CAPÍTULO 2
FICHEROS Y DOCUMENTO DE SEGURIDAD

1. FICHEROS Y TRATAMIENTOS DE DATOS

Se entiende por **tratamiento de datos** las 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.

Fichero: es todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. Estos pueden ser:

- **Automatizado:** se refiere a todo conjunto organizado de datos de carácter personal que permita acceder a la información relativa a una persona física determinada utilizando procedimientos de búsqueda automatizados, es decir, información almacenada en soportes informáticos y se encuentran organizados de manera que se pueda acceder a los datos personales utilizando cualquier tipo de aplicación o procedimiento informatizado.

- **No automatizados:** todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.

Además, también pueden ser:

- **Ficheros de titularidad privada:** los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.
- **Ficheros de titularidad pública:** los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

Las medidas de seguridad exigibles a los ficheros y tratamientos de datos personales se clasifican en tres niveles: Básico, Medio y Alto.

NIVEL ALTO	Datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico; recabado con fines policiales sin consentimiento de las personas afectadas; y derivados de actos de violencia de género.
NIVEL MEDIO	Datos relativos a la comisión de infracciones administrativas o penales; que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito); de Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias; de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros; de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias; de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social; que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas; y de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización.
NIVEL BÁSICO	Datos de nombre, apellidos, DNI, nacionalidad, firma, firma electrónica, imagen, número de la seguridad social, correo electrónico, teléfono, etc. Además, datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando: los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros; se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero; y en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

Los ficheros de datos de carácter personal de titularidad privada, serán notificados a la Agencia de Protección de Datos, por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación.

La notificación previa a la inscripción de los ficheros en la Agencia de Protección de Datos ha de contener:

- Identificación del responsable del fichero.
- La identificación del fichero.
- Finalidades y usos del fichero.
- El sistema de tratamiento empleado para su organización.
- El colectivo de personas sobre las que se obtienen datos.
- El procedimiento y procedencia de los datos.
- Las categorías de los datos.
- El servicio o unidad de acceso.
- La indicación del nivel de medidas de seguridad básico, medio o alto exigible.

- Identificación en su caso, del encargado de tratamiento donde se encuentra ubicado el fichero.
- Los destinatarios de cesiones y transferencias internacionales de datos.

Recuerde

La notificación se realiza conforme al procedimiento establecido en el Capítulo IV del Título VIII del reglamento.

2. EL DOCUMENTO DE SEGURIDAD

El artículo 9.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD), establece que:

> *"[...]el responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".*

El Reglamento de desarrollo de la LOPD (RLOPD), aprobado por el Real Decreto 1720/2007, de 21 de diciembre, fue publicado en el BOE número 17, de 19 de enero de 2008. El Título VIII de este reglamento desarrolla las medidas de seguridad en el tratamiento de datos de carácter personal y tiene por objeto establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

El **Documento de Seguridad** es un documento interno de la organización, que debe mantenerse siempre actualizado. Disponer del documento de seguridad es una obligación para todos los responsables de ficheros y, en su caso, para los encargados del tratamiento, con independencia del nivel de seguridad que sea necesario aplicar.

Los apartados mínimos que debe incluir el documento de seguridad son los siguientes:

APARTADOS DEL DOCUMENTO DE SEGURIDAD
• Ámbito de aplicación del documento con especificación detallada de los recursos.
• Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido, así como la definición de las Políticas de Seguridad.
• Identificación de los elementos previstos para asegurar la inviolabilidad de la red informática.
• Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
• Procedimiento de notificación, gestión y respuesta ante las incidencias.
• Procedimiento de realización de las copias de respaldo de los datos.
• Elaboración de un inventario de copias de seguridad.
• Mecanismo de identificación y autenticación, de los usuarios para el acceso autorizado a los sistemas de información.
• Sistemas de contraseñas para el control de acceso a la información.
• Funciones y obligaciones del personal.
• Identificación del Responsable del Fichero y del Responsable de Seguridad.
• Relación del personal autorizado para el acceso físico a los locales donde se encuentran ubicados los sistemas de información.
• Registro de entrada y salidas de soportes informáticos.
• Medidas de seguridad a adoptar en los sitios Web del cliente.

En caso de haber contratado la prestación de servicios por terceros para determinados ficheros, en el documento de seguridad se debe hacer constar esta circunstancia, indicando una referencia al contrato y su vigencia, así como los ficheros objeto de este tratamiento.

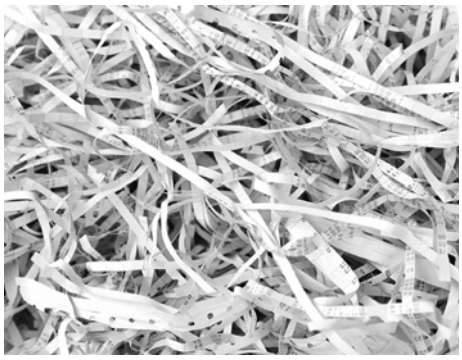
Si se ha contratado la prestación de servicios en relación con la totalidad de los ficheros y tratamientos de datos del responsable, y dichos servicios se prestan en las instalaciones del encargado del tratamiento se podrá delegar en este la llevanza del documento de seguridad.

3. MEDIDAS DE SEGURIDAD

Con la elaboración del Documento de Seguridad (DS) se establece la elaboración, implantación y difusión de procedimientos de:

- Tratamiento y acceso a la documentación, y custodia de la misma.
- Notificación y gestión de incidencias.
- Asignación de autorizaciones y responsabilidades, por ejemplo, en relación con:
  - La aprobación o negación de acceso a los documentos.
  - El mantenimiento del registro de incidencias.
  - Nombramiento de responsables de seguridad.
- Gestión de todos los mecanismos que limiten accesos no autorizados:
  - Archivadores o armarios con llave, reubicación de la documentación en zonas de acceso restringido o que estén bajo vigilancia permanente (requerido para datos de Nivel Alto), etc.

– Gestión de procedimientos de destrucción de documentos, e inventario de la instalación de mecanismos al efecto: trituradoras de papel, contratación de servicios especializados, etc.



– Ejecución de auditorias bienales obligatorias (como se viene haciendo para ficheros automatizados), para datos de Nivel Medio o Alto.
– Para datos de nivel alto (entre los que se incluye la información sobre la salud de personas), deben identificarse los accesos realizados a los documentos, para lo cual puede ser recomendable implantar un libro de control de accesos a la documentación. Este podría ser a su vez informatizado.

A continuación vamos a establecer las medidas de seguridad de acuerdo con el nivel de protección y sistema de tratamiento:

Nivel Básico

- **Personal**

  Respecto del personal se debe establecer las funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas. Definición de las funciones de control y las autorizaciones delegadas por el responsable. Difusión entre el personal, de las normas que les afecten y de las consecuencias por su incumplimiento.

- **Incidencia**

  Se establece un registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras. Procedimiento de notificación y gestión de las incidencias.

- **Control de acceso**

  Consiste en la relación actualizada de usuarios y accesos autorizados. Control de accesos permitidos a cada usuario según las funciones asignadas. Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. Concesión de permisos de acceso sólo por personal autorizado. Mismas condiciones para personal ajeno con acceso a los recursos de datos.

- **Gestión de soportes**

  Incluye el inventario de soportes, identificación del tipo de información que contiene, o sistema de etiquetado, acceso restringido al lugar de almacenamiento, autorización de las salidas de soportes (incluidas a través de e-mail) y medidas para el transporte y el desecho de soportes.

Solo ficheros automatizados

- **Identificación y autenticación**

  Se trata de establecer la identificación y autenticación personalizada, procedimiento de asignación y distribución de contraseñas, almacenamiento ininteligible de las contraseñas y periodicidad del cambio de contraseñas, que no puede ser superior a un año.

- **Copia de respaldo**

  Debe contener la copia de respaldo semanal, procedimientos de generación de copias de respaldo y recuperación de datos, verificación semestral de los procedimientos, reconstrucción de los datos a partir de la última copia, grabación manual en su caso, si existe documentación que lo permita, pruebas con datos reales, copia de seguridad y aplicación del nivel de seguridad correspondiente.

Solo ficheros no automatizados

- **Criterios de archivo**

  El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO).

- **Almacenamiento**

  Se deben establecer los dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura.

- **Custodia soportes**

  Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados.

Nivel Medio

- **Responsable de seguridad**

  El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad). El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento.

- **Auditoria**

  Al menos cada dos años, interna o externa. Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad. Verificación y control de la adecuación de las medidas. Informe de detección de deficiencias y propuestas correctoras. Análisis del responsable de seguridad y conclusiones elevadas al responsable del fichero.

Solo ficheros automatizados

- **Incidencia**

  Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente. Autorización del responsable del fichero para la recuperación de datos.

- **Control de acceso**

  Se debe incluir el control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.

- **Identificación y autenticación**

  Limite de intentos reiterados de acceso no autorizado.

- **Gestión de soportes**

  Tiene que tener el registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizado para recepción/entrega.

Nivel Alto

Solo ficheros automatizados

- **Control de acceso**

  El control de accesos debe contener un registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado. Debe ser revisado el registro mensualmente por el responsable de seguridad.

  Los datos de este control deben conservarse durante dos años. No es necesario este registro si el responsable del fichero es una persona física y es el único usuario.

- **Gestión de soportes**

  Tiene que tener un sistema de etiquetado confidencial, un cifrado de datos en la distribución de soportes, un cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas).

- **Copias de respaldo**

  Contiene la copia de respaldo y procedimientos de recuperación en un lugar diferente del que se encuentren los equipos.

- **Telecomunicaciones**

  Debe de contener explicación de la transmisión de datos a través de redes electrónicas cifradas.

Solo ficheros no automatizados

- **Control de acceso**

  Contiene el control de accesos autorizados y la identificación de accesos para documentos accesibles por múltiples usuarios.

- **Almacenamiento**

  Los modos de almacenamientos son: armarios, archivadores de documentos en áreas con acceso protegido mediante puertas con llave.

- **Copia o reproducción**

  Solo puede realizarse por los usuarios autorizados. Y debe especificar cómo se destruyen las copias desechadas.

- **Traslado documentación**

  Medidas que impidan el acceso o manipulación.

Además de estas medidas de seguridad, según el nivel de protección y de si se trata de ficheros automatizados o no, existen otras medidas de seguridad que se han de tener en cuenta:

- Los accesos a través de redes de telecomunicaciones deben garantizar un nivel de seguridad equivalente al de los accesos en modo local.
- La ejecución de trabajos fuera de los locales del responsable o del encargado del tratamiento debe ser previamente autorizada por el responsable del fichero, constar en el documento de seguridad y garantizar el nivel de seguridad.
- Los ficheros temporales deberán cumplir el nivel de seguridad correspondiente y serán borrados una vez que hayan dejado de ser necesarios.
- El acceso facilitado a un encargado del tratamiento deberá constar en el documento de seguridad y deberá comprometerse al cumplimiento de las medidas de seguridad previstas.

1. ¿Qué se entiende por fichero?

2. ¿Qué ha de contener la notificación previa a la inscripción de los ficheros en la Agencia de Protección de Datos?

3. ¿Qué establece el artículo 9.1. de LOPD?

4. Indica cuáles son los niveles de protección.

Ejercicios de Repaso y Autoevaluación