Manual de usuario en materia de protección de datos de carácter personal

CURIA PROVINCIAL DE LA ORDEN HOSPITALARIA DE HERMANOS DE SAN JUAN DE DIOS PROVINCIA BETICA

CABERSEG

ÍNDICE

1. Introducción

La protección de los datos de carácter personal de los ciudadanos ha sido regulada por el legislador español mediante la L.O. 15/1999 (LOPD) y una serie de normas que la desarrollan y complementan, que establecen toda una serie de medidas de obligado cumplimiento para aquellas entidades que, en el ejercicio de su actividad, sometan a tratamiento este tipo de datos de carácter personal.

El RD 1720/2007 (Reglamento de desarrollo de la LOPD, o RDLOPD), desarrolla los principios y obligaciones dispuestos en la LOPD.

La LOPD y el RDLOPD, cuyo objeto principal lo constituye la salvaguarda del derecho al honor, la intimidad personal y la propia imagen de las personas físicas, atribuyen determinadas funciones y obligaciones a todas aquellas personas que intervienen en el tratamiento de los ficheros donde se almacenan los datos de carácter personal.

La Ley impone sanciones económicas muy elevadas a las organizaciones privadas (sanciones que pueden llegar - sólo por una infracción - hasta los 600.000 euros) y sanciones no económicas pero si de otra índole (publicidad de la sanción, inmovilización temporal del fichero, etc.) a las organizaciones públicas.

Es, por tanto, objeto de este manual el detallar las funciones y obligaciones que, como usuario de los ficheros con datos de carácter personal de la entidad, le corresponde conocer y respetar.

2. Glosario de términos básicos

DATOS DE CARÁCTER PERSONAL: cualquier información concerniente a personas físicas identificadas o identificables.
Es decir, cualquier dato que podamos relacionar con personas físicas. En el ámbito de las empresas esas personas serán normalmente potenciales clientes, clientes, proveedores, trabajadores de la empresa, terceros o personas de contacto. En algunos ámbitos concretos de actividad puede que los datos se refieran a otras personas como pacientes, asociados ... o por ejemplo en el ámbito público dichos afectados son los ciudadanos, contribuyentes etc., además de algunos afectados comunes al ámbito privado: por ejemplo los empleados, proveedores, contactos, etc... Téngase en cuenta que no sólo se refiere a personas identificadas (cuando tengamos su nombre) sino también cuando esas personas sean razonablemente identificables por ejemplo a través de un identificador: por ejemplo número de colegiado, DNI, IP, correo electrónico etc...
AFECTADO O INTERESADO: persona física titular de los datos.
Es la persona cuyos datos se tratan, es decir: el cliente, paciente, ciudadano, empleado, proveedor, contacto, etc...
TRATAMIENTO DE DATOS: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
Téngase en cuenta que a tenor de la definición de tratamiento que da la Ley cualquier operación que se haga con ellos: grabarlos, modificarlos, conservarlos, enviarlos, etc., constituirá tratamiento.
FICHERO: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. Es decir, cualquier dato que tengamos sobre personas físicas en cualquier tipo de soporte, tanto papel como a nivel informático.
El concepto de fichero no se corresponde necesariamente con una base de datos, sino que siempre que exista un conjunto de datos que estén organizados mediante algún criterio, nos encontraremos ante la existencia de un fichero. Obviamente una aplicación informática de nóminas constituye un ejemplo de fichero, pero también lo puede constituir una tabla de datos en Word, sin olvidar que también es aplicable este concepto a los datos no automatizados: por ejemplo un archivo A-Z.
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.
El responsable del fichero normalmente coincidirá con la organización: la empresa, asociación, institución, empresarios individual, profesional, etc. y es a quien se le imponen la mayoría de las obligaciones en protección de datos siendo, por tanto, normalmente el responsable de las sanciones que - en su caso - se impongan. Ello sin perjuicio de que el responsable del fichero pueda nombrar una persona física que le represente.
ENCARGADO DEL TRATAMIENTO: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
El encargado del tratamiento es un tercero (normalmente una empresa pero no necesariamente) que le presta un servicio al responsable del fichero y que para ello requiere acceder a datos del responsable. Ejemplos típicos de encargados lo son la asesoría laboral, contable o fiscal (que acceden a los datos de empleados, clientes o proveedores de su cliente para asesorarle), empresas de mantenimiento de hardware o software, etc. El servicio que presta el encargado no tiene porqué ser remunerado. La relación entre el responsable y el encargado se debe regular mediante un contrato cuyo contenido establece el artículo 12 de la LOPD.
USUARIOS: sujeto o proceso autorizado a acceder a datos o recursos.
Normalmente un usuario será una persona que accede a datos de la organización. El usuario podrá tener diferentes perfiles de acceso y ser un usuario interno o externo (un usuario de otra organización que accede a nuestro sistema para prestar un servicio, por ejemplo mantenimiento informático).
RESPONSABLE INTERNO DEL FICHERO: persona o personas responsables de la información.
Normalmente se corresponden con los jefes de departamentos o jefes de unidades.

RESPONSABLE DE SEGURIDAD: El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.
El responsable de seguridad puede ser uno o varios y son los encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero, que es a quien en primera instancia se le pueden imponer en su caso las sanciones que contempla la Ley. Ello es sin perjuicio de que el responsable de seguridad si no cumple con sus obligaciones pueda tener responsabilidad laboral o disciplinaria.
CONSENTIMIENTO: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
Téngase en cuenta que el consentimiento es el eje vertebral de la protección de datos y ello exige que como regla general no se puedan tratar datos de nadie sin su consentimiento, sin perjuicio de que en ocasiones esta obligación está exenta. Por ejemplo: cuando los datos se traten en el marco de la relación negocial, laboral o administrativa, cuando exista una Ley que disponga lo contrario, etc...
COMUNICACIÓN DE DATOS: Toda revelación de datos realizada a una persona distinta del interesado.
La cesión de datos debe estar, salvo excepciones, necesariamente consentida por el interesado. Por ello, es importante no comunicar datos de carácter personal a otras personas físicas o jurídicas, salvo que se disponga del consentimiento de dicha persona o se esté ante alguna de las excepciones previstas por la Ley.

3. Niveles de seguridad de los datos

Las medidas de seguridad que dispone el RDLOPD se dividen en tres niveles, según la sensibilidad de los datos que se contienen en los ficheros: nivel básico, medio y alto. Las medidas se aplican de modo acumulativo.

Tenga en cuenta que deberán cumplirse - como mínimo - las medidas correspondientes al nivel asignado al fichero. Sin embargo, el Responsable de Seguridad podrá implementar medidas de nivel superior cuando lo considere oportuno.

NIVEL	DESCRIPCIÓN
Básico	• Todos
Medio	• Los relativos a la comisión de infracciones administrativas o penales. • Los relativos al art. 29 LOPD (ficheros de solvencia patrimonial y crédito). • Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias. • Aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. • Aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social. • Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros. • Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.
Alto	• Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. • Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas. • Aquellos que contengan datos derivados de actos de violencia de género.
EXCEPCIONES	• A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento (registro de accesos). • En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando: a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros. b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad. c) También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

4. Funciones y obligaciones de los usuarios

El personal que, para el correcto desarrollo de su labor, tiene autorizado acceso a datos personales, tiene las siguientes obligaciones:

CON RESPECTO A FICHEROS AUTOMATIZADOS

1. OBLIGACIONES GENERALES

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

Constituye una obligación del personal notificar al responsable del fichero o de seguridad en su caso las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en su Capítulo 5.

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

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

1. Administradores del sistema, encargados de administrar o mantener el entorno operativo /informático de los Ficheros automatizados. Este personal deberá estar explícitamente relacionado, 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.

2. Usuarios de los Ficheros, o personal que usualmente accede a los Ficheros, y que también deben estar explícitamente relacionados.

Los usuarios de los Ficheros de datos personales son aquellas personas autorizadas para acceder a los datos o recursos protegidos.

Además del personal anteriormente citado, se ha definido un Responsable de Seguridad, cuyas funciones serán las de coordinar y controlar las medidas definidas en el Documento de Seguridad, sirviendo al mismo tiempo de enlace con el Responsable del Fichero, sin que esto suponga en ningún caso una delegación de la responsabilidad que corresponde a éste último.

Este documento es de obligado cumplimiento para todos ellos.

Funciones y Obligaciones que afectan a todo el personal

Ficheros de Nivel Básico

Conocer las medidas de seguridad que afectan al desarrollo de sus funciones así como las consecuencias en que pudieran incurrir en caso de incumplimiento de dichas medidas.

Identificación y Autenticación. (Salvaguarda y protección de contraseñas)

Acceder al sistema de información por medio de un procedimiento que permita la identificación de forma inequívoca y personalizada, a través de contraseña.

Hacer un buen uso de las contraseñas, respetando la confidencialidad de las mismas, que son personales e intransferibles.

Asegurar la confidencialidad de las contraseñas y en el caso de que la contraseña fuese conocida de forma fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como una incidencia y proceder de inmediato a su cambio.

Control de accesos.

Acceder de forma autorizada únicamente a aquellos datos y recursos necesarios para el desarrollo de sus funciones.

Puestos de trabajo

Garantizar que la información que se muestra en los puestos de trabajo no sea visible a personas no autorizadas.

Al abandonar el puesto de trabajo, activar un protector de pantalla, de manera que impida la visualización de los datos.

Retirar de forma inmediata todos los documentos impresos de la impresora, para evitar así, el acceso de usuarios no autorizados a los datos personales.

Destruir todo el papel cuyo destino sea la papelera, evitando así el acceso a información confidencial.

Gestión de incidencias.

Comunicar las incidencias al Responsable de Seguridad o al Departamento de Sistemas. En caso de no comunicar las incidencias, se considerará falta grave contra la seguridad del Fichero por parte del usuario.

Ficheros de Nivel Medio

Únicamente podrá acceder al Centro de Procesos de Datos (CPD), el personal autorizado.

Funciones y Obligaciones para el personal contratado.

En los contratos laborales figurará una cláusula que garantice el compromiso de confidencialidad de los trabajadores, por el que se obligan al deber de secreto respecto de la información a la que tengan acceso.

Tener conocimiento de la existencia del Manual de Usuario LOPD, tanto el personal contratado, como aquellas personas con las que la Entidad mantenga una relación mercantil.

Acceder únicamente a los datos personales a los que estén autorizadas, tanto las personas contratadas laboralmente, como aquellas con las que la Entidad mantenga una relación mercantil.

Funciones y Obligaciones con las empresas prestadoras de servicios.

Celebrar un contrato de prestación de servicio con todas aquellas empresas que presten un servicio a la organización, indicando el tipo de tratamiento que han de realizar las distintas empresas y que medidas de seguridad tienen que adoptar.

Incluir en los contratos de prestación de servicios que se suscriban con empresas cuyo servicio no conlleva tratamiento de datos de carácter personal, una cláusula regulando expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto de aquellos datos que hubiera podido conocer durante la prestación del servicio.

Cuando se contrate un servicio puntual concertado por el centro, (por ejemplo servicio informático), firmar una cláusula de confidencialidad o introducir esa cláusula en la hoja de encargo profesional del servicio que se contrate.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los soportes y documentos que los contengan, o a los recursos del sistema de información.

Ficheros afectados de CURIA PROVINCIAL DE LA ORDEN HOSPITALARIA DE HERMANOS DE SAN JUAN DE DIOS PROVINCIA BETICA
OBRA SOCIAL
META4
FINANCIALS
CURRICULUM
HERMANOS
FORMACIÓN EXTERNA
AGENDA
REVISTA
VIDEOVIGILANCIA
HISTORIAL CLÍNICO

CON RESPECTO A FICHEROS NO AUTOMATIZADOS

1. Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la sociedad.
2. Mantener debidamente custodiadas las llaves de acceso a las instalaciones de la sociedad, a sus despachos y a los armarios, archivadores u otros elementos que contenga ficheros no automatizados con datos de carácter personal, debiendo poner en conocimiento del Responsable de Seguridad cualquier hecho que pueda haber comprometido esa custodia.
3. Cerrar con llave las puertas de los despachos al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.
4. Comunicar al Responsable de Seguridad, conforme al procedimiento de notificación, las incidencias de seguridad de las que tenga conocimiento.

5. Queda prohibido el traslado sin autorización de su superior, de cualquier listado o documento análogo con datos de carácter personal en los que se almacene información titularidad de la sociedad, fuera de los locales de la misma.
6. Guardar todos los soportes físicos o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.
7. Asegurarse de que no quedan documentos impresos que contengan datos protegidos impresos en la bandeja de salida de la impresora.
8. Únicamente las personas autorizadas para ello en el listado de accesos podrán introducir, modificar o anular los datos contenidos en los ficheros objeto de protección. Los permisos de acceso de los usuarios a los diferentes ficheros son concedidos por el Responsable de Seguridad, previa autorización del Responsable del Departamento del usuario que solicita el acceso. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no está autorizado, deberá ponerlo en conocimiento de su superior, que una vez autorizado lo comunicará al Responsable de Seguridad.
9. Ficheros de carácter temporal son aquellos en los que se almacenan datos de carácter personal, generados para el cumplimiento de una necesidad determinada, siempre y cuando su existencia no sea superior a un mes. Los ficheros de carácter temporal deben ser destruidos una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán contemplarse las medidas de seguridad contenidas en este documento.

5. Gestión de incidencias

Se entiende por incidencia cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

En caso de conocer alguna incidencia ocurrida, el usuario debe comunicarla al responsable de seguridad competente que adoptará las medidas oportunas.

Las incidencias pueden afectar tanto a ficheros automatizados como no automatizados.

Ejemplos de incidencias comunes que pudieran afectar a los datos personales contenidos en ficheros automatizados, son las siguientes:

- Alteración en los permisos, altas o bajas de usuarios.
- Accesos no autorizados.
- Bloqueo de cuenta por reiteración de intentos de conexión fallidos.
- Pérdida de datos.

Por su parte algunos ejemplos de incidencias que pueden afectar a ficheros no automatizados son los siguientes:

- Robo o pérdida de llaves de lugares o soportes en donde se almacenen dichos ficheros no automatizados.
- Desaparición de documentos o soportes que contengan datos personales.

No obstante dicha relación no es taxativa y debe comunicar al responsable de seguridad cualquier incidencia que afecte a la seguridad de los datos de carácter personal.

El procedimiento de gestión de incidencias implantado en la organización es el siguiente:

1. El usuario que tenga conocimiento de la incidencia se responsabiliza directa y personalmente de recabar la siguiente información: tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas. Dicha información deberá entregarla a continuación y sin demora al Responsable del departamento para su comprobación y validación, el cual lo remitirá al Responsable de Seguridad.

2. El Responsable de Seguridad tomará de inmediato las medidas oportunas para que, en el menor tiempo posible, se subsane la anomalía que haya generado la incidencia.
3. En el caso de que se hayan visto afectados ficheros con datos de nivel medio o alto y sea necesario llevar a cabo algún procedimiento de recuperación de datos, será imprescindible que el Responsable del Departamento que trata dicho fichero, autorice la ejecución del citado procedimiento.
4. No registrar una incidencia de la que se haya tenido conocimiento, o no comunicarla al Responsable, será considerado una falta contra la que se impondrán las sanciones previstas para este tipo de faltas especificadas en la normativa laboral aplicable a la organización.

Los responsables de seguridad designados por la organización para la gestión de incidencias son:

CARGO	NOMBRE	EMAIL
Responsable de Seguridad en Aspectos Legales	Manuel José García Romero	Manueljose.Garcia@sjd.es
Responsable de Seguridad en Aspectos Técnicos	Manuel José García Romero	Manueljose.Garcia@sjd.es
Responsable de Seguridad en Aspectos de Procedimientos	Manuel José García Romero	Manueljose.Garcia@sjd.es

6. Ejercicio de derechos

La legislación sobre protección de datos otorga a los interesados una serie de derechos que estos podrán ejercitar en relación con sus datos personales. Estos derechos son el derecho de acceso, rectificación, oposición y cancelación, en relación con sus datos personales.

Existen unos usuarios (a los que denominamos usuarios de atención) que son los encargados de recoger estas peticiones (Departamento de Administración). No obstante tenga en cuenta que en el caso de que usted reciba una consulta verbal o petición de ejercicio de derechos deberá actuar siguiendo el procedimiento establecido por la organización:

El procedimiento de gestión y resolución de ejercicios de derecho consiste en:

1. Ante la consulta (por ejemplo llamada) sobre algún ejercicio de derechos por parte de algún interesado:
   - Dar información sobre en qué consiste el Derecho, plazos etc... Es decir sobre el procedimiento.
   - No ofrecerle datos sobre la persona, sobre el fondo del asunto, etc.
   - Tomar nota (sólo tomar nota) de la persona de que se trata (de su identidad) y del motivo.
   - Hacerle llegar (si lo pide) el impreso correspondiente para ejercitar el derecho por una vía que permita dejar constancia (reporte de fax o copia email).
2. Ante la recepción de alguna petición de ejercicio de derechos (normalmente por carta, fax o email), remitir la solicitud inmediatamente a la Responsable de Atención al Cliente si se trata de datos de clientes, y para cualquier otro fichero, remitir la petición al responsable de seguridad.
3. Ante cualquier otra cuestión en esta materia, acudir al responsable de seguridad.

Los responsables designados por la organización para la resolución de las peticiones de ejercicio de derechos son:

CARGO	NOMBRE	EMAIL
Responsable de Seguridad en Aspectos Legales	Manuel José García Romero	Manueljose.Garcia@sjd.es

7. Procedimiento para el uso del correo electrónico

La organización ha definido una política de uso y control del correo. Como usuario deberá conocerla y cumplirla.

El procedimiento de uso y control del correo electrónico de la organización es el siguiente:

Los usuarios tienen prohibido el empleo del correo electrónico (interno o externo) para el envío de información de carácter personal de nivel alto, salvo que cuenten con autorización expresa del Responsable de seguridad. En cualquier caso, el envío de esta información se realizará siempre cifrando el correo, o bien adoptando cualquier otro tipo de medida que evite el acceso o manipulación de la información por terceros.

8. Procedimiento para los envíos telemáticos

El RDLOPD, para los ficheros de nivel alto, obliga al cifrado de datos o la utilización de cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros, cuando los mismos vayan a ser objeto de transmisión a través de redes públicas o redes inalámbricas.

El envío de datos a través de redes de telecomunicaciones supone la adopción de una serie de medidas organizativas y técnicas que se han de respetar y constituyen el procedimiento a seguir. Este procedimiento afecta a diversos niveles:

1) A nivel organizativo:

a) Los usuarios deben conocer (y así se debe reflejar en su manual y/o en las normas usuario del sistema de información) las pautas a seguir al respecto.

b) El usuario deberá contar con la autorización del Responsable del Fichero o del Responsable de Seguridad, que tenga atribuidas estas funciones por delegación.

2) A nivel técnico, el Usuario, bien por su propia cuenta, mediante los mecanismos que se hubieran puesto a disposición o bien, por parte del Responsable de Seguridad y/o técnico informático, debe proceder al cifrado de los datos o la utilización de cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

9. Procedimiento de registro de entrada/salida de soportes

El procedimiento de entrada de soportes y documentos a los que se refiere el presente documento es el siguiente:

Los únicos soportes informáticos con datos de carácter personal que se manejan son las cintas con copias de seguridad (back-up) de la información corporativa, que son controladas y mantenidas por el Departamento de Informática. El usuario no podrá utilizar soportes para contener datos de carácter personal sin la autorización del encargado del tratamiento y en el caso de que se tenga autorización, dichos soportes deberán ser inventariados.

El procedimiento de salida de soportes y documentos a los que se refiere el presente documento es el siguiente:

Ficheros de Nivel Básico.

La salida de soportes informáticos que contengan datos de carácter personal fuera de los locales donde está ubicado el Fichero, ha de ser expresamente autorizada por el Responsable del Fichero.

Se realizará el transporte con la correspondiente autorización.

Se custodiarán los soportes con la debida diligencia.

Ficheros de Nivel Medio.

Cuando los soportes vayan a salir fuera de los locales donde 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.

Ficheros de Nivel Alto

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.

Además en las entradas y salidas de dichos soportes, deberá registrarse la siguiente información:

	ENTRADA o SALIDA	**Identificación Del soporte**	**Fecha y hora**	**Emisor / Receptor**	**Número de soportes**	**Información Contenida**	**Forma de envío**	**Persona responsable de entrega / recepción**
1.								
2.								
3.								
4.								
5.								

10. Procedimiento de desechado y reutilización de soportes automatizados

El desechado y/o reutilización de soportes y documentos que contienen datos personales, tanto en ficheros automatizados como no automatizados, pueden suponer el acceso indebido por parte de terceros a los datos personales que se contienen en los mismos, si no se realiza de forma correcta.

En el caso de soportes automatizados (medida a adoptar para TODOS LOS NIVELES) siempre que vaya a desecharse cualquier soporte automatizado que contenga datos de carácter personal (cualquiera que sea su nivel) deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior. También deberá procederse al borrado de la documentación cuando el soporte vaya a reutilizarse.

La organización ha definido un procedimiento para el desechado o reutilización de soportes automatizados, el mismo se detalla a continuación. Como usuario deberá conocerlo y cumplirlo: Cuando haya que desechar o destruir un soporte magnético, previamente se borrará la información que contiene y luego se procederá a su destrucción física, en un crematorio o partiéndolo en trozos, de forma que resulte imposible volver a usarlo.

Los métodos a utilizar dependerán del soporte en cuestión, en primer lugar y como medida estándar se tratará de eliminar la información existente de los soportes magnéticos, borrándola y grabando encima una información irrelevante.

En los ordenadores que sean retirados por cambio, debe garantizarse la inexistencia de información sensible mediante un formateo de bajo nivel.

En caso de no ser posible, (discos duros averiados), deberá garantizarse su destrucción física mediante aplastamiento o taladro.

Siempre que se deseche un fichero en papel o cualquier otro soporte que contenga datos de carácter personal o confidencial, incluyendo discos compactos (CD o DVD), tarjetas de memoria, memorias USB o discos flexibles, estos deberán ser destruidos en una máquina trituradora que impida el posterior acceso a la información.

11. Procedimiento de desechado y reutilización de soportes no automatizados

El desechado y/o reutilización de soportes y documentos que contienen datos personales, tanto en ficheros automatizados como no automatizados, pueden suponer el acceso indebido por parte de terceros a los datos personales que se contienen en los mismos si no se realiza de forma correcta.

En el caso de soportes no automatizados (medida que se ciñe al NIVEL ALTO, pero que se puede ampliar si así se indica en el procedimiento a otros niveles) deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Todo usuario deberá conocer y cumplir el procedimiento establecido por la organización para el desechado de soportes no automatizados, que se indica a continuación.

Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante una máquina trituradora de papel, para evitar el acceso a la información contenida en el mismo o su recuperación posterior. Las medidas a aplicar serán:

En el caso de que se trate de documento en papel, cuando éstos contengan datos de carácter personal, queda prohibida su reutilización (a modo de papel reciclado). En todo caso, se procederá a su destrucción mediante el uso de la destructora de papel.

12. Procedimiento de custodia de soportes no automatizados

Algunos dispositivos de almacenamiento de los documentos que contengan datos de carácter personal disponen de mecanismos que obstaculizan su apertura. En relación con aquellos soportes que no dispongan de dichos

mecanismos, se encontraran al cargo de una persona que los custodiara e impedirá en todo momento que pueda ser accedida por persona no autorizada.

13. Procedimiento de archivo de ficheros no automatizados

Una vez los documentos hayan sido utilizados para el fin con que se solicitaron o se obtuvieron, serán entregados, devueltos o destruidos. Sólo se guardarán archivados cuando sea estrictamente necesaria su conservación. Las copias, por contener la misma información que los documentos originales, se tratarán de idéntica manera que los mismos.

Los ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos concretos o auxiliares deberán cumplir con las mismas medidas de seguridad que el resto de archivos.

En general, no se conservará en documentación en papel aquella información que esté disponible a través de las diferentes aplicaciones, salvo que haya obligación legal de mantenerla.

14. Procedimiento de restricción de acceso a ficheros no automatizados

El procedimiento de ubicación de áreas restringidas de la organización es el siguiente:

CASO A:

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.

CASO B:

Atendidas las características de los locales no es posible disponer de áreas cerradas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente, por lo que se propone como medida alternativa la siguiente: (por ejemplo que permanecerán vigiladas en todo momento por personal responsable de ello).

15. Procedimiento de copia y reproducción de documentos

En el caso de ficheros no automatizados que contengan datos de nivel alto, las copias o reproducciones únicamente puedan ser realizadas bajo el control del personal autorizado por el Responsable interno del Fichero.

El usuario deberá conocer y cumplir el procedimiento para la copia o reproducción de documentos.

El procedimiento de copia y reproducción de documentos de la Organización es el siguiente:

La generación de copias o la reproducción de los documentos únicamente podrán ser realizadas bajo el control del personal autorizado por el Responsable interno del Fichero.

Deberá procederse a la destrucción de las copias o reproducciones desechadas, de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

16. Procedimiento de traslado de documentación

Se han definido medidas para proceder al traslado de documentación de **nivel alto**. Como usuario deberá conocerlas y cumplirlas.

Siempre que se requiera realizar un traslado de información con datos carácter personal a otras ubicaciones dentro del Centro o a otras dependencias, el solicitante deberá ponerse en contacto con el/los responsable/s del fichero, quién deberá aprobar o rechazar dicha solicitud.

Todo el traslado de la información se realizará adoptando las medidas de seguridad dirigidas a impedir el acceso o manipulación de la información. El traslado de dicha información se deberá realizar de una de las siguientes formas:

1. El/los responsable/s del fichero deberán custodiar la información en maletines cerrados con llave u otro dispositivo equivalente, el personal del Centro o empresas subcontratadas deberán trasladar la documentación, en el destino de la información el encargado del traslado deberá firmar un acuse de recibo.

2. El/los responsables del fichero deberán custodiar la información en sobres precintados en el cual se indicará la clasificación del nivel de seguridad asignado a la información, el solicitante del traslado, la fecha y un contador numérico de los sobres enviados. En el destino de la información el encargado del traslado deberá firmar un acuse de recibo.

17. Responsables de seguridad

El Responsable de seguridad es el encargado de autorizar, coordinar, controlar y en algunos casos ejecutar las medidas de seguridad dispuestas en materia de protección de datos.

Tenga en cuenta que esta persona es muy importante en el funcionamiento de un sistema de protección de datos y que ante cualquier duda o cuestión en materia de protección de datos deberá de dirigirse a él.

Los responsables de seguridad designados por la organización son los siguientes:

CARGO	NOMBRE	EMAIL
Responsable de Seguridad en Aspectos Legales	Manuel José García Romero	Manueljose.Garcia@sjd.es
Responsable de Seguridad en Aspectos Técnicos	Manuel José García Romero	Manueljose.Garcia@sjd.es
Responsable de Seguridad en Aspectos de Procedimientos	Manuel José García Romero	Manueljose.Garcia@sjd.es