GESTIÓN DE PROYECTOS INFORMÁTICOS

T7:LEY DE PROTECCIÓN DE DATOS

VLADYSLAV KUCHMENKO
JAVIER DAVID SUÁREZ HUACON
ADRIAN FERNANDEZ HERNANDEZ
PLÁCIDO ANTONIO LÓPEZ ÁVILA
PABLO VERGARA CABAÑERO

Índice

LA AGENCIA DE PROTECCIÓN DE DATOS

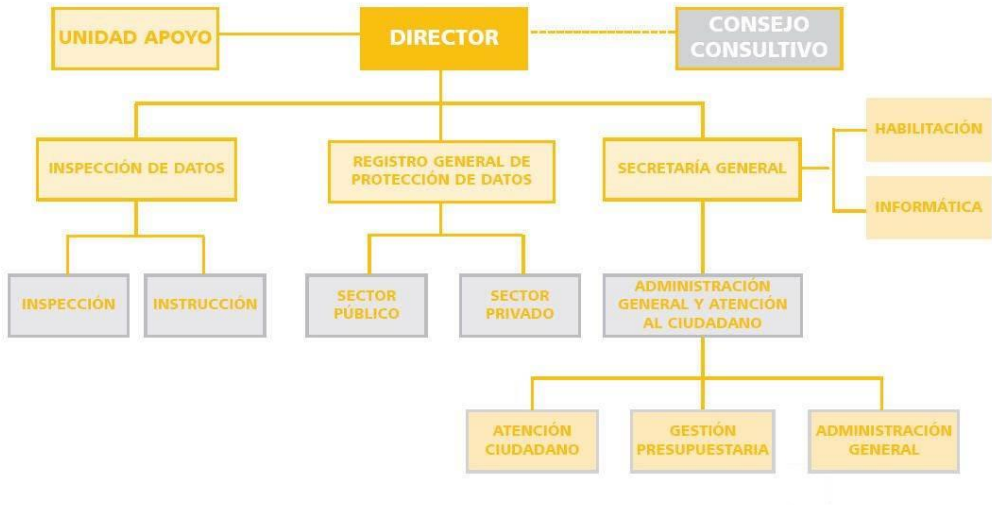
La Agencia Española de Protección de Datos (AEPD) es un órgano especializado encargado de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, especialmente en lo relativo al ejercicio de los derechos esenciales de los ciudadanos (los derechos de acceso, rectificación, cancelación y oposición).

Se trata de un ente público con personalidad jurídica propia y plena capacidad pública y privada que actúa con plena independencia de las Administraciones Públicas y que se relaciona con el Gobierno a través del Ministerio de Justicia.

Todo lo relacionado con la naturaleza, organización y funciones de la AEPD se encuentra regulado en el Título VI de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal y en el Real Decreto 428/1993, de 26 de Marzo, por el que se aprueba el Estatuto de la AEPD.

Organización

LA AEPD está estructurada en los siguientes departamentos:



- **El Director**, representa y dirige la AEPD.
- **El Consejo Consultivo**; es un órgano colegiado cuya misión principal es asesorar al Director.
- **El Registro General de Protección de Datos**; es el órgano encargado de velar por la publicidad de la existencia de ficheros de datos personales con miras a hacer posible el ejercicio de sus derechos por parte de los ciudadanos.
- **La Inspección de datos**; es el órgano al que corresponde el ejercicio de la potestad inspectora de la Agencia con el fin de comprobar la legalidad de los tratamientos.
- **La Secretaría General de la Agencia**; es el órgano encargado de apoyar el correcto funcionamiento de la agencia.

Funciones de la AEPD

Tal y como establece el artículo 37 de la Ley Orgánica 15/1999 las funciones de la AEPD son las siguientes:

- Velar por el cumplimiento de la legislación sobre la protección de datos y controlar su aplicación, en especial a lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
- Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias
- Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.
- Atender las peticiones y reclamaciones formuladas por las personas afectadas.
- Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de datos de carácter personal.
- Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.
- Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.
- Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.
- Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.
- Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la infromación adicional que el Director de la Agencia determine.
- Redactar una memoria anual y remitir al Ministerio de justicia.
- Ejercer el control y adoptar las autorizaciones que procedan en relación conlos movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.
- Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.
- Cuantas otras la sean atribuidas por normas legales o reglamentarias.

Potestad AEPD

Para que la AEPD pueda llear a cabo sus funciones, el artículo 40 de la Ley de Protección de Datos le concede la denominada “potestad de inspección de ficheros”, que consiste en la facultad de que dispone la Agencia para inspeccionar los ficheros que refiere a la LOPD, recabando cuanta información sea precisa. Para dotar de mayor efectividad a la potestad, la propia LOPD otorga a sus inspectores la consideración de autoridad pública en lo que se refiere al desempñeo de sus cometidos, estando obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

REGISTRO DE FICHEROS

Es una de las obligaciones que siempre que se proceda al tratamiento de datos personales, definidos en el art. 3a) de la Ley Órganica 15/1999, como “cualquier información concerniente a personas físicas o identificables”, que suponga la inclusión de dichos datos en un fichero, considerado por la propia norma, artículo 3.b), como “conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso”, el fichero se encontrará sometido a la Ley, siendo obligatoria su inscripción en el Registro General de Protección de Datos (RGPD).

De conformidad con lo dispuesto en el artículo 55 del RLOPD, todo fichero de datos de carácter personal de titularidad pública o privada, con excepción de aquellos ficheros que están expresamente excluidos de la aplicación de la LOPD en su artículo 2.2, como los ficheros mantenidos por las personas físicas en el ejercicio de actividades exclusivamente personales o domésticas (p.e.: agendas de familiares y amigos, ficheros de fotografías personales), serán notificados a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos.

No solicitar la inscripción de los ficheros de datos de carácter personal en el RGPD constituye infracción leve, con arreglo a lo dispuesto en el artículo 44.2.b) de la LOPD. Según el artículo 58 del RLOPD, la inscripción de los ficheros deberá encontrase actualizada en todo momento, por lo que cualquier modificación que afecte al contenido de la inscripción, así como su supresión deberá ser notificada a la AEPD para proceder a la inscripción de la modificación o a la cancelación del fichero.

Tanto para inscribir, como para suprimir o modificar la inscripción de un fichero en el Registro General de Protección de Datos, se deberá cumplimentar el modelo establecido en la Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, (B.O.E. 181 de 31 de julio de 2006), por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos, así como los formatos y requerimientos a los que deben ajustarse las notificaciones remitidas en soporte informático o telemático.

Están obligados a notificar la creación de ficheros para su inscripción en el RGPD, de acuerdo con lo dispuesto en la LOPD, aquellas personas físicas o jurídicas, de naturaleza pública o privada, u órgano administrativo, que procedan a la creación de ficheros que contengan datos de carácter personal. También aquellos entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados y sean responsables de ficheros de datos de carácter personal.

La creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el “Boletín Oficial del Estado” (BOE) o diario oficial correspondiente.

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de datos.

Naturaleza del los ficheros

La LOPD estipula que podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad y se respeten las garantías que la Ley establece para la protección de las personas.

El artículo 5.1.m) del RLOPD define los ficheros públicos como aquellos "de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado 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 públicas".

La determinación de la titularidad pública de los ficheros no ofrece dificultades cuando nos referimos a órganos de las administraciones públicas, órganos constitucionales o de relevancia constitucional, pero cuando se trata de corporaciones de derecho público o de entidades que atienden tanto al ejercicio de potestades públicas como a intereses privados se hace preciso determinar qué ficheros de los que puedan ser responsables son de una u otra titularidad para su correcta creación e inscripción en el Registro General de Protección de Datos.

Colegios Profesionales

Los Colegios Profesionales son Corporaciones de derecho público, los fines esenciales de estas Corporaciones la ordenación del ejercicio de las profesiones, la representación exclusiva de las mismas y la defensa de los intereses profesionales de los colegiados así como ejercer cuantas funciones le sean encomendadas por la Administración.

Junto al ejercicio de estas potestades públicas sometidas al derecho administrativo, realizan otras actividades íntegramente sometidas al derecho privado, por lo que dependiendo de la actividad que desarrollen, administrativa o privada, tendrán ficheros de dos naturalezas, públicos o privados.

Los **ficheros públicos** los que contengan los datos de carácter personal correspondientes a la incorporación de colegiados, al ejercicio de las funciones públicas de ordenación y control de la actividad profesional que dichas entidades tienen asignadas legal o estatutariamente o que les sean encomendadas por las Administraciones Públicas competentes, así como al ejercicio de la potestad sancionadora

Los **ficheros de titularidad privada** serían los creados con la única finalidad de llevar a cabo la gestión interna del Colegio o Consejo o de adoptar mecanismos que faciliten el desempeño de la profesión colegiada cuando la adopción no implique el ejercicio de potestades administrativas ni lleve aparejada la existencia de un acto administrativo

Cámaras de Comercio, Industria, Servicios y Navegación

Cámaras Oficiales de Comercio, Industria, Servicios y Navegación y las correspondientes de cada Comunidad Autónoma, las definen como Corporaciones de derecho público, integrantes de la denominada Administración Corporativa, que ejercen potestades públicas sometidas al derecho administrativo, junto con el ejercicio de otras actividades íntegramente sometidas al derecho privado.

Se podrían considerar ficheros de **titularidad pública** los ficheros propios de las Cámaras Oficiales que contengan los datos de carácter personal correspondientes a las funciones público-administrativas necesarias para el cumplimiento de sus fines y el ejercicio de las funciones que tiene atribuidas legalmente como los relativos a "Censo público de empresas de las Cámaras", “Censo Electoral de las Cámaras", "Formación", etc.

Serían **ficheros privados** los correspondientes al desempeño de otras actividades íntegramente sometidas al derecho privado, como los relativos a la gestión de recursos humanos del personal que presta sus servicios en la Cámara: "Nominas”, “Empleados”, “Laboral”, etc.

Cámaras Agrarias, Consejos Reguladores de Denominaciones de Origen e Indicaciones Geográficas Protegidas, Comunidades de Regantes

Las consideraciones expuestas para las Cámaras de Comercio, Industria y Navegación son de aplicación a estas Corporaciones de derecho público.

Fundaciones

La ley establece que las fundaciones del sector público estatal “no podrán ejercer potestades públicas”, por lo que sus ficheros tendrán la consideración de **ficheros privados**.

Consorcios

Los ficheros de los Consorcios serán **públicos** o **privados** dependiendo de que su finalidades sean ejercicio de potestades públicas, sin que la presencia de una Administración pública en un consorcio sea un criterio definitorio de titularidad pública.

Federaciones deportivas

La ley del Deporte establece que las Federaciones deportivas españolas, bajo coordinación y tutela del Consejo Superior de Deportes ejercerán una serie de funciones, entre otras, la de calificar y organizar, en su caso, las actividades y competiciones deportivas de ámbito estatal.

El Tribunal Supremo atribuye a las federaciones deportivas, no obstante su carácter de entidades privadas, un carácter mixto en atención a las funciones que ejercen, ya que junto a las atribuciones que le son propias también ejercen por delegación funciones públicas de carácter administrativo.

En consecuencia, los ficheros de las Federaciones deportivas que se creen para el ejercicio de las funciones públicas de carácter administrativo serían de **titularidad pública**, como los de federados, competiciones y resultados, controles de salud y de dopaje, sanciones, mientras que aquellos ficheros que respondieron a actividades propias de las Federaciones deportivas, como el de empleados, o proveedores, serían de **titularidad privada**.

Notarías

La ley establece que los ficheros creados de forma automatizados de datos de carácter personal del Cuerpo de Notarios crea los siguientes ficheros de titularidad pública de las notarías:

- *"Administración y organización de la notaría"*
- *"Personal de la notaría"*

A su vez, la ley reguladora de determinadas obligaciones de los notarios en el ámbito de la prevención del blanqueo de capitales dispone de la creación del **fichero de titularidad pública**:

- *"Cumplimiento de las obligaciones de tratamiento y comunicación de datos derivados de lo dispuesto en el artículo 17 y 24 de la Ley del notario"*

Como **fichero de titularidad privada**, las notarías han creado el fichero de:

- *"Videovigilancia"*

LOS DOCUMENTOS DE SEGURIDAD

El documento de seguridad establece las medidas de índole técnica y organizativa que los responsables de los tratamientos o los ficheros y los encargados de tratamiento han de implantar para garantizar la seguridad en los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de datos de carácter personal.

Este documento de Seguridad en materia de Protección de Datos, es un documento que deben tener todas las empresas/profesionales que, están sujetos a la obligatoriedad y el cumplimiento de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.

Es decir toda persona con acceso a los datos personales, o que intervenga en alguna fase del tratamiento de los mismos, debe ceñirse a lo establecido en el documento de seguridad, en el cual se establecerán claramente las funciones y obligaciones del personal.

Por tanto es responsabilidad del responsable del fichero adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Entre estas medidas, se encuentran la elaboración e implementación de la normativa de seguridad mediante un documento de obligado cumplimiento que recogerá los siguientes puntos:

1. La íntegra identificación de la empresa, la actividad y servicios que presta y sobre todo el ámbito de aplicación del Documento de Seguridad.
2. Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
3. Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
4. Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
5. Procedimientos de notificación, gestión y respuesta antes las incidencias.
6. Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
7. Las medidas que sean necesarias adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

Los requisitos plasmados en el punto anterior, son los establecidos por el **artículo 88.3 del Reglamento de desarrollo de la Ley Orgánica 15/1999**, son suficientes siempre y cuando la actividad se encuentre incorporada dentro del nivel básico de seguridad.

De lo contrario habría que sumar algunos requisitos más, es decir, si la actividad esté catalogada tanto en el nivel medio o nivel alto de seguridad, tendríamos que implementar dentro del Documento de Seguridad dos contenidos más:

1. La identificación del responsable o responsables de seguridad.
2. Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

EL PERSONAL INVOLUCRADO

La agencia Española de Protección de Datos está encargada de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
Los sujetos que pueden intervenir en el tratamiento de datos personales son los siguientes:

1. El responsable del fichero o tratamiento
2. El afectado o interesado
3. El encargado del tratamiento

El responsable del fichero o tratamiento

Es responsable del fichero o tratamiento la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. Podrá ser la empresa como tal (sociedad) o el empresario individual si es persona física.

El afectado o interesado

Persona física, titular de los datos que sean objeto del tratamiento de datos como 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.

El encargado del tratamiento

El responsable del tratamiento será el obligado a cumplir con los deberes de inscripción del fichero, informar a los afectados, recabar el consentimiento, permitir el ejercicio del derecho a los titulares, asegurar el secreto y confidencialidad de los datos, y garantizar la seguridad de los mismos.

Sin embargo si analizamos el artículo 12 dedicado al acceso a los datos por cuenta de terceros, que es el único que contiene las funciones del encargado del tratamiento vemos que el legislador ha entendido que se trata siempre de una figura externa a la organización con la que habrá que mediar el correspondiente contrato en el que necesariamente ha de constar que:

- El encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.
- No los aplicará o utilizará con fin distinto al que figure en dicho contrato.
- No los comunicará, ni siquiera para su conservación a otras personas.
- Está obligado a implementar las medidas de seguridad a que se refiere el artículo 9 de la LOPD.

CONTROL DE ACCESOS

Control de accesos es un mecanismo que en función de la identificación autenticada permite acceder a datos o recursos.Se establecen tres niveles , Nivel básico:(nombre,apellidos,dirección,teléfono,número de la cuenta corriente) , Nivel medio:(información de la hacienda pública,infracciones administrativas o penales,información de servicios financieros,información sobre solvencia patrimonial y crédito,datos que permiten elaborar un perfil del afectado),Nivel alto:(ideología,religión, creencias,origen racial , salud, vida sexual).

Las medidas de seguridad de cada nivel son acumulativas : el nivel medio cumplirá con las medidas de seguridad del básico y el nivel alto con las dos inferiores.

Nivel Básico

En el artículo 91 de LOPD se establecen los siguientes puntos del nivel de seguridad básico:

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Si cumplimos los 5 puntos anteriormente descritos obtendremos mayor seguridad a la hora de tratar con datos.
Con el cumplimiento del primer punto se minimizan los riesgos de que un usuario malicioso pueda acceder a datos sensibles los cuales no necesita para desempeñar su labor.
Con el cumplimiento del segundo punto seguimos minimizando riesgos del mal uso de datos a posteriori de forma que cuando un usuario ya no necesita el acceso a datos para el desempeño de su labor se le retiren los permisos de acceso a dichos datos.
Con el cumplimiento del tercer punto minimizamos los riesgos dificultando el acceso a datos o restringiendo el acceso a los mismos.
Con el cumplimiento del cuarto punto , se debe tener documentación de quien tiene acceso a la información sensible y para qué , para en caso de necesitarlo poder depurar responsabilidades.
Con el cumplimiento del quinto punto nos aseguramos de que cualquier persona que tenga acceso a algún dato se someta a las mismas obligaciones que propietario o administrador de dicho dato.

En el artículo 92 de LOPD se establecen los siguientes puntos del nivel de seguridad básico:

1. Los soportes y documentos que **contengan datos de carácter** personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser **accesibles por el personal autorizado** para ello en el documento de seguridad.
2. La **salida de soportes** y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento **deberá ser autorizada por el responsable** del fichero o encontrarse debidamente autorizada en el documento de seguridad.
3. En el **traslado de la documentación** se adoptarán las medidas dirigidas a **evitar** la sustracción, **pérdida** o **acceso indebido** a la información durante su transporte.
4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal 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.
5. La **identificación** de los soportes que contengan datos de carácter personal que la organización considerase **especialmente sensibles** se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los **usuarios con acceso autorizado** a los citados soportes y documentos **identificar su contenido**, y que dificulten la identificación para el resto de personas.

Nivel Medio

En el artículo 97 de LOPD se establecen los siguientes puntos de nivel de acceso medio:

1. Deberá establecerse un sistema de registro de **entrada** de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.
2. Igualmente, se dispondrá de un sistema de registro de **salida** de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

En el artículo 99 de LOPD se establecen los siguientes puntos de nivel de acceso medio:

1. Exclusivamente el **personal autorizado** en el documento de seguridad podrá tener acceso a los **lugares donde se hallen instalados los equipos físicos** que den soporte a los sistemas de información.

Si cumplimos el punto anteriormente descrito obtendremos mayor seguridad a la hora de tratar con datos. Ya que solo el personal autorizado y de confianza podrá acceder a los datos físicos garantizando de esta forma que la seguridad de los mismos.

Nivel Alto

En el artículo 101 de LOPD se establecen los siguientes puntos de nivel de acceso alto:

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.
2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.
3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

En el artículo 103 de LOPD se establecen los siguientes puntos de nivel de acceso alto:

1. De cada intento de 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.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.
5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:
    a. Que el responsable del fichero o del tratamiento sea una persona física.
    b. Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales. La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

GESTIÓN DE SOPORTES Y DOCUMENTOS

Nivel Básico

En el artículo 92 de LOPD se establecen los siguientes puntos:

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad. Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.
2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.
3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal 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.
5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Nivel Medio

En el artículo 101 de LOPD se establecen los siguientes puntos:

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.
2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Nivel Alto

En el artículo 101 de LOPD se establecen los siguientes puntos:

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.
2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte. Asimismo, se cifran los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.
3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

COPIAS DE SEGURIDAD

La LOPD obliga a todas las organizaciones, empresas e instituciones a garantizar la seguridad de los datos de carácter personal que tratan y almacenan en sus sistemas de información y clasifica estos datos en tres niveles de seguridad. Básico, Medio y Alto. Si trata datos de nivel básico, debemos irnos al artículo 94 del RLOPD y si los datos son de nivel alto al 102 del mismo reglamento.

Copias de seguridad para datos de nivel básico

Deben cumplir las medidas de seguridad de nivel básico en relación a las copias de seguridad, aquellos ficheros que contengan datos identificativos de personas físicas (nombre, teléfono, email, dirección, fotografías o, por ejemplo, datos bancarios).

En estos supuestos las copias de seguridad cumplirán, al menos, los siguientes requerimientos:

- La copia deberá ser con una periodicidad semanal, a menos que en ese período no se hubieran actualizado los datos. Pocas empresas actualizan los datos con una periodicidad superior a la semanal, por lo que a la práctica la periodicidad suele ser diaria.
- El proceso de copias debe garantizar que los datos se recuperarán al momento previo a cualquier incidente.
- Cada 6 meses debe comprobarse el correcto uso del sistema de copias de seguridad.
- En caso de realizar pruebas para la implantación o modificaciones de los sistemas de seguridad, previamente deberá realizarse una copia de seguridad.

Medidas de seguridad del Nivel básico:

- Ámbito de aplicación y especificación de los recursos protegidos.
- Medidas, normas y procedimientos.
- Funciones y obligaciones del Personal
- Estructura de los ficheros y descripción de los sistemas de información que los trata.
- Procedimientos de notificación, gestión y respuesta ante las incidencias.
- Procedimientos de copias y recuperación de los datos.
- Identificación y autentificación.
- Control de acceso.

Copias de seguridad para datos de nivel medio

Aquí se encuentran los datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, Servicios Financieros, solvencia patrimonial y crédito.

Afecta especialmente a la Administración Pública, entidades financieras y al sector jurídico.

Medidas de seguridad del Nivel Medio, además de las básicas:

- Se nombrará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas en el Documento de Seguridad.
- Los sistemas de información y sistemas se someterán a auditoría interna o externa.
- Identificación y autentificación inequívoca.

- Control de acceso físico a los locales donde estén los sistemas de información con datos de carácter personal.
- Gestión de soportes con mayor grado de control y de identificación. Mínimo semanalmente.
- Gestión de incidencias con consignación de procedimientos.

Copias de seguridad para datos de nivel alto

Son los datos relacionados con la ideología, origen racial, salud, creencias, afiliación sindical, religión y sexo.

Afecta especialmente a los centros de formación, partidos políticos, salud, RR. HH., clubs y agrupaciones de ocio y todas las empresas que gestionan sus nóminas.

El artículo 102 explica que deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Medidas de seguridad del Nivel Alto, además de las de nivel medio:

- La distribución de datos en soporte digital se hará encriptado.
- Registro de acceso a los datos, se guardará como mínimo:
    - Identificación del usuario.
    - Fecha y hora en que se realizó.
    - Fichero accedido y si ha sido autorizado o denegado.
- Se mantendrán como mínimo 2 años los datos registrados.
- Control de acceso físico a los locales donde estén los sistemas de información con datos de carácter personal.
- La copia se guardará en un lugar diferente a donde se encuentren los sistemas de información.
- La transmisión de datos por redes de telecomunicaciones se realizará cifradas.

Normas respecto a las copias de seguridad

Según la normativa el responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Se establecerán procedimientos para la recuperación de datos que deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

El responsable del fichero debe proceder a verificar el correcto funcionamiento de estas copias al menos una vez cada seis meses.

De lo expuesto se deduce que si el procedimiento no garantiza la reconstrucción total de los datos al momento anterior a su pérdida o destrucción no se está cumpliendo con la exigencia de la norma,

pudiendo vulnerar la normativa sobre protección de datos (artículo 9 LOPD). También es exigible para el caso de ficheros de imágenes de personas identificables.

En el caso de que no sea posible guardar una copia de los ficheros en un lugar distinto y no sujeto a los mismos riesgos, se deberán adoptar medidas complementarias para paliar el riesgo, tales como ubicar la copia en armarios ignífugos, implantación de sistemas anti incendio, etc.).

En estos casos, cuando la sede del responsable cuente con distintas estancias o niveles de edificación se entenderá por lugar distinto una estancia diferenciada del lugar principal en el que se ubiquen los sistemas de información, preferiblemente en planta distinta y más protegida y se deberá hacer constar estas circunstancias en el documento de seguridad.

La obligación de realizar copias de respaldo no es aplicable a los ficheros no automatizados, con independencia del resto de medidas aplicables en este tipo de ficheros, entre las que deberán observarse las previsiones establecidas en el Reglamento.

Qué dice la normativa

- Art. 101.2 Cifrado de los datos:
  La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos garantizando que dicha información no sea vista ni manipulada durante su transporte. Para la encriptación se recomienda un cifrado de 128 bits.

- Art. 103. Registro de accesos:
  El administrador no tiene acceso a los datos salvo autorización expresa del cliente. En el caso de necesitar ejecutar una recuperación en el Data-Center, el usuario debe proporcionar su clave de seguridad. El acceso queda registrado.

- Art. 102. Copias de respaldo en un lugar diferente a aquél en que se encuentran los equipos informáticos que los tratan:
  Obligatorio en las copias para la protección de datos de alto nivel

- Art. 104. Transmisión de datos por redes de Telecomunicaciones. Los datos deben transmitirse, cifrados y comprimidos, bajo protocolo de comunicación seguro.
- Art. 94.2. Verificación periódica de la copia:
  El responsable del fichero se encargará de verificar cada seis meses la correcta definición, aplicación y funcionamiento de los procedimientos de realización de copias de respaldo y recuperación de datos.

Sanciones por el incumplimiento de la normativa

El incumplimiento de la normativa sobre las copias de seguridad puede dar lugar a sanciones económicas, que en función de su gravedad pueden ser:

- Leves: No cumplir las instrucciones de la Agencia de Protección de Datos, poseer datos obsoletos, no rectificar o cancelar inexactitudes, etc. De 601 a 60.101 €.

- Graves: Crear ficheros con finalidades distintas al objeto legítimo de la entidad, tratar datos por parte de un centro sin la existencia de un contrato que recoja la problemática de la protección de datos, etc. De 60.101 a 300.506 €.
- Muy graves: Comunicación o cesión no permitida de datos personales, vulneración de principios para datos especialmente protegidos. De 300.506 a 601.012 €.

SEGUIMIENTO Y CONTROL (AUDITORÍA LOPD)

El nivel del control en una auditoría en la LOPD cambia si nos referimos a ficheros automatizados. Aun así, se aplica la misma normativa para los niveles de seguridad tanto altos como medios, aunque en el Reglamento de desarrollo de la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal si se establecen diferencias por el nivel de seguridad para la realización de una auditoría.

El artículo referente a la auditoría en LOPD hace referencia a la frecuencia de las auditorías, esta será de dos años como máximo y se pueden realizar de forma interna por parte de la empresa, o mediante la contratación de una empresa externa que se haga cargo de todo el proceso. Si se trata de ficheros automatizados se deben realizar auditorías extraordinarias cuando los cambios a los sistemas de datos sean sustanciales. Esto se lleva a cabo para comprobar que las medidas de seguridad se cumplen en todo momento.

La finalización de la auditoría se realiza con un informe que, junto con dictaminar la adecuación a los términos legales, también indica las deficiencias y propone medidas correctas y recomendaciones. El informe se analizará por un responsable de seguridad y el del fichero, para así tomar las medidas necesarias y quedará a disposición de la Agencia Española de Protección de Datos.
Se debe establecer cuáles son los ficheros con datos de carácter personal objeto de la auditoría, tratamientos sobre los mismos, sistemas de tratamiento, procedimientos…

El objetivo del seguimiento es determinar si las medidas de seguridad que se han establecido son adecuadas de acorde con los términos legales. Su realización se precisa para ficheros de nivel medio o alto. La lleva a cabo la propia empresa o empresas externas. Se realiza cada dos años. Si se han realizado cambios importantes también debe llevarse a cabo una auditoría para comprobar la adecuación, adaptación y eficacia de las medidas de seguridad.

Una buena planificación se realiza determinando los recursos necesarios para llevar a cabo la auditoría, las fuentes de información, la ubicación del fichero…

RECOLECCIÓN DE DATOS

Esta recolección, abarca entre otros los siguientes datos:

- Relación de ficheros, estructura y contenido.
- Políticas de seguridad y procedimientos (registro de incidencias, copias de respaldo y recuperación, identificación y autorización, borrado de soporte, cifrado…).
- Documento de seguridad y auditorías anteriores.
- Diseño físico y lógico de los sistemas de información.
- Relación de usuarios, accesos autorizados y sus funciones.
- Inventario de soportes y registro de entrada y salida de soportes.
- Registros de acceso e informes de revisión de los mismos.
- Entrevistas a usuarios, técnicos de sistemas, responsables…
- Inspección visual

EVALUACIÓN DE PRUEBAS

Para verificar el cumplimiento de las disposiciones del Reglamento se pueden realizar las siguientes comprobaciones:

- ASPECTOS GENERALES
  - La clasificación del nivel de seguridad, debe ser adecuada respecto a la naturaleza de la información contenida en cada uno de los ficheros y su finalidad.
  - Creación, modificación o borrado de ficheros con datos de carácter personal desde la última auditoría.
- ENCARGADO DE TRATAMIENTO
  - Realización del tratamiento por una persona distinta al responsable del fichero. Además, realizar una formalización mediante contrato conforme a lo establecido en el artículo 12 de la LOPD y artículos 20 a 22 del RLOPD.
  - Si la realización de este encargo se realiza en los locales del responsable, dejar constancia de esta circunstancia en el Documento de Seguridad, y por escrito en el mismo contrato del compromiso del personal encargado de tratamiento respecto al cumplimiento de las medidas de seguridad recogidas en el Documento de Seguridad del responsable.
  - Cuando el tratamiento se realiza mediante acceso remoto a los sistemas del responsable establecer alguna limitación a la incorporación de los datos a sistemas o soportes distintos de los del responsable. Junto a esto, dejar constancia de las circunstancias el Documento de Seguridad del responsable.
  - Si la prestación se hace en locales propios del encargado de tratamiento (distintos de los del responsable) este debería realizar un documento de seguridad y en este identificar el fichero y al responsable de este, detallando las medidas de seguridad a implementar.
- PRESTACIÓN DE SERVICIO SIN ACCESO A DATOS PERSONALES
  - Adoptar las medidas necesarias para limitar el acceso del personal a los datos privados, soportes y recursos.
  - Si se trata de personal ajeno, recoger en el contrato la prohibición expresa de acceder a los datos personales, así como la obligación de secreto respecto a los datos que hubieran podido conocer con motivo de la prestación de servicio.
- DELEGACIÓN DE AUTORIDADES
  - Delegar a las autorizaciones que el Reglamento atribuye al responsable en otras personas, y hacer constar en el Documento de Seguridad las personas habilitadas para otorgar estas autorizaciones y las personas en quienes recae dicha delegación.
- RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO
  - Autorizados expresamente por el responsable del fichero el almacenamiento de datos personales en dispositivos portátiles o los tratamientos fuera de los locales del responsable o del encargado.
  - Garantizar el nivel de seguridad de acorde con el tipo de fichero tratado.
- FICHEROS TEMPORALES O COPIAS DE TRABAJO
  - ¿Cumplen el nivel de seguridad correspondiente?
  - Destruirlos o borrarlos cuando ya no son necesarios.
- DOCUMENTOS DE SEGURIDAD
  - Elaboración del Documento de Seguridad.

    - Que este documento este actualizado y contenga los aspectos mínimos exigidos por el Reglamento.
    - Adecuar el contenido a la normativa vigente en este momento en materia de seguridad de los datos de carácter personal.
    - Modificar las contraseñas con una periodicidad establecida, preferentemente con un tiempo inferior a un año.
    - Especificar cuál es el personal autorizado para la concesión, alteración o anulación de accesos autorizados sobre datos o recursos.
    - Especificar cuál es el personal autorizado para acceder a los lugares donde se almacenan los soportes informáticos.
    - Si el tratamiento se realiza por cuenta de terceros reflejar los ficheros afectados por el encargo, con referencia expresa al contrato, así como la identificación del responsable y el periodo de vigencia.
    - Reflejar en el Documento de Seguridad si los datos personales se incorporan y tratan exclusivamente en los sistemas del encargado.
    - Especificar qué medidas hay que adoptar en caso de desechado o reutilización de soportes.
- FUNCIONES Y OBLIGACIONES DEL PERSONAL
    - Definir claramente las funciones y obligaciones del personal con acceso a datos de carácter personal y los sistemas de información.
    - Reflejar todas estas funciones en el documento de seguridad.
    - Definir las funciones de control o autorizaciones delegadas por el responsable del fichero.
    - Conocimiento por parte del personal de las medidas de seguridad que afectan al desarrollo de sus funciones.
- REGISTRO DE INCIDENCIAS
    - Crear un procedimiento eficaz de notificación y gestión de incidencias de seguridad.
    - Disponer de un registro de incidencias donde se reflejen todos los datos exigidos en el Reglamento.
    - Revisión periódicamente del registro de incidencias para su análisis y adopción de medidas correctoras de las incidencias anotadas.
- CONTROL DE ACCESO
    - Existencia de mecanismos que impidan que los usuarios accedan a datos o recursos distintos de los autorizados.
    - Exclusivamente el personal autorizado podrá realizar la concesión, alteración o anulación de accesos autorizados sobre datos y recursos.
    - Establecer los criterios conforme a los cuales se otorga la autorización de los accesos a los datos y a los recursos.
    - El personal ajeno al responsable que tiene acceso a los datos y recursos de éste debe encontrarse sometido a las mismas condiciones y obligaciones que el personal propio.
- GESTIÓN DE SOPORTES Y DOCUMENTOS
    - Identificar el tipo de información contenido en el soporte o documento.
    - Almacenar los soportes o documentos en lugares de acceso restringido.
    - Existencia de mecanismos por los que solamente puedan acceder las personas autorizadas en el Documento de Seguridad.

    - Dejar constancia en el Documento de Seguridad, si fuera el caso, de la imposibilidad de cumplir con las obligaciones establecidas en el Reglamento sobre identificación, inventariado y acceso a los soportes dadas sus características físicas.
    - Tomar las medidas adecuadas en el traslado de documentación para evitar la sustracción, pérdida o acceso indebido durante su transporte.
    - Cuando se desecha un soporte o documento conteniendo datos de carácter personal, adoptar las medidas adecuadas para evitar el acceso a la información o su recuperación posterior cuando se procede a su destrucción o borrado.
    - Para los soportes con datos de carácter personal considerados especialmente sensibles por la organización emplear sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto.
- IDENTIFICACIÓN Y AUTENTICACIÓN
    - Existencia de una relación de usuarios con acceso autorizado y actualizada.
    - Emplear procedimientos de identificación y autenticación para dicho acceso.
    - El mecanismo de acceso y verificación de autorización de los usuarios les debe identificar de forma inequívoca y personalizada.
    - Uso de un procedimiento de asignación, distribución y almacenamiento de contraseñas que garantice la confidencialidad e integridad.
    - Cambiar las contraseñas con la periodicidad establecida en el documento de seguridad.
    - Emplear algoritmos hash de encriptación para mantener las contraseñas ininteligibles.
- COPIAS DE RESPALDO Y RECUPERACIÓN
    - El responsable del fichero debe definir de forma adecuada los procedimientos de realización de copias de respaldo y recuperación de los datos.
    - Reflejar estos procedimientos en el Documento de Seguridad.
    - Verificar la correcta aplicación de estos procedimientos de forma periódica.
    - Garantizar la reconstrucción de los datos al estado en que se encontraban antes de producirse la pérdida o destrucción.
    - Si esta pérdida o destrucción afecta a ficheros parcialmente automatizados, grabar manualmente los datos dejando constancia en el Documento de Seguridad.
    - Realizar copias de respaldo semanalmente.
- ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES
    - Garantizar un nivel de seguridad alto a los accesos a datos mediante redes de comunicaciones.
    - Transmitir todos los datos cifrados a través de la red.
- AUDITORIAS
    - Si ha habido modificaciones sustanciales en el sistema de información realizar a continuación una auditoría para verificar la adaptación, adecuación y eficacia de las medidas de seguridad.
    - Incluir los datos, hechos y observaciones en los que se basaban en los informes de las auditorías anteriores.
    - Implementar las medidas correctoras propuestas por auditorías anteriores de forma eficaz.

- CRITERIOS DEL ARCHIVO
    - Establecer una legislación específica con criterios para el archivo de soportes o documentos, garantizando en estos criterios la conservación de documentos, la localización y consulta de la información.
- ALMACENAMIENTO DE LA INFORMACIÓN
    - Los dispositivos de almacenamiento de documentos deben disponen de mecanismos que obstaculicen su apertura. Si sus características físicas no permiten adoptar esta medida el responsable debe adoptar medidas para imposibilitar el acceso no autorizado.
- CUSTODIA DE SOPORTES
    - Custodiar correctamente la documentación cuando ésta no se encuentra archivada en los dispositivos de almacenamiento por estar en revisión o tramitación, impidiendo en todo momento que sea accedida por persona no autorizada.

BIBLIOGRAFÍA

http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/reglamento_lopd/index-ides-idphp.php

http://noticias.juridicas.com/base_datos/Admin/rd1720-2007.t8.html

http://www.iee.es/pages/bases/articulos/derint023.html

http://mikelgarcialarragan.blogspot.com.es/2013/08/medidas-de-seguridad-lopd-i-funciones-y.html