los soportes que contengan datos del Fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.

- ✓ 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.

- ✓ Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso del Fichero, que no estén por tanto relacionadas en el ***ANEXO H. Personal Autorizado para Acceder al 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, utilizando para ello el documento adjunto en el ***Procedimiento de Gestión de Soportes.***

- ✓ El responsable del Fichero mantendrá un libro de registro de entradas y salidas donde se guardarán los formularios de entradas y de salidas de soportes descritos en el ***Procedimiento de Gestión de Soportes***, con la indicación del 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 autorizados.

- ✓ 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.

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

- ✓ Han de utilizarse las destructoras de documentos existentes para destruir cualquier soporte en papel, plástico, cintas o cualquier otro medio que contenga Datos de Carácter Personal y ya no sea necesaria su utilización.

12 ENTRADA / SALIDA DE DATOS POR RED Y TELECOMUNICACIONES

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

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

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

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

- ✓ La transmisión de Datos de Carácter Personal de nivel alto a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

13 PROCEDIMIENTO 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.

- ✓ 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.
- ✓ 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 ***Procedimiento de Respaldo y Recuperación***.

Será necesaria la autorización por escrito del Responsable del Fichero tal y como se indica en el ***Procedimientos de Notificación y Gestión de Incidencias***, 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.

Para Ficheros, a los que corresponda un nivel de seguridad alto, la copia de respaldo y procedimientos asociados, deben almacenarse en lugar separado del habitual donde reside el Fichero y que reúna las medidas de seguridad apropiadas.

14 CONTROLES PERIÓDICOS DE VERIFICACIÓN

Para ficheros de nivel alto, la veracidad de los datos contenidos en los anexos de este documento, así como el cumplimiento de las normas que contiene deberán ser periódicamente comprobados, de forma que puedan detectarse y subsanarse anomalías. Estos controles son exigibles para ficheros de nivel alto.

- ✓ El responsable de seguridad del Fichero comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados del ***ANEXO H. Personal Autorizado para Acceder al Fichero***, se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al Fichero, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador o administradores del Fichero. Además de estas comprobaciones periódicas, el administrador comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al Fichero.

- ✓ Se comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación del Fichero según lo estipulado en el apartado ***GESTION DE SOPORTES***, de este documento.

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

- ✓ El responsable de seguridad, verificará, con periodicidad al menos trimestral, el cumplimiento de lo previsto en los apartados ***GESTION DE INCIDENCIAS*** y ***GESTION DE SOPORTES***, de este documento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.

- ✓ El responsable del fichero junto con el responsable de seguridad, analizarán con periodicidad al menos trimestral las incidencias registradas en el libro correspondiente, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, adoptar las medidas correctoras que limiten esas incidencias en el futuro.

- ✓ Al menos cada dos años, se realizará una auditoría, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de seguridad, identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoría serán analizados por el responsable de seguridad, quien propondrá al responsable del Fichero las medidas correctoras correspondientes.

- ✓ Para ficheros de nivel alto los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad sin que se deba permitir, en ningún caso la desactivación de los mismos. El responsable de seguridad se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

Los resultados de todos estos controles periódicos, así como de las auditorías serán adjuntados a este Documento de Seguridad en el ***ANEXO N. Controles Periódicos y Auditorías.***

15 CUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD

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.

Todas las personas que tengan acceso a los datos del 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.