Protección de datos y seguridad de la información

4ª EDICIÓN ACTUALIZADA

Incluye contenido sobre "DERECHO AL OLVIDO"

Julio César Miguel Pérez

Ra-Ma®

Protección de datos y seguridad de la información

Guía práctica para ciudadanos y empresas

4ª Edición actualizada

Protección de datos y seguridad de la información

Guía práctica para ciudadanos y empresas

4ª Edición actualizada

Julio César Miguel Pérez

Ra-Ma®

La ley prohíbe
Copiar o Imprimir este libro

Protección de datos y seguridad de la información Guía práctica para ciudadanos y empresas. 4ª edición

ISBN de Edición en Papel: 978-84-9964-560-5

Editado por:
RA-MA, S.A. Editorial y Publicaciones
Calle Jarama, 33, Polígono Industrial IGARSA
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: editorial@ra-ma.com
Internet: www.ra-ma.es y www.ra-ma.com

Maquetación y diseño portada: Antonio García Tomé

ISBN: 978-84-9964-591-9

E-Book desarrollado en España en Octubrede 2015

A las tres mujeres más importantes de mi vida:

Mi madre, Milagros.

Mi mujer, Verónica.

Mi hija, Jimena.

Gracias por vuestro cuidado, comprensión
y apoyo incondicional.

ÍNDICE

PRÓLOGO

Una nueva realidad

Vivimos inmersos en la sociedad de la información. Constantemente estamos suministrando nuestros datos a profesionales, empresas y organismos de todo tipo. Por ejemplo, damos nuestros datos a la compañía que nos provee del servicio de telefonía, a la que nos provee de la energía eléctrica, cuando compramos un producto, cuando contratamos a un fontanero, un seguro, al alquilar una película, cuando pagamos con tarjeta, etc. Los ejemplos son interminables.

Cada día se están tratando millones y millones de datos personales para poder gestionar los servicios que se utilizan.

Es indudable que alguien podría, sobre la base del «rastro» que vamos dejando en las entidades con las que interactuamos, establecer un perfil completo de nuestra personalidad. A través de los productos que compramos o alquilamos, las webs, foros y comunidades que visitamos, etc., se pueden conocer nuestros gustos, aficiones, preferencias, así como deducir nuestras creencias, religión, orientación sexual y demás datos íntimos.

Gracias a las nuevas tecnologías, este proceso podría automatizarse con relativa facilidad, pudiendo cruzarse diversas bases de datos para «extraer» de ellas todos los datos de una persona en concreto. Esto permitiría elaborar un perfil tan completo, tan nutrido de datos, que posibilitaría a la entidad que realiza el proceso conocer más de esa persona, más incluso que lo que ella misma se conoce.

Esto puede verse con más claridad si nos paramos a observar el fenómeno de las redes sociales, que se nutren de los datos personales que los usuarios depositan

y que luego la red social usa para enviar publicidad dirigida a esos usuarios sobre la base de los gustos, aficiones y preferencias que ellos mismos introducen en sus perfiles.

Como puede deducirse de esto, el uso de las nuevas tecnologías puede suponer una gran amenaza para la privacidad de las personas, y es necesario articular unos mecanismos que permitan garantizar la intimidad y libertad personal, de tal manera que el uso de estas tecnologías no erosione estos derechos fundamentales.

En esta obra vamos a ver tanto la perspectiva del ciudadano que suministra los datos personales y los derechos que le asisten, como la perspectiva del responsable, con las obligaciones y principios que debe cumplir para poder tratar los datos cumpliendo en todo momento la normativa.

PARTE I

LA PROTECCIÓN DE LOS DATOS PERSONALES DE LOS CIUDADANOS

1

LOS DERECHOS DE LOS CIUDADANOS

«Aquellos que cederían la libertad esencial para adquirir una pequeña seguridad temporal, no merecen ni libertad ni seguridad».

Benjamin Franklin

1.1 ¿QUÉ ES UN DATO PERSONAL?

Un dato personal es cualquier información concerniente a una persona.

El nombre y apellidos, la fecha de nacimiento, el teléfono, la dirección postal o el correo electrónico son datos personales. Como también lo son el número de cuenta, la matrícula del coche, los ingresos que se perciben o el historial médico.

Dichos datos pueden ser recogidos en ficheros tanto de administraciones públicas como de entidades privadas, que los utilizan para desarrollar su actividad.

A través de los datos personales almacenados (bienes adquiridos y lugar de adquisición, perfil en las redes sociales, fotografías, historial médico, etc.), se puede deducir el nivel adquisitivo de una persona, así como sus gustos, aficiones e intereses.

Nuestros datos dicen todo de nuestra persona.

1.1.1 Sensibilidad de los datos

Si profundizamos un poco más en los datos personales de un individuo, nos daremos cuenta de que existen unos datos más sensibles que otros.

Esta sensibilidad está establecida en función del daño que puede causar a una persona la revelación de dicha información.

Por ejemplo, no es lo mismo que se revele el número de teléfono de una persona que su historial médico; en especial, si tiene alguna enfermedad que puede provocar su exclusión social.

Atendiendo a esto, la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) establece una serie de requisitos tanto para la adquisición como para la conservación y cesión de los datos, y que son más exigentes cuanto mayor es la sensibilidad de la información recogida.

1.1.2 El tratamiento de datos

A lo largo de esta obra nos vamos a referir numerosas veces al tratamiento de datos. Pero ¿qué es el tratamiento de datos?

Se denomina tratamiento de datos a cualquier operación que se realice con los datos personales: recogida, grabación, almacenamiento, consulta, modificación, utilización, cancelación, supresión, etc.

Es decir, todas las operaciones realizadas durante el ciclo de vida de los datos —desde su recogida inicial a través de, por ejemplo, un formulario, la grabación posterior en un soporte informático, las técnicas y operaciones que luego se realicen con ellos (filtrado, consulta, envío de comunicaciones, etc.) hasta su supresión final, cuando han dejado de ser necesarios— se denomina tratamiento de datos.

Y a lo largo de todo el tratamiento de datos personales se debe aplicar y respetar la Ley Orgánica de Protección de Datos de Carácter Personal.

Figura 1.1. Ejemplo de recogida de datos personales a través de un formulario en una web

1.2 LA PROTECCIÓN DE DATOS Y LOS CIUDADANOS

Quizás, la normativa de protección de datos personales puede considerarse como la «última ley» de las sociedades modernas.

Una vez que el individuo tiene garantizados los derechos fundamentales que le permiten vivir y desarrollarse como persona (protección, vivienda, dignidad, etc.), el «último derecho» sería disponer de total autonomía para decidir quién maneja los datos que a él se refieren y para qué.

En España, esto se plasma en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, conocida comúnmente con el acrónimo LOPD.

La LOPD establece que los datos personales son propiedad de la persona a la que se refieren dichos datos. Por tanto, el propio individuo es el que tiene la potestad para decidir qué entidades los tratan y con qué fines, así como la confidencialidad respecto a los mismos.

Para garantizar esto, la LOPD desarrolla una serie de principios que son aplicables en todo el ciclo de vida de los datos, desde la recogida inicial de la información, pasando por su conservación y uso, hasta la supresión final.

1.2.1 Nuestros derechos como ciudadanos

Como ciudadanos tenemos una serie de derechos que pretenden garantizar que seamos dueños y decisores en la utilización de nuestros datos personales.

Los derechos de los ciudadanos, a modo resumido, son los siguientes:

- **En la recogida de los datos:** derecho a que sólo sean recogidos si el titular ha dado su consentimiento previo, siendo informado de quién va a utilizar los datos, para qué se van a emplear y qué derechos puede ejercer dicho titular.

- **En la conservación y el uso:** derecho a que los datos sean actuales, a que no se utilicen para otra finalidad distinta a la que se informó en la recogida, a que no se cedan a otras entidades sin obtener antes el consentimiento del titular y a que sea preservada la confidencialidad y seguridad de los mismos.

- **En la supresión:** derecho a que sean destruidos de forma segura y definitiva.

1.3 LA RECOGIDA DE LOS DATOS PERSONALES

El primer paso del tratamiento de datos personales es su obtención. Cada entidad recoge los datos de una forma determinada, según los procedimientos que tiene establecidos para ello.

La recogida de los datos se puede realizar de diversas formas:

- **Por escrito:** cuando rellenamos un formulario en papel para realizar el alta en un servicio, o para que nos manden una revista, por ejemplo.

- **Online:** cuando rellenamos un formulario en Internet para darnos de alta en una red social o en algún otro servicio.

- **Verbal:** cuando contratamos algo por teléfono, o damos nuestros datos en un comercio para que nos den de alta en su sistema.

- **Por captación:** cuando nuestra imagen es captada por una cámara de vigilancia colocada en el lugar que estamos visitando.

Siempre que recoja datos personales, el responsable del fichero debe cumplir con estas obligaciones:

- Información.
- Consentimiento.

En caso de que el responsable obtenga los datos sin cumplir con las obligaciones establecidas, se entenderá que no está legitimado para tratar los datos recogidos en estas condiciones.

1.3.1 Información

Toda persona tiene el derecho de conocer a quién va a dar sus datos, qué van a hacer con ellos y cómo puede ejercer sus derechos.

Para poder decidir si se autoriza o no a que se traten los datos personales de un individuo, éste debe conocer previamente los detalles de dicho tratamiento, pudiendo ser sancionado por ello el responsable del fichero si no ha informado debidamente.

Así, quien recoge los datos nos debe informar de forma clara y comprensible de:

- La existencia de un fichero en el que se incluirán nuestros datos.
- La identidad y dirección del responsable del fichero.
- La finalidad para la cual se van a utilizar los datos facilitados.
- Cómo ejercer los derechos de acceso, rectificación, cancelación y oposición.
- Si van a ceder los datos a un tercero. En este caso nos deben informar también del sector de actividad del tercero y el uso que este tercero va a dar a los datos facilitados (así como la identidad y dirección del tercero en el momento en que le cedan los datos).

IMPORTANTE

Si el responsable es una persona física, deberá indicar su nombre y apellidos, y si es una persona jurídica, su razón social. No es válido que sólo se indique el nombre comercial, pues precisamente lo que se pretende conseguir con la LOPD es que el titular conozca claramente a quién está suministrando sus datos, sin que la identidad del responsable del fichero quede oculta por un nombre comercial o una marca.

Existen varias formas de informar:

- **A través de carteles:** esta modalidad se utiliza cuando los datos personales se recogen verbalmente en el establecimiento del responsable o en caso de existir cámaras de videovigilancia.
- **Por escrito:** si los datos se recogen a través de un formulario en papel, la información requerida debe estar necesariamente en dicho formulario (normalmente, está en la parte inferior con un tamaño de letra más reducido).
- **Online:** en caso de que los datos personales se recojan a través de un formulario en Internet, es necesario que el usuario acepte de forma expresa la *Política de Privacidad* que regula el tratamiento de los datos recogidos a través de dicho formulario y que debe incluir la información mencionada anteriormente.
- **Verbalmente:** se utiliza cuando la contratación o la atención se realiza de forma telefónica.

Todas estas maneras de informar son perfectamente válidas, siempre que la información se proporcione de forma clara, accesible y previamente a la captación de los datos.

EJEMPLO DE CLÁUSULA INFORMATIVA EN FORMULARIO

De acuerdo con lo establecido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos de que los datos aportados serán incluidos en un fichero del que es titular Construyendo Futuro Informático S. L., con la finalidad de realizar la gestión fiscal, contable y administrativa de los servicios solicitados. Le informamos también sobre sus derechos de acceso, rectificación, cancelación y oposición, que podrá ejercer en su domicilio social, sito en Av. Madrid, 10 – 34004, Palencia.

IMPORTANTE

La información que tiene que proporcionar el responsable debe estar adecuada a la forma en que obtiene los datos de los titulares.

1.3.2 Consentimiento

Los datos personales sólo pueden recogerse y tratarse si el titular de los mismos ha dado su consentimiento.

Además, para que el consentimiento otorgado por el titular de los datos sea válido han de cumplirse ciertas características que detallamos a continuación:

- **Libre:** el consentimiento debe ser otorgado sin que existan coacciones de ningún tipo (salvo que la ley obligue a facilitar nuestros datos, en cuyo caso nos deben informar del carácter obligatorio de los datos que tenemos que aportar y de las consecuencias derivadas si nos negamos a facilitar dicha información).

- **Revocable:** el haber otorgado consentimiento en un momento determinado no lo consolida de por vida. Cualquier consentimiento que hayamos otorgado libremente lo podemos revocar en cualquier momento.

- **Específico:** el consentimiento debe ir referido a un tratamiento concreto y para una finalidad determinada. No es válido que traten nuestros datos para cualquier cosa que deseen. Deben indicarnos de forma concreta para qué van a usarlos.

- **Informado:** no es posible otorgar consentimiento sobre algo que desconocemos. Por ello, debemos tener toda la información a nuestra disposición antes de aportar los datos.

- **Inequívoco:** es preciso que nos indiquen expresamente una acción u omisión que implique la existencia del consentimiento (consentimiento expreso o tácito) para que tengamos claro cómo vamos a otorgarlo.

1.3.2.1 TIPOS DE CONSENTIMIENTO

- **Consentimiento expreso:** se otorga a través de una acción específica del titular, como una firma o el marcado de una casilla.

- **Consentimiento tácito:** se considera otorgado simplemente con que, teniendo el titular la oportunidad de oponerse al tratamiento de sus datos durante un tiempo, no haga nada (suelen ser 30 días). Por ejemplo, si le dicen al titular que sus datos van a ser incluidos en un fichero si no manifiesta su oposición en un plazo de 30 días, es un consentimiento tácito, ya que el titular no tiene que hacer nada para otorgarlo, la simple inacción otorga el consentimiento.

1.3.3 Excepciones al consentimiento

Existen casos en los que nuestros datos pueden tratarse sin nuestro consentimiento. La LOPD establece las siguientes excepciones, en las cuales no es necesario obtener nuestro consentimiento para tratar los datos:

- **Ley:** cuando lo autorice una norma con rango de ley.

- **Administraciones públicas:** cuando se recojan por parte de las Administraciones públicas en el ejercicio de sus competencias. Por ejemplo, estaremos en el padrón de habitantes de nuestro Ayuntamiento, nos guste o no, porque es necesario para la gestión de los impuestos.

- **Fuentes accesibles:** cuando los datos figuren en fuentes accesibles al público. Por ejemplo, cuando utilizan los datos de la guía telefónica para enviarnos publicidad (aunque sí podremos oponernos al tratamiento de nuestros datos).

- **Interés vital:** cuando el tratamiento tenga por finalidad satisfacer un interés vital del interesado. Por ejemplo, en caso de urgencia médica grave, se podría acceder a los datos del paciente o realizar pruebas de las que se obtendrá información personal para salvar su vida. Los profesionales y centros de salud a los que acudamos (públicos o privados) también podrán tratar nuestros datos de salud sin nuestro consentimiento, puesto que este se considera otorgado por el mero hecho de acudir a ellos.

- **Exista una relación:** cuando los datos se refieran a las partes de un contrato o precontrato, o exista una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento. Por ejemplo, al contratar una línea de teléfono hay datos, como los identificativos o los relativos a la cuenta bancaria para girar los recibos del consumo, que obligatoriamente hemos de facilitar a la compañía.

- **Investigación policial:** cuando los datos se recojan en el marco de una investigación policial, siempre que sea necesario.

1.3.4 Datos especialmente protegidos y consentimiento

Como ya he indicado antes, existen datos que por su relevancia en cuanto a la intimidad o a la no discriminación merecen una especial protección. En este caso, el consentimiento se refuerza de forma significativa, de manera que se elimina dentro de las opciones el consentimiento tácito y, además, se refuerza el consentimiento expreso.

Son datos especialmente protegidos los que revelen:

- Ideología.
- Afiliación sindical.
- Religión.
- Creencias.

Estos datos sólo podrán ser tratados con nuestro consentimiento expreso y por escrito, advirtiéndonos además de nuestro derecho a no prestarlo.

La LOPD también confiere especial protección, por entender que su difusión podría afectar a nuestra intimidad, a los datos que revelen nuestra:

- Salud.
- Origen racial.
- Vida sexual.

Para recoger este tipo de datos se requiere nuestro consentimiento expreso (difiere del anterior porque no tiene que ser necesariamente por escrito).

1.3.5 Cesión de datos y consentimiento

Una cesión de datos personales se produce cuando éstos se comunican a alguien distinto del responsable[1], de las personas que prestan sus servicios al responsable y del titular de los datos, es decir, un «tercero».

El consentimiento también afecta a las cesiones de datos personales. Como regla básica: sólo con el consentimiento del titular de los datos o cuando una ley lo permita pueden cederse datos personales[2].

Para que sea válido el consentimiento que otorgamos para la cesión de datos personales nos han de informar previamente de la misma, indicándonos la actividad desarrollada por el cesionario[3] y la finalidad a la que va a destinar los datos que se van a ceder. Además, en el momento que se produzca la primera cesión de datos han de informarnos de ello, indicándonos así mismo la naturaleza de los datos cedidos, la finalidad del fichero y el nombre y dirección del cesionario.

1.3.6 Consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma

Si durante el proceso de formalización de un contrato encontramos que nos solicitan consentimiento para finalidades no relacionadas con el objeto del mismo (por ejemplo, para enviarnos publicidad) o para realizar una cesión de datos, el responsable del fichero debe permitirnos manifestar nuestra negativa a través de una casilla claramente visible y que no se encuentre ya marcada en el documento que se nos entrega para formalizar el contrato.

EJEMPLO DE CLÁUSULA INFORMATIVA EN CONTRATO

De acuerdo con lo establecido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos de que los datos aportados serán incluidos en un fichero del que es titular Construyendo

1 Responsable: entidad que almacena y trata los datos (empresa, Administración, asociación, etc.).

2 Si se desea profundizar en este tema, en la segunda parte de esta obra se explican en detalle las excepciones que se aplican al consentimiento para la cesión de datos personales.

3 Cesionario: entidad a la que se comunican los datos personales.

Futuro Informático S. L., con la finalidad de realizar la gestión fiscal, contable y administrativa de los servicios solicitados. Así mismo, consiente que los datos sean utilizados para mandarle información comercial sobre nuestros productos y servicios. También consiente que sus datos sean cedidos a empresas del sector financiero para que le envíen publicidad de sus servicios. Le informamos también sobre sus derechos de acceso, rectificación, cancelación y oposición, que podrá ejercer en su domicilio social, sito en Av. Madrid, 10 – 34004, Palencia.

[ ] No deseo que me manden comunicaciones comerciales.
[ ] No deseo que mis datos sean cedidos a otras empresas.

1.4 EL TRATAMIENTO DE DATOS PERSONALES

Como indicábamos antes, con la expresión «tratamiento de datos» nos referimos a cualquier operación que se realiza con los datos.

La LOPD no sólo establece una serie de requisitos informativos y de obtención de consentimiento en la recogida de los datos, sino que regula de forma detallada todo el ciclo de vida de la información, estableciendo una serie de obligaciones encaminadas a garantizar la calidad y seguridad de los datos personales.

1.4.1 Calidad

A través del principio de calidad de los datos, la LOPD regula los límites dentro de los cuales pueden ser recogidos y utilizados, así como su actualización y cancelación:

- **Proporcionalidad:** los datos que se recojan deben ser adecuados, pertinentes y no excesivos para la finalidad a la que se van a destinar. Debe haber una proporcionalidad entre los datos que se solicitan y la finalidad a la cual van a ser destinados. Es decir, si me solicitan los datos para hacerme una factura, por ejemplo, sería adecuado pedirme el nombre, apellidos, NIF y domicilio. En cambio, sería desproporcionado que me pidiesen para esa misma finalidad cuántos hijos tengo o cuáles son mis ingresos.

- **Finalidad:** los datos personales sólo podrán utilizarse para las finalidades indicadas en el momento de la recogida. Cualquier uso de esos datos para una finalidad distinta a la indicada exigirá nuestro consentimiento informado sobre ella.

- **Exactitud:** los datos personales deberán ser puestos al día, de forma que respondan a nuestra situación real en todo momento. Hemos de tener en cuenta que actualmente muchas decisiones que nos afectan —la concesión de una beca o de un requerimiento, por ejemplo— dependen de la exactitud de los datos. Por ello, la entidad que los trata tiene la obligación de corregir los datos erróneos cuando tenga constancia de ello, ya sea a petición del titular o de oficio.
- **Cancelación:** los datos deberán ser cancelados cuando dejen de ser necesarios o pertinentes para la finalidad para la cual fueron recogidos. Es decir, cuando no sean ya necesarios —por ejemplo, si se trata de un *curriculum vitae* y ha terminado el proceso de selección de personal—, deben ser cancelados de oficio por el responsable.
- **Almacenamiento:** el responsable debe almacenar los datos de forma que permitan el ejercicio del derecho de acceso. De esta forma se garantiza que los titulares de los datos puedan ejercer sus derechos. Más adelante veremos estos derechos en profundidad.
- **Recogida lícita:** se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos. Es decir, el responsable debe recoger los datos sin utilizar engaños u otras artimañas.

1.4.2 Seguridad

Tal y como establece la normativa, el responsable del fichero debe adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales, para evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Es decir, debe tener establecidos una serie de procedimientos y controles que garanticen la integridad, disponibilidad y confidencialidad de la información que trata.

A través de la implantación de una serie de medidas de seguridad, debe asegurarse de que los datos son en todo momento veraces, están disponibles cuando se necesitan y sólo acceden a ellos las personas autorizadas.

Estas medidas de seguridad que debe implantar el responsable se dividen en tres niveles: básico, medio y alto. En función del tipo de datos tratados —identificativos, de solvencia, de salud, etc.— debe aplicar unas medidas de seguridad[4] u otras.

4 En la segunda parte de esta obra se desarrollan en detalle las medidas de seguridad que se deben aplicar en función del nivel de seguridad requerido por el tipo de datos que se tratan.

- **Exactitud:** los datos personales deberán ser puestos al día, de forma que respondan a nuestra situación real en todo momento. Hemos de tener en cuenta que actualmente muchas decisiones que nos afectan —la concesión de una beca o de un requerimiento, por ejemplo— dependen de la exactitud de los datos. Por ello, la entidad que los trata tiene la obligación de corregir los datos erróneos cuando tenga constancia de ello, ya sea a petición del titular o de oficio.
- **Cancelación:** los datos deberán ser cancelados cuando dejen de ser necesarios o pertinentes para la finalidad para la cual fueron recogidos. Es decir, cuando no sean ya necesarios —por ejemplo, si se trata de un *curriculum vitae* y ha terminado el proceso de selección de personal—, deben ser cancelados de oficio por el responsable.
- **Almacenamiento:** el responsable debe almacenar los datos de forma que permitan el ejercicio del derecho de acceso. De esta forma se garantiza que los titulares de los datos puedan ejercer sus derechos. Más adelante veremos estos derechos en profundidad.
- **Recogida lícita:** se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos. Es decir, el responsable debe recoger los datos sin utilizar engaños u otras artimañas.

1.4.2 Seguridad

Tal y como establece la normativa, el responsable del fichero debe adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales, para evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Es decir, debe tener establecidos una serie de procedimientos y controles que garanticen la integridad, disponibilidad y confidencialidad de la información que trata.

A través de la implantación de una serie de medidas de seguridad, debe asegurarse de que los datos son en todo momento veraces, están disponibles cuando se necesitan y sólo acceden a ellos las personas autorizadas.

Estas medidas de seguridad que debe implantar el responsable se dividen en tres niveles: básico, medio y alto. En función del tipo de datos tratados —identificativos, de solvencia, de salud, etc.— debe aplicar unas medidas de seguridad[4] u otras.

4 En la segunda parte de esta obra se desarrollan en detalle las medidas de seguridad que se deben aplicar en función del nivel de seguridad requerido por el tipo de datos que se tratan.

Cuanto mayor sea la afectación respecto a la intimidad de los datos tratados, mayor será el nivel de seguridad y más exigentes las medidas de seguridad que debe aplicar para su almacenamiento.

1.4.3 Desechado de los datos personales

Lamentablemente, son frecuentes las noticias en los medios de comunicación que informan de que una determinada entidad ha desechado datos personales tirándolos al contenedor de basura directamente sin antes destruirlos —*curriculum vitae*, facturas, historiales clínicos, etc.—, afectando gravemente de este modo a la privacidad de esas personas y acarreando cuantiosas sanciones a la entidad que ha cometido la infracción.

Hemos de tener en cuenta también qué tipo de obligaciones de seguridad deben respetarse en la última fase del tratamiento, esto es, la destrucción de los datos personales cuando han dejado de ser necesarios. Para ello, los datos han de destruirse de forma segura y sin que sea posible su posterior recuperación, tanto si están en formato papel como si están en soporte digital.

En estos casos, normalmente, el responsable deberá hacer uso de medios técnicos, como una trituradora de papel o un *software* para el borrado seguro de discos duros cuando, por ejemplo, se deseche un equipo informático. De este modo se tiene la certeza de que los datos quedan definitivamente destruidos antes de proceder a su desechado.

1.4.4 Secreto

El responsable y todos los que intervengan en cualquier fase en el tratamiento de los datos personales están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el responsable del fichero.

El deber de secreto es primordial en la protección de datos, pues la confidencialidad de la información depende de que las personas que intervienen en su tratamiento lo respeten en todo momento y a lo largo del tiempo.

Si alguien infringe este deber de secreto, puede ser sancionado duramente por la Agencia Española de Protección de Datos, pues esta infracción está calificada como grave.

1.5 LOS DERECHOS DEL TITULAR

La LOPD tiene articulados una serie de derechos para que los ciudadanos puedan ejercer de forma efectiva el control sobre su información personal. Estos derechos son los de acceso, rectificación, cancelación y oposición, conocidos como los derechos ARCO.

A través de estos derechos podemos conocer la información que sobre nosotros tiene un responsable, así como de dónde la ha obtenido y a quién se la ha cedido. También podemos rectificar nuestros datos si no son veraces o incluso cancelarlos si no deseamos que sean utilizados por una determinada entidad.

1.5.1 Aspectos que se deben tener en cuenta

Debemos tener en cuenta una serie de aspectos a la hora de ejercer los derechos ARCO ante un responsable:

- **Derecho personalísimo:** el ejercicio de los derechos ARCO es personalísimo y debe ser ejercido directamente por el titular de los datos u otorgando la representación a otra persona. Los derechos serán denegados si lo solicita una persona distinta del titular de los datos y no acredita su representación.

- **Ejercicio directo ante el responsable:** los derechos ARCO se ejercen directamente ante el responsable del fichero que gestiona nuestros datos personales. En caso de omisión por su parte, podemos pedir la tutela de la Agencia Española de Protección de Datos.

- **Gratuito:** el ejercicio de los derechos debe ser sencillo y gratuito. No puede suponer un ingreso adicional para el responsable, que deberá atender cualquier solicitud que le sea debidamente presentada. No es acorde con la normativa, por ejemplo, el necesario envío de una carta certificada, o la llamada a un teléfono de tarificación adicional.

- **Respuesta obligada:** el responsable debe respondernos siempre, incluso si no figuran datos personales del titular que ha ejercido el derecho en sus ficheros. En caso de que la solicitud no reúna los requisitos deberá solicitar la subsanación de los mismos. El personal del responsable también debe ser capaz de informarnos en todo momento sobre cómo ejercer nuestros derechos.

1.5.2 Procedimiento para ejercer los derechos ARCO

Para ejercer cualquier derecho debemos dirigir una comunicación al responsable del fichero o tratamiento en la que conste:

- Nuestro nombre y apellidos.
- Nuestra fotocopia del DNI/NIF y, en su caso, de la persona que lo representa, así como el documento que acredita tal representación.
- La petición en que se concreta la solicitud.
- Nuestra dirección a efectos de notificaciones.
- La fecha y nuestra firma.
- Los documentos acreditativos de la petición que formula, si son necesarios.

1.5.3 El derecho de acceso

El derecho de acceso nos permite obtener información sobre nuestros datos de carácter personal que están siendo objeto de tratamiento.

Características de este derecho:

- **Información proporcionada:** nos permite conocer las finalidades del tratamiento que se está realizando, así como el origen de dichos datos y las cesiones previstas de los mismos.
- **Plazo de respuesta:** la petición debe ser atendida en un máximo de un mes desde la recepción de la solicitud, haciéndose efectivo el derecho de acceso en un máximo de 10 días desde ese momento.
- **Intervalo:** entre la petición de un ejercicio de acceso y el siguiente ante un mismo responsable han de pasar al menos 12 meses, salvo que se acredite un interés legítimo para ello.

- **Recepción de la información:** al ejercitar el derecho de acceso podremos optar por recibir la información a través de uno o varios de los siguientes medios:
  - Visualización en pantalla.
  - Escrito, copia o fotocopia remitida por correo.
  - Telecopia.
  - Correo electrónico u otros sistemas de comunicaciones electrónicas.
  - Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

1.5.4 El derecho de rectificación

El derecho de rectificación nos permite corregir errores sobre aquellos datos que resulten ser inexactos o incompletos, de forma que los mismos respondan de manera veraz a nuestra situación actual.

Características de este derecho:

- **Información que se debe proporcionar:** tenemos que indicar la corrección que deba realizarse y deberá ir acompañada de la documentación justificativa de los cambios solicitados.
- **Plazo de respuesta:** la petición debe ser atendida en un máximo de 10 días desde la recepción de la solicitud.
- **Propagación:** si los datos rectificados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de 10 días contados desde la recepción de dicha comunicación, proceda así mismo a rectificar los datos.

1.5.5 El derecho de cancelación

Este derecho permite que se supriman nuestros datos dentro del tratamiento efectuado por un responsable (bien porque ya no tengamos relación con él o porque los datos son inadecuados o excesivos).

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido dicho plazo, deberá procederse a la supresión de los datos.

Características de este derecho:

- **Información que se debe proporcionar:** tenemos que indicar los datos a los que se refiera la cancelación, aportando documentación justificativa si es necesaria.

- **Plazo de respuesta:** la petición debe ser atendida en un máximo de 10 días desde la recepción de la solicitud.

- **Propagación:** si los datos cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda así mismo a cancelar los datos.

1.5.6 El derecho de oposición

El derecho de oposición es el que posee el afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

1. Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una ley no disponga lo contrario.

2. Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, cualquiera que sea la empresa responsable de su creación.

3. Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal. (Nota: lo veremos más en detalle en la Parte II de esta obra, en el apartado «Derecho de impugnación de valoraciones».)

El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo indicado más abajo.

Características de este derecho:

- **Información que se debe proporcionar:** tenemos que indicar los datos a los que se refiera la oposición, motivando la misma adecuadamente y aportando documentación justificativa si es necesaria. En el caso de ficheros cuya finalidad sea la realización de actividades de publicidad y prospección comercial, no es necesario aportar motivo alguno.

- **Plazo de respuesta:** la petición debe ser atendida en un máximo de 10 días desde la recepción de la solicitud.

- **Propagación:** si el derecho de oposición se ejercitase ante una entidad que hubiera encomendado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de 10 días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero, a fin de que el mismo atienda el derecho del afectado en el plazo de 10 días desde la recepción de la comunicación, dando cuenta de ello al afectado.

1.5.7 Tutela de derechos y denuncia de infracciones

En caso de que el responsable no atienda o deniegue de forma injustificada nuestra petición de ejercicio de un derecho, podremos dirigirnos a la Agencia Española de Protección de Datos, solicitando la tutela del mismo.

También podremos presentar una denuncia ante una infracción de cualquier tipo, ya sea de la normativa de protección de datos o el envío de comunicaciones comerciales por medios electrónicos (*spam*).

Dentro de las competencias que la Agencia Española de Protección de Datos tiene asignadas está la potestad de inspeccionar y sancionar las infracciones que se produzcan en la normativa de protección de datos y en el envío de comunicaciones comerciales por medios electrónicos.

Para ello iremos a su página web (http://www.agpd.es), y en la sección «Canal del Ciudadano» dispondremos de todo lo necesario para poder presentar la denuncia.

1.5.8 Derecho de consulta

El derecho de consulta permite que cualquier persona pueda conocer, recabando para ello la información oportuna del Registro General de Protección de Datos, la siguiente información:

- La existencia de tratamientos de datos de carácter personal y los detalles del mismo (descripción, estructura, cesiones, etc.).
- Las finalidades del mismo.
- La identidad del responsable del tratamiento.

Para ello, todos los responsables están obligados por ley a inscribir sus ficheros ante el Registro General de Protección de Datos.

Este registro puede consultarse desde la dirección http://www.agpd.es, en la sección «Ficheros Inscritos».

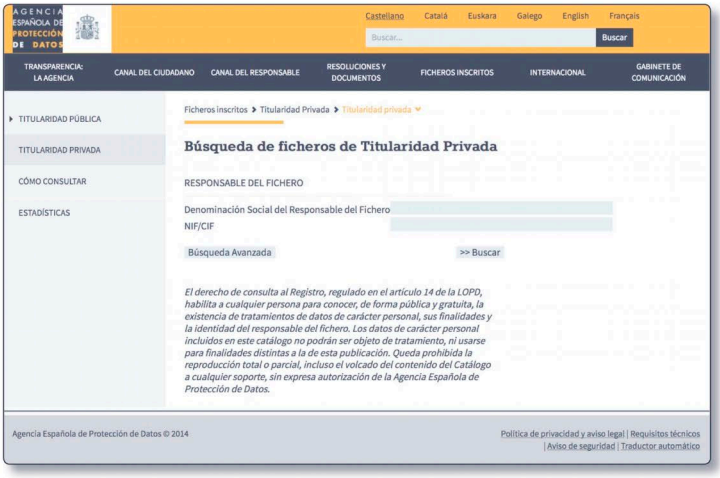


Figura 1.2. Formulario para realizar consulta de ficheros inscritos de la AEPD.Fuente: http://www.agpd.es

1.5.9 Derecho a indemnización

Aunque la cuantía económica de las sanciones que impone la Agencia Española de Protección de Datos a aquellas entidades que incumplen la normativa de protección de datos no va a parar a los afectados por las infracciones, la ley establece un derecho a indemnización cuando los afectados —como consecuencia del incumplimiento por parte del responsable de lo dispuesto en la LOPD— sufran daño o lesión en sus bienes o derechos.

Es decir, que si la revelación, por ejemplo, de determinados datos personales por parte de un responsable me ha supuesto un daño o perjuicio, tengo todo el derecho a exigir una indemnización a dicho responsable.

Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

En el caso de ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

2

USUARIOS, INTERNET Y PROTECCIÓN DE DATOS

«Internet es una gigantesca máquina de espionaje al servicio del poder. Debemos luchar contra esta tendencia y convertirla en un motor de transparencia para el público, no sólo para los poderosos».

Julian Assange

2.1 INTRODUCCIÓN

El ciberespacio se ha convertido en un nuevo medio, tan transitado o más que el medio físico tradicional. La expansión de Internet durante estos años ha sido imparable. Tal es la magnitud actualmente que quien no dispone de un acceso a Internet está excluido de numerosas facetas de la vida social y económica.

Nunca antes en la historia ha sido posible acceder a tanta información de forma tan sencilla y accesible. Estamos inmersos en la Sociedad de la Información, que va dando paso, poco a poco, a la Sociedad del Conocimiento.

Internet hace posible realizar numerosas gestiones sin necesidad de acudir presencialmente: gestionamos nuestras cuentas con las credenciales que nos proporciona el banco; contratamos viajes, alojamientos y excursiones; realizamos todo tipo de compras en la Red y pagamos con la tarjeta de crédito.

Otro fenómeno es el auge de las redes sociales, que nos permiten estar en todo momento conectados con otros usuarios y compartir con ellos momentos

especiales (fotos del último viaje, logros profesionales, etc.). Sin embargo, hemos de tener especial cuidado con lo que compartimos, puesto que a lo mejor determinadas cosas pueden afectar a nuestra vida en un futuro o limitar el acceso como candidatos a un determinado puesto (si vamos a optar a un puesto de responsabilidad, a lo mejor no es buena idea colgar en las redes sociales las fotos de las fiestas a las que nos invitan los fines de semana, y que suelen terminar a altas horas de la mañana y sin mucha sed). Aunque el acceso a estas redes sociales es «gratuito», debemos tener en cuenta que lo que estamos proporcionando a cambio de dicho acceso son nuestros datos personales (identificación, fotos, reflexiones, mensajes privados, etc.). Es más, cada interacción que realizamos —compartir una foto, dar a «Me gusta», indicar que estamos contentos, etc.) queda almacenada, y va nutriendo de información nuestro perfil. Esta información es utilizada por la red social para conocernos cada vez mejor y mostrarnos publicidad acorde a nuestros gustos e intereses.

Es indudable que Internet nos ha facilitado la vida y ha puesto a nuestra disposición más información de la que seríamos capaces de asimilar en varias vidas. Sin embargo, no todo son ventajas en su uso. Los ciberdelincuentes están al acecho en todos los rincones. Nuestra información personal es extremadamente apetecible para ellos, puesto que las estafas y fraudes requieren del previo acceso a nuestra información personal, y esta información está ahora más expuesta que nunca.

En Internet existe un numeroso código malicioso que aguarda a ser ejecutado para robarnos nuestra información personal o para proporcionar un acceso a un usuario no autorizado que le permita utilizar nuestro equipo para cometer fraudes y otros actos delictivos.

Es necesario que entre todos fomentemos una cultura de protección de datos en la Sociedad de la Información, ya que ello posibilitará que los ciudadanos podamos hacer un uso responsable de Internet y de la información que aportamos y compartimos en este medio.

En este capítulo vamos a analizar los principales riesgos que comporta el uso de Internet, sobre todo de cara a la privacidad y el robo de información personal, así como una serie de recomendaciones para tratar de prevenir o mitigar estos riesgos.

2.2 IDENTIFICACIÓN Y AUTENTICACIÓN EN INTERNET

La identificación correcta de los usuarios y su autenticación es sin duda uno de los pilares sobre los que se asientan los servicios que se ofrecen a través de Internet.

Desde el inicio de Internet se ha hecho necesario establecer mecanismos que restrinjan el acceso y permitan comprobar que las personas que se conectan a un servicio determinado son quienes dicen ser, impidiendo el acceso fraudulento a los datos y servicios.

El reconocimiento y validación de la identidad de los usuarios es algo indispensable para realizar la prestación de servicios y la autorización de accesos. El objetivo de la misma es que, tanto los servicios como los accesos, sólo puedan ser realizados por los legítimos usuarios que han sido previamente autorizados.

Estos mecanismos nos permiten acceder a diversos servicios, como la banca electrónica, la administración electrónica, el comercio electrónico, u otros servicios de carácter restringido, como el correo electrónico, el almacenamiento de documentos en la nube o la gestión de nuestros perfiles en la redes sociales, entre otros.

Para poder utilizar cualquiera de los servicios descritos en el párrafo anterior es necesario confirmar la identidad de la persona que va a utilizar dicho servicio. Debemos tener en cuenta que la importancia de disponer de unos mecanismos efectivos para validar el acceso a los servicios se incrementa con la oferta cada vez mayor de servicios que se ofrecen por Internet y para los cuales es necesario gestionar la identidad y el acceso de las personas que acuden a ellos.

A continuación, vamos a detallar los términos y mecanismos más utilizados para conceder el acceso a los usuarios a través de Internet.

2.2.1 Acceso a los servicios en Internet

Es preciso garantizar que únicamente acceden al servicio y a la información los usuarios debidamente autorizados. Para ello, se deben realizar tres pasos:

1. **Identificación:** indica al sistema cuál es la cuenta de usuario que se va a utilizar. Normalmente, es lo que se rellena en el campo «usuario».

2. **Autenticación:** el sistema debe comprobar entonces que ese usuario es quien dice ser, a través, por ejemplo, de la introducción de una contraseña. Es lo que se rellena en el campo «contraseña».

3. **Autorización:** el sistema, una vez verificada la identidad del usuario, debe comprobar que dicho usuario tiene autorizado el acceso al servicio o recurso que desea utilizar.

2.2.2 Mecanismos de autenticación

Existen diversas maneras de autenticación del usuario en función del mecanismo o tecnología que se aplique. Podemos clasificar los sistemas en estos tipos:

- Sistemas basados en algo que el usuario conoce (contraseña).
- Sistemas basados en algo que el usuario posee (DNI electrónico, *token*[4], etc.).
- Sistemas basados en una característica física del usuario, también denominados biométricos (reconocimiento de huella dactilar, voz, rostro, patrón ocular, etc.).
- Sistemas mixtos, que combinan dos o más de los descritos anteriormente.

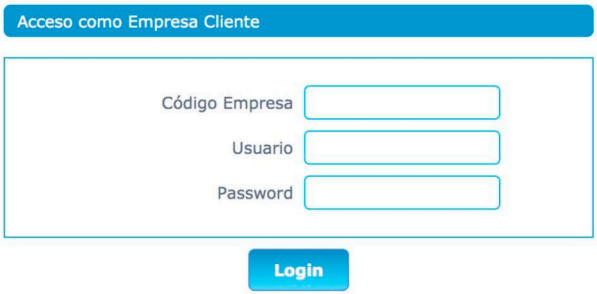


Figura 2.1. Formulario de entrada que utiliza contraseña para autenticar al usuario

4 Token: dispositivo electrónico que se le da a un usuario autorizado de un servicio para facilitar el proceso de autenticación. Los tokens tienen un tamaño pequeño y su diseño permite llevarlos cómodamente en el bolsillo, la cartera o un llavero.

2.2.3 La contraseña de acceso

La contraseña es sin duda el sistema de autenticación preferido en Internet por el bajo coste y la flexibilidad que ofrece para ser utilizada desde múltiples dispositivos (un *token*, por ejemplo, normalmente requiere que el dispositivo disponga de un puerto USB).

La contraseña de acceso es un conjunto de caracteres escrito por el usuario que lo autenticará ante el sistema de información.

La fortaleza de un sistema basado en contraseña de acceso radica precisamente en la fortaleza de la misma. Por tanto, debe ser:

- Secreta.
- Personal.
- Intransferible.
- Modificable sólo por el titular.
- Difícil de averiguar.

2.2.4 Riesgos inherentes a la contraseña

El uso de contraseña como autenticación al sistema lleva parejo una serie de riesgos:

- Pérdida u olvido de la misma.
- Substracción por parte de un tercero.
- No renovación periódica de la misma.
- Descuidos en la operativa (no cerrar la sesión cuando se abandona el sistema informático).

2.2.5 Normas para construir las contraseñas

Para garantizar la seguridad es necesario seguir una serie de normas a la hora de construir las contraseñas:

- Una longitud mínima de 8 caracteres, combinando letras, números, mayúsculas y minúsculas, así como caracteres especiales (*$%&/-!=+).
- Evitar todas aquellas contraseñas deducibles por terceros y asociadas a parámetros comunes del usuario (fechas de nacimiento, nombre de familiares, matrículas de coches, aficiones, etc.).

Algunos consejos para construir una contraseña óptima:

- Use un acrónimo de algo fácil de recordar. Ejemplo: ElsCocBic (Elsa, Coche, Bici).
- Añada un número al acrónimo para mayor seguridad. Ejemplo: ElsCocBic7 (Elsa, Coche, Bici, Número).
- Mejor si la frase origen no es conocida por otros. Ejemplo: Verde19ydos (Verano del 92).
- Realice reemplazos de letras por signos o números. Ejemplo: 3duard0-6arc1a.

2.2.6 Normas de uso de la contraseña

Para garantizar la confidencialidad de la contraseña es preciso cumplir las siguientes normas de uso:

- No utilice la misma contraseña para todos los servicios en Internet. Si un delincuente la averigua, dispondrá de acceso a todos esos servicios.
- Sea cauto a la hora de introducir su contraseña para no ser visto.
- No observe a otros mientras lo hacen.
- No escriba la clave en papelitos ni en *post-it* ni en archivos sin cifrar.
- No comparta su contraseña con otros.
- No pida la contraseña de otro.
- Si por algún motivo tuvo que escribir la clave, no la deje al alcance de terceros (debajo del teclado, en un cajón del escritorio) y *nunca* pegada al monitor.
- *Nunca* envíe su clave por correo electrónico, ni la mencione en una conversación, ni se la entregue a nadie, aunque sea o diga ser el administrador del sistema.
- No mantenga una contraseña indefinidamente. Cámbiela regularmente.

2.3 EL CÓDIGO MALICIOSO

En Internet existe una cantidad ingente de código malicioso que está a la espera de que lo ejecuten en un sistema informático y que tiene distintos propósitos, aunque ninguno bueno.

Se denomina código malicioso o *malware* a cualquier programa escrito para producir inconvenientes, destrucción, utilizar los recursos de los usuarios o recabar información de los equipos sin el conocimiento de su propietario.

Hay diversos tipos de código malicioso, como virus, *spywares* o troyanos.

2.3.1 Virus

Un virus es un *malware* que tiene por objetivo alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario.

Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de éste y tienen la capacidad de autoreplicarse. Para ello, una vez ha sido ejecutado el programa infectado por el virus —algo que, por supuesto, el usuario desconoce—, se carga en memoria y toma el control del sistema operativo, infectando los programas que son llamados a ejecución y añadiendo el código del virus a éstos, produciéndose la propagación del mismo.

Además, los virus suelen contener una carga dañina (*payload*) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas.

2.3.2 Spyware

El *spyware* o programa espía es un *software* que recopila información de un ordenador y después la transmite a un usuario externo sin el conocimiento del propietario de la computadora.

Sin embargo, a diferencia de los virus, no se intenta replicar en otros ordenadores, por lo que funciona como un parásito.

2.3.3 Troyano

Un troyano es un código malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que al ejecutarlo le brinda a un atacante acceso remoto al equipo infectado.

Los troyanos pueden realizar múltiples tareas —robar información del equipo y mandarla a un servidor remoto, realizar capturas de pantalla, abrir la webcam y el micrófono, etc.—, pero normalmente abren una puerta trasera en el equipo para permitir su control remoto por parte de un usuario no autorizado.

A diferencia de un virus, un troyano no necesariamente provoca daños, pues éste no es su objetivo. Su fin es permitir que un usuario no autorizado acceda al equipo, normalmente para robar datos bancarios o información personal.

2.3.4 Qué puede hacer el código malicioso

El código malicioso puede realizar diversas acciones en los sistemas, en función de la finalidad que pretenda conseguir (hacer daño, obtener información, capturar nuestro equipo para su uso, etc.).

En concreto, puede:

- Borrar archivos del disco duro para que el equipo quede inoperativo.
- Almacenar contenido ilegal en su equipo.
- Instalar otros programas maliciosos.
- Infectar un equipo y usarlo para atacar a otros.
- Obtener información sobre usted: los sitios web que visita, sus hábitos…
- Monitorizar las pulsaciones del teclado para robar las credenciales.
- Grabar sus conversaciones activando el micrófono o su imagen activando su webcam.
- Ejecutar comandos en la computadora, como si lo hubiera hecho usted.
- Robar archivos del equipo; por ejemplo, aquéllos con información personal, financiera, fotos, etc.

2.3.5 Recomendaciones de seguridad

- No instale *software* de fuentes no fiables. Acuda siempre al sitio web oficial del fabricante.
- Mantenga su sistema operativo actualizado, instale siempre las últimas actualizaciones del fabricante y los *service packs*[5].
- Utilice un buen antivirus, que incluya también la detección de *spywares* y troyanos, y manténgalo actualizado.
- Realice copias de seguridad del contenido de su equipo de forma periódica.
- Si duda de un *software*, sea precavido y no lo instale.
- Instale un *firewall*[6] y monitorice las conexiones que su equipo realiza para detectar posibles conexiones remotas.

2.4 LA NAVEGACIÓN

Quizás una de las cosas que más se hacen en Internet es navegar por las páginas web. Tenemos millones y millones de páginas por las que navegar y sumergirnos en información de todo tipo. Sin embargo, no podemos obviar los riesgos inherentes a la navegación, que son numerosos.

La descarga de ficheros o la aparición de ventanas emergentes que nos inviten a descargar algo en un atractivo anuncio pueden esconder en realidad un *software* malicioso, que espera pacientemente ser ejecutado.

Por otro lado, antes de suministrar ningún dato personal en un formulario hemos de asegurarnos de la identidad de la entidad que los está recogiendo, y debemos revisar en detalle su *Política de Privacidad* para evitar desagradables sorpresas. Muchos concursos a los que podemos inscribirnos son en realidad un completo fraude, que permite obtener rápidamente los datos de miles de personas que luego se van a vender de forma ilícita.

---

5 Los programas denominados Service Pack consisten en un grupo de actualizaciones que corrigen y mejoran aplicaciones y sistemas operativos. Son lanzados por el propio fabricante.

6 Los firewall o cortafuegos son dispositivos diseñados para bloquear los accesos no autorizados a la Red, permitiendo al mismo tiempo los accesos autorizados.

2.4.1 Recomendaciones de seguridad

- Navegue siempre con un antivirus activo y actualizado.
- Tenga instaladas las últimas actualizaciones del sistema operativo y del navegador para evitar «agujeros» de seguridad.
- Establezca la configuración de seguridad del navegador en un nivel alto.
- Borre periódicamente las *cookies* del navegador y los archivos temporales para evitar ser rastreado continuamente.
- Configure el navegador para que bloquee las ventanas emergentes.
- Antes de descargar un archivo, asegúrese de que es fiable.
- Si accede al equipo de otra persona o público, utilice el modo «navegación privada» del navegador.
- Antes de suministrar ningún dato personal en un sitio web, asegúrese de que éste dispone de una *Política de Privacidad* y que en la misma se detalla la identificación del responsable y su dirección, así como la finalidad para la cual se recogen los datos y cómo se pueden ejercer los derechos ARCO. Obviamente, no debemos suministrar más datos de los necesarios según la finalidad para la cual estamos aportando dichos datos.
- Antes de introducir datos sensibles, como el número de tarjeta de crédito, debe asegurarse de que la conexión entre nuestro navegador y el servidor está cifrada (lo sabremos porque aparecerá un candado en el navegador).

2.5 EL CORREO ELECTRÓNICO

El correo electrónico es una herramienta muy versátil que permite la comunicación y el envío de mensajes entre ubicaciones muy distantes entre sí de forma casi inmediata.

Es una de las herramientas más utilizadas por los usuarios y las entidades.

Sin embargo, presenta una serie de problemas de seguridad que se deben tener en cuenta para prevenir engaños, falsificaciones, correo no solicitado, código malicioso, ataques de *phishing*, etc.

2.5.1 Código malicioso

A través del correo electrónico se puede distribuir de forma muy rápida y efectiva código malicioso que infecte nuestro sistema, bien sea a través de un fichero adjunto al correo recibido —que esconde un virus o un troyano—, o como un enlace contenido en el cuerpo del correo y que va a servir para descargar ese código malicioso.

Debemos ser muy críticos con los ficheros adjuntos, abriéndolos sólo si estamos seguros de su licitud. Si no estamos esperando una factura por correo, no debemos hacer caso al correo que nos indica que nos adjunta la factura que supuestamente estábamos esperando.

Mención especial merecen los *ransomware*, que es un tipo de código malicioso que cifra los documentos de un equipo y pide un rescate. Estos *ransomware* normalmente se propagan a través de un correo que parece ser de una fuente legítima, y por medio de ingeniería social nos insta a pulsar un enlace para ser descargado y ejecutado. Una vez ejecutado, el código malicioso cifra todos los ficheros del equipo que tienen una extensión determinada (.docx, .xlsx, etc.), exigiendo el pago de un rescate para que nos envíen la clave de descifrado.

2.5.1.1 RECOMENDACIONES DE SEGURIDAD CONTRA EL CÓDIGO MALICIOSO

Para evitar ser infectados por código malicioso que utiliza el correo electrónico como canal de entrada a nuestro equipo hemos de tener en cuenta una serie de recomendaciones:

- Mantenga actualizado su programa de correo electrónico.
- No abra archivos adjuntos de origen desconocido.
- No abra archivos adjuntos que no espera recibir, aunque le parezca que su origen es conocido.
- No abra adjuntos que tengan extensiones ejecutables o más de una extensión.

2.5.2 Spam

Spam son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas.

Aunque se puede hacer *spam* por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

Usualmente, los mensajes indican como remitente del correo una dirección falsa, de modo que no sirve de nada contestar a los mensajes de *spam*. Por ahora, el servicio de correo electrónico no puede identificar los mensajes de forma que se pueda discriminar la verdadera dirección de correo electrónico del remitente de otra falsa.

Los *spammers* utilizan varias técnicas para construir largas listas de direcciones de correo a las cuales enviarles luego *spam*:

- Búsqueda de direcciones en páginas web y foros. De hecho, hay programas diseñados para ir rastreando la web y recopilando las direcciones de correo electrónico que encuentran (esto se conoce como «cosecha» de correos).
- Captura de direcciones en cadenas de mensajes.
- Suscripciones a Listas de correo.
- Compra de bases de datos de direcciones de correo.
- Acceso no autorizado en servidores de correo.
- Por ensayo y error: se generan aleatoriamente direcciones, y se comprueba luego si han llegado los mensajes.

2.5.2.1 RECOMENDACIONES DE SEGURIDAD CONTRA EL *SPAM*

Para evitar ser víctima de los *spammers*, o al menos minimizar la exposición a éstos, es conveniente cumplir una serie de recomendaciones de seguridad:

- No deje su dirección de correo electrónico en cualquier formulario o foro de Internet.
- No responda a los correos no solicitados. Bórrelos.
- Active los filtros de correo no deseado del navegador o proveedor de correo electrónico.

- No configure la «respuesta automática» para los mensajes que soliciten un acuse de recibo.
- No responda a los pedidos de acuse de recibo de orígenes dudosos.
- Evite reenviar cadenas de mensajes.
- Lea cuidadosamente las condiciones del servicio de su proveedor de correo electrónico, especialmente si proporciona cuentas gratuitas.
- Si envía un mensaje a varios destinatarios, no utilice el campo «Destinatario» o «CC» (Con Copia), pues está revelando a los receptores las direcciones de correo del resto de destinatarios. Utilice mejor el campo «CCO» (Con Copia Oculta). De este modo, ninguno de los receptores del mensaje podrá acceder a las direcciones del correo del resto de destinatarios. Hemos de tener en cuenta además que si alguien denuncia esto ante la Agencia Española de Protección de Datos, la entidad que ha realizado el envío utilizando el campo CC, en lugar de CCO, puede ser sancionada.

2.5.3 Phishing

Phishing, o suplantación de identidad, es un término que denomina un modelo de fraude que se comete mediante el uso de un tipo de ingeniería social. Se caracteriza por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

El cibercriminal, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial por correo electrónico. El *phisher* pide, a través de un correo electrónico con apariencia lícita, el envío de determinada información, o bien dentro del correo tiene un *link* hacia una página fraudulenta que es una réplica de la auténtica (suele ser a la página de un banco con objeto de «validar» los datos de acceso al mismo). Cuando, a través del enlace que hay en el correo electrónico, accedemos a esa página fraudulenta e intentamos hacer *login* en ella, realmente estamos proporcionando nuestras credenciales de acceso, quedando éstas almacenadas en una base de datos para su uso o venta posterior.

2.5.3.1 RECOMENDACIONES DE SEGURIDAD CONTRA EL *PHISHING*

En el caso de recibir peticiones de envío de información confidencial, o un correo indicando que realicemos *login* en un enlace incluido en el mismo, es conveniente cumplir las siguientes recomendaciones:

- Confirmar telefónicamente con la entidad la petición.
- Nunca enviar por correo información confidencial sin cifrar.
- Verificar el origen del correo.
- Verificar el destino de los enlaces (comprobar a través de su dirección y su certificado de seguridad que es la entidad que dice ser).
- Si tenemos dudas, no actuar antes de asegurarnos.

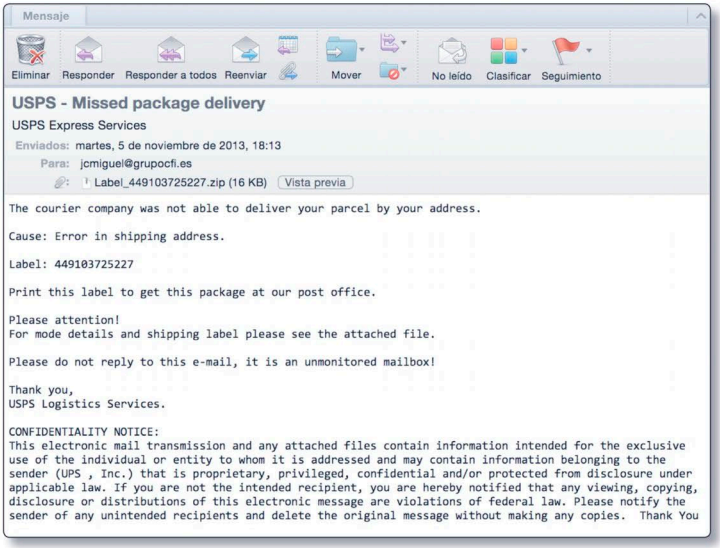


Figura 2.2. Falso correo de una supuesta empresa de transporte con un fichero adjunto que «parece» ser una etiqueta. En realidad contiene un malware

2.6 INGENIERÍA SOCIAL

La ingeniería social es un conjunto de acciones que se realizan con el fin de obtener información a través de la manipulación de usuarios legítimamente autorizados para acceder a la misma.

Se compone de una variedad de trucos, engaños o artimañas que permiten confundir a una persona para que entregue información confidencial, ya sea la propia información, los datos necesarios para acceder a ésta o la forma de saltar la seguridad de un sistema.

El *phishing* que hemos visto anteriormente no deja de ser ingeniería social, puesto que el usuario es engañado para que introduzca sus credenciales en un sitio fraudulento y, de este modo, capturarlas.

La ingeniería social se basa en estos cuatro principios:

1. El primer movimiento de un ser humano hacia otro suele ser de confianza.
2. En general, nos gusta y queremos ayudar.
3. No nos gusta decir «no».
4. A todos nos gusta que nos alaben.

Hemos de tener siempre presente que el factor humano es el eslabón más débil en la cadena de la seguridad de la información.

2.6.1 Recomendaciones de seguridad contra la ingeniería social

- Tenga en cuenta que su entidad financiera no le va a solicitar nunca información por correo electrónico o que «valide» sus credenciales de acceso.
- Si recibe un correo extraño, en otro idioma o que está traducido «automáticamente», desconfíe.
- Desconfíe de las ofertas económicas que le llegan a su correo y que le ofrecen grandes beneficios.

- No olvide que aunque un correo «parezca» provenir de un conocido, a lo mejor no es así. Si desconfía, asegúrese de que el correo es legítimo por otro medio (por ejemplo, una llamada de teléfono), puesto que la cuenta puede estar comprometida.

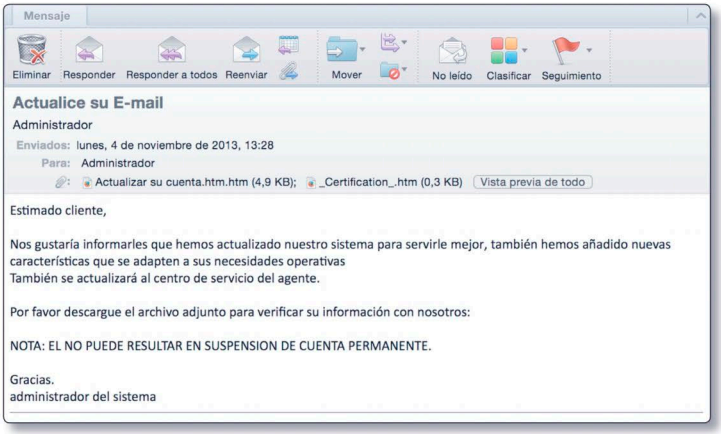


Figura 2.3. Falso correo que intenta engañarnos para que descarguemos un fichero

Se dice que el único ordenador seguro es el que está desenchufado, en una caja fuerte, con la cerradura sellada y enterrada bajo hormigón. Aun así, existen riesgos.

Los entendidos en ingeniería social responden que siempre existirá un ser humano dispuesto a enchufarlo…

2.7 LAS REDES P2P

Se entiende como red P2P (*Peer to Peer*) a la red informática que no tiene clientes y servidores fijos, sino que consta de una serie de nodos que se comportan simultáneamente como clientes y como servidores de los demás nodos de la red, permitiendo la compartición de archivos entre los miembros de la misma.

Estas redes permiten el funcionamiento de los programas típicos de descarga de música, vídeos, películas, etc.

Las redes P2P se basan en la instalación de un programa en el equipo que quiere pertenecer a esa red. En la instalación se establecen unas carpetas compartidas en las que se van a almacenar los archivos descargados y que a su vez son puestos a disposición del resto de miembros de esa red.

2.7.1 Riesgos de las redes P2P

El uso de redes P2P entraña una serie de riesgos para los sistemas y las comunicaciones, entre los cuales podemos destacar:

- Multitud de puertos abiertos en el sistema y exposición de riesgo.
- Consumo excesivo de ancho de banda.
- Compartición de archivos que el usuario no deseaba compartir.
- Descarga no intencionada de código malicioso.
- Descarga ilegal de contenido con propiedad intelectual o pedófilo.

2.7.2 Recomendaciones de seguridad

- El equipo debe tener antivirus instalado y actualizado.
- Descargue el programa para conectarse de sitios fiables; en caso contrario, podría contener un virus o un troyano.
- Lea atentamente las condiciones de uso, antes de aceptar el contrato, pues podría estar permitiendo el uso de su ordenador o el acceso a sus datos.
- Monitorice el estado de su sistema después de la instalación, asegurándose de que no se ha instalado nada más (por ejemplo, un troyano) y de que no se producen conexiones sospechosas.
- Revise las carpetas que está compartiendo en su equipo; a lo mejor está compartiendo algo que no desea. Lo ideal es utilizar un equipo en exclusiva para esto y que no tenga ninguna otra información.
- Tenga cuidado con lo que descarga, pues puede contener código malicioso o no ser lo que espera.
- Antes de ejecutar cualquier programa descargado, analícelo con el antivirus.

- Si tiene hijos, tenga especial precaución y vigile atentamente lo que descargan: mucho contenido no es lo que parece ser.

- Instale un cortafuegos, pues normalmente el equipo está encendido las 24 horas del día y es conveniente limitar el acceso a los puertos.

- De vez en cuando, apague el *router*[7] al menos cinco minutos para que su IP pública se refresque (y cambie).

- En caso de que el programa le pida definir un nombre de usuario, proporcione un alias que no tenga ninguna relación con su identidad verdadera.

- Analice periódicamente el equipo en busca de *malware*.

2.8 LOS BUSCADORES

Un buscador es un sistema informático que busca archivos almacenados en servidores web gracias a sus *spider* (también llamado «araña web»).

Los *spider* son programas que inspeccionan las páginas de la web de forma metódica y automatizada. Recorren la web indexando las páginas que encuentran en una base de datos para ofrecer luego, como resultado, una lista de páginas relacionadas con una búsqueda concreta realizada.

El resultado de la búsqueda, «Página de resultados del buscador», es un listado de direcciones web en el que se mencionan temas relacionados con las palabras clave buscadas por el usuario, facilitando la localización de las páginas web más relevantes con relación a la búsqueda realizada.

7 Router: dispositivo que proporciona conectividad entre redes. Se suele utilizar para conectarse a Internet.

Los servicios de búsqueda más avanzados guardan el historial de búsquedas y la navegación del propio usuario para ofrecerle un resultado más óptimo y personalizado.

Esto puede impactar de forma significativa en la privacidad de un individuo, pues conocer todo el historial de búsquedas y navegación de un usuario concreto revela una gran cantidad de información sobre sus intereses, entre otras cosas.

Por otro lado, nosotros mismos podemos ser objeto de una búsqueda, y la información que hemos publicado en Internet en diversos lugares relacionada con dicha búsqueda (nombre, apellidos, *e-mail*, fotos, vídeos, etc.) quedar expuesta a cualquiera.

2.8.1 Recomendaciones de seguridad

- Borre con regularidad los archivos temporales de Internet, el historial de navegación y las *cookies*.
- Vigile lo que publica sobre usted en foros abiertos y otros lugares públicos de Internet.
- No publique nada inadecuado o innecesario sobre otros.
- Lea atentamente las condiciones de uso del servicio y la *Política de Privacidad*.
- Búsquese a sí mismo regularmente y observe la información que aparece.

2.9 LAS REDES SOCIALES

Las redes sociales han supuesto una auténtica revolución en Internet. Nunca antes ha sido tan fácil conectar con cientos o miles de personas y compartir con ellas información de todo tipo. Cada día millones de personas manifiestan en las redes sociales sus inquietudes, reflexiones y pensamientos. De la misma forma hacen partícipes a los demás de sus logros, viajes y aspiraciones, compartiendo con ellos textos, fotografías y vídeos de su vida personal y profesional.

Sin embargo, como todo, las redes sociales tienen dos caras. Una es la cara amable. Con ella mis amigos pueden seguir mi evolución personal y profesional y yo la de ellos. La otra cara es menos amable, pues lo que publico en la Red, si no establezco correctamente la configuración de privacidad de la misma, puede ser visto por cualquiera.

Por poner un ejemplo, los ladrones ya no necesitan vigilar una casa para comprobar si los dueños están de vacaciones o no. Sólo deben estar atentos a la gente que comparte en las redes sociales que está de vacaciones para enterarse de los posibles objetivos que tiene disponibles para asaltar.

Hemos de tener en cuenta otro factor de suma importancia: nosotros no somos los clientes de la red social, somos los usuarios. Los clientes son los que pagan las facturas (normalmente, los que contratan publicidad en la misma). Nosotros, los usuarios que la utilizamos, somos en realidad la mercancía con la que se comercia. «Pagamos» por usar la red social con los datos que ponemos a su disposición, con las reflexiones que escribimos, con las fotos que subimos y con las interacciones que realizamos en ella. Todas las acciones que realizamos van nutriendo nuestro perfil de datos que evidencian nuestros intereses, aficiones, estilo de vida, etc. De esta forma, la red social nos puede mostrar anuncios que son de nuestro interés. Es más, según vamos realizando más y más interacciones (compartir una publicación, dar a «Me gusta», etiquetar una foto, etc.), mejor nos conoce la Red y más personalizados son los anuncios que nos muestra.

Por otra parte, desconocemos cómo hechos que ahora no nos importan mucho —como colgar una fotografía de una fiesta en la que hemos bebido un poco más de la cuenta— nos van a afectar en un futuro. Por ejemplo, a la hora de optar a un puesto de trabajo. Esto es algo que ya ocurre. Las personas encargadas de la selección de personal suelen revisar la actividad en las redes sociales de los posibles candidatos.

Si deseamos proteger nuestra privacidad, debemos conocer las implicaciones que tiene el que todo lo que realizamos en la Red quede registrado y actuar en consecuencia para mantener una identidad digital saneada. Si hay algo que no debemos olvidar es que cada vez más nuestra identidad digital va a condicionar nuestra identidad física.

El problema fundamental es que la configuración por defecto de las redes sociales habitualmente está diseñada para compartir todo con todos. De esta forma, la información que vamos subiendo a la red social está disponible para cualquiera que quiera acceder a ella, incluidos los buscadores.

2.9.1 Recomendaciones de seguridad

- Revisar la Política de Privacidad y las condiciones generales de uso de la red social antes de darnos de alta en ella.
- Estar atentos a los cambios en la Política de Privacidad o las condiciones generales y cancelar la cuenta si no estamos de acuerdo con algún aspecto.
- Revisar la configuración de privacidad de la red social y ajustarla a nuestras preferencias.
- Tener precaución a la hora de publicar fotos y vídeos, en especial si en ellos aparecen terceras personas.
- No etiquetar a otras personas en los contenidos audiovisuales sin su previo consentimiento.
- Aceptar sólo a las personas que conozcamos.
- No publicar información precisa de nuestra dirección que permita ubicarnos físicamente.
- Utilizar una contraseña robusta y diferente para cada red social.

2.10 INTERNET Y LOS MENORES

Cada vez es más frecuente el acceso a Internet por parte de los menores.

Lo utilizan de forma cotidiana, tanto para realizar búsquedas de información para un trabajo de clase como para encontrar vídeos que les enseñen a patinar, jugar en red con otros amigos, intercambiarse las fotos de la última excursión o mantener el contacto con los amigos a través de las redes sociales, por poner algunos ejemplos.

Son los llamados «nativos digitales», que se mueven por el medio bastante mejor que los adultos, pues han nacido inmersos en él.

Sin embargo, los menores no perciben ni comprenden todavía la necesidad de proteger su información personal, ni cómo ésta puede condicionarlos en el futuro.

Es necesario que nosotros, los padres y educadores, mantengamos una serie de precauciones encaminadas a proteger a los menores en Internet.

2.10.1 Recomendaciones de seguridad

- Conocer el medio. Es necesario que padres y educadores conozcamos Internet, cómo funciona y los beneficios y peligros que entraña para poder educar adecuadamente a los menores.

- Informar a los menores de los peligros que conlleva el uso de Internet. Debemos advertirles de que igual que en la vida física no deben hablar con desconocidos, esto es aplicable a Internet, donde no deben intercambiar información ni fotografías con desconocidos, así como no aceptar ninguna invitación de conexión.

- Concienciarlos sobre los riesgos de publicar o compartir material gráfico en Internet y sus posibles consecuencias.

- Instalar el equipo en una zona común de la casa, como el salón, por ejemplo, y establecer unos horarios de uso.

- Navegar con ellos, indicándoles los sitios peligrosos y las páginas seguras (al igual que hacemos con ellos en la vida física).

- Indicarles que no proporcionen sus datos en ningún formulario web si antes no lo hemos supervisado nosotros.

- Instalar algún control parental que filtre las páginas para evitar que por accidente pueda navegar por sitios no adecuados u ofensivos.

- Si se detecta alguna conducta desagradable u ofensiva en alguna red social, denunciarlo a la propia red. Si es una conducta delictiva, denunciarlo a las Fuerzas y Cuerpos de Seguridad del Estado.

- Controlar la información que el menor publica en su perfil, asegurándonos de que no revela su nombre completo, localización precisa u otra información no adecuada.

2.11 LA RESPONSABILIDAD DE LOS USUARIOS

Tradicionalmente, la capacidad de elaborar y difundir noticias y material audiovisual era algo reservado a los periodistas y los medios de comunicación. Tanto los periodistas como los medios tenían claros sus deberes y responsabilidades en cuanto a lo que publicaban.

Sin embargo, esto ha cambiado. Internet ha hecho posible que cualquiera pueda «convertirse» en periodista y ser capaz de generar y compartir información de todo tipo —textos, fotografías y vídeos— con el mundo entero.

Sin embargo, hemos de tener en cuenta que también asumimos la responsabilidad sobre todo lo que publicamos en nuestra página, blog o red social.

Amenazar, difamar o faltar al honor a una persona en Internet no es menos delito que hacerlo en el mundo físico. Es más, en Internet esto se ve agravado por la gran capacidad de difusión que tiene el medio. Y lo que en el medio físico es un insulto o una amenaza que sólo es escuchada por unas pocas personas, en Internet puede convertirse en algo incontrolable, causando un gran impacto y graves perjuicios a la persona afectada.

Para evitar publicar algo que nos pueda acarrear un grave disgusto conviene seguir una serie de recomendaciones que a continuación detallamos.

2.11.1 Recomendaciones para realizar publicaciones

- Respetar la dignidad de las personas, en especial la de los menores.
- No publicar informaciones que no sean veraces o de interés público.
- No publicar informaciones no contrastadas o rumores.
- No grabar ni publicar fotografías o vídeos sin el consentimiento de las personas que aparecen en ellos.
- No publicar información que pueda poner en riesgo a alguna persona o identificar dónde vive o dónde se encuentra.
- Retirar o rectificar la información si el afectado, de modo justificado, lo solicita.
- Cumplir con la Ley Orgánica de Protección de Datos de Carácter Personal cuando proceda.

3

EL DERECHO AL OLVIDO

«Internet es mucho más que una tecnología. Es un medio de comunicación, de interacción y de organización social».

Manuel Castells

3.1 INTRODUCCIÓN

Imaginémonos un mundo en el que ninguna información desaparece. Todo queda almacenado para siempre. Las fotos que publicamos, las reflexiones que escribimos, nuestros errores. Todo, absolutamente todo lo que se publica, queda registrado. En especial, los errores, por el impacto mediático. Bueno, no hace falta que imagine mucho. Eso ocurre actualmente. Se llama Internet.

Está claro que todos podemos cometer un error. Y como consecuencia puede ocurrir que aparezcamos en una noticia publicada en Internet, que a lo mejor en ese momento tiene sentido que aparezca por ser algo relevante.

El problema ocurre cuando después de un largo tiempo —pongamos años después— alguien utiliza un buscador e introduce nuestro nombre como clave de búsqueda y lo primero que aparece es esa noticia.

A lo mejor ya hemos pagado por el error cometido, a lo mejor ni lo habíamos cometido y la rectificación de la noticia aparece más abajo de la noticia inicial, en otra publicación que nadie mira, porque el impacto de la primera noticia eclipsa lo demás.

Todo el mundo tiene derecho a una segunda oportunidad. ¿O no?

El pasado no tiene por qué condicionar el futuro. ¿O sí?

El problema real no es la noticia, ni que se mantenga la publicación en Internet a lo largo del tiempo. El problema real es que los buscadores rastrean la Red hasta sus entrañas, y son capaces de hacer aflorar la información que existe en Internet sobre cualquier persona que busquemos, apareciendo hoy en pantalla hechos y noticias que pueden haber ocurrido hace mucho, mucho tiempo y que pueden lastrar la vida futura de esa persona.

Tiene sentido entonces que, al igual que antes de la aparición de Internet los errores quedaban olvidados y acumulando polvo en las hemerotecas, haya ahora algún procedimiento que permita «borrar» esos errores incómodos una vez haya transcurrido un tiempo, de forma que cuando se introduzca el nombre de esa persona en un buscador no aparezcan.

Este derecho, reconocido en el ámbito europeo a través de una sentencia del Tribunal de Justicia de la Unión Europea, es lo que se denomina «derecho al olvido».

3.2 EL DERECHO AL OLVIDO

Se puede definir como el derecho que tiene un ciudadano a borrar, bloquear o suprimir información personal propia que se considera obsoleta por el transcurso del tiempo o que de alguna manera afecta el libre desarrollo de alguno de sus derechos fundamentales.

Sin embargo, este derecho colisiona frontalmente con los derechos a la libertad de expresión y a la libertad de información.

Por otra parte, si de forma habitual pueden eliminarse parte o la totalidad de las noticias ocurridas en el pasado, ¿cómo sabremos, después de un tiempo, que lo que consultamos sobre una fecha pasada es fiable y no han sido eliminadas personas o detalles posteriormente? ¿Cómo sabremos que no se está manipulando el pasado, y además de forma legal?

Como observamos, la solución no es sencilla.

Sin embargo, analizando la situación, vemos que realmente lo que afecta a la persona no es la noticia en sí, pues no deja de ser algo que sucedió en un momento determinado. Lo que perjudica de verdad a esa persona es la rapidez con la que aflora esa noticia en el momento en que se realiza una búsqueda con su nombre y apellidos, con lo que un hecho ocurrido en el pasado termina afectando gravemente al presente y futuro de ese individuo.

La solución pasa entonces no por eliminar la noticia de la fuente original, sino por eliminar de la base de datos del buscador el enlace hacia la noticia cuando la búsqueda se realiza introduciendo el nombre y apellidos de la persona, de forma que no aparezca dicha noticia en los resultados de búsqueda.

3.2.1 Claves para entender su funcionamiento

A continuación, se muestran una serie de claves que nos van a ayudar a entender el funcionamiento de este derecho, así como sus límites:

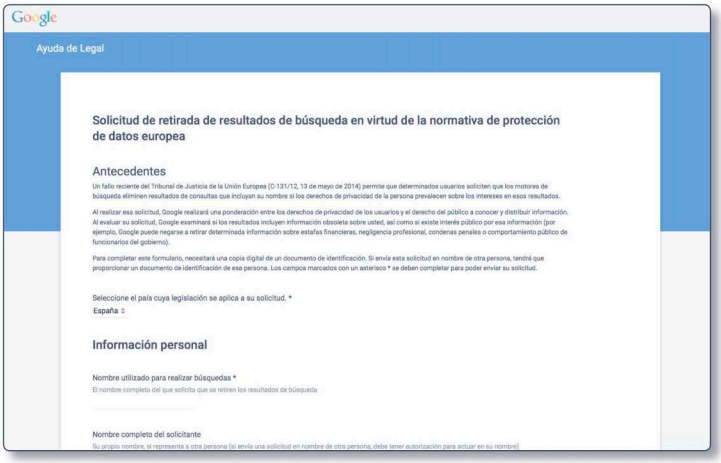
- No se elimina la noticia original de la fuente original. Es decir, la noticia original, si es veraz, permanece en el medio en que ha sido publicada sin ninguna alteración.
- Se elimina únicamente la referencia a dicha noticia de los resultados de búsqueda, cuando la búsqueda se realiza introduciendo el nombre y apellidos de la persona afectada.
- Si se busca la noticia por otros parámetros que no sea el nombre y apellidos de la persona —por ejemplo, la matrícula del coche—, o por el nombre y apellidos de otra persona que aparezca en la noticia y que no haya solicitado este derecho, la noticia entonces aparecerá en los resultados de búsqueda.
- Sólo se aplica en las webs de buscadores externos, como Google, Yahoo, Bing[8], etc. En los buscadores internos de webs no será de aplicación. Es decir, que en el buscador interno del propio medio de comunicación que ha publicado la noticia será posible encontrar la referencia indicando el nombre y apellidos del afectado.
- La petición de retirada de la referencia se debe realizar ante el buscador, el cual deberá ponderar caso por caso si prevalece la libertad de información o los derechos individuales de la persona.
- En caso de que el buscador rechace la reclamación, el ciudadano deberá acudir a la Agencia Española de Protección de Datos o a los tribunales ordinarios.
- El derecho al olvido sólo se aplica en la Unión Europea.

8 Google, Yahoo y Bing son marcas registradas por sus respectivos propietarios.

3.3 EJERCICIO DEL DERECHO AL OLVIDO

El derecho al olvido, como hemos indicado anteriormente, ha de ejercerse ante el propio buscador que proporciona los resultados de búsqueda, el cual dispondrá de un formulario para poder efectuar la solicitud.

En el caso de Google —sin duda, el buscador utilizado por excelencia—, éste es el formulario para solicitar la retirada de resultados de búsqueda:


Google

Ayuda de Legal

Solicitud de retirada de resultados de búsqueda en virtud de la normativa de protección de datos europea

Antecedentes

Un fallo reciente del Tribunal de Justicia de la Unión Europea (C-131/12, 13 de mayo de 2014) permite que determinados usuarios soliciten que los motores de búsqueda eliminen resultados de consultas que incluyan su nombre si los derechos de privacidad de la persona prevalecen sobre los intereses en esos resultados.

Al realizar esa solicitud, Google realizará una ponderación entre los derechos de privacidad de los usuarios y el derecho del público a conocer y distribuir información. Al evaluar su solicitud, Google examinará si los resultados incluyen información obsoleta sobre usted, así como si existe interés público por esa información (por ejemplo, Google puede negarse a retirar determinada información sobre estafas financieras, negligencia profesional, condenas penales o comportamiento público de funcionarios del gobierno).

Para completar este formulario, necesitará una copia digital de un documento de identificación. Si envía esta solicitud en nombre de otra persona, tendrá que proporcionar un documento de identificación de esa persona. Los campos marcados con un asterisco * se deben completar para poder enviar su solicitud.

Seleccione el país cuya legislación se aplica a su solicitud. *

España

Información personal

Nombre utilizado para realizar búsquedas *

El nombre completo del que solicita que se retiren los resultados de búsqueda

Nombre completo del solicitante

Su propio nombre, si representa a otra persona (si envía una solicitud en nombre de otra persona, debe tener autorización para actuar en su nombre).

En este formulario se nos solicita la siguiente información:

- **País cuya legislación se aplica a la solicitud** (recordemos que el derecho al olvido aplica no sólo a España, sino a toda la Unión Europea).
- **Nombre utilizado para realizar búsquedas.** Aquí se indica el nombre completo del que solicita que se retiren los resultados de búsqueda.
- **Nombre completo del solicitante.** Se indica en este apartado el nombre completo de la persona que realiza la solicitud (normalmente es igual al apartado anterior). En caso de que el solicitante represente a otra persona, debe tener autorización para actuar en su nombre.

- **Relación con el solicitante.** En caso de enviar la solicitud en nombre de otra persona, se debe especificar su relación con ella (por ejemplo, «padre» o «abogado»).
- **Dirección de correo electrónico de contacto.** Dirección a la que se van a enviar los correos electrónicos relacionados con la solicitud.
- **URL de resultados que quiere que se retiren.** Aquí se debe especificar, una por una, las URL[9] que se solicita retirar, así como:
  - Los motivos por los que la página web enlazada se refiere al solicitante (porque tuve un grave accidente de coche, por ejemplo).
  - Y los motivos por los que la inclusión de cada URL como resultado de búsqueda resulta irrelevante, obsoleto o inaceptable de cualquier otro modo (porque fue hace cinco años y me está causando un enorme perjuicio por este motivo…).
- **Copia legible del documento de identidad.** Se debe adjuntar una copia escaneada del Documento Nacional de Identidad para que Google pueda verificar la identidad del solicitante.
- **Confirmación de que la información indicada es precisa.** Para ello se debe marcar la casilla aceptando que la información de la solicitud es precisa y que es la persona afectada por las páginas web identificadas, o que se dispone de la autorización de la persona afectada para enviar la solicitud.
- **Firma.** Aquí se pide firmar la solicitud. Sólo hay que poner nombre y apellidos.
- **Firmado el [fecha].** Indicar la fecha en la que se realiza la solicitud.
- **Enviar.** Por último, enviar el formulario.

Ya sólo queda esperar a que Google se ponga en contacto con nosotros para confirmar la retirada de los enlaces, solicitarnos más información o denegarnos la solicitud.

En este último caso, podremos acudir a la Agencia Española de Protección de Datos o a los tribunales ordinarios para reclamar nuestro derecho.

---

9 La URL es la dirección completa de la página. Se puede encontrar en la barra del navegador después de hacer clic en el resultado de búsqueda en cuestión.

PARTE II

LAS OBLIGACIONES DE LOS RESPONSABLES

4

LA LOPD Y LOS RESPONSABLES

«El valor que percibe tu cliente es el tiempo que le dedicas a él, no el que empleas en la oficina».

Julio César Miguel Pérez

4.1 INTRODUCCIÓN

En la primera parte de esta obra hemos visto los derechos que asisten a los ciudadanos en la protección de sus datos personales.

Pero para que haya unos derechos irremediablemente tiene que haber unas obligaciones.

En esta segunda parte vamos a ver la normativa de protección de datos personales, pero desde la perspectiva de los responsables del fichero. Es decir, de la empresas, administraciones, asociaciones, etc., que almacenan y gestionan datos personales para el desempeño de su actividad o sus funciones.

Para ello, vamos a entrar más a fondo en los detalles más técnicos y formales de la normativa. Entre otras cosas, veremos qué debe contener necesariamente una cláusula informativa, cuándo y en qué situaciones es necesario pedir consentimiento, qué medidas de seguridad se deben aplicar a los datos personales en función de su sensibilidad, cuándo se pueden ceder datos personales a otras entidades, etc.

Hemos de tener en cuenta que el cumplimiento de esta normativa, si bien no es una tarea difícil, exige un conocimiento en detalle de la misma para que no sea incumplida por puro desconocimiento, tanto por la organización como por los miembros de la misma.

Al igual que hay leyes obvias —todos sabemos que no debemos matar a otro ser humano, independientemente de que la ley lo prohíba expresamente—, la LOPD no es una de ésas. Un empresario o trabajador puede, tranquilamente, arrojar un montón de albaranes con datos personales sin destruir al cubo de la basura y no percibir de forma natural que ha cometido una infracción. Precisamente por la falta de obviedad que tiene esta ley, todos los sujetos que intervienen en el tratamiento deben ser cuidadosamente formados para evitar su vulneración y las cuantiosas sanciones que acarrea su incumplimiento.

4.2 LA PROTECCIÓN DE DATOS PERSONALES

La protección de datos de carácter personal hace referencia al derecho fundamental del individuo a decidir sobre sus propios datos frente al tratamiento masivo de los mismos, especialmente como consecuencia de la aparición y desarrollo de las nuevas tecnologías de la información y las comunicaciones.

Los ciudadanos son cada vez más conscientes de los derechos que los asisten en materia de protección de datos, así como de la existencia de un organismo —la Agencia Española de Protección de Datos— a la que pueden pedir la tutela de sus derechos cuando perciben que están siendo vulnerados.

Por otra parte, las empresas cada vez perciben más el valor que tienen los datos almacenados en sus ficheros, y la necesidad de una protección efectiva de los mismos.

Esto va construyendo una sociedad de la información en la que cada vez se es más consciente y se percibe el alto valor de la información que se posee —ya sean datos de carácter personal u otro tipo de datos internos de la empresa, como los datos de facturación, presupuestos, planes, estrategias, etc.—, y de la necesidad de salvaguardarla frente a pérdidas, fugas, acceso, alteración no autorizada, etc.

4.2.1 A quién incumbe la LOPD

La ley obliga a todos los profesionales, empresas, organizaciones y organismos públicos y privados que traten con datos de carácter personal.

Esto aglutina, entre otros, a los siguientes colectivos:

- Profesionales liberales.
- Autónomos.
- AA. PP.
- Entidades jurídicas.
- Asociaciones.
- Comunidades de propietarios

4.3 MARCO LEGAL

4.3.1 Ley Orgánica 15/1999, de 13 de diciembre

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

A través de esta ley se regula la recogida y el tratamiento de los datos de carácter personal de trabajadores, clientes, proveedores, etc.

4.3.1.1 OBJETO DE LA LEY

El objeto de la Ley Orgánica es garantizar y proteger, en lo concerniente al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

4.3.1.2 ANTECEDENTES

Ya en la Constitución española de 1978, en su artículo 18, se establece lo siguiente:

«Artículo 18.1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen».

«Artículo 18.4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos, y el pleno ejercicio de sus derechos».

4.3.2 Real Decreto 1720/2007, de 21 de diciembre

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

El Reglamento de la LOPD desarrolla, de forma sistemática, los principios, derechos, obligaciones y procedimientos que garantizan el derecho fundamental a la protección de datos de carácter personal regulado por la Ley Orgánica 15/1999.

4.3.3 Ley 25/2009, de 22 de diciembre

La Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la ley sobre el libre acceso a las actividades de servicios y su ejercicio, conocida como Ley Ómnibus). Esta ley modifica 47 leyes estatales con el objeto de simplificar al máximo todos los procedimientos administrativos en el sector servicios.

De cara a la LOPD, añade una Disposición Adicional a la Ley de Seguridad Privada 23/1992, de 30 de julio, que modifica su artículo 5.1 e), por la cual, los prestadores de servicios o las filiales de las empresas de seguridad privada que vendan, entreguen, instalen o mantengan equipos técnicos de seguridad, siempre que no incluyan la prestación de servicios de conexión con centrales de alarma, quedan excluidos de la legislación de seguridad privada. Con lo cual, no se exige la necesidad de que la instalación de un sistema de videovigilancia sea realizada por una empresa autorizada de seguridad si dicha instalación no está conectada a una central de alarmas.

4.3.4 Real Decreto 3/2010, de 8 de enero

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Este Real Decreto modifica el artículo 81.5 b) del RD 1720/2007, el cual condicionaba una de las excepciones para poder aplicar un nivel básico a ficheros o tratamientos de datos especialmente protegidos, siempre que los datos estuviesen en *formato manual* y de forma incidental o accesoria se contuviesen esos datos especialmente protegidos pero sin guardar relación con su finalidad. Con la modificación, pasa a tener la siguiente redacción: «Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad», de forma que *no es requisito condicionante* para su aplicación el *sistema de tratamiento empleado*.

4.3.5 Sentencia de 15 de julio de 2010, de la Sala Tercera del Tribunal Supremo

La Sentencia de 15 de julio de 2010, de la Sala Tercera del Tribunal Supremo, declara nulos los artículos 11, 18, 38.2 y 123.2 de la disposición reglamentaria, así como la frase del artículo 38.1.a), que dice así: «... y al respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero» del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

4.3.6 Ley 2/2011, de 4 de marzo

La Ley 2/2011, de 4 de marzo, de Economía Sostenible modifica de forma sustancial el régimen sancionador de la LOPD, graduando la sanción en función de diversos factores.

4.3.7 Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos

La Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, regula la grabación, captación, transmisión, conservación y almacenamiento de imágenes de personas físicas, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

4.4 QUÉ SON DATOS DE CARÁCTER PERSONAL

Un dato de carácter personal es cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Los datos personales, pues, permiten identificar a una persona, así como revelar información de la misma.

Persona identificada: toda persona cuya identidad está determinada.

Persona identificable: toda persona cuya identidad pueda determinarse, ya sea directamente o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

Vamos a matizar el concepto «identificable». Tenemos una cámara de videovigilancia que recoge imágenes de las personas que acceden a un determinado lugar. Si las imágenes se captan con una resolución tal que permitan identificar a una persona, ésta sería una persona identificable, y estaría dentro del ámbito de la ley; en caso contrario, si la resolución es tan baja que no permite identificar a dicha persona, no lo estaría.

Cada vez que alguien recoge y trata, entre otros, los siguientes datos, estamos ante un supuesto regulado por la LOPD:

- Nombre y apellidos.
- Fecha de nacimiento.
- Teléfono fijo o móvil.
- Dirección postal.
- Correo electrónico.
- DNI/NIF.
- Fotografía.
- Grabación de vídeo.
- Categoría laboral.
- Estudios.
- Aficiones.
- Salud.
- Cualquier otra información de la que se desprendan datos personales.

4.5 CLASIFICACIÓN DE LOS DATOS DE CARÁCTER PERSONAL

Los datos de carácter personal se pueden clasificar en:

- **Datos identificativos:** nombre y apellidos, dirección postal, dirección electrónica, teléfono, DNI/NIF, SS/mutualidad, imagen, voz, firma o huella digitalizada, firma electrónica, etc.

- **Datos de características personales:** estado civil, familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, lengua materna, características físicas o antropométricas.

- **Datos de circunstancias sociales:** características de alojamiento, vivienda, situación militar, propiedades y posesiones, aficiones y estilo de vida, pertenencia a clubes y asociaciones, licencias, permisos y autorizaciones.

- **Datos académicos y profesionales:** formación y titulaciones, historial del estudiante, experiencia profesional, pertenencia a colegios o a asociaciones profesionales.

- **Datos de empleo:** profesión, puesto de trabajo, datos no económicos de nómina, historial del trabajador.

- **Datos de información comercial:** actividades y negocios, licencias comerciales, suscripciones a publicaciones y medios de comunicación, creaciones artísticas, literarias, científicas o técnicas.

- **Datos económicos, financieros y de seguros:** ingresos y rentas, inversiones y bienes patrimoniales, créditos, préstamos y avales, datos bancarios, planes de pensiones, jubilación, datos económicos de nómina, deducciones impositivas, impuestos, seguros, hipotecas, subsidios y beneficios, historial de créditos, tarjetas de crédito.

- **Datos de transacciones de bienes y servicios:** bienes y servicios suministrados por el afectado, bienes y servicios recibidos por el afectado, transacciones financieras, compensaciones, indemnizaciones.

- **Datos especialmente protegidos:** ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

4.6 QUÉ SON DATOS ESPECIALMENTE PROTEGIDOS

No es lo mismo tratar datos meramente identificativos, como el nombre y los apellidos, el NIF o el domicilio, para, por ejemplo, realizar una factura, que tratar datos que puedan comprometer a una persona, como deudas, enfermedades, orientación sexual, afiliación sindical, etc.

Hay datos de carácter personal que son mucho más sensibles que otros, atendiendo al grado de intimidad que revelan del individuo al que se refieren.

Son datos especialmente protegidos los siguientes:

- Ideología.
- Afiliación sindical.
- Religión.
- Creencias.
- Origen racial.
- Salud.
- Vida sexual.

4.6.1 Consideraciones a la hora de tratar datos especialmente protegidos

Los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias sólo podrán ser tratados con el consentimiento expreso y por escrito del afectado. Cuando se recabe el consentimiento del afectado, se le advertirá de su derecho a no prestarlo.

Los datos que hacen referencia al origen racial, la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando lo disponga una ley o el afectado consienta expresamente.

NOTA

Más adelante veremos la información que se debe proporcionar y el modo de obtener el consentimiento.

4.7 QUÉ ES UN FICHERO

Un fichero es un conjunto organizado de datos de carácter personal, que permita el acceso a dichos datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de creación, almacenamiento, organización y acceso.

Es decir, cualquier conjunto organizado de datos de carácter personal —ya sea en soporte informático o papel— se considera un fichero.

4.7.1 Tipos de ficheros

1. **Ficheros automatizados.** Son aquellos que están en soporte informático. Por ejemplo:
   - Base de datos.
   - Hoja de cálculo.
   - Documento de texto.
   - La grabación de una cámara de videovigilancia.
2. **Ficheros no automatizados.** Son aquellos que están en soporte papel o similar. Por ejemplo:
   - Listado en papel de clientes, proveedores, etc.
   - Nóminas.
   - *Curriculum vitae*.
3. **Ficheros mixtos.** Son aquellos que están tanto en soporte informático como en soporte papel o similar. Por ejemplo:
   - Facturas. Suelen estar en papel y en el programa de gestión de la empresa.
   - Presupuestos. Confeccionados a través de una aplicación informática, y se guarde el presupuesto tanto en papel como en el equipo informático.
   - Nóminas. En caso de que las confeccione la propia empresa a través de una aplicación informática, los datos suelen estar en la propia aplicación y, además, en papel.

4.8 EL RESPONSABLE DEL FICHERO

El responsable del fichero es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Es decir, el responsable es la empresa u organización que decide sobre el fichero en cuestión, tanto el contenido del mismo como el uso que se hace de su información.

Cuando el responsable del fichero es una empresa, para el desarrollo de sus actividades, generalmente es responsable, al menos, de dos ficheros:

- El fichero donde almacena los datos de sus clientes.
- El fichero donde almacena los datos de sus trabajadores.

El responsable del fichero *asume toda la responsabilidad sobre el uso y protección de los datos de carácter personal* que están bajo su control.

4.9 OBLIGACIONES DEL RESPONSABLE DEL FICHERO

El responsable del fichero tiene tres obligaciones con respecto a los ficheros de los que es titular.

4.9.1 Legalizar los ficheros

Antes de crear ningún fichero que contenga datos de carácter personal, la entidad deberá notificarlo previamente a la Agencia Española de Protección de Datos.

Este proceso conlleva dos pasos:

- Análisis de los datos tratados.
- Inscripción del fichero en el Registro General de Protección de Datos.

4.9.2 Legitimar el tratamiento

El responsable del fichero deberá legitimar el tratamiento de los datos contenidos en los ficheros de los que es responsable sobre la base de unos principios fundamentales:

- Calidad de los datos.
- Derecho de información en la recogida de datos.
- Consentimiento del afectado.
- Datos especialmente protegidos.
- Datos relativos a la salud.

- Seguridad de los datos.
- Deber de secreto.
- Comunicación de datos.
- Acceso a datos por cuenta de terceros.
- Atención a los derechos de los afectados.

NOTA

Se considerará que está legitimado para realizar el tratamiento de los datos personales si cumple todos y cada uno de los principios que establece la LOPD.

4.9.3 Proteger los datos

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

El responsable del fichero o tratamiento deberá implantar las medidas que sean necesarias para garantizar la seguridad de los datos frente a:

- Alteraciones.
- Pérdidas.
- Acceso no autorizado.

Siempre teniendo en cuenta la tecnología disponible y los riesgos a que están expuestos los datos.

A continuación, detallamos cada una de estas amenazas.

4.9.3.1 ALTERACIÓN

Se considera una alteración cualquier modificación de los datos que contiene un fichero, de forma que éstos no reflejen fehacientemente la realidad de los mismos; ya sea por acción humana o mal funcionamiento en el proceso de tratamiento de los datos (por ejemplo, al actualizar una aplicación, cambia el valor de un campo).

4.9.3.2 PÉRDIDA

Una pérdida es la destrucción total o parcial de los datos que contiene un fichero.

4.9.3.3 ACCESO NO AUTORIZADO

Es el acceso a los datos de carácter personal por una persona no autorizada por el responsable del fichero para dicho acceso.

NOTA

Las medidas que el responsable del fichero debe implantar deben tratar de *preservar la integridad, disponibilidad y confidencialidad* de los datos de carácter personal que se tratan.
Esto se verá en detalle en capítulos posteriores

4.10 DEFINICIONES

NOTA

Aunque el glosario de términos se sitúa normalmente al final de la publicación, considero que es de suma importancia para la correcta comprensión de este curso tener claro el significado de cada uno de los términos que van a aparecer posteriormente.

A los efectos previstos por la LOPD y su Reglamento de Desarrollo, se entenderá por:

- **Afectado o interesado:** Persona física titular de los datos que sean objeto del tratamiento.

- **Cancelación:** Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento, excepto para su puesta a disposición de las Administraciones Públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades.

  Transcurrido ese plazo deberá procederse a la supresión de los datos.

- **Cesión o comunicación de datos:** Tratamiento de datos que supone su revelación a una persona distinta del interesado.

- **Consentimiento del interesado:** Toda manifestación de voluntad, libre, inequívoca, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

- **Dato disociado:** aquel que no permite la identificación de un afectado o interesado.

- **Datos de carácter personal:** Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

- **Datos de carácter personal relacionados con la salud:** Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

- **Destinatario o cesionario:** La persona física o jurídica, pública o privada u órgano administrativo al que se revelen los datos.

  Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

- **Encargado del tratamiento:** La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

  Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

- **Exportador de datos personales:** La persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente reglamento, una transferencia de datos de carácter personal a un país tercero.

- **Fichero:** Todo conjunto organizado de datos de carácter personal que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

- **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.

- **Fichero no automatizado:** 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 aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

- **Importador de datos personales:** La persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

- **Persona identificable:** Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

- **Procedimiento de disociación:** Todo tratamiento de datos personales que permita la obtención de datos disociados.

- **Responsable del fichero o del tratamiento:** Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

  Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

- **Tercero:** La persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

  Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

- **Transferencia internacional de datos:** Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

- **Tratamiento de datos:** Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

En relación con las medidas de seguridad que se deben adoptar para garantizar la protección de los datos de carácter personal, se entenderá por:

- **Accesos autorizados:** autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

- **Autenticación:** procedimiento de comprobación de la identidad de un usuario.

- **Contraseña:** información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

- **Control de acceso:** mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

- **Copia de respaldo:** copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

- **Documento:** todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

- **Ficheros temporales:** ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

- **Identificación:** procedimiento de reconocimiento de la identidad de un usuario.

- **Incidencia:** cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

- **Perfil de usuario:** accesos autorizados a un grupo de usuarios.

- **Recurso:** cualquier parte componente de un sistema de información.

- **Responsable de seguridad:** persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

- **Sistema de información:** conjunto de ficheros, tratamientos, programas, soportes y, en su caso, equipos empleados para el tratamiento de datos de carácter personal.

- **Sistema de tratamiento:** modo en que se organiza o utiliza un sistema de información.

- Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

- **Soporte:** objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

- **Transmisión de documentos:** cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

- **Usuario:** sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

5

EL TRATAMIENTO DE LOS DATOS PERSONALES

«Nunca consideres el estudio como una obligación, sino como una oportunidad para penetrar en el bello y maravilloso mundo del saber».

Albert Einstein

5.1 QUÉ ES EL TRATAMIENTO DE LOS DATOS

El tratamiento de datos es cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Todas las operaciones que se realizan con los datos, incluyendo la propia recogida de los mismos, es lo que se denomina tratamiento de datos.

Para entender esto, vamos a suponer, por ejemplo, que una empresa ha creado un fichero, denominado LABORAL. En este fichero guarda los datos personales de los trabajadores: nombre, apellidos, dirección, NIF, número de la Seguridad Social, categoría, puesto, fecha de nacimiento, etc.

Los datos son recogidos del propio trabajador y utilizados después, entre otras cosas, para elaborar los contratos, nóminas y seguros sociales.

También son cedidos estos datos a las administraciones pertinentes (Agencia Tributaria, Seguridad Social, etc.).

Cuando el trabajador ha estado un período de baja, entrega el parte de baja para archivarlo. Este parte de baja que ha entregado y que la empresa guarda es incluido dentro del fichero LABORAL.

Todas y cada una de las operaciones realizadas por esta empresa con esos datos es lo que se denomina tratamiento de datos personales.

5.1.1 Momentos en el tratamiento de los datos

En el tratamiento de datos personales tenemos tres momentos fundamentales:

5.1.1.1 RECOGIDA DE LOS DATOS

Es el momento en que se recogen los datos personales. Puede ser del propio interesado, de un tercero o de fuentes accesibles al público.

En el caso que nos ocupa, es el momento en que el trabajador nos proporciona sus datos personales para iniciar la relación laboral.

5.1.1.2 CONSERVACIÓN Y UTILIZACIÓN DE LOS DATOS

Es el momento en que introducimos los datos recogidos en el fichero y los utilizamos para una finalidad específica, por ejemplo, elaborar las facturas, nóminas, contratos, etc.

En el caso del ejemplo, es el momento en que introducimos los datos en el fichero LABORAL y los utilizamos para el mantenimiento de la relación laboral (contratos, nóminas, etc.).

5.1.1.3 COMUNICACIÓN DE LOS DATOS

Es el momento en que comunicamos los datos o el resultado del tratamiento a terceros. Esto es conocido como «cesión o comunicación de datos», ya sea a una entidad o a una administración.

En el caso que tratamos, se produce en el momento en que comunicamos los datos de esos trabajadores, así como el resultado de dicho tratamiento a entidades o administraciones, como, por ejemplo, la Agencia Tributaria, a la que comunicamos las retenciones que hemos efectuado a ese trabajador y la Seguridad Social en las tablas de cotización (tc1 y tc2) que le suministramos.

En cada uno de estos momentos existen unas obligaciones específicas y definidas.

5.2 TRATAMIENTOS DE DATOS INCLUIDOS EN EL ÁMBITO DE LA LEY

La LOPD será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de esos datos por los sectores público y privado.

Están incluidos dentro de la LOPD tanto los datos de carácter personal registrados en soporte informático como los registrados en soporte papel.

Y es de aplicación tanto para las entidades privadas como para los organismos públicos.

La LOPD es de obligado cumplimiento para:

- Empresas.
- Autónomos.
- Profesionales liberales.
- Asociaciones.
- Comunidades de vecinos.
- Organismos y Administraciones Públicas.

5.3 TRATAMIENTOS DE DATOS EXCLUIDOS DEL ÁMBITO DE LA LEY

Los siguientes tratamientos de datos no estarán sometidos a la normativa vigente sobre protección de datos (LOPD):

1. Los tratamientos de datos referidos a ***personas jurídicas***.

2. Los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en:

   - Su nombre y apellidos.
   - Funciones o puestos desempeñados.
   - Dirección postal o electrónica profesional.
   - Teléfono y número de fax profesional.

Es decir, las típicas ***tarjetas de visita*** **y las** ***agendas de contactos*** que *sólo* incorporen los datos descritos están fuera del ámbito de la LOPD, siempre que la finalidad sea contactar con la empresa en la que trabaja.

- Los ***datos relativos a empresarios individuales***, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros.

NOTA

Los ***datos relativos a profesionales liberales*** (arquitectos, abogados, médicos, etc.), ***sí están dentro de la LOPD.***

3. Los datos referidos a ***personas fallecidas***.

4. Los ficheros y tratamientos realizados o mantenidos por personas físicas en el ejercicio de ***actividades exclusivamente personales o domésticas***.

   Sólo se consideran relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.

5. A los ficheros y tratamientos sometidos a la normativa sobre protección de materias clasificadas.

6. A los ficheros y tratamientos establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

5.4 TRATAMIENTOS DE DATOS PROHIBIDOS

Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

No podemos crear ficheros cuya única finalidad sea recabar datos especialmente protegidos de sujetos.

Esto se aplica tanto a ficheros automatizados como a ficheros no automatizados.

5.5 SUJETOS QUE INTERVIENEN EN EL TRATAMIENTO DE LOS DATOS

En el tratamiento de los datos personales intervienen, o pueden intervenir, los siguientes sujetos:

- **El afectado o interesado:** es la persona física titular de los datos que sean objeto del tratamiento.

  Estos datos pueden proceder del mismo sujeto, de fuentes accesibles al público o de otra entidad, a través de una cesión.

- **El responsable del fichero: es la entidad que** decide sobre la finalidad, contenido y uso del fichero y/o tratamiento.

  El responsable del fichero, en el marco empresarial, es la empresa titular del fichero, es decir, la empresa que crea, mantiene y decide sobre el fichero.

- **El encargado del tratamiento:** es la entidad que trata datos personales por cuenta del responsable del fichero.

  El encargado del tratamiento es la entidad que realiza un servicio al responsable del fichero, y para poder llevar a cabo dicho servicio necesita acceder a los datos de carácter personal del responsable del fichero.

  Por ejemplo, la asesoría que realiza las nóminas de los trabajadores de una empresa es encargada del tratamiento.

6

LA INSCRIPCIÓN DE LOS FICHEROS

«Si piensas que la educación es cara, prueba sin ella».

Benjamin Franklin

6.1 INTRODUCCIÓN

La inscripción de los ficheros de datos personales en el Registro General de Protección de Datos (RGPD) es la primera obligación para el responsable del fichero.

A través de la inscripción de ficheros se pone a disposición de todos los ciudadanos el conjunto de ficheros entre los que pueden encontrarse sus datos personales, y ante cuyos responsables pueden ejercer directamente los derechos de acceso, rectificación, cancelación y oposición.

Los ficheros inscritos en el RGPD son de libre y pública consulta, y se realiza a través de la web de la Agencia Española de Protección de Datos (www.agpd.es), que dispone de un potente filtro con el que es posible realizar búsquedas.

6.2 EL CONCEPTO DE FICHERO A NIVEL DE INSCRIPCIÓN

En la inscripción ante el RGPD se debe considerar «fichero» como el conjunto de bases de datos, tablas, ficheros planos, documentación en papel, etc.,

distribuidos en una o más localizaciones físicas, y cuya finalidad o tratamiento es aquella que nos interesa inscribir.

Para poder definir correctamente los distintos ficheros que maneja una entidad es necesario abstraerse del concepto informático de «fichero» y pensar en términos de finalidad: qué datos personales estoy gestionando y cuál es el objetivo del tratamiento.

Se deberán inscribir tanto los ficheros automatizados como los no automatizados.

Además, el nivel de medidas de seguridad que se debe aplicar deberá ser coherente con todos los componentes del «fichero».

6.2.1 Tratamiento de datos en distintos soportes

Cuando los datos de carácter personal estén almacenados en diferentes soportes, automatizados y no automatizados, o exista una copia en soporte no automatizado de un fichero automatizado, se requerirá una sola notificación referida a dicho fichero.

Es decir, si tenemos un fichero principal, por ejemplo, CLIENTES, y hacemos copia de respaldo en varios discos duros externos, únicamente debe realizarse una inscripción.

6.3 INSCRIPCIÓN DE LOS FICHEROS

Antes de comenzar el tratamiento de datos de carácter personal, el responsable del fichero debe notificar su inscripción en el RGPD.

Igualmente, debe notificar las modificaciones y supresiones de los ficheros ya inscritos.

El RGPD inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario, podrá pedir que se completen los datos que falten o se proceda a su subsanación.

La inscripción de un fichero de datos personales es declarativa. La AEPD y el RGPD no prejuzgan la veracidad de la información contenida en la notificación de inscripción, ni que se hayan cumplido el resto de las obligaciones derivadas de la LOPD.

Cuando el responsable del fichero notifica la inscripción, se está comprometiendo a cumplir con todas las obligaciones que marca la LOPD.

En la web de la Agencia Española de Protección de Datos (www.agpd.es) se encuentra el sistema NOTA, a través del cual se puede solicitar la inscripción de los ficheros en el RGPD.

6.3.1 Notificación de inscripción

La notificación de inscripción de un fichero debe contener necesariamente los siguientes extremos:

1. Identificación del responsable del fichero.
2. Identificación del fichero.
3. Finalidades y usos previstos.
4. Sistema de tratamiento empleado.
5. Colectivo de personas sobre las que se obtienen los datos.
6. Procedimiento y procedencia de los datos.
7. Estructura básica del fichero, descripción detallada de los datos identificativos, y en su caso, de los especialmente protegidos, así como las categorías de datos incluidas en el mismo.
8. Las cesiones o comunicaciones de datos previstas.
9. Las transferencias internacionales de datos previstas.
10. Los servicios o unidades ante los que pueden ejercerse los derechos de acceso, rectificación, cancelación y oposición.
11. La identificación del encargado del tratamiento, en su caso.
12. La indicación del nivel de medidas de seguridad básico, medio o alto exigible.

6.3.2 Notificación de modificación

La notificación de modificación del fichero debe indicar las modificaciones producidas en cualquiera de los extremos anteriores.

6.3.3 Notificación de supresión

La notificación de supresión de los ficheros establecerá:

1. El destino que se va a dar a los datos.

2. O las previsiones que se adopten para su destrucción.

6.4 OTRAS INSCRIPCIONES

Además de inscribir en el RGPD los ficheros tratados por las entidades privadas, son objeto de inscripción ante el RGPD:

- Los ficheros de las administraciones, entes y organismos públicos.
- Las autorizaciones de transferencias internacionales de datos de carácter personal con destino a países que no presten un nivel de protección equiparable al de la LOPD.
- Los códigos tipo.
- Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

6.5 PUBLICIDAD DE LOS FICHEROS INSCRITOS

El RGPD debe velar por la publicidad de los tratamientos y ficheros de datos personales existentes, con la finalidad de facilitar al ciudadano el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición. Por ello, el RGPD es de pública y gratuita consulta.

De esta manera, se cumple el objetivo de la inscripción de ficheros en el RGPD: facilitar que cualquier persona pueda conocer la existencia de tratamientos de carácter personal, sus finalidades y la identidad del responsable del tratamiento.

El catálogo de ficheros inscritos en el RGPD —que se puede consultar en www.agpd.es— contiene información sobre los siguientes aspectos:

1. El responsable del fichero.
2. El servicio o unidad ante el que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
3. La identificación del fichero.
4. Las finalidades y usos previstos del fichero o tratamiento.
5. El origen y procedencia de los datos.
6. Colectivo de personas sobre el que se obtienen los datos de carácter personal.
7. Los tipos de datos, estructura y organización del fichero.
8. Los destinatarios de las cesiones y/o transferencias internacionales de datos.

7

PRINCIPIOS DE LA PROTECCIÓN DE DATOS

«Al final no os preguntarán qué habéis sabido, sino qué habéis hecho».

Jean de Gerson

7.1 PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Cualquier organización, ya sea de carácter público o privado, que trate con datos de carácter personal tiene obligación de cumplir con la LOPD.

Con independencia del número de registros que tenga almacenados, tanto si los trata de manera automatizada como si no, la LOPD debe aplicarse.

Los ficheros más comunes que almacena cualquier tipo de empresa son los ficheros de personal, nóminas, clientes, proveedores y, cada vez más, videovigilancia.

El simple almacenamiento de datos, como el nombre, apellidos, dirección de los clientes, y/o empleados, supone la aplicación de la LOPD.

El tratamiento de los datos de carácter personal se considera legitimado siempre y cuando se respeten los principios que vamos a desarrollar en este capítulo.

Sobre los principios que vamos a analizar, es básico que la organización analice los flujos de información que se producen en su organización y se asegure de su conformidad de acuerdo con los siguientes principios:

- Calidad de los datos.
- Derecho de información en la recogida de datos.
- Consentimiento del afectado.
- Datos especialmente protegidos.
- Datos relativos a la salud.
- Seguridad de los datos.
- Deber de secreto.
- Comunicación de datos.
- Acceso a los datos por cuenta de terceros.

Es importante destacar que la ley define como responsable del fichero o tratamiento a la persona física o jurídica, ya sea de naturaleza pública o privada u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, el contenido y el uso del fichero, es decir, el responsable legal de la posesión y utilización de los datos de carácter personal, y sobre la que recaerán las posibles sanciones que pudieran imponerse.

Se suele designar como responsable del fichero o tratamiento a la persona jurídica propietaria del fichero.

7.2 CALIDAD DE LOS DATOS

El principio de calidad de los datos establece los límites que tiene una organización para el tratamiento de datos de carácter personal: recogida, uso, actualización, almacenamiento y cancelación.

7.2.1 Recogida de datos

De forma general, la LOPD establece que sólo se podrán recoger datos de carácter personal para su tratamiento, y someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Es decir, que los datos recogidos y tratados tienen que ser los adecuados y no excesivos para las finalidades para las que se hayan obtenido.

EJEMPLO

Supongamos que estamos recogiendo los datos de un cliente para elaborar una factura de un televisor que ha adquirido.

Los datos identificativos —como nombre, apellidos, dirección, NIF— serían adecuados, pertinentes y no excesivos.

En cambio, si además le preguntamos por su estado civil, situación laboral, o cualquier otro dato no relacionado con esa finalidad determinada —que es elaborar la factura—, esos datos a mayores sobre los estrictamente necesarios serían considerados excesivos para esa finalidad y no se podrían ni deberían recabar.

Así mismo, los datos deben ser obtenidos y tratados de forma leal y lícita; por tanto, se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

7.2.2 Uso de los datos

Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de las finalidades determinadas, explícitas y legítimas del responsable del tratamiento.

Los datos de carácter personal objeto del tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

Es decir, los datos recabados sólo se podrán utilizar para las finalidades que el afectado conoce y para las que ha dado consentimiento, y no se podrán utilizar con finalidades distintas a las que se informó en el momento de la recogida.

EJEMPLO

Cuando un trabajador se incorpora a una empresa para iniciar una relación laboral, éste debe suministrar sus datos personales.

La empresa sólo puede utilizar dichos datos personales para el mantenimiento de la relación laboral que los une (elaborar las nóminas, seguros sociales, control de asistencia, etc.).

Esa empresa no puede utilizar los datos de ese trabajador para ninguna otra finalidad.

7.2.3 Actualización de los datos

Los datos de carácter personal serán exactos y puestos al día, de forma que respondan con veracidad a la situación actual del afectado.

Si los datos de carácter personal resultan ser inexactos o incompletos, serán puestos al día de oficio en el plazo de 10 días desde el conocimiento de la inexactitud.

Si los datos han sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de 10 días, la rectificación o cancelación efectuada.

Es decir, se deberá propagar dicha rectificación o cancelación hacia toda la cadena de cesionarios, de forma que todos dispongan de la información para tener los datos exactos y puestos al día.

7.2.4 Almacenamiento

Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

Los datos personales deben estar organizados de forma que permitan ágil y diligentemente el acceso a los datos personales de un individuo en concreto, para ponerlos a su disposición en caso de que ejercite su derecho de acceso.

7.2.5 Cancelación

Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada.

7.2.6 Tratamiento con fines estadísticos, históricos o científicos

No se considerará finalidad incompatible el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos.

Para la determinación de estos fines se deberá acudir a la legislación que resulte aplicable en cada caso, y en particular:

1. La Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública.
2. La Ley 16/1985, de 25 de junio, del Patrimonio histórico español.
3. La Ley 13/1986, de 14 de abril, de Fomento y coordinación general de la investigación científica y técnica.
4. Así como a sus respectivas disposiciones de desarrollo.
5. La normativa autonómica en estas materias.

7.2.7 Conclusiones

Con relación al principio de calidad en el tratamiento de datos personales, debemos observar lo siguiente:

1. **Adecuación a la finalidad:** sólo se podrán tratar datos personales que sean adecuados, pertinentes y no excesivos para las finalidades determinadas, legítimas y explícitas para las que se hayan obtenido.
2. **Finalidad exclusiva:** los datos recogidos no se podrán utilizar con finalidades distintas a las que se informó en la recogida.
3. **Fecha de caducidad:** los datos recogidos serán cancelados cuando ya no sean necesarios para la finalidad que se recogieron.
4. **Exactitud:** los datos recogidos deberán ser en todo momento exactos, actuales y completos. El responsable del fichero o tratamiento deberá velar para que esto sea así.

5. **Propagación:** las rectificaciones efectuadas en los datos para que éstos resulten ser exactos, actuales y completos deberán propagarse hacia todas las entidades a las que previamente se hubieran comunicado esos datos.

7.3 DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS

Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

1. De la existencia de un fichero o tratamiento de datos de carácter personal al cual se van a incorporar o tratar los datos que suministre.

2. De la identidad y dirección del responsable del fichero o tratamiento o, en su caso, de su representante.

3. De cuál es la finalidad de los datos recogidos.

4. De los destinatarios de la información.

5. Del carácter obligatorio o voluntario de aportar los datos solicitados.

6. De las consecuencias de la obtención de los datos o de la negativa a proporcionarlos.

7. De la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

Esta información debe ser aportada por el responsable del fichero o tratamiento *la primera vez que se recaben datos*, y no será necesario hacerlo posteriormente, siempre y cuando no haya modificaciones en algunos de los aspectos de la información, como la dirección del responsable, la finalidad, los destinatarios de la información, etc.

Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de los datos medios situados en territorio español, deberá designar un representante en España.

Los atributos que debe tener la información proporcionada para que sea conforme con este principio son: previo, expreso, preciso e inequívoco.

1. **Previo:** la información debe ser proporcionada antes de que el interesado entregue sus datos personales. Si se le informa posteriormente, no es válido y se está incumpliendo (salvo en los casos que la información no se recabe del propio interesado, como veremos más adelante).
2. **Expreso:** se detallan todos los aspectos que debe recoger la información —responsable del fichero, finalidad, destinatarios, obligatoriedad, consecuencias, derechos— y son claramente interpretables por el interesado.
3. **Preciso:** el mensaje debe ser conciso, no más extenso de lo necesario y que no dificulte el entendimiento del mensaje por el interesado.
4. **Inequívoco:** la percepción de la información recibida por el interesado no debe dar lugar a error o a dobles interpretaciones.

7.3.1 Recogida del propio interesado

Cuando los datos procedan del propio interesado y se utilicen *cuestionarios u otros impresos* para la recogida de los datos, figurarán en los mismos, en forma claramente legible, las advertencias legales referidas antes.

EJEMPLO CLÁUSULA MODELO QUE SE DEBE INCORPORAR EN LA RECOGIDA DE DATOS

De acuerdo con lo establecido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos de que los datos aportados serán incluidos en un fichero del que es titular *(razón social del responsable del fichero)* y pueden ser utilizados con la finalidad de (*indicar para qué se utilizarán los datos*). Así mismo, podrán ser comunicados a (*indicar empresas o categorías de empresas, su actividad y la finalidad de la comunicación*). Le informamos también sobre sus derechos de acceso, rectificación, cancelación y oposición, que podrá ejercer en el domicilio social de (*razón social del responsable del fichero*), sito en (*domicilio social del responsable del fichero*).

7.3.1.1 EXCEPCIONES EN LA INFORMACIÓN PROPORCIONADA

Cuando la naturaleza de los datos personales que se solicitan o las circunstancias en las cuales se recaban dichos datos permitan deducir claramente:

- El carácter obligatorio o voluntario de aportar los datos solicitados.
- Las consecuencias de la obtención de los datos o de la negativa a proporcionarlos.
- La posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

No será necesario incluir esa información concreta en la recogida de datos, aunque sí el resto de la información descrita anteriormente.

7.3.2 Datos procedentes de fuentes accesibles al público

Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, ***en cada comunicación que se dirija al interesado*** se le informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.

A tal efecto, el interesado deberá ser informado de que sus datos han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos, *en todas y cada una de las comunicaciones* que se le dirijan.

7.3.3 Datos procedentes de otra entidad

Cuando los datos de carácter personal no hayan sido recabados del propio interesado sino que procedan de otra entidad, el afectado deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero *dentro de los tres meses siguientes* al momento de registro de los datos de:

1. Contenido del tratamiento.
2. Procedencia de los datos.
3. Existencia de un fichero o tratamiento de datos de carácter personal al cual se van a incorporar o tratar los datos que suministre.
4. Identidad y dirección del responsable del fichero o tratamiento o, en su caso, de su representante.
5. Cuál es la finalidad de los datos recabados.

6. Los destinatarios de la información.

7. La posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

Este supuesto es de aplicación, por ejemplo, cuando una empresa efectúa una comunicación de datos personales a otra empresa que se adhiere al grupo de empresas existente.

Hemos de tener en cuenta que si ya hemos informado con anterioridad al titular de los datos de todos los puntos anteriores —por ejemplo, en la propia recogida o mandando una comunicación a tal efecto—, no es necesario hacerlo al registrar sus datos.

7.3.4 Excepciones al deber de información

En cuanto al deber de información, con respecto a datos de carácter personal ***que no han sido recabados del propio interesado***, no será necesario realizarlo:

1. Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad y prospección comercial. En este caso, se informará en cada una de las comunicaciones dirigidas al interesado.

2. Cuando los datos procedan de otra entidad y el afectado ya ha sido informado con anterioridad, no será necesario informarle de nuevo.

3. Cuando lo prevea expresamente una ley.

4. Cuando el tratamiento tenga fines históricos, estadísticos o científicos.

5. Cuando esa información al interesado resulte imposible o exija esfuerzos desproporcionados, según el criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

7.3.5 Supuestos especiales

En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global

de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza contemplada por la normativa mercantil no se producirá cesión de datos.

Aun en este supuesto, permanece el deber de informar al interesado según lo expuesto en el desarrollo de este principio.

7.3.6 Conclusiones

Con relación al principio de información en la recogida de los datos personales, debemos observar lo siguiente:

- **Si los datos proceden del propio afectado:** incluir las cláusulas informativas en los formularios de recogida.
- **Si los datos proceden de fuentes accesibles al público y se destinan a la actividad de publicidad o prospección comercial:** informar al afectado en cada comunicación que se le dirija.
- **Si los datos proceden de otra entidad:** informar al afectado dentro de los tres meses siguientes.

7.4 CONSENTIMIENTO DEL AFECTADO

Para tratar datos de carácter personal no basta con haber informado al afectado en los términos contenidos en el principio de información al interesado que ya se ha detallado. Es preciso, además, *contar con su consentimiento inequívoco* para poder efectuar dicho tratamiento.

El principio del consentimiento está íntimamente ligado al de información, ya que sólo cuando el interesado sea informado de los detalles del tratamiento (finalidad, responsable, cesiones, etc.) podrá decidir libremente si otorga su consentimiento al tratamiento de sus datos.

Los cuatro atributos del consentimiento para que sea válido son:

- **Libre:** obtenido sin que exista ningún vicio del consentimiento en los términos regulados por el Código Civil.
- **Específico:** referido a una operación concreta del tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento.
- **Informado:** que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que se lleva a cabo (principio de información al interesado).
- **Inequívoco:** es preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento (consentimiento expreso o tácito).

7.4.1 Norma general

Los datos de carácter personal únicamente podrán ser objeto de *tratamiento o cesión* si el interesado hubiera *prestado previamente su consentimiento* para ello.

La solicitud del consentimiento *deberá ir referida a un tratamiento* o serie de tratamientos concretos, *con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran* (responsable, cesiones previstas, etc.).

7.4.2 Excepciones

No obstante, será posible el tratamiento o cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:

- Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los siguientes supuestos:
  - El tratamiento tenga por objeto satisfacer un interés legítimo del responsable del tratamiento amparado por dichas normas.
  - El tratamiento sea necesario para que el responsable de éste cumpla un deber que le impongan dichas normas.

- Los datos objeto del tratamiento o cesión *figuren en fuentes accesibles al público* y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades del interesado.
- Se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias.
- *Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.*
- El tratamiento de los datos tenga por finalidad satisfacer un interés vital del interesado (concretado en los términos del apartado 6 del artículo 7 de la LOPD).

Y siempre que no se vulneren los derechos y libertades fundamentales del interesado.

En los casos que no sea necesario, el consentimiento del afectado para el tratamiento de los datos personales —y siempre que una ley no disponga de lo contrario— podrá revertirse cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En este caso, el responsable del tratamiento excluirá los datos relativos al afectado.

7.4.3 Forma de recabar el consentimiento

El consentimiento de los afectados para el tratamiento de sus datos personales podrá recabarse de forma expresa o tácita.

7.4.3.1 CONSENTIMIENTO EXPRESO

Es el otorgado a través de una acción específica del interesado, como una firma o el marcado de una casilla en un formulario.

El *consentimiento expreso y por escrito* de los afectados es imprescindible[10] para el tratamiento de los datos de carácter personal que revelen la ideología,

10 Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin prejuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

afiliación sindical, religión y creencias. Además, se debe advertir al afectado de su derecho a no prestar dicho consentimiento.

Al tratar datos especialmente protegidos de salud, vida sexual u origen racial, el consentimiento debe ser *expreso*, aunque no necesariamente por escrito.

7.4.3.2 CONSENTIMIENTO TÁCITO

El consentimiento tácito es el que se entiende concedido por parte del interesado aun sin haber realizado un acto concreto de asentimiento ante el responsable del fichero; basta con que teniendo la oportunidad de oponerse al tratamiento de sus datos, no lo haga.

7.4.3.2.1 Método para recabar el consentimiento tácito

El responsable podrá dirigirse al afectado, informándole en los términos previstos por el principio de información y *deberá concederle un plazo de 30 días para manifestar su negativa* al tratamiento, advirtiéndole que en caso de no producirse a tal efecto se entenderá que consiente el tratamiento de sus datos personales.

Cuando se trate de responsables que presten al afectado un servicio que genere información o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o facturación del servicio prestado, siempre que se realice de forma claramente visible.

7.4.3.2.2 Seguimiento

Será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

Si hacemos un envío a un conjunto de interesados para obtener su consentimiento tácito y algunos de esos envíos son devueltos, los datos personales referidos a tales envíos devueltos deberán ser excluidos del tratamiento, ya que si no han podido ser informados, difícilmente podrán otorgar algún tipo de consentimiento.

7.4.3.2.3 Manifestar la negativa al tratamiento

Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos.

Se podrán utilizar, entre otros, los siguientes métodos:

- Envío prefranqueado al responsable del tratamiento.
- Llamada a un número de teléfono gratuito.
- Llamada a los servicios de atención al público ya establecidos.

7.4.4 Consentimiento para la cesión de datos

Cuando se solicite consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la *finalidad a la que se destinarán los datos* respecto de cuya comunicación se solicita el consentimiento y el tipo de *actividad desarrollada por el cesionario* (que es el destinatario de los datos).

En caso contrario, el consentimiento será nulo.

7.4.4.1 EXCEPCIONES

Será posible la cesión de datos de carácter personal sin el consentimiento del interesado cuando:

- La cesión esté autorizada por una norma con rango de ley.
- Cuando se trate de datos recogidos de fuentes accesibles al público.
- La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de datos. En este caso, la cesión sólo será legítima en cuanto se limite a la finalidad que la justifique.
- La comunicación que deba efectuarse tenga por destinatario:
  - El Defensor del Pueblo.
  - El Ministerio Fiscal o los Jueces o Tribunales.
  - El Tribunal de Cuentas.
  - Las instituciones autonómicas con funciones análogas.

  Y se realice en el ámbito de las funciones que la ley les atribuya expresamente.
- La cesión entre Administraciones Públicas cuando concurra uno de los siguientes supuestos:

- Tenga por objeto el tratamiento con fines históricos, estadísticos o científicos.
- Los datos de carácter personal hayan sido elaborados por una Administración Pública con destino a otra.
- La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

- La cesión de datos personales sobre la salud entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas.

7.4.4.2 ACREDITACIÓN DEL CONSENTIMIENTO

Corresponde al responsable del tratamiento acreditar la existencia de consentimiento del afectado —ya sea expreso o tácito— por cualquier medio de prueba admisible en derecho.

7.4.4.2.1 Acreditación del consentimiento expreso

El responsable del fichero deberá conservar el soporte en el que conste el consentimiento otorgado por el afectado.

7.4.4.2.2 Acreditación del consentimiento tácito

Aquí surge un problema: por un lado, el responsable del fichero tiene que probar que las cartas llegaron a su destino; por otro, los afectados pueden asegurar que nunca recibieron el envío.

No se puede confiar algo tan delicado a la buena fe de los interesados.

Existen varias soluciones para garantizar la prueba del envío:

- Obtener un *acta de manifestación notarial* que de fe del envío de las cartas a los destinatarios, incluyendo la relación de destinatarios.

- *Subcontratar un servicio de mailing* que *incluya el reparto* del envío y el *control de las devoluciones*, las cuales deberán ser recogidas y devueltas al responsable del fichero para que no las considere como consentimientos tácitos obtenidos de los interesados y proceda a excluirlos del tratamiento. La empresa contratada deberá proporcionar un certificado con los envíos

realizados y las devoluciones que se han producido, de forma que se pueda utilizar como prueba ante una posible reclamación.

7.4.5 Revocación del consentimiento

El consentimiento otorgado para el tratamiento de los datos de carácter personal de una persona podrá ser revocado cuando exista una causa justificada para ello y no se le atribuyan efectos retroactivos.

Deberá poder hacerlo a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento.

Se podrán utilizar, entre otros, los siguientes métodos:

- Envío prefranqueado al responsable del tratamiento.
- Llamada a un número de teléfono gratuito.
- Llamada a los servicios de atención al público ya establecidos.

En cambio, no se considerarán conformes los siguientes supuestos:

- Envío de cartas certificadas o semejantes.
- Servicios de telecomunicaciones que impliquen una tarificación adicional al afectado.
- Cualquier otro medio que implique un coste adicional al interesado.

7.4.5.1 PLAZO

El responsable cesará en el tratamiento de los datos en el plazo de 10 días a contar desde la recepción de la revocación del consentimiento, sin prejuicio de bloquear los datos conforme a lo dispuesto en el artículo 16.3[11] de la LOPD.

11 *Artículo 16.3 de la LOPD.* La cancelación dará lugar al bloqueo de los datos, conservándolos únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido dicho plazo, deberá procederse a la supresión.

7.4.5.2 CONFIRMACIÓN

Además, si el interesado ha solicitado al responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a su solicitud.

7.4.5.3 REVOCACIÓN PARA DATOS CEDIDOS PREVIAMENTE

Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios en el plazo de 10 días para que éstos cesen en el tratamiento de los datos (en caso de que aún lo mantengan).

7.4.6 Tratamiento de datos de menores de edad

Para poder tratar datos personales de menores de catorce años se requerirá el consentimiento de los padres.

Además, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible para ellos.

7.4.6.1 LIMITACIONES

En ningún caso podrán recabarse de los menores datos que permitan obtener información sobre los demás miembros del grupo familiar o sobre las características del mismo, como:

- Datos relativos a la actividad profesional de los progenitores.
- Información económica.
- Datos sociológicos.
- O cualquier otro dato.

Sin el consentimiento de los titulares de tales datos.

Sin embargo, podrán recogerse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización necesaria para tratar los datos de ese menor.

7.4.6.2 COMPROBACIÓN DE LA EDAD

Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo:

- La edad del menor.
- La autenticidad del consentimiento prestado por los padres, tutores o representantes.

7.4.7 Consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma

Si el responsable del tratamiento solicita el consentimiento del afectado *durante el proceso de formación de un contrato* para finalidades que no guardan relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir que el afectado manifieste expresamente su negativa al tratamiento o cesión de datos.

En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible *y que no se encuentre ya marcada* en el documento que se entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa.

EJEMPLO

Si en un contrato para suministrar un servicio a un interesado pedimos su consentimiento para enviarle información sobre los otros productos, debemos permitir que el interesado se oponga, colocando una casilla así:

[ ] Si no desea permitir el tratamiento de sus datos conforme a la finalidad indicada, marque esta casilla.

7.4.8 Conclusiones

Con relación al principio de consentimiento en el tratamiento de los datos personales, debemos observar lo siguiente:

1. **Obtener el consentimiento del afectado.** Como norma general, siempre se debe obtener el consentimiento, salvo las excepciones previstas.

2. **Consentimiento revocable.** El interesado podrá revocar el consentimiento, que deberá hacerse efectivo en 10 días.

3. **Propagación de la revocación.** En el caso de que los datos hayan sido cedidos a terceros y el interesado revoque el consentimiento otorgado, el responsable del tratamiento deberá informar a los cesionarios en un máximo de 10 días para que éstos, a su vez, cesen en el tratamiento de los datos.

7.5 DATOS ESPECIALMENTE PROTEGIDOS

Son datos especialmente protegidos los que revelan información que puede ser comprometida para el individuo al que se refieren. En el tratamiento de estos datos se extreman las cautelas que se deben tener en cuenta, tanto en la recogida como posteriormente en el tratamiento y la cesión.

Recordemos que son datos especialmente protegidos los siguientes:

- Ideología.
- Afiliación sindical.
- Religión.
- Creencias.
- Origen racial.
- Salud.
- Vida sexual.

7.5.1 Recogida, tratamiento y cesión de datos especialmente protegidos

Para *recabar, tratar* y *comunicar* datos de carácter personal que revelen la *ideología, afiliación sindical, religión* o *creencias* es preciso recabar el *consentimiento expreso y por escrito*.

Cuando en relación con estos datos se proceda a recabar el consentimiento del interesado, se le *advertirá de su derecho a no prestarlo.*

7.5.1.1 EXCEPCIONES

Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros.

Aun en este caso, la *cesión* de dichos datos *precisará siempre* el *previo consentimiento* del afectado.

7.5.1.2 ORIGEN RACIAL, SALUD Y VIDA SEXUAL

Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando:

- Por razones de interés general así lo disponga una ley.
- El afectado consienta expresamente.

7.5.2 Tratamiento de datos especialmente protegidos sin consentimiento

Podrán ser objeto de tratamiento los datos especialmente protegidos cuando resulte necesario para:

- Prevención o diagnóstico médico.
- Prestación de asistencia sanitaria o tratamientos médicos.
- Gestión de servicios sanitarios.

Y siempre que dicho tratamiento se realice por:

- Un profesional sanitario sujeto a secreto profesional.
- Otra persona sujeta a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos especialmente protegidos cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

7.5.3 Ficheros prohibidos

Quedan prohibidos los ficheros creados con la *finalidad exclusiva* de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

7.5.4 Conclusiones

La recogida, tratamiento y cesión de datos especialmente protegidos debe realizarse cumpliendo escrupulosamente la ley, ya que las infracciones en este principio son catalogadas como «muy graves», con sanciones desde 300.001 a 600.000 euros.

Como norma general, es necesario recabar el:

- Consentimiento *expreso y por escrito* para datos de:
  - Ideología.
  - Afiliación sindical.
  - Religión.
  - Creencias.
- Consentimiento *expreso* para datos de:
  - Origen racial.
  - Salud.
  - Vida sexual.

7.6 DATOS RELATIVOS A LA SALUD

Las instituciones, los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Es decir, cuando acudimos a un centro sanitario por motivos de salud, ya estamos autorizando que se traten nuestros datos personales relativos a la salud.

7.6.1 Cesión de datos relativos a la salud

Los datos de carácter personal relativos a la salud sólo podrán ser cedidos en alguno de los siguientes supuestos:

- El afectado consienta expresamente la cesión.
- La cesión esté autorizada por una ley.
- Cuando la cesión sea necesaria para solucionar una urgencia que requiera acceder a un fichero.
- Para realizar estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

No será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas.

7.7 SEGURIDAD DE LOS DATOS

Otra de las obligaciones más importantes que tiene el responsable del fichero o tratamiento, además de informar en la recogida y de obtener el consentimiento de los afectados, es la de *proteger los datos personales que recoge, trata y/o almacena.*

Los riesgos a que están expuestos los ficheros pueden venir tanto de la acción humana como de circunstancias naturales o de accidentes fortuitos.

Resulta necesario que el responsable del fichero adopte las medidas adecuadas y necesarias para garantizar la protección de los datos de carácter personal para evitar su destrucción, pérdida, alteración, difusión o acceso no autorizado.

Por tanto, 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.

Es decir, no serán las mismas medidas de seguridad las que deberán implantarse para el tratamiento de datos meramente identificativos que para el tratamiento de datos especialmente protegidos. *El tratamiento de datos más comprometidos requiere de más medidas de seguridad.*

En un capítulo posterior, referido a las medidas de seguridad que es necesario implantar, se detallan las mismas.

7.7.1 Ficheros que no reúnan las condiciones de seguridad

No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones requeridas con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

7.7.2 Conclusiones

Quizás la aplicación y cumplimiento de las medidas de seguridad que deban implantarse en función de los datos tratados sea la labor más ardua de la protección de datos, ya que requiere disciplina y continuidad en el tiempo. Sin embargo, es esencial para garantizar la seguridad de los datos frente a acciones humanas o accidentes fortuitos o sucesos naturales.

Muchas entidades cumplen fielmente el registro de ficheros, los principios básicos de información, consentimiento, calidad, etc., y sin embargo, fallan escandalosamente en la implementación de las medidas de seguridad requeridas.

Hay que tener en cuenta que la *no adopción de las medidas de seguridad* requeridas por los datos que se van a tratar se considera infracción grave, con sanciones que van de 40.001 a 300.000 euros.

7.8 DEBER DE SECRETO

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos. Dichas obligaciones subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

La obligación de secreto incumbe a cualquier persona que haya intervenido en cualquier fase del tratamiento: recogida, grabación, actualización, bloqueo,

cancelación o cesión. Así mismo, es aplicable tanto al personal del responsable del fichero como al del encargado del tratamiento.

La obligación de secreto subsiste aun después de concluida la relación con el responsable del fichero o el encargado del tratamiento.

Además del secreto, tiene el deber de guardar los datos que se encuentren bajo su custodia, de forma que no tengan acceso a dichos datos personas no autorizadas.

Vulnerar el deber de secreto puede constituir una infracción leve, grave o muy grave, en función de la naturaleza de los datos revelados, y conlleva una *responsabilidad personal* para quien lo infrinja.

7.8.1 Conclusiones

Para garantizar la no difusión de los datos de carácter personal que se tratan es fundamental que el personal implicado en dicho tratamiento, así como el que pueda tener acceso a dichos datos, cumpla los siguientes deberes:

- Secreto respecto a los mismos.
- Guardar los datos que se encuentren bajo su custodia, de forma que no pueda acceder a los mismos el personal no autorizado.

7.9 COMUNICACIÓN DE DATOS

Según la LOPD, **cesión o comunicación de datos es cualquier** tratamiento de datos que supone su revelación a una persona distinta del interesado.

Es decir, *cualquier revelación de datos* de carácter personal *efectuada a una persona distinta del interesado* se considera una cesión o comunicación de datos.

7.9.1 Norma general

Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el *previo consentimiento* del interesado.

Es decir, poner a disposición los datos personales que estamos tratando a un tercero sólo podrá efectuarse cuando confluyan conjuntamente los dos requisitos establecidos por la LOPD:

- Que sea para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.
- Que se obtenga el previo consentimiento del interesado.

7.9.1.1 CÓMO OBTENER EL CONSENTIMIENTO DEL INTERESADO PARA LEGITIMAR LA CESIÓN DE DATOS ENTRE EMPRESAS

Hay dos maneras de recabar el consentimiento del interesado para poder efectuar la cesión de sus datos a otra entidad:

7.9.1.2 OBTENER EL CONSENTIMIENTO EN LA RECOGIDA DE LOS DATOS PERSONALES DEL INTERESADO

Uno de los aspectos que debemos informar al interesado en la recogida de sus datos personales es la finalidad de la recogida y los *destinatarios de la información*.

Dentro de este apartado se debe detallar la actividad que desarrollan dichos destinatarios y la finalidad a la que se destinarán los datos cedidos.

Si sobre dicha información se ha obtenido el consentimiento, el interesado también lo ha otorgado para que sus datos puedan ser cedidos a los destinatarios relacionados en dicha información y para la finalidad declarada en la cláusula.

7.9.1.3 OBTENER EL CONSENTIMIENTO POSTERIORMENTE

Si posteriormente a la recogida de los datos personales del interesado surge la necesidad de efectuar una cesión a un tercero, será preciso recabar previamente su consentimiento, informándole concretamente de:

- La finalidad a la que se destinarán los datos cuya comunicación se autoriza.
- El tipo de actividad de aquel a quien se pretenden comunicar.

7.9.2 Excepciones

El consentimiento exigido para la cesión de datos no será preciso cuando:

- Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los siguientes supuestos:
  - El tratamiento tenga por objeto satisfacer un interés legítimo del responsable del tratamiento amparado por dichas normas.
  - El tratamiento sea necesario para que el responsable del mismo cumpla un deber que le impongan dichas normas.

- Los datos objeto del tratamiento o cesión *figuren en fuentes accesibles al público* y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades del interesado.

- La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso, la cesión sólo será legítima en cuanto se limite a la finalidad que la justifique.

- La comunicación que deba efectuarse tenga por destinatario:
  - El Defensor del Pueblo.
  - El Ministerio Fiscal o los Jueces o Tribunales.
  - El Tribunal de Cuentas.
  - Las instituciones autonómicas con funciones análogas.

  Y se realice en el ámbito de las funciones que la ley les atribuya expresamente.

- La cesión entre Administraciones Públicas cuando concurra uno de los siguientes supuestos:
  - Tenga por objeto el tratamiento con fines históricos, estadísticos o científicos.
  - Los datos de carácter personal hayan sido elaborados por una Administración Pública con destino a otra.
  - La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

- La cesión de datos de carácter personal relativos a la salud sea necesaria para:
  - Resolver una urgencia que requiera acceder a un fichero.
  - Realizar estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.
- La cesión de datos personales sobre la salud entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas.

7.9.3 Informar adecuadamente

Cuando obtengamos el consentimiento para efectuar la cesión de datos, debemos tener en cuenta informar claramente al interesado de la *finalidad* a la que se destinarán los datos cuya comunicación se autoriza y el *tipo de actividad* de aquel a quien se pretenden comunicar.

Si la información que se ha facilitado al interesado *no permite conocer estos datos*, el consentimiento recabado para la cesión o comunicación de los datos de carácter personal *será nulo*. Dicha cesión será considerada *no consentida*, estimada como infracción muy grave, con una sanción de hasta 600.000 euros.

7.9.4 Consentimiento revocable

El consentimiento para la comunicación de datos de carácter personal tiene también carácter revocable, pudiendo ejercerlo el interesado en cualquier momento.

7.9.5 Comunicación de la cesión de datos

El responsable del fichero, *en el momento en que se efectúe la primera cesión de datos*, deberá informar de ello a los afectados, indicando así mismo la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

Esta norma se aplica a los ficheros de titularidad privada *en aquellos casos en los que es obligatorio recabar previamente el consentimiento del interesado para poder efectuar la cesión de los datos.* También se aplica cuando se cedan datos recogidos de fuentes accesibles al público y en caso de urgencias médicas o estudios epidemiológicos.

7.9.6 Obligaciones del receptor de la comunicación de datos

Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a cumplir las disposiciones de la LOPD.

Es decir, tienen a su vez que legalizar los ficheros, legitimar el tratamiento y proteger los datos. Desde ese momento es responsable del fichero o tratamiento.

Además, debe informar a los titulares de los datos, *dentro de los tres meses siguientes* al momento de registro de los datos —a no ser que lo hubiese hecho antes—, de lo siguiente:

- Del contenido del tratamiento.
- De la procedencia de los datos.
- De la existencia de un fichero o tratamiento de datos de carácter personal al cual se van a incorporar o tratar los datos que suministre.
- De la identidad y dirección del responsable del fichero o tratamiento o, en su caso, de su representante.
- De cuál es la finalidad de los datos recabados.
- De los destinatarios de la información.
- De la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

7.9.7 Conclusiones

Este principio de la LOPD es uno de los más delicados, ya que, precisamente, entre los *objetivos principales* de la LOPD está *evitar el tráfico indiscriminado de datos personales*, y garantizar el derecho que tienen los interesados a conocer quién está tratando sus datos y con qué finalidades.

Difícilmente podrán los interesados ejercer sus derechos sobre los datos personales si no tienen conocimiento de las entidades que los tratan y almacenan ni del uso que van a dar a dichos datos.

En general —y salvo las excepciones recogidas—, para poder tratar y comunicar datos de carácter personal a otras entidades —aunque sean empresas del mismo grupo—, respetando todas las obligaciones que impone la LOPD, se debe realizar de la siguiente forma:

1. Informar al interesado en la recogida de los datos personales.
2. Obtener su consentimiento para el tratamiento de los datos.

3. Recabar su consentimiento para la cesión de dichos datos.
4. Informar al afectado que dicha cesión se ha producido (una vez producida, claro está).

Las *sanciones* impuestas por el incumplimiento de este principio son las *más duras*, llegando hasta los 600.000 euros. Debemos ser sumamente cautelosos y tener especial cuidado a la hora de efectuar una cesión de datos a otra entidad.

7.10 ACCESO A LOS DATOS POR CUENTA DE TERCEROS

No se considerará comunicación de datos el acceso de un tercero a los mismos cuando sea necesario para la prestación de un servicio al responsable del tratamiento.

Es decir, la asesoría que realiza las nóminas del personal del responsable del fichero necesita para ello disponer de los datos personales de los trabajadores. Esa comunicación de datos —con objeto de cumplir dicho encargo— no sería considerada una cesión de datos, sino un encargo de tratamiento.

7.10.1 Regulación de la figura del encargado del tratamiento

Según la LOPD, el encargado del tratamiento es la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato, que deberá constar por escrito, o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente:

- Que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.
- Que no los aplicará o utilizará con fin distinto al que figure en dicho contrato.
- Que no los comunicará, ni siquiera para su conservación, a otras personas.
- Las medidas de seguridad que el encargado del tratamiento está obligado a implantar.

7.10.2 Fin de la relación contractual

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiera designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos.

7.10.3 Responsabilidad

En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato antes descrito, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

7.10.4 Conclusiones

El acceso a los datos por parte de un encargado del tratamiento no se considera cesión de datos, con lo cual no requiere el consentimiento previo del interesado, ni precisa que se le comunique la entidad que trata sus datos en concepto de encargado.

Eso sí, para que un acceso a los datos de carácter personal se considere un encargo de tratamiento, y no una cesión o comunicación de datos, se deberán cumplir los siguientes requisitos:

- Que se realice con objeto de prestar un servicio al responsable del fichero.
- Que se regule mediante un contrato que contenga los aspectos antes descritos.

Posteriormente profundizaremos en la figura del encargado del tratamiento.

8

EL ENCARGADO DEL TRATAMIENTO

«Vacía tu bolsillo en tu mente y tu mente llenará tu bolsillo».

Benjamin Franklin

8.1 EL ENCARGADO DEL TRATAMIENTO

El encargado del tratamiento es la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

El encargado del tratamiento es la persona o entidad que presta un servicio al responsable del fichero, servicio que para poder ser realizado necesita acceder a los datos de carácter personal registrados en uno o más ficheros del responsable del fichero.

El ejemplo más claro es la asesoría laboral que realiza las nóminas para la empresa. Para poder confeccionar las nóminas es imprescindible que la empresa le suministre los datos personales de los trabajadores. La asesoría es encargada del tratamiento para el fichero que almacena los datos de los trabajadores.

Cualquier entidad que tenga o pueda tener acceso a datos de carácter personal es encargada del tratamiento, debiendo cumplir una serie de obligaciones que describiremos más adelante.

Otros encargados del tratamiento, no tan claros como la asesoría pero igualmente importantes, pueden ser: la empresa que realiza el mantenimiento del *software* de gestión, o la empresa encargada de realizar un mailing a los clientes del responsable del fichero.

Ambas empresas, con objeto del desempeño de su servicio, tienen o pueden tener acceso a datos de carácter personal, siendo consideradas, igualmente, encargadas del tratamiento.

8.1.1 Formas de prestar el servicio

Hay distintas formas en que un encargado del tratamiento puede prestar el servicio al responsable del fichero:

- **Servicio prestado en los locales del responsable del fichero.** En este caso, el encargado del tratamiento se desplaza a los locales del responsable del fichero para efectuar el servicio. Por ejemplo, la empresa que realiza el mantenimiento *in situ* de la aplicación de gestión de la empresa.

- **Servicio prestado por acceso remoto.** En este caso, el servicio se realiza cuando de forma remota el encargado del tratamiento accede a los sistemas del responsable del fichero. Por ejemplo, un asesor externo que realiza las nóminas de los empleados vía remota utilizando la aplicación que está instalada en el sistema del responsable del fichero.

- **Servicio prestado en los locales propios del encargado del tratamiento.** En este caso, el servicio es prestado por el encargado en sus propios locales. Por ejemplo, la empresa que realiza el *mailing* a los clientes del responsable del fichero.

En cualquiera de estas formas, el responsable del fichero debe formalizar el contrato estipulado en el siguiente apartado con el encargado del tratamiento.

Todo acceso a los datos por el encargado del tratamiento deberá estar sometido a las medidas de seguridad correspondientes en función de los datos tratados y los riesgos a los que estén expuestos.

8.2 EL RESPONSABLE DEL FICHERO Y EL ENCARGADO DEL TRATAMIENTO

El acceso a los datos de carácter personal contenidos en un fichero por una entidad ajena al titular del fichero es una «brecha» en la seguridad de los datos.

Imaginemos que encargamos a una empresa externa la realización de un *mailing*. Para ello, le proporcionamos la base de datos de nuestros clientes, a quienes debe llegar la información que queremos enviar.

La empresa encargada de hacer el *mailing* «aprovecha» la ocasión para «copiar» la base de datos, y luego la vende a otras empresas, que, por ejemplo, envían publicidad a esas personas.

Los titulares de esos datos personales han dado consentimiento a la primera empresa para que trate sus datos, sin embargo, la realidad es que sus datos terminan siendo tratados en varias entidades, que ni siquiera conocen, y para cuyo tratamiento no han dado consentimiento, desconociendo la finalidad para la que van a ser utilizados los datos que proporcionaron a la primera empresa.

La consecuencia de esta situación es que andan circulando libremente entre empresas datos de carácter personal; además, los afectados no saben ni qué empresas están tratando sus datos ni para qué los están utilizando.

Pero lo más importante es que si no hemos formalizado un contrato con la empresa de *mailing* inicial, compartiremos responsabilidad con ella en la infracción ocasionada.

Cuando contratamos un servicio con una empresa externa, no pensamos que esta empresa va a utilizar los datos que le proporcionamos con otra finalidad que no sea el cumplimiento del encargo acordado. Pero, a veces, la realidad es otra.

Con objeto de evitar que los datos se utilicen con una finalidad distinta a la acordada, o puedan ser objeto de cesión no consentida a terceros, se establece la obligación de formalizar un contrato entre el responsable del fichero y el encargado del tratamiento.

En el contrato, que se deberá celebrar por escrito, o en alguna otra forma que permita acreditar su celebración, deberá establecerse expresamente:

- Que el encargado del tratamiento:
  - Sólo tratará los datos conforme a las instrucciones del responsable del fichero.

- No los aplicará ni utilizará con fin distinto al que figure en dicho contrato.
- No los comunicará, ni siquiera para su conservación, a otras personas.

- Las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

Este contrato debe formalizarse con todas y cada una de las entidades que tengan o puedan tener acceso a los datos de carácter personal incluidos en los ficheros del responsable.

Asimismo, el *responsable* del fichero *deberá velar por que el encargado del tratamiento reúna las garantías* para el cumplimiento de las medidas de seguridad exigibles en función de los datos tratados.

En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato formalizado, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

8.2.1 Obligaciones

Cada una de las partes implicadas —responsable del fichero y encargado del tratamiento— deben cumplir una serie de obligaciones en relación con el tratamiento de los datos personales.

El responsable del fichero debe cumplir las siguientes obligaciones:

- Inscribir los ficheros en el RGPD.
- Deber de información en la recogida de los datos personales.
- Obtener el consentimiento del afectado para el tratamiento.
- Atender los derechos de ARCO de los afectados.

Por otra parte, el encargado del tratamiento ***comparte***, a su vez, con el responsable del fichero las siguientes obligaciones:

- Adoptar las medidas de seguridad necesarias para garantizar la seguridad de los datos personales que trata.
- Deber de secreto profesional con respecto a los datos personales que trata.

8.3 PRESTACIONES DE SERVICIOS SIN ACCESO A DATOS PERSONALES

Cuando a los locales o sistemas del responsable del fichero accedan otras entidades con motivo de prestar un servicio que no implica el acceso a datos personales, también dicho servicio deberá quedar regulado por un contrato de prestación de servicios.

El contrato de prestación de servicios deberá recoger expresamente:

- La prohibición de acceder a los datos personales.
- La obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

El ejemplo más claro son los servicios de limpieza contratados y que son externos a la entidad responsable del fichero.

El personal de limpieza no tiene por qué manejar datos personales, pero puede conocer, de forma casual, datos personales de algún sujeto. De aquí la obligatoriedad de señalar en el contrato de prestación de servicios que se debe suscribir los extremos señalados anteriormente.

Este contrato no exime al responsable del fichero de su obligación de proteger los datos de carácter personal. Para ello deberá adoptar las medidas adecuadas que limiten el acceso a los datos personales, a los soportes que los contengan o a los recursos del sistema de información para la realización de trabajos que no impliquen el tratamiento de datos personales.

8.4 SUBCONTRATACIÓN DE SERVICIOS

El derecho básico de la normativa sobre protección de datos que el afectado disponga sobre la información que le concierne, y una vez que ha autorizado a un determinado responsable a que trate sus datos personales, supone que dicho responsable deberá conocer en cada momento qué terceras entidades acceden a dichos datos —siempre en su nombre—, a fin de garantizar al interesado que los datos de los que es titular no exceden del control de la entidad cuyo tratamiento ha sido aceptado por él.

Si hubiera posibilidad de subcontratar sucesivamente dicho tratamiento sin conocimiento del responsable, éste carecería de conocimiento para poder atender cualquier reclamación efectuada por los afectados, e incluso para conocer quién

accede en cada momento a los datos de carácter personal cuyo tratamiento ha sido consentido por el interesado.

El encargado del tratamiento no podrá subcontratar la realización de ningún tratamiento que le hubiera encomendado el responsable del fichero, salvo que hubiera obtenido de éste la autorización para hacerlo. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

Como mejor se entiende esto es con un ejemplo:

1. Una empresa contrata a un encargado del tratamiento para la realización de un encargo que implica el tratamiento de datos personales (por ejemplo, la asesoría que realiza la contabilidad, la fiscalidad y las nóminas). Deberá formalizar el correspondiente contrato con el encargado del tratamiento.

2. Esta empresa, a su vez, quiere subcontratar con otra la realización de este servicio (todo o parte); por ejemplo, quiere subcontratar con otra empresa la realización de las nóminas.

3. Antes de poder efectuar la subcontratación con la otra empresa, deberá pedir al responsable del tratamiento autorización para poder efectuar esta subcontrata. En caso de que el responsable del tratamiento acceda a dicha subcontratación, la misma se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

8.4.1 Excepciones

Será posible la subcontratación sin necesidad de autorización, siempre y cuando se cumplan los siguientes requisitos:

1. Que se especifiquen en el contrato los servicios que pueden ser objeto de subcontratación y, si fuera posible, la empresa con la que se vaya a subcontratar.

   Cuando en el contrato no aparece el nombre de la empresa con la que se vaya a subcontratar, el encargado del tratamiento deberá comunicar al responsable los datos que la identifiquen *antes* de proceder a la subcontratación.

2. Que el tratamiento de los datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

3. Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato de acceso a datos por cuenta de terceros descrito anteriormente.

   En este caso, el subcontratista será considerado encargado del tratamiento.

8.5 DESTINO DE LOS DATOS UNA VEZ FINALIZADA LA RELACIÓN CON EL ENCARGADO DEL TRATAMIENTO

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiera designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

El encargado del tratamiento tiene la obligación legal de devolver o destruir todos los datos de carácter personal que ha tratado una vez finalizada la relación con el responsable.

En el caso de que una previsión legal exija la conservación de los datos, éstos no deberán ser destruidos, sino devueltos al responsable del fichero para su conservación.

8.5.1 Conservación de los datos por el encargado del tratamiento

El encargado del tratamiento conservará debidamente bloqueados los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

Si el encargado del tratamiento necesita los datos de carácter personal que ha tratado para demostrar o probar algún tipo de responsabilidad en la relación con el responsable del tratamiento, podrá conservar los datos tratados, pero siempre debidamente bloqueados y sin hacer más uso de ellos.

9

LOS DERECHOS DE LOS AFECTADOS

«Para triunfar debes conocer lo que haces, debe gustarte lo que haces y debes creer en lo que haces».

Will Rogers

9.1 LOS DERECHOS ARCO

Los derechos de los afectados son: acceso, rectificación, cancelación y oposición (ARCO), que es preciso atender por la entidad en el adecuado plazo y forma.

Hay que tener especial cuidado y diligencia en la resolución satisfactoria del ejercicio de estos derechos, ya que de su omisión pueden derivarse cuantiosas sanciones.

El responsable del fichero deberá informar al personal que tiene acceso a datos de carácter personal del procedimiento que se debe seguir para facilitar a los interesados o afectados el ejercicio de sus derechos.

9.1.1 Quién puede solicitar los derechos ARCO

Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejecutados por el afectado.

Tales derechos se ejercitarán:

- Por el afectado, acreditando su identidad.
- Por su representante legal (acreditado), cuando el afectado se encuentre en situación de discapacidad o minoría de edad que le imposibilite para el ejercicio personal de estos derechos.
- Por un representante voluntario, expresamente designado para el ejercicio del derecho. En este caso, deberá constar claramente acreditada la identidad del representado, mediante DNI o documento equivalente, y la representación conferida por aquél.

Los derechos serán denegados cuando la solicitud sea formulada por una persona distinta del afectado y no se acredite que actúe en representación de aquél.

9.1.2 Condiciones para el ejercicio de los derechos

Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. El ejercicio de los derechos ARCO también será gratuito para el interesado.

No se considerarán conformes los supuestos siguientes:

- El envío de cartas certificadas o semejantes.
- La utilización de servicios de telecomunicaciones que impliquen tarificación adicional.
- Cualquier medio que implique un coste excesivo para el interesado.

9.1.3 Procedimiento

Deberá dirigirse una comunicación dirigida al responsable del fichero o tratamiento en la que conste:

- Nombre y apellidos del interesado.
- Fotocopia del DNI/NIF del interesado y, en su caso, de la persona que lo representa, así como el documento que acredita tal representación.
- Petición en que se concreta la solicitud.

- Por el afectado, acreditando su identidad.
- Por su representante legal (acreditado), cuando el afectado se encuentre en situación de discapacidad o minoría de edad que le imposibilite para el ejercicio personal de estos derechos.
- Por un representante voluntario, expresamente designado para el ejercicio del derecho. En este caso, deberá constar claramente acreditada la identidad del representado, mediante DNI o documento equivalente, y la representación conferida por aquél.

Los derechos serán denegados cuando la solicitud sea formulada por una persona distinta del afectado y no se acredite que actúe en representación de aquél.

9.1.2 Condiciones para el ejercicio de los derechos

Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. El ejercicio de los derechos ARCO también será gratuito para el interesado.

No se considerarán conformes los supuestos siguientes:

- El envío de cartas certificadas o semejantes.
- La utilización de servicios de telecomunicaciones que impliquen tarificación adicional.
- Cualquier medio que implique un coste excesivo para el interesado.

9.1.3 Procedimiento

Deberá dirigirse una comunicación dirigida al responsable del fichero o tratamiento en la que conste:

- Nombre y apellidos del interesado.
- Fotocopia del DNI/NIF del interesado y, en su caso, de la persona que lo representa, así como el documento que acredita tal representación.
- Petición en que se concreta la solicitud.

- Dirección a efectos de notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición que formula, en su caso.

El responsable del fichero o tratamiento *deberá contestar la solicitud* que se le dirija *en todo caso*, teniendo en cuenta que:

- Deberá responder incluso si no figuran los datos personales del afectado en sus ficheros.
- En caso de que la solicitud no reúna los requisitos, solicitar la subsanación de los mismos.
- Deberá guardar prueba del cumplimiento del deber, conservando la acreditación del mismo.
- Deberá adoptar las medidas oportunas para garantizar que el personal que tenga acceso a los datos pueda informar del procedimiento que debe seguir el afectado para el ejercicio de sus derechos.

En el supuesto de no contestar dentro de los plazos establecidos, o hacerlo de forma incompleta, el afectado podrá ponerlo en conocimiento de la AEPD, pudiendo abrir la misma un expediente sancionador y pudiendo derivarse del mismo una sanción.

9.1.4 Los derechos ante un encargado del tratamiento

Cuando los afectados ejerciten sus derechos ante un encargado del tratamiento, el encargado deberá trasladar la solicitud al responsable del fichero para que proceda a su resolución, salvo que en el contrato de encargo se haya pactado que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio de derechos de los afectados.

9.2 DERECHO DE ACCESO

El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como el origen de dichos datos y las cesiones previstas de los mismos.

9.2.1 Ejercicio del derecho de acceso

Al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:

- Visualización en pantalla.
- Escrito, copia o fotocopia remitida por correo, certificado o no.
- Telecopia.
- Correo electrónico u otros sistemas de comunicaciones electrónicas.
- Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento ofrecido por el responsable.

La información que se proporcione se dará de forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

9.2.2 Atención a la solicitud de acceso

El responsable del fichero o tratamiento resolverá la solicitud de acceso en el plazo *máximo* de *un mes desde la recepción* de la misma, teniendo en cuenta que el plazo cuenta de fecha a fecha.

En el caso de que no se dispongan de datos de carácter personal del afectado, deberá igualmente comunicarse esta circunstancia al mencionado afectado en el mismo plazo.

Transcurrido el plazo de diez días sin que de forma expresa se responda a la petición de acceso, el interesado podrá interponer una reclamación de tutela de sus derechos en la Agencia Española de Protección de Datos.

Si la solicitud es estimada, y el responsable del fichero o tratamiento no acompaña en su comunicación la información requerida, el acceso deberá hacerse efectivo durante los *diez días siguientes* a esa comunicación.

9.2.3 Denegación del acceso

El responsable del fichero o tratamiento podrá denegar el acceso en estos casos:

- Cuando la solicitud sea formulada por una persona distinta del afectado y no se acredita que actúa en representación de aquél.
- Cuando el derecho ya se ha ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.
- Cuando lo prevea una ley o una norma de derecho comunitario.

9.3 DERECHO DE RECTIFICACIÓN

El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

Este derecho está íntimamente ligado al principio de calidad de los datos; en concreto, al apartado que hace referencia a que los datos de carácter personal serán exactos y puestos al día, de forma que respondan con veracidad a la situación actual del afectado.

Por tanto, en el momento en que los datos del interesado sufran alguna variación, éste tiene derecho a que el responsable del fichero o tratamiento los sustituya por otros que respondan a su situación actual.

9.3.1 Ejercicio del derecho de rectificación

El afectado podrá ejercer el derecho de rectificación ante el responsable del fichero o tratamiento a través de la solicitud correspondiente, que deberá tener:

- Nombre y apellidos del interesado.
- Fotocopia del DNI/NIF del interesado y, en su caso, de la persona que lo representa, así como el documento que acredita tal representación.
- Petición en que se concreta la solicitud.
- Dirección a efectos de notificaciones, fecha y firma del solicitante.
- La corrección que se va a realizar.
- La documentación justificativa de lo solicitado.

9.3.2 Atención a la rectificación

El responsable del fichero o tratamiento resolverá la solicitud de acceso en el plazo *máximo de diez días desde la recepción* de la misma.

En el caso de que no se dispongan de datos de carácter personal del afectado, deberá igualmente comunicarse esta circunstancia al afectado en el mismo plazo.

Transcurrido el plazo de diez días sin que de forma expresa se responda a la petición de rectificación, el interesado podrá interponer una reclamación de tutela de sus derechos en la Agencia Española de Protección de Datos.

Si los datos rectificados hubieran sido cedidos previamente, el responsable del fichero o tratamiento deberá comunicar la rectificación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, así mismo, a rectificar los datos.

9.3.3 Denegación de la rectificación

El responsable del fichero o tratamiento podrá denegar el derecho de rectificación cuando:

- La solicitud sea formulada por una persona distinta del afectado y no se acredita que actúa en representación de aquél.
- Lo prevea una ley o norma de derecho comunitario de aplicación directa.
- Dichas normas impidan revelar a los afectados el tratamiento de los datos.

En todo caso, el responsable del fichero o tratamiento deberá informar al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos.

9.4 DERECHO DE CANCELACIÓN

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido dicho plazo, deberá procederse a la supresión de los datos.

9.4.1 Ejercicio del derecho de cancelación

El afectado podrá ejercer los derechos de rectificación y cancelación ante el responsable del fichero o tratamiento a través de la solicitud correspondiente, que deberá tener:

- Nombre y apellidos del interesado.
- Fotocopia del DNI/NIF del interesado y, en su caso, de la persona que lo representa, así como el documento que acredita tal representación.
- Petición en que se concreta la solicitud.
- Dirección a efectos de notificaciones, fecha y firma del solicitante.
- Los datos que se van a cancelar.

9.4.2 Atención a la cancelación

El responsable del fichero o tratamiento resolverá la solicitud de acceso en el plazo *máximo de diez días desde la recepción* de la misma.

En el caso de que no se dispongan de datos de carácter personal del afectado, deberá igualmente comunicarse esta circunstancia al mencionado afectado en el mismo plazo.

Transcurrido el plazo de diez días sin que de forma expresa se responda a la petición de cancelación, el interesado podrá interponer una reclamación de tutela de sus derechos en la Agencia Española de Protección de Datos.

Si los datos cancelados hubieran sido cedidos previamente, el responsable del fichero o tratamiento deberá comunicar la cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, así mismo, a cancelar los datos.

9.4.3 Denegación de la cancelación

El responsable del fichero o tratamiento podrá denegar el derecho de cancelación cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre el responsable del fichero o tratamiento y el interesado.

El responsable del fichero o tratamiento podrá denegar el derecho de rectificación y cancelación cuando:

- La solicitud sea formulada por una persona distinta del afectado y no se acredita que actúa en representación de aquél.
- Lo prevea una ley o norma de derecho comunitario de aplicación directa.
- Dichas normas impidan revelar a los afectados el tratamiento de los datos.

En todo caso, el responsable del fichero o tratamiento deberá informar al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos.

9.5 DERECHO DE OPOSICIÓN

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

1. Cuando no sea necesario su consentimiento para el tratamiento como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una ley no disponga lo contrario.
2. Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial.
3. Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

9.5.1 Ejercicio del derecho de oposición

El afectado podrá ejercer el derecho de oposición ante el responsable del fichero o tratamiento a través de la solicitud correspondiente, que deberá tener:

- Nombre y apellidos del interesado.
- Fotocopia del DNI/NIF del interesado y, en su caso, de la persona que lo representa, así como el documento que acredita tal representación.
- Petición en que se concreta la solicitud.
- Dirección a efectos de notificaciones, fecha y firma del solicitante.
- Cuando la oposición se realice sobre la base del apartado a) de los supuestos, deberán constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifiquen el ejercicio de este derecho.

9.5.2 Atención al derecho de oposición

El responsable del fichero o tratamiento resolverá la solicitud de acceso en el plazo *máximo de diez días desde la recepción* de la misma.

Si la solicitud es estimada, el responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejerce su derecho de oposición.

En el caso de que no se dispongan de datos de carácter personal del afectado, deberá igualmente comunicarse esta circunstancia al mencionado afectado en el mismo plazo.

Transcurrido el plazo de diez días sin que de forma expresa se responda a la petición de oposición, el interesado podrá interponer una reclamación de tutela de sus derechos en la Agencia Española de Protección de Datos.

9.5.3 Denegación del derecho de oposición

El responsable del fichero o tratamiento podrá denegar la solicitud del afectado en el supuesto de que una ley disponga la necesidad del tratamiento de los datos de carácter personal del interesado, pudiendo éste interponer una reclamación en la AEPD, demandando la tutela de sus derechos.

La comunicación de la denegación al derecho de oposición deberá estar motivada y realizarse en un plazo máximo de diez días desde la recepción de la solicitud.

9.6 DERECHO DE CONSULTA

Si recaba la información oportuna en el Registro General de Protección de Datos, cualquier persona podrá conocer:

- La existencia de tratamientos de datos de carácter personal.
- Sus finalidades.
- La identidad del responsable del tratamiento.

El Registro General es de consulta pública y gratuita.

El catálogo de ficheros inscritos en el RGPD que se puede consultar en www.agpd.es contiene información sobre los siguientes aspectos:

1. El responsable del fichero.
2. El servicio o unidad ante el que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
3. La identificación del fichero.
4. Las finalidades y usos previstos del fichero o tratamiento.
5. El origen y procedencia de los datos.
6. Colectivo de personas sobre el que se obtienen los datos de carácter personal.
7. Los tipos de datos, estructura y organización del fichero.
8. Los destinatarios de las cesiones y/o transferencias internacionales de datos.

9.7 DERECHO DE IMPUGNACIÓN DE VALORACIONES

Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos, o que les afecte de manera significativa, que se *base únicamente en un tratamiento automatizado de datos* destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad.

En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión.

La valoración sobre el comportamiento de los ciudadanos basado en un tratamiento automatizado de datos únicamente podrá tener valor probatorio a petición del afectado.

9.7.1 Excepciones

No obstante, los afectados podrán verse sometidos a decisiones con efectos jurídicos sobre ellos o que les afecten de manera significativa y basadas únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como rendimiento laboral, crédito, fiabilidad o conducta, cuando dicha decisión:

- Se haya adoptado en el marco de la celebración o ejecución de un contrato *a petición del interesado*. Siempre que se le otorgue la posibilidad de alegar lo que estime pertinente para defender su derecho o interés.
  - En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán las decisiones antes descritas y cancelará los datos en caso que no llegue a celebrarse finalmente el contrato.
    - Esté autorizada por una norma con rango de ley que establezca medidas que garanticen el interés legítimo del interesado.

9.8 DERECHO A INDEMNIZACIÓN

Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente ley por el *responsable* o el *encargado del tratamiento*, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

En el caso de ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

9.9 LA TUTELA DE LOS DERECHOS

Cuando a un interesado se le deniegue, total o parcialmente, el ejercicio de los derechos de ARCO, podrá ponerlo en conocimiento de la AEPD o, en su caso, del organismo competente en cada Comunidad Autónoma.

Si la AEPD considera que la reclamación formulada es procedente, podrá dictar una resolución de tutela de derechos.

El procedimiento para la tutela de derechos de la AEPD se desarrolla de la siguiente forma:

- El interesado pondrá en conocimiento de la AEPD el contenido de su reclamación y los preceptos de la LOPD que considera vulnerados.
- La AEPD, una vez recibida la reclamación, la comunicará al responsable del fichero para que, en un plazo de quince días, formule las alegaciones que estime pertinentes.
- Recibidas las alegaciones, o transcurrido el plazo de quince días, la AEPD podrá pedir informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y del responsable del fichero, y dictará resolución, que comunicará a ambos.
- El plazo máximo para dictar y notificar resolución será de seis meses, a contar desde la entrada en la AEPD de la reclamación del afectado o afectados.
- Contra la resolución del director de la AEPD se podrá interponer un recurso contencioso-administrativo.

9.9.1 Ejecución de la resolución

Si la resolución de tutela fuese estimatoria, se requerirá al responsable del fichero para que, en el plazo de diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de la tutela, debiendo dar cuenta por escrito de dicho cumplimiento a la Agencia Española de Protección de Datos.

10

LAS MEDIDAS DE SEGURIDAD

«Seis honrados servidores me enseñaron lo que sé; sus nombres son cómo, cuándo, dónde, qué, quién y por qué».

Rudyard Kipling

10.1 DISPOSICIONES GENERALES

La tercera de las tres obligaciones principales, por detrás de la inscripción de los ficheros y la legitimación del tratamiento de datos sobre la base de unos principios básicos, es la *obligación de proteger los datos personales que se traten.*

Para ello, el responsable del fichero o tratamiento y, en su caso, el encargado del tratamiento deben adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal que almacenen o traten.

La adopción de las medidas de seguridad tiene por finalidad evitar la alteración, pérdida y tratamiento o acceso no autorizado en los datos de carácter personal.

Para adoptar las medidas de seguridad debe tenerse en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de las personas o del medio natural o físico en el que se encuentren.

Es labor del responsable del fichero implantar las medidas de seguridad adecuadas tanto para los tratamientos automatizados como para los no automatizados.

10.1.1 Niveles de seguridad

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

10.1.1.1 NIVEL BÁSICO

Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificados de nivel básico.

10.1.1.2 NIVEL MEDIO

Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio en los siguientes ficheros o tratamientos de datos de carácter personal:

- Los relativos a la comisión de infracciones administrativas o penales.
- Aquellos cuyo objetivo sea la prestación de servicios de información sobre 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 financieras para finalidades relacionadas con la prestación de servicios financieros.
- Aquellos de los que sean responsables las Entidades Gestoras de 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 que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o la personalidad de los ciudadanos y que les permiten evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

10.1.1.3 NIVEL ALTO

Deberán implantarse, además de las medidas de seguridad de nivel básico y medio, las medidas de nivel alto en los siguientes ficheros o tratamientos de datos de carácter personal:

- 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.
- Aquellos 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, únicamente respecto al registro de accesos.

10.1.1.4 EXCEPCIONES A LAS MEDIDAS DEL NIVEL ALTO

Determinados ficheros que inicialmente deberían, por la naturaleza de los datos tratados, adoptar medidas de nivel alto, podrán adoptar medidas de seguridad de nivel básico.

Estos ficheros son los siguientes:

1. Los ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, cuando:
   - 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.
   - Se trate de ficheros o tratamientos en los que de forma *incidental o accesoria* se contengan aquellos datos *sin guardar relación con su finalidad.*
2. Los ficheros o tratamientos que contengan datos relativos a la *salud*, referentes únicamente al grado de discapacidad, o a la simple declaración de la condición de discapacidad o invalidez del afectado, *con motivo del cumplimiento de deberes públicos*.

10.1.1.5 MÍNIMOS EXIGIBLES

Las medidas incluidas en cada uno de los niveles escritos anteriormente tienen la condición de mínimos exigibles, sin prejuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero o tratamiento.

10.1.1.6 SEGREGACIÓN DE FICHEROS

Cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación, en cada caso, el nivel de medidas de seguridad correspondiente.

Podrá efectuarse esta segregación de ficheros siempre que:

- Puedan delimitarse los datos afectados y los usuarios con acceso a los mismos.
- Se haga constar en el Documento de Seguridad.

10.1.2 Encargado del tratamiento

Como recordamos, el encargado del tratamiento es la persona física o jurídica que trata datos personales por cuenta del responsable del fichero.

El encargado del tratamiento estará sometido al cumplimiento de las correspondientes medidas de seguridad, en función de la naturaleza de los datos que trate.

La LOPD contempla y regula las diferentes situaciones en las que puede encontrarse el encargado del tratamiento:

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un *encargado de tratamiento que preste sus servicios en los locales del responsable*, deberá hacerse constar esta circunstancia en el Documento de Seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado Documento de Seguridad.

2. Cuando dicho *acceso sea remoto*, habiéndose prohibido al encargado del tratamiento incorporar tales datos a sistemas o soportes distintos a los del responsable, deberá hacerse constar esta circunstancia en el Documento de Seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado Documento de Seguridad.

3. Si el servicio fuera prestado por el *encargado del tratamiento en sus propios locales*, ajenos a los del responsable del fichero, deberá elaborar un Documento de Seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo, e incorporando las medidas de seguridad que se van a implantar con relación a dicho tratamiento.

10.1.3 Prestaciones de servicios sin acceso a datos personales

La LOPD también regula los servicios que se presten y que no impliquen el acceso a datos de carácter personal; por ejemplo, personal de limpieza, seguridad, transporte, mantenimiento de instalaciones, etc.

El responsable del fichero o tratamiento deberá adoptar las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

10.1.4 Delegación de autorizaciones

Las autorizaciones que se atribuyen al responsable del fichero o tratamiento —como autorización para sacar soportes o tratar datos fuera de las instalaciones del responsable, etc.— pueden ser delegadas en las personas designadas a tal efecto.

En el Documento de Seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones, así como aquellas en las que recae dicha delegación.

En ningún caso esta designación supone una delegación de la responsabilidad, que corresponde al responsable del fichero.

10.1.5 Acceso a datos a través de redes de comunicaciones

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

10.1.6 Trabajo fuera de los locales del responsable del fichero o encargado del tratamiento

Cuando los datos personales se almacenen en dispositivos portátiles, o se traten *fuera de los locales* del responsable del fichero o del encargado del tratamiento, será preciso que exista una *autorización previa del responsable del fichero* o tratamiento y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Esta autorización tendrá que *constar en el Documento de Seguridad*, y podrá establecerse por un usuario o perfil de usuarios y determinándose un período de validez para las mismas.

10.1.7 Ficheros temporales o copias de trabajo de documentos

Los ficheros temporales o copias de trabajo de documentos que se crean exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda.

Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez haya dejado de ser necesario para los fines que motivaron su creación.

10.2 EL DOCUMENTO DE SEGURIDAD

El responsable del fichero o tratamiento deberá elaborar un Documento de Seguridad que *recogerá las medidas de índole técnica y organizativa* acordes a la normativa de seguridad vigente y que *será de obligado cumplimiento* para el personal con acceso a los sistemas de información.

El Documento de Seguridad podrá ser único y que comprenda todos los ficheros y tratamientos, o se podrán elaborar distintos documentos individualizados para cada fichero o agrupando varios, según las características de la organización. De esta forma, se podrán elaborar documentos:

- Por fichero o tratamiento.
- Por áreas funcionales.
- Por áreas geográficas.
- Por sistemas de tratamiento.

En todo caso, tendrá el carácter de documento interno de la organización, y se puede elaborar con el criterio que mejor convenga, pero no debemos olvidar que *tiene que estar actualizado en todo momento*. Cuanta más dispersión exista, mayor dificultad presentará su actualización.

El Documento de Seguridad no debe enviarse a la AEPD, sino que deberá mantenerse a su disposición en caso de que llegase a requerirlo.

10.2.1 Contenido del Documento de Seguridad

El documento deberá tener, como mínimo, los siguientes aspectos:

1. Ámbito de aplicación, con especificación detallada de los recursos protegidos.

   Deberán indicarse los recursos que se protegen. En caso de ficheros automatizados: *software*, bases de datos, redes, *hardware*, etc. En el caso de ficheros no automatizados: armarios, ficheros, etc.

2. Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido.

   Se centra en las medidas de protección de los datos de carácter personal, cómo y quién aplicará las medidas de seguridad: acceso de los usuarios a los datos, almacenamiento, transmisión, destrucción, copias de seguridad, etc.

3. Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal.

   Contienen la descripción de las obligaciones generales de secreto y confidencialidad, así como de comunicar las incidencias que se produzcan. Además, detalla las obligaciones particulares de determinados puestos que tienen un contacto con los datos personales mucho más crítico y sensible.

4. Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

   Deberá describir la estructura de los ficheros almacenados, así como la descripción detallada de los sistemas de información que los tratan: equipos, redes, comunicaciones, sistemas operativos, etc.

5. Procedimiento de notificación, gestión y respuesta ante las incidencias.

   El Documento de Seguridad deberá contener una serie de procedimientos que iremos señalando; uno de ellos será la notificación, gestión y respuesta ante incidencias, en el que se indicará, de forma clara y precisa, qué hay que hacer en caso de que se produzca una incidencia.

6. Los procedimientos de realización de copias de respaldo y recuperación de los datos en los ficheros automatizados.

   Deberán existir los procedimientos de realización de copias de respaldo y recuperación de los datos, de forma que sea posible reconstruir los ficheros en caso de pérdida, total o parcial, de los mismos.

7. Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como la destrucción de los documentos y soportes o, en su caso, la reutilización de estos últimos.

   Se deberán reflejar todas las medidas encaminadas para que nadie no autorizado acceda a los datos personales, ya sea en su traslado o posteriormente en su desecho.

10.2.2 Contenido en el caso de ficheros de nivel medio y alto

En el caso de que fueran de aplicación a los ficheros las medidas de nivel medio o alto, el Documento de Seguridad, además, deberá tener:

1. La identificación del responsable o responsables de seguridad.

   El responsable de seguridad podrá ser único, o podrán designarse varios responsables de seguridad.

2. Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

   Se deberán detallar las tareas de control que se van a realizar para garantizar que se cumplen las medidas de seguridad previstas en el Documento de Seguridad.

10.2.3 Existencia de un encargado del tratamiento

Cuando exista un tratamiento de datos por cuenta de terceros (por ejemplo, la asesoría fiscal, que trata los datos de sus clientes), el Documento de Seguridad deberá contener:

- La identificación de los ficheros que se traten en concepto de encargado del tratamiento.
- Referencia expresa al contrato que regula las condiciones del encargo.
- Identificación del responsable del fichero tratado.
- Período de vigencia del encargo.

En aquellos casos en los que los datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su Documento de Seguridad. Cuando tal circunstancia afecte a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del Documento de Seguridad, salvo en lo relativo a aquellos datos contenidos en los recursos propios. Este hecho se indicará de modo expreso en el contrato que regula dicho encargo, con especificación de los ficheros o tratamientos afectados.

10.2.4 Actualización

Una vez que se ha elaborado el Documento de Seguridad, no es para siempre, sino que se ha de actualizar y adecuar a los cambios relevantes que se produzcan:

1. En los sistemas de información.
2. En el sistema de tratamiento empleado.
3. En la organización.
4. En el contenido de la información incluida en sus ficheros o tratamientos.
5. Como consecuencia de los controles periódicos realizados.

Se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

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

10.2.5 Otra información que se debe incluir en el Documento de Seguridad

Aparte de la información antes descrita que debe contener el Documento de Seguridad en las medidas de seguridad que se deben aplicar a los ficheros, encontramos exigencias relativas a la inclusión de procedimientos, autorizaciones, registros y circunstancias que han de quedar reflejados en el Documento de Seguridad.

10.2.5.1 OTROS PROCEDIMIENTOS Y MEDIDAS

Junto a los procedimientos y medidas reflejados, deberán figurar, además, los siguientes:

- *Procedimiento de asignación, distribución y almacenamiento de contraseñas*, cuando sea el mecanismo de autenticación utilizado, así como la periodicidad con la que tienen que ser cambiadas, máximo de un año.
- *Procedimiento de acceso a la documentación de los ficheros no automatizados con nivel de seguridad alto*, estableciendo las pautas de acceso y registro del mismo, cuando dicho acceso sea necesario para otras personas no autorizadas.
- *Medidas alternativas al almacenamiento de ficheros no automatizados con nivel de seguridad alto,* cuando por las características de los locales del responsable del fichero no se pudieran cumplir las medidas de seguridad previstas en relación con el almacenamiento de dicha información.

10.2.5.2 RELACIONES DE PERSONAL AUTORIZADO

Otro grupo de información que debe constar en el Documento de Seguridad es el relativo al personal que autoriza y el autorizado para realizar determinadas actividades. De esta forma, encontramos:

- Personas que autorizan y que pueden delegar dichas autorizaciones.
- Personas en las que recae dicha delegación de otorgar autorizaciones.
- Personas autorizadas.

A continuación, detallamos el personal y las autorizaciones que deben aparecer en el Documento de Seguridad:

1. *Relación de personas habilitadas para otorgar autorizaciones y relación de personas en las que recae dicha delegación.*

   En el Documento de Seguridad debe aparecer esta relación de personas. En caso de que dicha información se almacene en un sistema, debe figurar dónde se encuentra ubicado y el procedimiento para obtener dicha relación.

2. *Personal autorizado para tratar datos fuera de los locales del responsable del fichero o del encargado del tratamiento.*

   La autorización podrá establecerse para un único usuario o para un perfil de usuarios.

3. *Relación de usuarios y perfiles de usuario que acceden al fichero, así como los accesos autorizados para cada uno de ellos.*

   Sólo podrán acceder a los ficheros que contengan datos de carácter personal los usuarios autorizados.

4. *Relación de personal autorizado para conceder, modificar y anular accesos.*

   A este personal se le denomina *administrador del fichero* y controla el acceso a los recursos.

5. *Personal autorizado para acceder a soportes y documentos.*

   Sólo el personal autorizado en el Documento de Seguridad podrá acceder a los soportes y documentos que contengan datos de carácter personal.

6. *Relación de usuarios autorizados para la salida de soportes y documentos.*

   Cualquier persona que saque datos personales fuera de los locales del responsable, incluidos los comprendidos y/o anexos a un correo electrónico, deberá ser autorizada por el responsable, o encontrarse debidamente autorizada en el Documento de Seguridad.

7. *Relación de responsables de la entrega y recepción de soportes y documentos que contengan datos de nivel medio y alto.*

Sólo estos responsables podrán entregar y recibir soportes y documentos que contengan datos de nivel medio y alto.

8. *Personal autorizado para el acceso físico a ficheros de nivel medio y alto.*

   Sólo 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.

9. *Personal autorizado para la recuperación de datos en ficheros de nivel medio y alto.*

   Sólo podrá efectuar el procedimiento de recuperación de datos el personal autorizado previamente.

10. *Personal autorizado para la copia o reproducción de documentos que contengan datos de nivel alto.*

    La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el Documento de Seguridad.

10.2.5.3 REGISTROS

Lo conforman los registros que exige el reglamento de la LOPD. Aunque no existe obligación expresa de que el registro se gestione en el propio Documento de Seguridad, en caso de que se haga de forma externa deberá indicarse en el Documento de Seguridad la ubicación del mismo y la forma de consultarlo.

Los registros que es necesario *elaborar y mantener* son:

- *Inventario de soportes y documentos.*

  Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen y ser inventariados.

- *Registro de incidencias.*

  Se deben registrar las incidencias que afecten o puedan afectar a los datos de carácter personal. Si el registro se lleva de forma informática, es conveniente imprimirlo periódicamente y anexarlo al Documento de Seguridad.

- *Registro de la realización de pruebas con datos reales.*

  Se debe evitar la realización de pruebas con datos reales, pero si no es posible, se debe tener en cuenta que:

  - Debe asegurarse el nivel de seguridad correspondiente a los datos tratados.
  - Se debe realizar una copia de seguridad.
  - Se debe anotar su realización en el Documento de Seguridad.

- *Registro de entrada y salida de soportes y documentos que contengan datos de nivel medio y alto.*

  Si el registro se lleva de forma informática, es conveniente imprimirlo periódicamente y anexarlo al Documento de Seguridad.

- *Registro de accesos a la documentación que contenga datos de nivel alto.*

  Obligatorio en el caso de documentos que puedan ser utilizados por múltiples usuarios.

10.2.5.4 OTRAS CIRCUNSTANCIAS QUE DEBEN MOTIVARSE EN EL DOCUMENTO DE SEGURIDAD

Además de toda la información anterior que es necesario incluir en el Documento de Seguridad, deben motivarse debidamente las siguientes circunstancias:

- *Segregación de datos.*

  En caso de que sea posible segregar datos para aplicar otro nivel de medidas de seguridad diferentes al del sistema principal, deberá hacerse constar esta circunstancia en el Documento de Seguridad.

- *Imposibilidad de proceder a la identificación e inventario de soportes o documentos.*

  En el caso de que sea imposible etiquetar e inventariar los soportes y documentos que contengan datos de carácter personal porque las características físicas del mismo imposibiliten su cumplimiento, deberá quedar constancia motivada de ello en el Documento de Seguridad.

- *Grabación manual de datos en un proceso de recuperación.*

En el caso de pérdida o destrucción de ficheros parcialmente automatizados —y siempre que exista documentación que permita grabar manualmente los datos que no ha sido posible restaurar—, se deberán grabar manualmente —y documentar esta circunstancia en el Documento de Seguridad—, así como los datos que han tenido que ser grabados de esta manera.

- *Tratamiento de datos en dispositivos portátiles que no permitan su cifrado.*

  En el caso de datos personales que requieran de medidas de seguridad de nivel alto y sea preciso tratarlos en dispositivos portátiles que no permitan su cifrado, este hecho 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.

- *Exclusión del registro de accesos.*

  En los ficheros automatizados que contengan datos de nivel alto es obligatorio mantener un registro de accesos; sin embargo, se exceptúa esta obligación en el caso de que concurran estas dos circunstancias:

  - Que el responsable del fichero o tratamiento sea una persona física
  - Que el responsable del fichero o tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

  Y se haga constar expresamente en el Documento de Seguridad.

10.2.6 Conclusiones

El Documento de Seguridad es el eje sobre el que giran todas las medidas de seguridad que es necesario implantar en el tratamiento de datos de carácter personal.

Así mismo, refleja la realidad de la organización en cuanto a ficheros, usuarios, permisos, accesos, sistemas, autorizaciones, registros, circunstancias particulares y demás información relevante para garantizar la seguridad de los datos de carácter personal almacenados.

Es algo «vivo» y en continua actualización, que debe reflejar en todo momento la situación actual de la organización.

Un Documento de Seguridad que no refleje de forma fehaciente la realidad de la organización, que no esté actualizado con los cambios que se producen en los ficheros, el personal y los sistemas, es algo que no tiene ningún valor para la organización ni para la AEPD.

La infracción por no tener Documento de Seguridad, o bien tenerlo pero sin actualizar, de forma que no refleje la realidad de la organización, es calificada por la AEPD como grave, con sanciones de 40.001 a 300.000 euros.

10.3 MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS AUTOMATIZADOS

Las siguientes medidas de seguridad se aplican a ficheros y tratamientos automatizados.

10.3.1 Medidas de seguridad de nivel básico

10.3.1.1 FUNCIONES Y OBLIGACIONES DEL PERSONAL

1. Se deben definir y documentar en el Documento de Seguridad las *funciones y obligaciones de cada uno de los usuarios o perfiles* de usuarios[12] con acceso a los datos de carácter personal.

2. También se definirán las *funciones de control o autorizaciones delegadas* por el responsable del fichero o tratamiento.

3. Se debe *informar* al personal de una forma clara *de las normas de seguridad* que afecten al desarrollo de sus funciones, así como las consecuencias de su incumplimiento.

Es decir, debemos hacer un análisis de la organización y del personal, sintetizando las funciones de cada uno de ellos, y agruparlos en colectivos de perfiles de usuarios, definiendo los accesos, recursos y privilegios que tiene cada uno de estos perfiles.

12 Perfil de usuario: accesos autorizados a un grupo de usuarios.

Así mismo, debemos documentar esta relación de personas o perfiles en el Documento de Seguridad, al igual que las funciones de control (administradores del fichero) y las autorizaciones delegadas.

Además, el personal debe estar informado de las normas de seguridad que deben acatar y lo que le puede suceder si las incumple.

Esto se articula mediante la firma de un compromiso de confidencialidad y deber de secreto en el cual el trabajador se compromete al secreto profesional y al deber de guardar los datos que trate. Así mismo, se le dará a conocer sus funciones, las medidas de seguridad que debe cumplir y las consecuencias de su incumplimiento.

10.3.1.1.1 Finalidad

En muy alta medida, la seguridad de los datos depende de las personas que manejan dichos datos.

Es primordial para la organización tener definidos los datos a los que accede cada uno de los distintos puestos de la organización, de forma que se le proporcione acceso estrictamente a los datos que le son necesarios para el desempeño de sus funciones.

Para esto necesitamos analizar y documentar los distintos perfiles existentes, así como los privilegios y accesos concedidos a cada uno de ellos.

Por otra parte, es necesario que todas las personas involucradas en el tratamiento comprendan y apliquen las medidas de seguridad recogidas en el Documento de Seguridad.

De la misma forma, deben ser totalmente conscientes de las consecuencias de incumplir sus obligaciones.

10.3.1.2 REGISTRO DE INCIDENCIAS

- Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal.
- Dicho procedimiento debe constar en el Documento de Seguridad.
- Se deberá establecer un registro en el que se ha constar la siguiente información:
  - Tipo de incidencia.

- Momento en que se ha producido o detectado.
- Persona que realiza la notificación.
- A quién se le comunica.
- Los efectos que se hubieran derivado de la misma.
- Medidas correctoras aplicadas.

10.3.1.2.1 Finalidad

- Que exista un procedimiento definido y conocido por todos los usuarios para notificar y gestionar correctamente las incidencias que se produzcan o puedan producirse.

- Garantizar la prevención y seguridad de los datos, siendo imprescindible para la realización de informes periódicos y el establecimiento de medidas correctivas la necesidad de disponer de un registro con las incidencias que se han producido.

10.3.1.2.2 Definición de incidencia

Se considerará incidencia cualquier anomalía que afecte o pueda afectar a la seguridad de los ficheros con datos de carácter personal, de forma que constituya o pueda constituir un riesgo para la confidencialidad o integridad de su información.

Se deberán tener en cuenta, entre otras, las siguientes incidencias:

- Pérdida de información de algún fichero de datos de carácter personal.

- Modificación de datos personales por personal no autorizado o desconocido.

- Existencia de sistemas de información sin las debidas medidas de seguridad.

- Los intentos de acceso no autorizados a ficheros de carácter personal.

- El conocimiento por terceros de la clave de acceso al sistema.

- El intento no autorizado de salida de un soporte.

- La existencia de soportes sin inventariar y que contengan datos personales.

- La destrucción total o parcial de un soporte que contenga datos de carácter personal.
- La caída del sistema de seguridad informática que posibilite el acceso a datos personales por personas no autorizadas.
- El cambio de la ubicación física de ficheros con datos de carácter personal.

10.3.1.2.3 Procedimiento de notificación de incidencias

Debe existir un procedimiento de notificación y gestión de incidencias, y dicho procedimiento debe quedar formalmente descrito en el Documento de Seguridad.

El procedimiento debe describir los pasos necesarios para la correcta notificación y gestión de las incidencias que se produzcan, y deberá ser comunicado a todos los trabajadores que traten con datos de carácter personal.

La obligación de notificar la incidencia recae en la persona o personas que detecten la anomalía que afecte o pueda afectar a la seguridad de los datos personales, y deberá seguir el procedimiento documentado para notificar al responsable del registro de incidencias, que a su vez la anotará en el registro de incidencias y la comunicará al responsable de seguridad (en muchas organizaciones será la misma persona).

Una vez notificada, el responsable de seguridad realizará las acciones necesarias para corregir dicha incidencia.

Se deberán determinar los efectos derivados de la incidencia, así como las medidas correctoras que se deben aplicar. El responsable del registro de incidencias deberá cumplimentar el resto de los apartados con estos datos.

Se debe revisar periódicamente dicho registro y elaborar un informe interno con las medidas correctivas propuestas para evitar estas incidencias en el futuro o minimizar el impacto en caso de producirse.

El conocimiento y la no notificación o no registro de una incidencia por un trabajador será considerada una falta contra la seguridad del sistema por dicho trabajador.

10.3.1.2.4 El registro de incidencias

Se debe crear un registro de incidencias con, al menos, los siguientes campos: tipo de incidencia, el momento en el 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. Dicho registro afecta tanto a ficheros automatizados como no automatizados.

La creación del registro de incidencias puede ser en papel o en soporte informático.

- **Registro de incidencias en papel.** En caso de habilitar un registro de incidencias en papel, se anexarán al Documento de Seguridad los eventos que se van produciendo.

- **Registro de incidencias automatizado.** Se podrá crear también un registro de incidencias en soporte informático a través de alguna aplicación de hoja de cálculo o base de datos, que nos permita al acceso a su información de forma cómoda y nos facilite efectuar listados.

En caso de gestión automatizada, debemos hacer constar en el Documento de Seguridad el sistema informático utilizado. Así mismo, es conveniente imprimir periódicamente las incidencias registradas y anexarlas al Documento de Seguridad.

REGISTRO DE INCIDENCIAS					
N.º DE INCIDENCIA		FECHA		HORA	
TIPO DE INCIDENCIA					
DESCRIPCIÓN:					
EFECTOS DERIVADOS:					
MEDIDAS CORRECTORAS:					
PERSONA QUE COMUNICA LA INCIDENCIA					
PERSONA QUE RECIBE LA NOTIFICACIÓN					

10.3.1.3 CONTROL DE ACCESO

- Cada usuario accederá únicamente a los datos y recursos necesarios para el desarrollo de sus funciones.
- Deberá existir una relación actualizada de usuarios y perfiles de usuario, con los accesos autorizados para éstos.
- Se deberán establecer mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados.
- La concesión, alteración o anulación de permisos de acceso sólo podrá realizarse por el personal autorizado en el Documento de Seguridad.
- 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 propio.

10.3.1.3.1 Finalidad

- Limitar el acceso a los datos a los usuarios que lo precisen para sus funciones, evitando que «todo el personal acceda a todos los datos».
- Disponer de una relación actualizada de usuarios y sus accesos autorizados.
- Limitar la gestión de altas, bajas y privilegios de los usuarios al personal debidamente autorizado.
- Garantizar que todas las personas que tienen acceso a los datos cumplen las medidas de seguridad implantadas.

10.3.1.3.2 Acceso a los datos sólo por usuarios autorizados

Se debe garantizar que los usuarios sólo acceden a los datos y recursos necesarios para el desempeño de sus funciones.

Previamente al acceso a los datos, se han de conceder las autorizaciones pertinentes.

Implantar los mecanismos necesarios para impedir el acceso a datos no autorizados a los distintos usuarios, así como una adecuada gestión del control de acceso que garantice que los usuarios no van a poder acceder a datos, recursos o funcionalidades no autorizadas.

10.3.1.3.3 Relación de usuarios y accesos

Mantener una relación actualizada de usuarios y perfiles de usuario, y el tipo de acceso autorizado. En la relación de usuarios y accesos deberán constar los siguientes datos:

- Fichero al que accede.
- Nombre y apellidos del usuario.
- Perfil al que pertenece.
- Identificador asignado.
- Fecha de alta.
- Fecha de baja.

Así mismo, deberá existir una relación de perfiles que especifique detalladamente los accesos y privilegios que tiene asignados cada perfil.

Relación de usuarios y accesos informatizada

Si la relación de usuarios y accesos se mantiene de forma informatizada, indicar en el Documento de Seguridad el sistema de información utilizado, y es conveniente imprimir periódicamente la relación de usuarios y adjuntarla al anexo correspondiente.

En este caso, recordar que se deberá incluir dicha lista dentro de la planificación de las copias de seguridad de la organización.

10.3.1.3.4 Política de control de acceso

Los procedimientos de control de acceso deben tener en cuenta el ciclo de vida del usuario, desde su alta en el sistema hasta la baja en el mismo.

Gestión de las altas y bajas de los usuarios

Se debe elaborar y redactar un procedimiento o política de registro de altas y bajas de usuarios, cobrando mayor importancia su estricto cumplimiento cuantos más usuarios accedan al sistema. La política debe cumplir, entre otros, los siguientes extremos:

- Asignar un identificador único por usuario, sin que diferentes usuarios puedan compartirlo.
- En caso de baja definitiva de un usuario, eliminar inmediatamente sus derechos de acceso.
- En caso de baja temporal, bloquear su identificación.
- Revisar periódicamente la lista de usuarios, eliminando los usuarios redundantes y los que ya no estén de alta, así como revisión de los recursos a los que tienen acceso permitido.
- Incorporación en el contrato laboral de una cláusula de sanción en caso de realizar accesos no autorizados.

10.3.1.3.5 Mecanismos que impiden el acceso a los usuarios no autorizados

El responsable del fichero debe establecer e implantar los mecanismos que impidan el acceso por personal no autorizado a los ficheros.

En el caso de ficheros automatizados, establecer mecanismos de seguridad con el siguiente criterio: «Todo lo que no está explícitamente autorizado, está prohibido».

Seguir una política de «arriba-abajo», es decir, comenzar protegiendo el acceso al servidor y sus recursos, seguir con las aplicaciones de gestión utilizadas y terminar protegiendo el acceso a los puestos de trabajo.

Proteger el acceso al servidor

Proteger tanto el acceso físico como el acceso lógico al servidor.

- **Proteger el acceso físico al servidor.** Situar el servidor en una sala cerrada con llave o algún otro mecanismo de bloqueo similar. Únicamente debe disponer de la llave de acceso a la sala del servidor el personal debidamente autorizado para dar altas, bajas y modificaciones de usuarios.

- **Proteger el acceso lógico al servidor.** Para proteger el acceso al sistema operativo del servidor. Se debe eliminar o proteger con contraseña fuerte todas las cuentas que se crean por defecto, asegurándonos de que no queda ninguna sin proteger. Estas cuentas por defecto, con contraseñas conocidas, son las que suelen aprovechar terceras personas para acceder a los recursos no autorizados.

Proteger el acceso a los recursos del servidor

Los recursos (carpetas compartidas, aplicación de gestión, etc.) del servidor en los que se ubiquen datos personales no deben tener, por defecto, el acceso permitido para nadie. Posteriormente, se irá concediendo acceso a los usuarios autorizados que se dan de alta.

De esta forma, tenemos la seguridad de que sólo van a poder acceder a los recursos los usuarios que previamente dispongan de autorización para hacerlo.

Proteger el acceso a las aplicaciones de gestión

Habilitar el acceso a todas las aplicaciones de gestión utilizadas en la organización, previa introducción de un nombre de usuario y su contraseña asociada.

La caducidad de la contraseña deberá ser, como máximo, de un año.

Esta obligación se hace más relevante en el caso de ficheros de nivel alto, ya que debe quedar registrado el usuario que ha accedido, el momento, si el acceso ha sido autorizado o no y, en caso de ser autorizado, el registro al que ha accedido.

Para no complicar más de lo necesario la operativa de trabajo al personal, y evitar que, al final, apunten la contraseña o peguen un *post-it* en la pantalla, el nombre de usuario y la contraseña de acceso a las aplicaciones por cada usuario deberían coincidir con el nombre de usuario y contraseña de acceso al sistema operativo de su puesto de trabajo.

Proteger el acceso a los puestos de trabajo

Limitar el acceso al sistema operativo de los puestos de trabajo a los usuarios debidamente autorizados. No se debe poder acceder a ningún sistema sin introducir la correspondiente contraseña de acceso o cualquier otro método alternativo que garantice que la persona que está accediendo está autorizada para hacerlo.

10.3.1.3.6 Procedimiento para conceder acceso autorizado

El responsable del fichero tiene que definir e incluir en el Documento de Seguridad los procedimientos y criterios de concesión, alteración o anulación de los accesos autorizados.

A su vez, deberán constar en el Documento de Seguridad las correspondientes autorizaciones que determinan las personas formalmente asignadas para conceder las autorizaciones de acceso al resto del personal.

10.3.1.3.7 Personal ajeno

En las instalaciones puede existir personal ajeno que no perteneciendo a la organización tenga acceso a los recursos; por ejemplo, el personal de mantenimiento de las aplicaciones o de los sistemas; en este caso, el personal externo debe cumplir con los mismos requisitos de seguridad que el personal propio. Dichas obligaciones deben figurar en el contrato que se suscriba, ya sea con dicho personal o con la empresa de quien depende.

10.3.1.4 GESTIÓN DE SOPORTES Y DOCUMENTOS

1. Los soportes y documentos que contengan datos de carácter personal deben permitir:

   - Identificar el tipo de información que contienen.
   - Ser inventariados.
   - Ser accesibles únicamente por el personal autorizado.

   Se exceptúan estas obligaciones cuanto 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 personales fuera de los locales debe ser autorizada por el responsable del fichero.

3. En el traslado de documentación se evitará su pérdida o acceso indebido.

4. Cuando un soporte o documento sea destruido o borrado, deben adoptarse las medidas necesarias que impidan la posterior recuperación de su información.

5. La identificación de soportes con información sensible se podrá realizar a través de un etiquetado que sea comprensible sólo para los usuarios con acceso autorizado.

10.3.1.4.1 Finalidad

Imagínese una organización en la que existan datos de carácter personal en varios soportes: CD, memorias USB, discos duros externos, etc.; sin inventariar, sin controlar. Además, que se almacenen en cualquier lugar: en el armario del despacho, en el cajón, encima de la mesa, etc. ¿Qué seguridad tendrán esos datos? ¿Cómo sabremos que hemos perdido un soporte si ni siquiera sabemos los soportes que tenemos?

Para poder garantizar la seguridad de los soportes con datos de carácter personal que tiene una organización y llevar un control sobre ellos es preciso que estén etiquetados e inventariados, así como seguir una serie de normas en cuanto a acceso, almacenaje y traslado.

10.3.1.4.2 Identificación, inventariado y almacenamiento

En la identificación, inventariado y almacenamiento de soportes no incluiremos los discos duros insertos en los PC, ya que forman parte de los sistemas de información y éstos ya están inventariados en el Documento de Seguridad.

Identificación

Los soportes que contengan datos de carácter personal deberán ser identificados, de forma que se distingan de los demás soportes.

Un ejemplo de etiqueta identificativa podría ser:

ID: HDCLI001
CONTENIDO: FICHERO CLIENTES

La etiqueta consta de dos partes:

- Un código identificativo, que describe el tipo de soporte que es: HDCLI (disco duro externo) seguido de un número (001). Este número será correlativo para cada nuevo soporte de este tipo dado de alta.

- Descripción del contenido del soporte, indicando los datos que contiene.

Este sistema de etiquetado es un ejemplo ilustrativo. Se podría haber escogido otro sistema; por ejemplo, el departamento al que hace referencia el soporte seguido de un número correlativo: VTS001; significaría que pertenece al departamento de ventas y es el soporte número 001. *La organización debe decidir el sistema que se va a utilizar y describirlo en el Documento de Seguridad.*

Como recomendación adicional, los soportes que contengan ficheros con datos de carácter personal y se saquen de los locales de la organización (por ejemplo, la copia de seguridad) deberían ser etiquetados de forma comprensible y con significado para los usuarios autorizados, pero que dificulten la identificación para el resto de las personas, tal y como se detalla más adelante. Además, la información contenida debería ir encriptada. Esto ofrecería una gran protección para la información contenida en ellos ante una eventual pérdida del soporte y el posible acceso no autorizado por terceras personas.

Inventario de soportes

El responsable de seguridad, o cualquier persona en la que haya delegado formalmente, dispondrá de una relación actualizada de los soportes que contengan datos de carácter personal.

En dicha relación constará la identificación del soporte, el tipo de soporte o documento y la información que contiene, así como la fecha de alta y la fecha de baja o destrucción del soporte.

Periódicamente —recomendable una vez al mes—, el responsable de seguridad deberá revisar el inventario de soportes y cotejarlo con los soportes que existan en la organización, realizando las correspondientes actualizaciones en la relación para reflejar la situación actual.

Inventario de soportes en papel. En caso de habilitar un inventario de soportes en papel, se anexará al Documento de Seguridad y se actualizará cuando exista un alta o baja de soporte con datos personales.

Inventario de soportes automatizado. Se podrá crear también un inventario en soporte informático a través de alguna aplicación de hoja de cálculo o base de datos, que nos permita al acceso a su información de forma cómoda y nos facilite efectuar listados. En este caso, se deberá incluir en el Documento de Seguridad el equipo donde se puede obtener el inventario, así como el procedimiento que se debe

seguir. Es conveniente imprimir periódicamente el inventario de soportes y anexarlo al Documento de Seguridad.

INVENTARIO DE SOPORTES Y/O DOCUMENTOS				
Identificación	Tipo de soporte o documento	Información contenida	Fecha alta	Fecha baja
HDEX001	Disco duro externo	FICHERO CLIENTES	28/02/08	

Figura 10.1. Modelo de inventario de soportes con datos

Almacenamiento de soportes

Como medida general, todos los soportes y documentos que contengan datos de carácter personal deberán almacenarse en lugares a los que únicamente tengan acceso las personas autorizadas a tratar dicha información.

Se evitarán en todo momento los cajones y armarios sin llave de cierre, la superficie de las mesas de trabajo y, en general, todo lugar accesible o manipulable por terceros que haga posible el acceso no autorizado a la información.

No se debe almacenar ningún soporte ni documento fuera de los lugares previstos para su custodia cuando no sean utilizados.

Los soportes que contengan copias de seguridad deberían almacenarse en un armario ignífugo, cerrado con llave u otro mecanismo de bloqueo similar.

Debe existir una relación actualizada de los lugares donde se almacenan los soportes que contienen datos personales —tanto manuales como automatizados—, así como los usuarios autorizados a acceder a cada uno de esos lugares.

10.3.1.4.3 Salida de soportes y documentos de los locales

La salida de soportes y documentos fuera de las instalaciones del responsable del fichero sólo se podrá realizar por el personal previamente autorizado en el Documento de Seguridad.

Esto incluye también la salida de información a través de redes de comunicaciones, como el correo electrónico, transferencia de ficheros, etc.

10.3.1.4.4 Traslado de documentación

En el traslado de la documentación se deberán adoptar las medidas necesarias para evitar la sustracción, pérdida o acceso indebido durante su transporte.

Se debe realizar el transporte de la documentación en una cartera u otro contenedor que disponga de un mecanismo de bloqueo por llave o combinación, de forma que no sea posible el acceso a la información por parte de personas no autorizadas.

Así mismo, debe ser custodiada en todo momento por la persona que realiza el transporte.

10.3.1.4.5 Destrucción y borrado de soportes y documentos

Siempre que se deseche cualquier soporte o documento que contenga datos personales, deberá procederse a su borrado o destrucción.

En el caso de documentos en papel, se deberán desechar pasándolos por una trituradora de papel que los destruya, haciendo imposible la recuperación de la información que contenían.

Para soportes y/o documentos electrónicos se debe utilizar alguna de las abundantes herramientas que existen para realizar un borrado seguro de la información, de forma que sea imposible realizar un recuperado posterior de dicha información.

Este punto de destrucción y borrado es de aplicación también a los equipos informáticos obsoletos que se desechan, ya que antes de deshacerse de ellos o destinarlos a otro fin, se debe eliminar toda la información que contienen a través de alguna herramienta de borrado seguro del disco duro y que haga imposible recuperar su contenido.

10.3.1.4.6 Etiquetado de soportes con datos especialmente sensibles

Para el etiquetado de soportes con datos de carácter personal especialmente sensibles es conveniente realizarlo sin ofrecer ningún tipo de información explícita sobre el contenido de dicho soporte que permita identificar su contenido a los usuarios autorizados, y sin embargo dificulte la identificación para el resto de las personas.

Un ejemplo de etiqueta identificativa para este tipo de soportes podría ser:

ID: HDEX001S

La etiqueta consta de:

- Un código identificativo que describe el tipo de soporte que es: HDEX (disco duro externo) seguido de un número (001). Este número será correlativo para cada nuevo soporte de este tipo dado de alta. En caso de que el tipo de soporte sea un DVD, la ID sería: DVD001, y así con todos.

- La letra «S» del final indica que se trata de un soporte con datos de carácter personal especialmente sensibles.

Como se puede ver, no existe en el etiquetado ningún dato que nos indique de forma directa el tipo de información que contiene. Además, este tipo de etiquetado no dice nada a quien no conoce el sistema, pero les indica a los usuarios autorizados que es un soporte que alberga información cuya protección es de suma importancia.

En el caso de soportes que contengan algún fichero de nivel alto —o su copia de seguridad—, esta forma de etiquetado —que no revela los datos que contiene ni la organización a la que pertenece el soporte—, junto con el encriptado de la información que contiene, proporciona una gran seguridad frente a su eventual pérdida y el posible acceso no autorizado por terceras personas.

El sistema que hemos descrito es un ejemplo que sirve para ilustrar de manera concreta un sistema de etiquetado de soportes de estas características. Después, la organización escogerá el que mejor le parezca implementar, describiendo el sistema utilizado en el Documento de Seguridad.

10.3.1.5 IDENTIFICACIÓN Y AUTENTICACIÓN

1. Se debe garantizar la correcta identificación y autenticación de los usuarios.

2. Se debe identificar de forma inequívoca y personalizada a los usuarios que intenten acceder al sistema de información, y se debe verificar que están autorizados.

3. Debe existir un procedimiento de asignación, distribución y almacenamiento de contraseñas.

4. Una vez al año, como mínimo, se deben cambiar las contraseñas de acceso.

10.3.1.5.1 Finalidad

Es imposible controlar que sólo accedan a los ficheros automatizados los usuarios autorizados si no existe un mecanismo que limite dicho acceso a los usuarios que no disponen de la mencionada autorización.

Para que el responsable del fichero garantice que sólo acceden a los ficheros automatizados los usuarios debidamente autorizados, se debe implementar un sistema que:

- Compruebe la identidad del usuario (identificación).
- Valide su acceso al sistema (autenticación).
- Le permita acceder únicamente a los datos y recursos asignados para ese usuario o perfil al que pertenece (autorización).

En el caso de autenticación mediante contraseña, se deberá cambiar la misma al menos una vez al año, ya que de otra manera, al final, la contraseña terminaría siendo conocida por el resto del personal y perdería su utilidad restrictiva.

10.3.1.5.2 Mecanismos de identificación y autenticación

Existen diversas maneras de identificación y autenticación del usuario en función del mecanismo o tecnología que se aplique. Podemos clasificar los sistemas en estos tipos:

- Sistemas basados en algo que el usuario conoce (contraseña).
- Sistemas basados en algo que el usuario posee (DNI electrónico, *token*, etc.).
- Sistemas basados en una característica física del usuario, también denominados biométricos (reconocimiento de huella dactilar, voz, rostro, patrón ocular, etc.).
- Sistemas mixtos, que combinan dos o más de los descritos anteriormente.

Todos estos mecanismos, desde los más sencillos (contraseñas) a los más sofisticados (biométricos), suelen necesitar de fondo, y con objeto de poder autenticar a la persona de cara a un servidor (en el que se albergan los datos y recursos), de un identificador y un autenticador, cuya construcción y gestión explicamos detalladamente en el siguiente epígrafe.

10.3.1.5.3 Identificación y autenticación

El proceso de identificación y autenticación no debe confundirse con el proceso de autorización de acceso permitido, descrito anteriormente.

Previamente a la asignación del identificador, debe seguirse el procedimiento de concesión de acceso que consta en el Documento de Seguridad. En este procedimiento se asigna un perfil al nuevo usuario y se le incluye en la relación de usuarios y accesos.

Cada usuario que accede al sistema debe tener su propio identificador. No puede haber dos o más usuarios compartiendo un mismo identificador.

La contraseña se deberá almacenar en el sistema de forma ininteligible, garantizando su confidencialidad e integridad.

Construcción del identificador (identificación)

El identificador es lo que suele llamarse el «nombre de usuario». Deberá seguirse un procedimiento de asignación de identificadores a los usuarios del sistema. El procedimiento y la persona encargada de dar de alta y baja a usuarios y conceder acceso a datos y recursos deben estar claramente identificados en el Documento de Seguridad.

La función del identificador es doble: identificar al usuario autorizado y definir su capacidad de acceso a los datos y recursos del sistema.

Éstos son algunos ejemplos de identificador para el nombre Álvaro Miguel Pérez:

- Primera letra del nombre seguido del primer apellido (amiguel).
- Tres primeras letras del nombre seguido del primer apellido (alvmiguel).
- Primera letra del nombre seguido del primer apellido y la inicial del segundo apellido (amiguelp).

Cualquiera de estos sistemas es válido; lo importante es respetar el procedimiento escogido para la asignación de identificadores, ya que esto proporcionará claridad y permitirá la identificación precisa e inequívoca del usuario.

Construcción del autenticador (autenticación)

Una vez asignado el identificador, el responsable de dar acceso al sistema debe construir un código alfanumérico que será adjudicado a ese identificador para permitir su acceso a los datos y recursos que tenga autorizados. Este código recibe el nombre de autenticador o contraseña.

El autenticador será secreto, y el usuario no deberá revelarlo a nadie, considerándose la comunicación del mismo a otro usuario una falta grave para la seguridad del sistema.

En caso de pérdida del autenticador, o de sospecha de conocimiento del mismo por terceras personas, el usuario deberá solicitar al responsable del sistema un nuevo código.

Se debe tener en cuenta que la fortaleza del acceso al sistema radica en el autenticador, que es el que valida el acceso al sistema y sus recursos. Para garantizar la seguridad es necesaria una correcta gestión de las contraseñas, siendo recomendable aplicar los siguientes procedimientos:

- Aplicar una política de contraseñas «óptimas», estableciendo para ello una longitud mínima de 8 caracteres que combine letras, números, mayúsculas y minúsculas, así como caracteres especiales (*$%&/-!=+).
- Evitar todas aquellas contraseñas deducibles por terceros y asociadas a parámetros comunes del usuario (fechas de nacimiento, nombre de familiares, matrículas de coches, aficiones, etc.).
- Firma por parte de los usuarios de una cláusula de confidencialidad, obligando a la no comunicación de su contraseña a terceros.
- Limitar el número de intentos fallidos de acceso al sistema.
- Establecer la periodicidad de cambio de las contraseñas a menos de 365 días, tal y como detalla el epígrafe 4 del presente capítulo.

Los sistemas operativos actuales permiten automatizar la parte técnica de estos procedimientos a través de la configuración correcta de las políticas de seguridad que llevan implícitas. Se pueden configurar, a través de estas políticas, los siguientes parámetros:

- Longitud mínima.
- Complejidad.
- Las últimas contraseñas que recuerda el sistema, no pudiéndose repetir.
- Caducidad de la contraseña.
- Número máximo de intentos fallidos antes del bloqueo de la cuenta.

Concesión de acceso a datos y recursos (autorización)

Sobre la base del perfil asignado al usuario, el responsable concederá acceso para ese identificador a los datos y recursos que le son necesarios para el desempeño de sus funciones.

10.3.1.5.4 Implementación de la identificación y autenticación

Los lugares donde se debe exigir al usuario su identificación y autenticación y, por tanto, debemos realizar su correcta implementación son fundamentalmente dos:

Acceso al sistema operativo

Cuando el equipo arranca, se puede acceder al sistema operativo introduciendo el nombre de usuario y la contraseña. Los datos que introduzcamos aquí, siempre que sean válidos, proporcionarán el acceso al sistema operativo y realizarán la identificación del usuario contra el servidor, que darán acceso a los datos y recursos previamente asignados a este identificador.

Acceso a las aplicaciones de gestión de la organización

Para que el usuario pueda acceder a las aplicaciones de gestión de la organización (base de datos de clientes, pacientes, contabilidad, facturación, etc.) y establecer su nivel de acceso y permisos dentro de la aplicación se debe implementar la identificación y autenticación también en la entrada de dicho *software*.

Al igual que con el acceso al sistema operativo, cada usuario debe tener un único identificador, no pudiendo utilizar varios usuarios el mismo identificador.

En el caso de aplicaciones que accedan a ficheros de nivel alto esto es especialmente relevante, ya que a través de esta identificación se podrá realizar correctamente el registro de acceso exigido.

Normalmente, el acceso a las aplicaciones de gestión es independiente del acceso a los datos y recursos del servidor, con lo cual se debe realizar una doble implementación:

- **Con relación a los recursos del servidor:** proporcionar a cada identificador el acceso a los recursos necesarios para que pueda acceder a los datos y a la aplicación (o aplicaciones) de gestión necesarias para realizar las funciones del usuario.

- **Con relación a la aplicación de gestión:** proporcionar a cada identificador el acceso y definir los permisos de ese usuario dentro de la propia aplicación de gestión. Esto se debe realizar con cada aplicación de gestión a la que el usuario deba tener acceso.

Con objeto de simplificar y mejorar la gestión de los usuarios, se debe construir el mismo identificador para las aplicaciones de gestión y para el acceso a los recursos del servidor.

Las contraseñas asignadas para la entrada a las aplicaciones de gestión deben seguir también las políticas establecidas en cuanto a longitud mínima, complejidad, número de intentos fallidos y caducidad.

Sistemas SINGLE SIGN-ON (SSO)

No podemos pasar este apartado sin olvidar los recientes sistemas Single Sign-On (SSO), que permiten que el usuario se autentique una sola vez a la entrada del sistema operativo, y no se tenga que autenticar más para el acceso a los datos y aplicaciones de gestión que utiliza, ya que el sistema proporciona la autenticación necesaria para el acceso a *cada* aplicación utilizada por el usuario.

La alta seguridad de este sistema la proporciona, precisamente, su sencillez de cara al usuario, ya que, una vez validado su acceso, no se precisa de ninguna contraseña para el acceso a las aplicaciones y los datos, evitándose así el típico *post-it* pegado en la pantalla con la clave de entrada de las aplicaciones que utiliza. Se evita, además, que un usuario acceda de manera fraudulenta a las aplicaciones utilizando el identificador y contraseña de otro usuario que sí dispone de dicho acceso.

Cuando se combina este sistema junto con algún otro de tipo biométrico, como, por ejemplo, reconocimiento de huella dactilar, se consigue una altísima seguridad en el acceso a los datos, sin que el usuario tenga que recordar (e incluso saber) ninguna contraseña. De esta forma, además, se evita la suplantación de la identidad y el acceso no autorizado a los datos por una tercera persona.

10.3.1.5.5 Caducidad de las contraseñas

La periodicidad de cambio de las contraseñas deberá detallarse en el Documento de Seguridad, y nunca será superior a un año.

10.3.1.5.6 Políticas de seguridad en los sistemas operativos

A fin de gestionar de manera automática las políticas de seguridad de la organización, en los sistemas operativos modernos es posible configurar las directivas de seguridad, definiendo el tamaño y la complejidad de la contraseña, período de caducidad, bloqueo de cuenta y demás aspectos relacionados.

10.3.1.6 COPIAS DE RESPALDO Y RECUPERACIÓN

1. Se debe realizar copia de respaldo de los datos, al menos una vez por semana, salvo que en ese tiempo no se haya producido ninguna actualización de los datos.

2. Será posible recuperar los datos en el mismo estado que estaban antes de la pérdida o destrucción.

3. El responsable del fichero verificará, al menos cada seis meses, la validez del sistema de copia de seguridad en cuanto a programación y funcionamiento.

4. Las pruebas previas a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad de los datos, se anote su realización en el Documento de Seguridad y se haya realizado antes una copia de seguridad de los datos.

10.3.1.6.1 Finalidad

Es necesario establecer procedimientos de copia de respaldo para los datos automatizados que garanticen su recuperación frente a pérdidas o destrucción.

Independientemente de la existencia de una ley de obligatorio cumplimiento, a toda organización le interesa mantener una copia de seguridad de los datos que le son necesarios para la realización de su actividad, de forma que pueda recuperar el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

10.3.1.6.2 Copias de respaldo y recuperación

Se deberá mantener copia de seguridad de los datos personales actualizados, al menos de forma semanal, salvo que en dicho período no se haya producido ninguna actualización de datos.

El procedimiento de copia de seguridad deberá estar documentado formalmente en el Documento de Seguridad. Puede existir un único procedimiento para todos los ficheros, o un procedimiento distinto para cada uno de los ficheros, atendiendo tanto al nivel de los datos tratados como a su criticidad y al esfuerzo de reconstrucción en caso de pérdida de éstos.

El procedimiento de copia de seguridad descrito en el Documento de Seguridad deberá incluir, como mínimo, los siguientes datos:

- Los ficheros con datos de carácter personal incluidos.
- Procedimiento detallado de realización.
- Programación o periodicidad.

La diferencia entre la fecha de la pérdida y la fecha de la copia de seguridad marcará el esfuerzo de reconstrucción de los datos, ya que se deberá reconstruir de forma manual la información introducida o actualizada entre estas fechas. En caso de tener que realizar dicha introducción manualmente, deberá quedar constancia motivada de este hecho en el Documento de Seguridad.

El procedimiento de recuperación de datos deberá garantizar su reconstrucción en el estado en que se encontraban los datos al momento de producirse la pérdida o destrucción.

Métodos de realización de copias de seguridad

La realización de copias de seguridad se podrá realizar, de forma general, de dos formas:

- **Manual.** La persona designada para realizar la copia de seguridad realizará de forma manual la copia de seguridad, con la periodicidad descrita en el Documento de Seguridad. La copia de seguridad se podrá realizar en diversos medios: CD, DVD, cinta, disco duro externo, memoria USB, etc.

- **Automática.** A través de la utilidad de copia de seguridad del propio sistema operativo o de otras utilidades disponibles en el mercado. Se podrá programar la realización automática de la copia de seguridad, asegurando su realización frente al olvido de la copia manual. Es conveniente, no obstante, revisar periódicamente que, efectivamente, se está realizando la copia en los intervalos programados.

10.3.1.6.3 Verificación de los procedimientos

Cuando se ha producido una pérdida de datos y se echa mano de la copia de seguridad, es relativamente frecuente comprobar que o bien los datos incluidos en la copia de seguridad no incluyen todos los ficheros que creíamos o la información que contienen está corrupta. Esto último, en sistemas de cinta, es extremadamente frecuente debido a la degradación que sufren con el uso y a la no sustitución de las mismas en el plazo que marca el fabricante.

Con objeto de evitar este escenario, que hace imposible la reconstrucción de los datos en el momento en que se encontraban al producirse la pérdida, se establece que el responsable del fichero debe verificar, al menos semestralmente, la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de datos.

La verificación de los procedimientos de copia de respaldo deberá incluir:

- Revisión de los ficheros incluidos en la copia de seguridad.
- Verificación de su realización, según la programación descrita en el Documento de Seguridad.
- Recuperación de algún fichero en una ubicación alternativa, de forma que tengamos la garantía de que vamos a poder recuperar los datos el día que los necesitemos.

10.3.1.6.4 Pruebas con datos reales

Siempre que se realice una implantación o una modificación de los sistemas de información que traten con ficheros de carácter personal, las pruebas que sea necesario realizar no se efectuarán con datos reales, salvo que se asegure el nivel de seguridad que corresponde al fichero tratado, se anote su realización en el Documento de Seguridad y, previamente, se haya realizado una copia de seguridad.

10.3.1.6.5 Registro de la recuperación de datos

La pérdida o destrucción de los datos de carácter personal de un fichero es una incidencia grave, y como tal debe quedar registrada en el registro de incidencias habilitado en la organización.

En dicho registro se deberán incluir las circunstancias de la pérdida o destrucción, los ficheros afectados y los datos que se han recuperado.

En caso de tener que grabar datos manualmente, quedará constancia de esto incluyendo los datos que han sido necesarios grabar a mano.

10.3.2 Medidas de seguridad de nivel medio

10.3.2.1 RESPONSABLE DE SEGURIDAD

1. Se deben designar uno o más responsables de seguridad, encargados de coordinar y controlar las medidas definidas en el Documento de Seguridad.

2. Esta figura puede ser única para el conjunto de ficheros y tratamientos o diferenciada por los sistemas de información.

3. La responsabilidad sobre el incumplimiento de las medidas de seguridad no recae sobre el responsable de seguridad, sino sobre el responsable del fichero.

10.3.2.1.1 Finalidad

La figura del responsable (o responsables) de seguridad surge de la necesidad de que en la organización haya alguien que vele por el cumplimiento de las medidas de seguridad y colabore con el responsable del fichero en la difusión del Documento de Seguridad. Esta figura tendrá más relevancia cuanto mayor sea la organización.

10.3.2.1.2 Responsable de seguridad

Aunque el reglamento exige la designación del responsable de seguridad a partir del nivel medio, puede ser necesaria esta figura desde nivel básico dependiendo del tamaño de la organización.

Es importante que la designación del responsable o responsables de seguridad se realice sobre personas y puestos que tengan cierta relevancia en la organización y no sobre personal puramente técnico, ya que deberá tener cierta capacidad «reprendedora» sobre las acciones que infrinjan las medidas de seguridad establecidas.

10.3.2.1.3 Responsabilidades

Las principales funciones del responsable de seguridad son:

- Habilitar el registro de incidencias a disposición de todos los usuarios.
- Colaborar con el responsable del fichero en la difusión y comprensión del Documento de Seguridad y, en especial, las funciones y obligaciones del personal.
- Coordinar la puesta en marcha de las medidas de seguridad y controlar el cumplimiento de las mismas.
- Analizar las incidencias registradas y, en colaboración con el responsable del fichero, poner en marcha las medidas correctoras necesarias que limiten estas incidencias en el futuro.
- Comprobar periódicamente:
  - Que el Documento de Seguridad esté actualizado.
  - La correcta y efectiva realización de las copias de seguridad.
  - La validez de la lista de usuarios y las autorizaciones pertinentes.
  - El correcto cumplimiento de lo previsto con las entradas y salidas de datos, en soporte, papel y de forma electrónica.
- Definirá el plan de auditorías y analizará los informes de auditoría, proponiendo medidas al responsable del fichero.
- Controlará directamente los mecanismos que registren los accesos a los ficheros de carácter personal que requieren medidas de nivel alto, además de analizar mensualmente la información registrada al respecto y emitir un informe al responsable del fichero con las conclusiones obtenidas.

10.3.2.2 AUDITORÍA

- A partir del nivel medio, y de forma bianual, se deberá realizar una auditoría que verifique el correcto cumplimiento tanto de la ley como del reglamento.
- Deberá realizarse también cuando se realicen modificaciones sustanciales en los sistemas de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.
- El informe de auditoría deberá:
  - Dictaminar sobre la adecuación de las medidas y controles a la LOPD y RLOPD.
  - Identificar las deficiencias que puedan existir.
  - Proponer medidas correctoras o complementarias.
  - Incluir datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.
- Los informes de auditoría serán analizados por el responsable de seguridad, que elevará las conclusiones al responsable del fichero.
- Los informes de auditoría deberán quedar a disposición de la AEPD.

10.3.2.2.1 Finalidad

Revisar periódicamente el cumplimiento dentro de la organización de su correcta adecuación a la LOPD y a su reglamento de desarrollo.

Obtener un análisis de las deficiencias encontradas, así como de las medidas correctoras o complementarias necesarias.

10.3.2.2.2 Auditoría

A partir del nivel medio, y de forma bianual, se deberá realizar una auditoría de los sistemas de información y las instalaciones de tratamiento y almacenamiento de datos. Esta auditoría deberá verificar el cumplimiento tanto de la ley como de su reglamento de desarrollo.

Desde el punto de vista informático y técnico, se deberán analizar los sistemas de información y su ubicación, y la correcta implantación de las medidas que les correspondan según el nivel de seguridad requerido por los ficheros que tratan.

Desde el punto de vista jurídico, se deberán analizar las cláusulas informativas, los documentos de recogida de datos, los contratos suscritos por la organización, etc.

Por tanto, para que la auditoría se realice en las debidas condiciones es preciso que la persona que realice la auditoría disponga tanto de conocimientos informáticos como jurídicos, o bien que se realice por un equipo que integre profesionales tanto del campo de la informática como del derecho.

La auditoría puede realizarse tanto por personal interno de la misma organización como por personal externo perteneciente otra empresa. En cualquier caso, deberá realizarse por personal independiente y debidamente cualificado.

Aunque la periodicidad ordinaria es de dos años, se deberá realizar de forma extraordinaria si los cambios que se realizan en los sistemas de información son sustanciales. En este caso, el cómputo de dos años se reinicia de nuevo.

10.3.2.2.3 El informe de la auditoría

La pieza clave de la auditoría realizada es el informe de auditoría. Recordemos que éste deberá:

1. Dictaminar sobre la adecuación de las medidas y controles a la ley y su reglamento de desarrollo.

2. Identificar las deficiencias encontradas.

3. Proponer medidas correctoras o complementarias necesarias.

4. Incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

Como se puede desprender de todos estos requisitos, el informe de auditoría es sumamente completo, tanto del punto de vista informático como jurídico. Se deberán justificar debidamente todas las conclusiones y recomendaciones propuestas.

El informe de auditoría debe ser analizado por el responsable de seguridad, que elevará sus conclusiones al responsable del fichero para que adopte las medidas adecuadas.

Este informe deberá quedar a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas. Esto no significa que haya que remitirlo ninguna entidad, sino que el responsable del fichero deberá *conservarlo* y proporcionarlo ante una eventual petición del mismo.

10.3.2.3 GESTIÓN DE SOPORTES Y DOCUMENTOS

- Debe existir un registro de entrada y salida de soportes y documentos.
- El registro de entrada deberá incluir:
  - Tipo de documento o soporte.
  - Fecha y hora.
  - El emisor.
  - Número de documentos o soportes incluidos en el envío.
  - Tipo de información que contienen.
  - La forma de envío.
  - La persona responsable de la recepción que deberá estar debidamente autorizada.
- El registro de salida deberá incluir:
  - Tipo de documento o soporte.
  - Fecha y hora.
  - El receptor.
  - Número de documentos o soportes incluidos en el envío.
  - Tipo de información que contienen.
  - La forma de envío.
  - La persona responsable de la entrega que deberá estar debidamente autorizada.

10.3.2.3.1 Finalidad

Para poder tener controlada la información de carácter personal que entra y sale de la organización, así como garantizar una trazabilidad respecto a la misma, es preciso disponer de un registro de entrada y salida de dicha información.

10.3.2.3.2 Registro de entrada y salida

Se amplían las medidas de nivel básico recogidas anteriormente respecto a la gestión de soportes y documentos.

Deberán quedar registradas todas las entradas y salidas de soportes y/o documentos de las instalaciones del responsable del fichero. Para ello se deberá completar el registro de entradas y salidas correspondiente a tal efecto.

Esto incluye tanto las entradas y salidas de documentos y soportes manuales (CD, disco duro externo, memoria USB, etc.) como las salidas que se realicen a través de correo electrónico.

Registro de entradas y salidas en papel

En caso de habilitar un registro de incidencias en papel, se anexarán al Documento de Seguridad los registros que se van produciendo.

Registro de entrada y salidas automatizado

Se podrá crear también un registro de entradas y salidas en soporte informático a través de alguna aplicación de hoja de cálculo o base de datos, que nos permita al acceso a su información de forma cómoda y nos facilite efectuar listados.

En caso de gestión automatizada, debemos hacer constar en el Documento de Seguridad el sistema informático utilizado. Así mismo, es conveniente imprimir periódicamente los movimientos registrados y anexarlos al Documento de Seguridad.

Debemos incluir en el proceso de copia de seguridad de la organización la salvaguarda de dicho registro.

El acceso a dicho registro deberá estar limitado exclusivamente al personal autorizado, con objeto de evitar su alteración por terceras personas.

10.3.2.3.3 Consideraciones especiales

Aunque el reglamento de la LOPD sólo se alude como medio de transporte de información a través de redes de comunicaciones, los ficheros comprendidos y/o anexos a un correo electrónico, debemos recordar que también es posible transportar datos por otros medios, como FTP o mensajería instantánea. Está dentro de la lógica y del espíritu de la ley registrar estas entradas y salidas de la misma forma que se registran las que se producen a través de correo electrónico.

10.3.2.4 IDENTIFICACIÓN Y AUTENTICACIÓN

Se deberá implementar un mecanismo que limite el número de intentos no autorizados para acceder al sistema de información.

10.3.2.4.1 Finalidad

Evitar que una persona pueda acceder a un sistema de información utilizando el sistema de prueba y error hasta averiguar la contraseña de acceso.

10.3.2.4.2 Limitar el número de intentos para acceder al sistema operativo

Entre las políticas de seguridad que llevan incorporadas los sistemas operativos actuales, una de ellas es la posibilidad de definir el número de intentos fallidos antes de que se bloquee el acceso al usuario y no le permita más intentos. También se puede establecer el tiempo que ese usuario va a permanecer bloqueado antes de que pueda volver a intentar el acceso al sistema.

Configurando adecuadamente estos dos parámetros, junto con los descritos anteriormente en cuanto a la construcción de la contraseña en lo relativo a longitud, complejidad y número de contraseñas que recuerde el sistema para no repetir, se puede asegurar un nivel de seguridad muy alto frente a accesos por personas no autorizadas.

Aunque el artículo no establece cuántas veces se puede intentar el acceso antes de que el mecanismo lo impida, lo habitual es establecer esta limitación a tres intentos.

10.3.2.4.3 El acceso a las aplicaciones de gestión

Cada vez hay más aplicaciones de gestión que incorporan políticas de seguridad en cuanto a la limitación del número de intentos de acceso fallidos.

En caso de que las aplicaciones de gestión utilizadas y que acceden a ficheros con datos de carácter personal permitan definir tal limitación, se deberá habilitar el número de intentos de acceso fallidos, al igual que se realiza con el acceso sistema operativo.

10.3.2.5 CONTROL DE ACCESO FÍSICO

Exclusivamente, el personal autorizado podrá acceder a las dependencias (oficinas, despachos, centro de datos, etc.) donde se encuentran los equipos físicos

(ordenadores, portátiles, etc.) que dan soporte a los sistemas de información que acceden a datos de carácter personal.

10.3.2.5.1 Finalidad

Restringir el acceso físico a los equipos únicamente al personal autorizado.

10.3.2.5.2 Control de acceso físico

Los lugares y dependencias que albergan los equipos que dan acceso a los sistemas de información con datos de carácter personal deberán tener acceso restringido; sólo el personal autorizado en el Documento de Seguridad podrá acceder a ellos.

Para garantizar esta limitación de acceso, los equipos físicos deberán estar en espacios cerrados en los que sólo disponga de acceso a ellos el personal debidamente autorizado.

10.3.2.6 REGISTRO DE INCIDENCIAS

- En el registro de incidencias de la organización deberán figurar, además de los existentes, los siguientes datos:
  - Procedimientos realizados de recuperación de datos.
  - Persona que ejecutó el proceso.
  - Datos restaurados.
  - Datos que han sido grabados manualmente en el proceso de recuperación.
- Para ejecutar los procedimientos de recuperación de datos será necesaria la autorización del responsable del fichero.

10.3.2.6.1 Finalidad

La recuperación de datos es un proceso delicado que suele darse a raíz de una incidencia grave, como la pérdida o destrucción de un equipo o soporte.

A partir del nivel medio, con datos de un mayor nivel de profundidad personal, es necesario detallar al máximo el proceso de recuperación, así como la persona que lo ejecutó, los datos que se han podido restaurar y los que se han tenido que grabar manualmente; también la autorización del responsable del fichero para la ejecución de los procedimientos.

10.3.2.6.2 Registro de incidencias

Esta medida añade una serie de datos adicionales que debe recoger el registro de incidencias.

En el registro de incidencias de la organización deben constar los siguientes datos:

- Tipo de incidencia.
- Fecha y hora en que se ha producido o detectado.
- Persona que realiza la notificación.
- A quién lo notifica.
- Efectos derivados de la incidencia.
- Medidas correctoras aplicadas.
- Procedimientos realizados de recuperación de datos.
- Persona que ejecutó el proceso.
- Datos restaurados.
- Datos que han sido grabados manualmente en el proceso de recuperación.

10.3.2.6.3 Autorización del responsable del fichero

Previamente a la ejecución de los procedimientos de recuperación, será necesaria la autorización del responsable del fichero.

10.3.2.6.4 Grabación manual de datos

En caso de pérdida o destrucción de ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita la reconstrucción de los datos al estado que se encontraban al tiempo de producirse la pérdida, se deberá proceder a grabar manualmente los datos, quedando constancia en el Documento de Seguridad.

10.3.3 Medidas de seguridad de nivel alto

10.3.3.1 GESTIÓN Y DISTRIBUCIÓN DE SOPORTES

- 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 las personas.

- La distribución de soportes que contengan datos personales se hará cifrando dichos datos, o mediante cualquier otro mecanismo que garantice que la información contenida no pueda ser accesible o manipulada cuando sea transportada fuera de los locales del responsable del fichero.

- De la misma forma, se deberán cifrar los datos que contengan los portátiles cuando se encuentran fuera de las instalaciones del responsable del fichero.

- Se evitará el uso de dispositivos portátiles en los que no se puedan cifrar los datos. Si es imprescindible el uso de este tipo de dispositivos, esta circunstancia debe constar en el Documento de Seguridad y se adoptarán las medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

10.3.3.1.1 Finalidad

Garantizar la protección de los datos de carácter personal especialmente comprometedores de dos formas:

- Evitando que personas no autorizadas identifiquen los soportes que contienen este tipo de datos.

- Cifrando la información que está fuera de las instalaciones del responsable del fichero, de forma que personas no autorizadas no puedan acceder a ella durante el transporte.

10.3.3.1.2 Cifrado

Se deberán cifrar tanto los soportes como los datos contenidos en los portátiles cuando salgan fuera de las instalaciones del responsable del fichero.

Si no es posible cifrar la información, se hará constar en el Documento de Seguridad y se adoptarán medidas compensatorias.

10.3.3.2 COPIAS DE RESPALDO Y RECUPERACIÓN

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación en un lugar diferente a los locales del responsable del fichero.

10.3.3.2.1 Finalidad

Proteger los datos de carácter personal de su pérdida o destrucción como consecuencia de desastres, como fuego, inundación, robo, etc., de forma que podamos recuperar los datos.

10.3.3.2.2 Dónde ubicar la copia

Debemos tener en cuenta la distancia de la copia respecto a los sistemas principales, de forma que guardar una copia en otra planta de un mismo edificio no los salvaría de un eventual incendio, perdiéndose igualmente los datos.

Debemos colocar la copia lo más alejada posible de los locales principales.

Actualmente, diversas empresas nos pueden proveer de un servicio de copia remota, aunque no debemos olvidar que debemos suscribir con dichas empresas el correspondiente contrato de encargado del tratamiento, ya que estamos depositando unos datos personales en sus sistemas.

10.3.3.3 REGISTRO DE ACCESOS

- 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.
  - Si ha sido autorizado o denegado.
- En caso de ser autorizado, se deberá guardar la información que permita identificar el registro accedido.
- El responsable de seguridad controlará los mecanismos, sin que puedan desactivarse o manipularse.
- El período mínimo de conservación de los datos registrados será de dos años.
- El responsable de seguridad revisará al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

- No será necesario dicho registro en caso de que concurran las siguientes circunstancias:
  - Que el responsable del fichero sea una persona física.
  - Que el responsable del fichero garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias deberá hacerse constar en el Documento de Seguridad.

10.3.3.3.1 Finalidad

Tener un historial de accesos a los ficheros que permita conocer la persona que ha realizado el acceso, así como el momento y el registro accedido.

Detectar intentos de acceso no autorizados a información sensible.

10.3.3.3.2 Informe

Para poder detectar intentos de acceso no autorizado, así como accesos extraños al fichero, es necesario que el responsable de seguridad analice periódicamente la información registrada y realice un informe que recoja las revisiones realizadas y los problemas detectados. Informe que deberá remitir al responsable del fichero para que aplique medidas en caso de ser necesario.

Dicho informe deberá realizarse con una *periodicidad mensual*.

10.3.3.3.3 Excepciones

En caso de que el responsable del fichero sea una persona física, y sólo él tenga acceso a los datos, es innecesario dicho registro de accesos. Estas circunstancias deberán constar en el Documento de Seguridad.

10.3.3.3.4 Comentarios

A la hora de adquirir un programa que gestione datos especialmente protegidos debemos asegurarnos de que cumple este requisito; de lo contrario, no permitirá el cumplimiento de la ley, y esto podría acarrearnos sanciones.

Además, el reglamento de la LOPD, en su disposición adicional, establece que los productos de *software* destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad —básico, medio o alto— que permiten alcanzar.

En el futuro, antes de adquirir un nuevo *software*, además de revisar las funcionalidades propias de la aplicación, deberemos estar atentos al nivel de seguridad que permiten alcanzar en cuanto al cumplimiento de la LOPD.

10.3.3.4 TELECOMUNICACIONES

La transmisión de datos de carácter personal de nivel alto a través de redes públicas o inalámbricas de comunicaciones se hará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

10.3.3.4.1 Finalidad

Garantizar que los datos personales transmitidos por redes de comunicaciones no sean accedidos ni manipulados por terceras personas no autorizadas; y en caso de que alguien intercepte los datos enviados, que le sea imposible acceder a la información.

10.4 MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS

Las siguientes medidas de seguridad se aplican a ficheros y tratamientos no automatizados.

10.4.1 Medidas de seguridad de nivel básico

10.4.1.1 OBLIGACIONES COMUNES

A los ficheros con datos de carácter personal no automatizados les será de aplicación las disposiciones aplicables con carácter general a los ficheros automatizados, en concreto:

1. Alcance.
2. Niveles de seguridad.
3. Encargado del tratamiento.
4. Prestaciones de servicios sin acceso a datos personales.
5. Delegación de autorizaciones.
6. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
7. Copias de trabajo de documentos.
8. Documento de Seguridad.

Así mismo, se le aplicará lo establecido por las medidas de seguridad de nivel básico para ficheros automatizados en lo relativo a:

1. Funciones y obligaciones del personal.
2. Registro de incidencias.
3. Control de acceso.
4. Gestión de soportes.

10.4.1.2 CRITERIOS DE ARCHIVO

- El archivo de soportes y documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación.

- Estos criterios deben garantizar:
  - La conservación de los documentos.
  - La localización y consulta de la información.
  - Posibilitar el ejercicio de los derechos ARCO.

- En los casos en que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

10.4.1.2.1 Finalidad

La finalidad es que la organización tenga unos criterios bien definidos para el archivo de los soportes y documentos, de forma que se garantice la conservación y localización de la información, así como el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

10.4.1.3 DISPOSITIVOS DE ALMACENAMIENTO

- Los dispositivos de almacenamiento de los documentos deberán disponer de mecanismos que obstaculicen su apertura.

- Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero adoptará medidas que impidan el acceso de personas no autorizadas.

10.4.1.3.1 Finalidad

Preservar la confidencialidad de los documentos, limitándose el acceso a las personas autorizadas.

10.4.1.3.2 Dispositivos de almacenamiento

Estos dispositivos pueden ser armarios, cajones, archivadores, etc., siempre que dispongan de cerradura o dispositivo similar que permita bloquear su apertura.

10.4.1.4 CUSTODIA DE SOPORTES

Mientras la documentación no se encuentre archivada en los dispositivos de almacenamiento, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

10.4.1.4.1 Finalidad

Preservar la confidencialidad de los documentos.

10.4.1.4.2 Custodia de soportes

La custodia de la documentación exige el compromiso de la persona que se encuentra al cargo de la misma, que tiene el deber de guardarla y protegerla.

10.4.2 Medidas de seguridad de nivel medio

10.4.2.1 RESPONSABLE DE SEGURIDAD

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas para las medidas de seguridad aplicables a los ficheros automatizados de nivel medio.

10.4.2.2 AUDITORÍA

Los ficheros no automatizados que deban sujetarse al nivel medio de medidas de seguridad se someterán, al menos cada dos años, a una auditoría que verifique el cumplimiento de las medidas de seguridad impuestas de la misma forma que se realiza para los ficheros automatizados de nivel medio y que hemos visto anteriormente.

10.4.3 Medidas de seguridad de nivel alto

Se adoptarán para ficheros no automatizados que deban implantarse medidas de seguridad de nivel alto:

10.4.3.1 ALMACENAMIENTO DE LA INFORMACIÓN

- Los armarios, archivadores u otros elementos en los que se almacenen los ficheros deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistema de apertura mediante llave u otro dispositivo equivalente.

- Dichas áreas deberán permanecer cerradas cuando no sea necesario el acceso a los documentos incluidos en el fichero.

- Si por las características físicas de los locales no es posible cumplir con este requisito, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el Documento de Seguridad.

10.4.3.1.1 Finalidad

Preservar la confidencialidad de los documentos, estableciendo como medida adicional que los elementos en los que se almacenan los ficheros deberán estar en recintos cerrados y a los que sólo puede acceder el personal que dispone de la llave que facilita la apertura de la puerta que da acceso al recinto.

10.4.3.2 COPIA O REPRODUCCIÓN

- La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el Documento de Seguridad.

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

10.4.3.2.1 Finalidad

Proteger la información más sensible de la difusión indiscriminada, así como asegurar su destrucción cuando es desechada.

10.4.3.3 ACCESO A LA DOCUMENTACIÓN

- Sólo el personal autorizado podrá acceder a la documentación.
- Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
- El acceso de personas no autorizadas deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido para ello en el Documento de Seguridad.

10.4.3.3.1 Finalidad

Que sólo el personal autorizado acceda a la documentación, y en caso de que accedan personas no autorizadas, dicho acceso quede registrado.

Cuando los documentos sean utilizados por varias personas, tener un registro de las personas que han accedido a cada documento.

10.4.3.3.2 Implementación

Para implementar el control de acceso a la documentación se podrá utilizar, por ejemplo:

- Plantillas básicas en soporte papel incorporadas al inicio del expediente.
- Registros automatizados en la gestión de entradas y salidas al archivo.
- Cualquier otro sistema o procedimiento que permita alcanzar la finalidad perseguida.

10.4.3.3.3 Comentarios

El trastorno que supone cumplir con esta medida está popularizando las aplicaciones de gestión documental, que permiten registrar todos los accesos que se produzcan a los documentos de forma automática y transparente para el usuario, así como restringir el acceso a los documentos al personal previamente autorizado.

11

LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

«No es la más fuerte de las especies la que sobrevive, ni la más inteligente, sino la más receptiva al cambio».

Charles Darwin

11.1 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

La Agencia Española de Protección de Datos (AEPD) es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa *con plena independencia* de las Administraciones Públicas en el ejercicio de sus funciones.

11.1.1 Misión

La misión de la AEPD es garantizar el cumplimiento de la legislación sobre protección de datos.

11.1.2 Medios

Para el cumplimiento de los fines que tiene encomendados, la AEPD cuenta con los siguientes bienes y medios económicos:

- Las asignaciones que se establezcan anualmente con cargo a los presupuestos generales del Estado.
- Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.
- Cualesquiera otros que legalmente puedan serle atribuidos.

11.1.3 Estructura

La AEPD cuenta con los siguientes órganos:

1. El director.
2. El Consejo Consultivo.
3. El Registro General de Protección de Datos.
4. La Subdirección General de Inspección de Datos.
5. La Secretaría General.

11.1.4 El director

El director dirige la AEPD y ostenta su representación. Es nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto por un período de cuatro años.

El director debe ejercer sus funciones con plena independencia y objetividad, y no estará sujeto a instrucción alguna en el ejercicio de aquéllas.

11.1.5 El Consejo Consultivo

El Consejo Consultivo es un órgano colegiado que asesora al director, y está compuesto por los siguientes miembros:

- Un diputado, propuesto por el Congreso de los diputados.
- Un senador, propuesto por el Senado.
- Un representante de la Administración General del Estado, designado por el Gobierno.
- Un representante de la Administración local, propuesto por la Federación Española de Municipios y Provincias.
- Un miembro de la Real Academia de la Historia, propuesto por ella misma.
- Un experto en la materia, propuesto por el Consejo Superior de Universidades.
- Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.
- Un representante del sector de ficheros privados, propuesto por el Consejo Superior de Cámaras de Comercio.

Los miembros del Consejo Consultivo serán nombrados y cesados por el Gobierno, y desempeñarán su cargo también por cuatro años, salvo renuncia, pérdida de la condición que le habilitó para ser propuesto o cese.

El Consejo Consultivo se reunirá cuando así lo decida el director de la AEPD que, en todo caso, lo convocará cada seis meses o cuando así lo soliciten la mayoría de sus miembros.

El director debe oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

11.2 FUNCIONES DE LA AEPD

Las funciones de la AEPD son:

1. Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial a lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

2. Emitir las autorizaciones previstas en la ley o en sus disposiciones reglamentarias.

3. Dictar, en su caso y sin prejuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la LOPD.

4. Atender a las peticiones y reclamaciones formuladas por las personas afectadas.

5. Proporcionar información a las personas acerca de sus derechos con materia de tratamiento de los datos de carácter personal.

6. 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 la LOPD y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

7. Ejercer la potestad sancionadora en los términos previstos por la LOPD.

8. Informar, con carácter preceptivo, los proyectos y disposiciones generales que desarrollen la LOPD.

9. Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

10. 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 información adicional que el director de la AEPD determine.

11. Redactar una memoria anual y remitirla al Ministerio de Justicia.

12. Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacionales en materia de protección de datos personales.

13. 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 respecto a las infracciones cometidas por las Administraciones Públicas.

14. Cuantas otras le sean atribuidas por normas legales o reglamentarias.

11.3 EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

El Registro General de Protección de Datos (RGPD) es un órgano cuyo objetivo es garantizar la publicidad de la existencia de ficheros de datos de carácter personal, de los tratamientos aplicados a dichos ficheros y de sus principales características; tiene por finalidad hacer posible el ejercicio de los derechos ARCO de los interesados.

Son objeto de inscripción en el RGPD:

- Los ficheros cuyos titulares sean las Administraciones Públicas.
- Los ficheros de titularidad privada.
- Las autorizaciones de transferencias internacionales de datos.
- Los Códigos Tipo.
- Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

Son funciones propias del RGPD:

- Instruir los expedientes de creación, modificación y cancelación de sus asientos.

- Instruir los expedientes de autorización de las transferencias internacionales de datos.
- Rectificar de oficio los errores materiales.
- Expedir certificaciones.
- Publicar una relación anual de los ficheros notificados e inscritos.

11.4 SUBDIRECCIÓN GENERAL DE INSPECCIÓN DE DATOS

La Subdirección General de Inspección de Datos es una unidad dentro de la AEPD que desempeña dos funciones clave para el cumplimiento de la LOPD:

1. La inspección o investigación.
2. La instrucción de los expedientes sancionadores y de los procedimientos de tutela de derechos.

11.4.1 La inspección

La AEPD puede realizar inspecciones de oficio o a instancias de los afectados, pueden ser periódicas o puntuales, de cualquier fichero, de titularidad pública o privada, y pueden realizarse en los locales en los que se hallen los ficheros y en los equipos informáticos correspondientes, recabando tanta información como necesiten para el cumplimiento de sus cometidos.

Los inspectores de la AEPD podrán:

- Solicitar la exhibición o el envío de documentos y datos, así como examinarlos en el lugar en que se encuentren depositados.
- Acceder a los locales donde se encuentran los soportes que contienen datos personales, así como inspeccionar los soportes y equipos físicos utilizados para el tratamiento.
- Requerir el pase de programas y examinar la documentación pertinente al objeto de determinar, en caso necesario, los algoritmos de los procesos que tratan los datos.

- Examinar los sistemas de transmisión y acceso a los datos.
- Realizar auditorías de los sistemas informáticos con miras a determinar su conformidad con las disposiciones de la LOPD.

El responsable del fichero estará obligado a permitir el acceso a los locales en los que se hallen los ficheros y los equipos informáticos previa exhibición de la autorización expedida por el director de la AEPD.

Los funcionarios que ejercen la inspección tienen la consideración de autoridad pública en el desempeño de sus cometidos y están obligados a guardar secreto sobre las informaciones que conozcan en el desempeño de sus funciones, incluso después de haber cesado en las mismas.

La obstrucción al ejercicio de la función inspectora de la AEPD, infracción tipificada como grave, puede estar sancionada con una multa desde los 40.001 a los 300.000 euros.

11.4.2 La instrucción

Corresponde también a la Subdirección General de Inspección de Datos la instrucción de los expedientes, que tratará de determinar las infracciones cometidas en contra de la legislación de protección de datos, a la vez que proponer justificadamente las posibles sanciones que correspondan.

Posteriormente, la resolución de los procedimientos sancionadores corresponde al director.

11.5 INFRACCIONES Y SANCIONES

Los *responsables de los ficheros* y los *encargados de los tratamientos* estarán sujetos al régimen sancionador establecido.

Las infracciones se califican como leves, graves o muy graves, estableciendo multas que van desde los 900 a los 600.000 euros.

11.5.1 Infracciones leves

Son infracciones leves, sancionadas con multa de 900 a 40.000 euros:

- No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta ley o en sus disposiciones de desarrollo.
- No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.
- El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando éstos sean recabados del propio interesado.
- La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el artículo 12 de la LOPD (recordemos que la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará —ni siquiera para su conservación— a otras personas. En el contrato se estipularán, así mismo, las medidas de seguridad que el encargado del tratamiento está obligado a implementar).

11.5.2 Infracciones graves

Son infracciones graves, sancionadas con multa de 40.001 a 300.000 euros:

- Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el Boletín Oficial del Estado o diario oficial correspondiente.
- Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta ley y sus disposiciones de desarrollo.
- Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la LOPD y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave.

- La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la LOPD.
- El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
- El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando éstos no hayan sido recabados del propio interesado.
- El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por la LOPD y sus disposiciones de desarrollo.
- Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
- No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma.
- La obstrucción al ejercicio de la función inspectora.
- La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en la LOPD y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave.

11.5.3 Infracciones muy graves

Son infracciones muy graves, sancionadas con multa de 300.001 a 600.000 euros:

- La recogida de datos en forma engañosa o fraudulenta.
- Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 y 5 del artículo 7 de la LOPD (datos especialmente protegidos y de comisión de infracciones penales o administrativas), salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7 (quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual).

- No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del director de la Agencia Española de Protección de Datos para ello.
- La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria.

11.5.4 Graduación de la cuantía de la sanción

La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:

1. El carácter continuado de la infracción.
2. El volumen de los tratamientos efectuados.
3. La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
4. El volumen de negocio o actividad del infractor.
5. Los beneficios obtenidos como consecuencia de la comisión de la infracción.
6. El grado de intencionalidad.
7. La reincidencia por comisión de infracciones de la misma naturaleza.
8. La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
9. La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
10. A cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

11.5.5 Disminución del grado de la infracción

El órgano sancionador establecerá la cuantía de la sanción, aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate en los siguientes supuestos:

1. Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado anterior.
2. Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
3. Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
4. Cuando el infractor haya reconocido espontáneamente su culpabilidad.
5. Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.

11.5.6 Apercibimiento

Excepcionalmente, el órgano sancionador podrá —previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior— no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:

1. Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta ley.
2. Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado, procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

11.5.7 Prescripción de las infracciones

Las infracciones prescribirán en los siguientes plazos:

- Muy graves: a los tres años.
- Graves: a los dos años.
- Leves: al año.

El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

11.5.8 Prescripción de las sanciones

Las sanciones prescribirán en los siguientes plazos:

- Impuestas por faltas muy graves: a los tres años.
- Impuestas por faltas graves: a los dos años.
- Impuestas por faltas leves: al año.

El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.

La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

11.5.9 Duración del procedimiento sancionador

Los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos, en ejercicio de las potestades que a la misma atribuyan esta u otras leyes, salvo los referidos a infracciones de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, tendrán una duración máxima de seis meses.

11.5.10 Inmovilización de ficheros

En los supuestos constitutivos de infracción grave o muy grave en que la persistencia en el tratamiento de los datos de carácter personal o su comunicación o transferencia internacional posterior pudiera suponer un grave menoscabo de los derechos fundamentales de los afectados y, en particular, de su derecho a la protección de datos de carácter personal, el órgano sancionador podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos.

Si el requerimiento fuera desatendido, el órgano sancionador podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

12

MISCELÁNEA

«Si alguien va cuesta abajo, no necesita motivación para ir más rápido, lo que necesita es educación para cambiar el rumbo».

Jim Rohn

12.1 VIDEOVIGILANCIA

La captación y/o el tratamiento de imágenes con fines de vigilancia es una práctica muy extendida en nuestra sociedad. La utilización de la videovigilancia repercute sobre los derechos de las personas, lo que obliga a fijar una garantías.

La videovigilancia permite la captación y/o grabación de información personal en forma de imágenes. Cuando su uso afecta a personas identificadas o identificables, esta información constituye un dato de carácter personal a efectos de la LOPD.

12.1.1 Aplicación de la LOPD a los tratamientos de imágenes

El concepto de dato personal incluye las imágenes cuando se refieran a personas identificadas o identificables. Por ello, la LOPD debe aplicarse al uso de cámaras, videocámaras y cualquier medio técnico análogo que capte y/o registre imágenes, ya sea con fines de vigilancia, control de personal u otros supuestos en que:

- Exista grabación, captación, transmisión, conservación o almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real o un tratamiento que resulte de los datos personales relacionados con aquéllas.

- Tales actividades se refieran a datos de personas identificadas o identificables.

12.1.2 Legitimación requerida

Para que se pueda utilizar un sistema de esta naturaleza, no basta con que éste reúna los requisitos técnicos que lo permitan funcionar. Debe existir *legitimación* para ello. Esto ocurrirá cuando:

- Se cuente con el consentimiento del titular de los datos personales.

- Una norma con rango de ley exima del consentimiento, como en los casos previstos por la Ley de Seguridad Privada o en el artículo 20 del Estatuto de los Trabajadores.

- Se dé alguna de las circunstancias previstas por el artículo 6.2 LOPD u 11.2 LOPD que resulten de aplicación a este tipo de medios.

Además, si la legislación vigente impone algún requisito adicional, éste deberá cumplirse.

12.1.3 Captación y tratamiento de las imágenes

El uso de videocámaras debe seguir ciertas reglas que rigen todo el proceso desde su captación, almacenamiento, reproducción y cancelación.

El responsable deberá tener en cuenta estos principios:

- Debe existir una relación de *proporcionalidad* entre la finalidad perseguida y el modo en que se traten los datos.

- Debe *informarse* sobre la captación y/o grabación de las imágenes.

- El uso de instalaciones de cámaras o videocámaras sólo es admisible cuando *no exista un medio menos invasivo*.

- Las cámaras y videocámaras instaladas en espacios privados *no podrán obtener imágenes de espacios públicos*.
  - Podrían tomarse imágenes parciales y limitadas de vías públicas cuando resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas.
- En cualquier caso, el uso de sistemas de videovigilancia deberá ser *respetuoso con los derechos* de las personas y el resto del ordenamiento jurídico.
- Las imágenes se conservarán por el *tiempo imprescindible* para la satisfacción de la finalidad para la que se recabaron.

12.1.4 Videovigilancia con fines de seguridad

Es el uso de cámaras con objeto de garantizar la seguridad de los bienes y las personas. Este uso conlleva una serie de obligaciones:

12.1.4.1 INSCRIPCIÓN DE FICHEROS

La utilización de sistemas de vigilancia mediante videocámaras puede dar lugar a la creación de ficheros. En este caso, habrá que notificar el fichero previamente a la AEPD para su inscripción en el RGPD. Esto ocurrirá siempre que exista algún tipo de grabación.

12.1.4.2 EXCEPCIONES

Hay sistemas que no registran imágenes, como los circuitos cerrados de televisión controlados mediante visualización en pantalla.

En este caso, no resulta necesario inscribirlos. Sin embargo, esto no exime del cumplimiento de los deberes establecidos por la LOPD y la instrucción 1/2006, que regula estos tratamientos.

12.1.4.3 DEBER DE INFORMAR

La información en la recogida de los datos es un derecho esencial de la persona y, por tanto, debe cumplirse en todo momento.

Para informar a las personas cuyas grabaciones se capten se debe utilizar un distintivo informativo, cuyo uso y exhibición es obligatorio.

El distintivo se ubicará como mínimo en los accesos a las zonas vigiladas, sean éstos exteriores o interiores. Debe tenerse en cuenta que si el lugar vigilado dispone de varios accesos, se debe colocar en todos ellos, al objeto de que la información sea visible con independencia de por donde se acceda.

Además, el responsable del fichero dispondrá de un impreso con toda la información a la que el interesado tiene derecho:

- De la existencia de un fichero, la finalidad de la recogida de los datos y de los destinatarios de la información.
- De la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del fichero o tratamiento o, en su caso, de su representante.

Este impreso deberá estar disponible, existiendo cuando menos la posibilidad de imprimirlo a petición del afectado.

12.1.4.4 CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS

La implantación de sistemas de videovigilancia puede dar lugar a dos tipos de prestación de servicios por parte de una empresa externa:

- Instalación y/o mantenimiento técnico de los equipos y sistemas de videovigilancia *sin acceso a las imágenes*. En este caso, la empresa de seguridad no posee la condición de encargada del tratamiento. Le corresponde al responsable que la contrató la adaptación de la instalación a los requisitos exigidos por la LOPD.

- Instalación y/o mantenimiento de los equipos y sistemas de videovigilancia con utilización de los equipos o *con acceso a las imágenes.* En este segundo caso, la empresa de seguridad será considerada encargada del tratamiento y debe cumplir con las obligaciones propias del encargado del tratamiento:

  - Formalizar un contrato en los términos dispuestos por la LOPD, cuyo contenido se determina atendiendo a las circunstancias concretas de la prestación del servicio y reflejando la realidad de la prestación realizada.

  - Cumplir las medidas de seguridad exigidas respecto a los datos tratados.

EJEMPLO

Las empresas de seguridad que prestan servicios combinados de central de alarmas y videovigilancia, de modo que cuando se activa la alarma se comprueban directamente las imágenes por el personal de la empresa de seguridad.

12.1.4.5 EMPRESA DE SEGURIDAD SIN ACCESO A LAS IMÁGENES

En los casos en que una empresa de seguridad, con motivo de la prestación de sus servicios, no acceda a las imágenes, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de dicha prestación.

12.1.5 Medidas de seguridad

El responsable de la instalación deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de las imágenes y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Por tanto, quien contrate los servicios de una empresa de seguridad (empresa, comunidad de propietarios, organismo público, etc.), debe cumplir con el deber de garantizar la seguridad de las imágenes en los términos establecidos por la LOPD y su reglamento de desarrollo.

Con carácter general, los ficheros de videovigilancia suelen tener nivel básico. No obstante, el responsable del fichero debe tener en cuenta que deberá evaluar el nivel de seguridad teniendo en cuenta la finalidad y el contenido de ese fichero.

Cualquier persona que en el ejercicio de sus funciones tenga acceso a los datos deberá observar la debida confidencialidad con relación a los mismos. El responsable será el encargado de dar a conocer esto a todo el personal implicado.

12.1.5.1 CANCELACIÓN DE OFICIO DE LAS IMÁGENES

El plazo máximo de cancelación de las imágenes será de *un mes*.

Por tanto, transcurrido este plazo, las imágenes deberán ser canceladas, lo que implica el bloqueo de las mismas, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo, deberá procederse a su supresión.

12.1.5.2 USO DE VIDEOCÁMARAS CON FINES DE CONTROL EMPRESARIAL

El artículo 20.3 del Estatuto de los Trabajadores faculta al empresario a adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. Entre estas medidas pueden estar la captación y/o tratamiento de imágenes *sin consentimiento*.

No obstante, tales prácticas se encuentran sometidas a la LOPD y la Instrucción 1/2006 de la AEPD, y deben cumplir con unos requisitos específicos:

- El tratamiento se limitará a las finalidades previstas por el Estatuto de los Trabajadores y/o, en todo caso, a finalidades legítimas reconocidas por la normativa vigente, debiendo cumplir en este último caso, adicionalmente, las previsiones específicas que sean de aplicación.
- Se respetará de modo riguroso el principio de proporcionalidad.
- Tendrán en cuenta los derechos específicos de los trabajadores.
- Se garantizará el derecho a la información en la recogida de las imágenes.
- Se procederá, en su caso, a la creación y/o inscripción del correspondiente fichero en el RGPD.
- Se garantizará la cancelación de las imágenes en el plazo máximo de 30 días, y únicamente podrán conservarse aquellas que registren una infracción o incumplimiento de los deberes laborales.
- Se garantizarán los derechos de acceso y cancelación.
- Se formalizarán, en su caso, los contratos de acceso a los datos por cuenta de terceros.
- Se adoptarán las correspondientes medidas de seguridad.

12.1.6 Conclusiones

Como se ha podido ver en este epígrafe, la captación de imágenes por cámaras, videocámaras y otros dispositivos similares está regulada mediante la LOPD, su reglamento de desarrollo y la Instrucción 1/2006 de la AEPD.

En función de la finalidad que se va a dar las imágenes captadas, existen una serie de obligaciones específicas que están reguladas y deben ser cumplidas, tanto por el responsable del fichero como por el encargado del tratamiento, si existe.

Antes de proceder a la captación de las imágenes, es necesario revisar la normativa vigente y adecuar el tratamiento a la misma.

12.2 TRATAMIENTOS PARA ACTIVIDADES DE PUBLICIDAD Y PROSPECCIÓN COMERCIAL

Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas utilizarán nombres y direcciones u otros datos de carácter personal cuando:

- Los mismos hayan sido obtenidos de *fuentes accesibles al público*, y el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento para estas actividades.

- O cuando hayan sido *facilitados* por los propios interesados u obtenidos con su *consentimiento* para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, habiéndose informado a los interesados de los sectores específicos y concretos de la actividad respecto a los que se podrá recibir información o publicidad.

12.2.1 Fuentes accesibles al público

Sólo tendrán el carácter de fuentes accesibles al público las siguientes:

- El censo promocional.

- Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.

- Las listas de personas pertenecientes a grupos profesionales que contengan únicamente los siguientes datos: nombre, título, profesión, actividad, grado académico e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.

- Los diarios y boletines oficiales.

- Los medios de comunicación social.

En todo caso, para que los supuestos enumerados puedan ser considerados fuentes accesibles al público será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación.

12.2.2 INFORMACIÓN AL AFECTADO

Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, deberá informarse al interesado *en cada comunicación* que se le dirija de los siguientes extremos:

1. Del origen de los datos.
2. De la identidad del responsable del tratamiento.
3. Los derechos que le asisten (acceso, rectificación, cancelación y oposición).
4. Ante quién puede ejercer dichos derechos.

A tal efecto, el interesado deberá ser informado de que sus datos han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos.

12.2.3 Ficheros de exclusión del envío de comunicaciones comerciales

Los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

12.2.4 Ficheros comunes de exclusión

Será posible la creación de ficheros comunes de exclusión, en los que sean objeto de tratamiento los datos personales que resulten necesarios para evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad.

Cuando un afectado manifieste ante un responsable concreto su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, deberá ser informado de la existencia de los ficheros comunes de exclusión, así como de la identidad de su responsable, su domicilio y la finalidad de su tratamiento.

El afectado podrá solicitar su exclusión respecto de un fichero concreto o su inclusión en ficheros comunes de excluidos de carácter general o sectorial.

Quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán, previamente, consultar los ficheros comunes que pudieran afectar a su actuación, a fin de evitar que sean tratados los datos de los afectados que hubiesen manifestado su oposición o negativa a ese tratamiento.

12.3 LOS CÓDIGOS TIPO

Los Códigos Tipo son acuerdos sectoriales, convenios administrativos o decisiones de empresa en los que se establecen —en función de los principales problemas de un determinado sector para cumplir la normativa sobre protección de datos— unas pautas de actuación, así como una definición de criterios uniformes de aplicación de la LOPD entre las organizaciones agrupadas a dicho Código Tipo.

Los Códigos Tipo tienen el carácter de códigos deontológicos o de buena práctica profesional, y son vinculantes para quienes se adhieran a los mismos.

12.3.1 Objetivo

EL objetivo de los Códigos Tipo es redactar y cumplir las mejores prácticas de la LOPD en las organizaciones agrupadas.

Para ello, los Códigos Tipo deben:

- Identificar los principales problemas de un sector determinado para cumplir la normativa sobre protección de datos.
- Concretar criterios específicos de aplicación de la normativa.
- Definir la aplicación de las medidas de seguridad, atendiendo los riesgos de ese sector concreto.

12.3.2 Contenido

Los Códigos Tipo deberán contener:

- Condiciones de organización para garantizar la LOPD.
- Régimen de funcionamiento.

- Procedimientos aplicables.
- Normas de seguridad del entorno, programas o equipos.
- Obligaciones de los implicados en el tratamiento y uso de la información personal.
- Las garantías para el ejercicio de los derechos ARCO de los interesados.

12.4 TRANSFERENCIA INTERNACIONAL DE DATOS

Una Transferencia Internacional de Datos (TID) es depositar o revelar los datos de carácter personal que la organización está tratando a una entidad que está en otro país, ya sea lo que esté haciendo, una cesión de datos o un acceso a datos por cuenta de terceros (encargado del tratamiento).

12.4.1 Norma general

Para efectuar una transferencia internacional de datos de carácter personal será precisa la *autorización previa del director* de la AEPD.

12.4.2 Excepciones

La autorización para la transferencia internacional de datos de carácter personal no será necesaria cuando:

- El Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección a juicio del director de la AEPD o la Comisión Europea.

  A través de la web de la Agencia (www.agpd.es) se puede consultar la relación de países aprobados.
- Resulte de la aplicación de tratados o convenios en los que sea parte España.
- Se haga a efectos de prestar o solicitar auxilio judicial internacional.
- Sea necesaria para la prevención o para el diagnóstico médico la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios.

- Se refiera a transferencias dinerarias conforme a su legislación específica.
- El afectado *haya dado su consentimiento inequívoco* a la transferencia prevista.
- Sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
- Sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
- Sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
- Sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

12.4.3 Notificación

Sea necesaria o no la autorización del director de la AEPD, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, siguiendo el procedimiento establecido a tal efecto.

12.4.4 Conclusiones

Estamos en un mundo globalizado, muchas de las operaciones que realizamos a través de Internet pueden suponer, sin nosotros saberlo, una transferencia internacional de datos.

Por ejemplo, supongamos que tenemos contratado un alojamiento para nuestra web con un proveedor de *hosting*. Si la web se utiliza para comercio electrónico, seguramente albergará bases de datos que incluirán datos de carácter personal.

El proveedor de ese *hosting* que alberga las bases de datos es un encargado de nuestro tratamiento, y se debe suscribir el correspondiente contrato de encargado del tratamiento con ese proveedor.

El proveedor, a su vez, debe implantar las medidas de seguridad requeridas por la LOPD con relación a dicho tratamiento y completar su Documento de Seguridad, de forma que incluya el fichero o ficheros que trata en concepto de encargado, la identificación del responsable del fichero, la vigencia del encargo y la referencia del contrato que regula las condiciones del mismo.

Supongamos, además, que ese proveedor nuestro es un revendedor de alojamiento de otro proveedor mayor que está en otro país. Sin nosotros saberlo, las bases de datos en las que estamos guardando los datos personales de nuestros clientes están alojadas en otro país, y estaremos realizando una transferencia internacional de datos *sin tener conocimiento de ello*, con las sanciones tan elevadas que puede suponer esto.

Debemos tener en cuenta todos estos factores, y debemos tener conocimiento, en última instancia, de dónde se alojan nuestros ficheros de datos personales, ya que un desliz en este aspecto puede salir muy caro.

13

SEGURIDAD DE LA INFORMACIÓN

«Invertir en conocimientos produce siempre los mejores beneficios».

Benjamin Franklin

13.1 FUNDAMENTOS DE LA SEGURIDAD DE LA INFORMACIÓN

13.1.1 Introducción

Todas las entidades, empresas, organismos, etc., con el desempeño de su actividad, generan y almacenan información, que puede ser más o menos valiosa.

Pongamos el caso de una empresa. En su actividad diaria genera información en forma de: clientes, proveedores, datos de contacto, pedidos, albaranes, facturas, proyectos, planos, nóminas, listados de ventas, planes estratégicos, desarrollo de productos, etc.

Hay información generada que puede ser muy valiosa para la *actividad de la empresa* (datos de contacto, clientes, pedidos, proyectos, etc.) y cuya pérdida supondría un grave problema para la continuidad de la misma.

Hay también otra información que se genera, como listados de ventas, facturación, planes de *marketing*, desarrollos de productos, estrategias, etc., cuya *revelación a otras empresas o personas* de la competencia podría suponer graves pérdidas económicas.

La información, por tanto, debe considerarse un activo importante con el que cuentan las organizaciones para satisfacer sus objetivos, razón por la cual tiene un alto valor para las mismas y es crítica para su desempeño y subsistencia.

Por tal motivo, al igual que el resto de los activos (como instalaciones, equipamiento, personal, etc.), *debe asegurarse que esté debidamente protegida.*

13.1.2 ¿Contra qué se debe proteger la información?

La información debe ser protegida contra una amplia gama de *amenazas*, como pueden ser:

- Alteraciones eléctricas (picos o cortes de suministro).
- Desastres (fuego, inundación, terremotos, etc.).
- Virus informáticos, *spywares*, troyanos, etc.
- Vandalismo, robo.
- Error humano (usuarios, operadores, programadores, etc.).
- Actos intencionados de dañar.
- Espionaje, filtraciones de información. Pueden ser:
  - Internos: personal propio o subcontratado.
  - Externos: piratas informáticos, *hackers*, etc.

13.1.3 La seguridad de la información

La información es, por tanto, un activo[13] que tiene valor para los procesos de negocio de la empresa.

La seguridad de la información es la protección de la *integridad*, *disponibilidad* y *confidencialidad* de la información, según el nivel requerido para los objetivos de negocio de la empresa.

13.1.3.1 INTEGRIDAD

Es la propiedad de salvaguardar la exactitud y completitud de los datos almacenados.

13 Activo: cualquier bien que tiene valor para la organización.

Consta de dos facetas:

- **Integridad de la información.** Asegurar que la información no haya sido alterada de manera no autorizada durante el almacenamiento, tratamiento o tránsito.
- **Integridad de los sistemas.** Asegurar la calidad de un sistema para cumplir una función definida de manera inequívoca, libre de cualquier manipulación no autorizada.

Es decir, que los datos almacenados reflejen la realidad y no hayan sido manipulados.

13.1.3.2 DISPONIBILIDAD

Es la propiedad de ser accesible y utilizable por una entidad autorizada.

Debemos asegurar que los sistemas funcionen puntualmente y que los servicios no sean denegados a los usuarios autorizados, es decir, que se tenga acceso en todo momento a la información.

13.1.3.3 CONFIDENCIALIDAD

Es la propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.

Asegurar que la información privada o confidencial no esté comunicada a personas no autorizadas, aplicándose durante el almacenamiento, tratamiento o tránsito.

13.1.4 Amenazas, vulnerabilidades y riesgos

13.1.2.1 QUÉ ES UNA AMENAZA

Una amenaza es cualquier evento que pueda afectar a los activos de información que posee la empresa (documentos, sistemas, comunicaciones, etc.) y que pueden afectar a la integridad, disponibilidad o confidencialidad de la información.

Se pueden clasificar en:

- **Intencionadas.** Son declaraciones intencionadas de producir daño. (*spywares*, virus, acceso no autorizado, etc.).
- **No intencionadas.** Es el potencial de que un incidente no querido pueda producir daños a la información. A su vez, pueden ser:
  - **Humanos:** falta de personal, error en las operaciones, descuidos, etc.
  - **Técnicos:** fallo de *hardware* o *software*, saturación del sistema, etc.
- **Desastres.** Pueden ser, a su vez:
  - **Naturales:** inundación, terremoto, huracán, etc.
  - **Intencionados:** vandalismo, fuego, etc.
  - **Accidentales:** fuego no intencionado, choque, etc.

13.1.2.2 QUÉ ES UNA VULNERABILIDAD

Es una necesidad o debilidad en un activo.

Son vulnerabilidades las siguientes:

- La necesidad de suministro eléctrico.
- Un equipo sin antivirus.
- Puertas abiertas (lógicas y físicas).
- Lugar no adecuado.

Una vulnerabilidad, por sí misma, no produce daños. Es un condicionante para que una amenaza afecte a un activo.

Por ejemplo, que esté libre el acceso que da al servidor no produce en sí un daño, pero es un condicionante para que una persona no autorizada acceda al mismo y lo provoque.

13.1.2.3 QUÉ ES EL RIESGO

El riesgo es el potencial de explotación de una vulnerabilidad de un activo por una amenaza.

Dicho con otras palabras, es la probabilidad o posibilidad de que una amenaza dada aproveche una vulnerabilidad para dañar un activo o grupo de activos de información.

Por ejemplo, si tenemos un equipo que accede a Internet y al correo electrónico sin antivirus, la *amenaza* de infección por virus explotará la *vulnerabilidad* del equipo (no tiene antivirus) para causar una infección. En este caso, el *riesgo* de infección es muy alto.

13.1.2.4 INCIDENTE DE SEGURIDAD

Un incidente de seguridad es un evento adverso que puede afectar a un sistema o red de computadoras, ya sea por acción humana, fallo técnico, accidente o desastre natural, y que comprometa o pueda comprometer la integridad, confidencialidad y/o disponibilidad de la información.

Son incidentes de seguridad, entre otros, los siguientes:

- El intento de acceso a los sistemas por alguien no autorizado.
- La salida o el intento de acceso no autorizado a datos.
- La pérdida o sustracción de un soporte con datos.
- La manipulación de la información por alguien no autorizado.

13.1.2.5 POR QUÉ AUMENTAN LAS AMENAZAS

Las amenazas y los incidentes de seguridad están aumentando notablemente debido a los siguientes factores:

- Mayor dependencia de los sistemas, servicios de información y tecnologías asociadas.
- Complejidad y vulnerabilidad de la tecnología empleada.
- Crecimiento exponencial de las redes y usuarios interconectados.
- Volumen de información cada vez más importante.
- Aumento de las bases de datos *on-line*.
- Inmadurez de las nuevas tecnologías.
- Alta disponibilidad de herramientas automatizadas para ataques a la seguridad.
- Técnicas de ingeniería social.
- Falta de concienciación y formación del personal.
- Rentabilidad de los ataques.

13.1.2.6 LA CLASIFICACIÓN DE LA INFORMACIÓN

En la época actual, la información ha alcanzado un valor, en algunos casos, incalculable. Ahora bien, la información no tiene un valor uniforme; hay información trivial y hay información altamente cualificada, y debemos distinguir una de la otra.

A la hora de implantar las medidas de seguridad, hemos de considerar el valor de la información que se va a proteger, ya que no es lo mismo proteger algo muy valioso que una cosa que vale poco.

Para ello es importante clasificar la información dándole el peso que le corresponde, y así protegerla más o menos, en función de su valor.

13.1.2.6.1 Las sensibilidades de la información

A la hora de clasificar la información, es preciso hacerlo sobre la base de lo sensible que sea a su destrucción, modificación o difusión:

1. **Destrucción.** La sensibilidad a su destrucción se refiere al borrado, a no tener disponibles los recursos, datos o programas. Toda la información que es necesaria para la supervivencia del negocio es sensible a su destrucción. Es vital para la supervivencia del negocio que esta información esté debidamente protegida. Esto afecta a la disponibilidad de la información.

2. **Modificación.** La sensibilidad a su modificación se refiere al cambio o manipulación de datos. Los cambios no autorizados de datos atentan contra la integridad de los datos, de forma que éstos no reflejan de manera fehaciente la realidad.

   Hay entidades muy sensibles a esto, como los bancos: ¿qué pasaría si alguien realizase una manipulación y pusiera un cero más en la cuenta de un usuario?. En general, todas las organizaciones que manejen información sensible.

3. **Difusión.** La sensibilidad a su difusión se refiere a los conocimientos que se adquieren a través de la información obtenida. Esta sensibilidad afecta a la confidencialidad de la información, y es proporcional al valor de los datos revelados.

   Información muy sensible a esto pueden ser los planes estratégicos de la empresa, desarrollos industriales, etc.

13.1.2.7 LA CONCIENCIACIÓN DE LOS USUARIOS

Un pilar fundamental en la seguridad de la información es la adecuada concienciación de los usuarios. Sin este ingrediente fundamental, cualquier plan de seguridad implantado está abocado al fracaso.

Hay que tener en cuenta que respetar las medidas de seguridad suele ser molesto, pesado y exige un sobreesfuerzo.

Si los usuarios no están lo bastante concienciados respecto a la finalidad de las mismas, tratarán de evitarlas, y sólo después de sufrir una catástrofe es cuando se darán cuenta de su importancia.

Para prevenir esto es muy importante una buena labor de concienciación, que en un principio conviene que sea externa y, posteriormente, interna y continua, y extensible a todo el personal de la empresa.

El objetivo de todo plan de concienciación es que los usuarios pasen por los siguientes estados, hasta completar el último:

1. **Inconscientemente-Incompetente:** en este estado, el usuario no es consciente de las amenazas ni de los riesgos a que está expuesto.

   Son síntomas de este estado las contraseñas pegadas en el monitor, instalación de programas de intercambio de música, acceso a páginas web de dudosa seguridad, etc.

2. **Conscientemente-Incompetente:** en este estado, el usuario conoce las amenazas y riesgos a los que está expuesto, pero no sabe cómo afrontarlas ni cómo actuar.

3. **Conscientemente-Competente:** el usuario conoce las amenazas y riesgos, y sabe perfectamente cómo actuar.

4. **Inconscientemente-Competente:** el usuario ya ha interiorizado las prácticas que debe seguir para proteger la información, y actúa en todo momento siguiéndolas de forma ya inconsciente.

13.2 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

Frente a la dependencia de los sistemas de información y al crecimiento de las amenazas existentes, se hace necesario para las organizaciones establecer un Sistema de Gestión de Seguridad de la Información.

Hay que tener en cuenta una premisa fundamental: la seguridad no es un producto, es un proceso; por tanto, *la seguridad no puede comprarse, pero puede gestionarse.*

13.2.1 Ventajas de gestionar la seguridad de la información

La Gestión de la Seguridad de la Información aporta a las empresas y organizaciones las siguientes ventajas:

- Evita interrupciones en las cadenas de trabajo, ya sea industrial o trabajos administrativos, con el ahorro de costes que esto trae consigo.
- Descubre fraudes de los propios empleados y los previene.
- Aumenta la calidad del servicio.
- Aumenta la competitividad de la empresa al evitar los riesgos de interrupciones en el ciclo de trabajo.
- Evita fraudes externos, especialmente espionaje industrial, comercial o intelectual de nuestros competidores.
- Disminuye el daño de males mayores, como desastres naturales, robos, incendios o vandalismo.
- Evita sanciones por incumplimiento de normativa, como la LOPD, la propiedad intelectual, etc.

13.2.2 Qué es un Sistema de Gestión de Seguridad de la Información (SGSI)

La seguridad de la información de una empresa u organización debe afrontarse de forma global, no fraccionada y como reacción puntual a algún fallo en la seguridad.

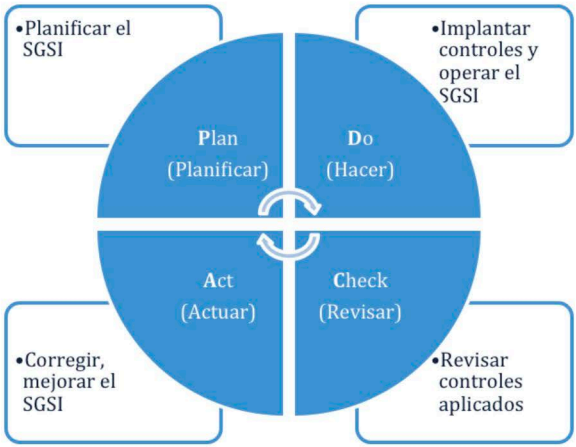
Es un error empezar a implantar medidas de seguridad por departamentos, parcelas o secciones sin tener un conocimiento global de lo que vamos a afrontar. Actuando de esta forma, puede que tengamos áreas muy protegidas y otras, en cambio —que pueden ser más importantes—, desprotegidas.

Podemos considerar que un Sistema de Gestión de Seguridad de la Información es:

Una *estructura organizativa, técnica* y *procedimental* que busca conseguir la seguridad de la información a través de:

- Análisis de la situación y planificación.
- Aplicación de controles.
- Revisión de su funcionamiento.
- Aplicación de mejoras y correcciones.

Esto en un ciclo sin fin (ciclo PDCA), de forma que en cada nueva vuelta se perfecciona el sistema, obteniéndose una mejor gestión de la seguridad de la información.



13.2.3 Cómo se implanta un SGSI

La implantación de un SGSI no es una tarea trivial que se realice en ratos libres, sino que es un proceso metódico, laborioso y costoso que debe ser planificado y justificado.

13.2.4 Fases en la implantación de un SGSI

La implantación de un SGSI exige diferentes tareas para cada una de las fases del ciclo PDCA.

13.2.5 Planificación del SGSI (Plan)

La planificación del SGSI es la parte más importante de su implementación, y recoge las siguientes tareas:

1. Definir los objetivos, propósitos y alcance del SGSI

   En primer lugar, se deben definir los objetivos que se pretenden alcanzar con el SGSI, así como los propósitos y el alcance.

   Por ejemplo, para una entidad que se dedica a tramitar subvenciones:

   - **Objetivo:** asegurar la confidencialidad, integridad y disponibilidad de los expedientes que tramitan.
   - **Propósitos:** nadie ajeno a su tramitación accede a los mismos, asegurando, además, que no hay filtraciones ni manipulación en los mismos, y la disponibilidad de la información, incluso en caso de pérdida total o parcial de la misma.
   - **Alcance:** proceso de tramitación de expedientes de clientes.

2. Valoración de riesgos

   La valoración de los riesgos permite valorar los riesgos a que está expuesta la organización para, posteriormente, tratarlos. Esta valoración conlleva los siguientes pasos:

   - **Valoración de los activos:** se deben valorar adecuadamente los activos de información que se poseen (datos, aplicaciones, equipos, servicios, instalaciones, soportes, personas, etc.).El valor de un activo se refiere al *impacto en el negocio* del daño a un activo de información en cuanto a su Confidencialidad, Integridad y Disponibilidad:
     - Pérdida de ingresos.
     - Cuota de mercado.
     - Imagen de la empresa.
     - Seguridad de las personas.
     - Consecuencias legales, multas, sanciones.
     - Coste de reposición/reconstrucción.
     - Incremento de gastos.

- **Identificar las amenazas** que puedan afectar a los activos.
- **Intencionadas.** Son declaraciones intencionadas de producir daño (*spywares*, virus, acceso no autorizado, etc.).
- **No intencionadas.** Es el potencial de que un incidente no querido pueda producir daños a la información. A su vez, pueden ser:
  - **Humanos:** falta de personal, error en las operaciones, descuidos, etc.
  - **Técnicos**: fallo de *hardware* o *software*, saturación del sistema, etc.
- **Desastres.** Pueden ser, a su vez:
  - **Naturales:** inundación, terremoto, huracán, etc.
  - **Intencionados:** vandalismo, fuego, etc.
  - **Accidentales:** fuego no intencionado, choque, etc.
- **Valoración de las vulnerabilidades** de los activos. Por ejemplo:
  - La necesidad de suministro eléctrico.
  - Equipo sin antivirus.
  - Puertas abiertas (lógicas y físicas).
  - Lugares no adecuados.
- **Valoración del riesgo** para cada uno de los activos. El riesgo es una función de:
  - La probabilidad de que una amenaza explote una vulnerabilidad de un activo.
  - El impacto resultante de dicho evento (que se materialice la amenaza) en la organización.

  Esta valoración da como resultado tres tipos de riesgos:
- **Riesgos asumibles:** son los que provocan un impacto tan pequeño en la organización que las contramedidas necesarias para mitigarlos podrían ser más costosas que el impacto que supondrían.
- **Riesgos no aceptables:** son los riesgos que provocan un daño en la organización y que es necesario tratar.

- **Riesgos críticos:** son los riesgos que, de materializarse, provocan un gran daño a la organización, pudiendo suponer incluso la desaparición de la actividad de la misma. Estos riesgos *hay que tratarlos de forma prioritaria.*

3. Tratamiento de los riesgos

   A través de la anterior fase, hemos hecho una valoración del riesgo para cada uno de los activos.

   Es la hora de tratar dicho riesgo. Para ello, tenemos varias posibilidades:

   - **Asumir el riesgo.** Podemos asumir aquellos riesgos que supongan un impacto nulo o trivial en los procesos de la organización.
   - **Evitar el riesgo.** Eliminar el activo o la amenaza que provoca el riesgo; suele ser difícil, y a menudo imposible.
   - **Transferir el riesgo.** Mediante una póliza de seguros. Si bien, aunque se recupere el valor económico, en el caso de pérdida de datos críticos pueden producir problemas importantes.
   - **Reducir el riesgo.** Estableciendo medidas y controles que disminuyan la probabilidad y/o el impacto o daño.

4. Identificación y selección de controles

   Una vez que hemos escogido los riesgos que vamos a reducir, es hora de identificar y seleccionar los controles que vamos a aplicar para disminuir la probabilidad y/o el impacto en caso de que se produzca.

   Por ejemplo, tenemos una amenaza: *el fuego*, a la que podemos aplicar estos dos controles:

   - **Disminuir la probabilidad:** instalar extintores, detectores de humos, alarmas de incendios, etc., de forma que reducimos la posibilidad de que, en caso de producirse una llama, el fuego consuma los equipos que albergan la información.
   - **Reducir el impacto:** guardar las copias de seguridad en armarios ignífugos y/o mantener una copia fuera de las instalaciones principales, de forma que, en caso de que el fuego consuma los equipos que albergan la información, dispongamos de otra copia de la misma.

13.2.6 Implantar los controles y el SGSI (Do-Hacer)

Una vez que tengamos claros los riesgos, el análisis de impacto en el negocio y los controles que deben implantarse, está la fase de la propia implantación de los controles y de «operar» el SGSI.

13.2.7 Revisar los controles y el SGSI (Check–Revisar)

El siguiente paso es revisar la eficacia de los controles implantados, y si cumplen con los objetivos marcados por el SGSI.

Para ello es necesario efectuar periódicamente auditorías internas que permitan dictaminar sobre la adecuación de las medidas y controles de Seguridad de la Información, así como identificar deficiencias y estudiar medidas correctoras o complementarias.

13.2.8 Mejorar el SGSI (Act–Actuar)

En función de las deficiencias detectadas en los controles y en la operativa del SGSI, es necesario identificar e implantar las acciones correctivas y preventivas para mejorar el rendimiento del SGSI.

El proceso de mejora incluye:

- Identificar nuevos controles debido a deficiencias encontradas en las etapas anteriores.
- Modificar los controles actuales para mejorar su eficiencia.
- Modificar los objetivos de seguridad y los controles asociados.
- Eliminar controles obsoletos.
- Comunicar los cambios efectuados.
- Modificar el diseño del SGSI.

13.2.9 Conclusiones

Aunque es un esfuerzo grande para una organización, una vez que tenga implantado el SGSI verá incrementada su productividad, reducido el riesgo de pérdidas y fugas de información y asegurada su continuidad frente a desastres naturales, accidentales o intencionados.

La implementación de un SGSI en una organización es algo que se ajusta a las necesidades de la misma; por ejemplo, una situación sencilla requiere de un SGSI simple.

Lo habitual es comenzar asegurando los procesos más críticos de la organización para, posteriormente, ir aumentando el alcance del SGSI hasta hacerlo extensible a todos los procesos de la misma.

13.3 PLAN DE CONTINGENCIAS Y CONTINUIDAD DE NEGOCIO

Uno de los controles que se puede implantar en el SGSI es el plan de contingencias y continuidad de negocio.

El plan de contingencias y continuidad de negocio puede definirse como el conjunto de procedimientos que permiten un rápido retorno a una situación suficientemente normalizada para que la actividad de la organización recupere un nivel aceptable después de una interrupción no prevista de sus sistemas de información.

Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de la organización.

13.3.1 Objetivos del plan

- Aumentar la probabilidad de continuidad de las funciones críticas de la organización en caso de que un incidente interrumpa las operaciones informáticas en las que se apoyan.
- Proporcionar un enfoque organizado ante cualquier incidente o interrupción del trabajo imprevista.
- Proporcionar una respuesta rápida y apropiada a cualquier incidente imprevisto, reduciendo el impacto de la interrupción de trabajo.
- Recuperar las funciones críticas del negocio ante un incidente que haya dejado las instalaciones informáticas dañadas o destruidas.
- Reducir el tiempo de recuperación y, por tanto, las pérdidas económicas resultantes del desastre.
- Reducir el impacto como consecuencia de la interrupción del servicio informático.
- Definir acciones y procedimientos que se vayan a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

13.3.2 Contenido

El plan de contingencias y continuidad comprende tres subplanes. Cada plan determina las contramedidas necesarias en cada momento del tiempo respecto a la materialización de cualquier amenaza:

- **El plan de respaldo.** Contempla las contramedidas preventivas *antes* de que se materialice una amenaza. Su finalidad es evitar dicha materialización.
- **El plan de emergencia.** Contempla las contramedidas necesarias *durante* la materialización de una amenaza, o inmediatamente después. Su finalidad es paliar los efectos adversos de la amenaza.
- **El plan de recuperación.** Contempla las medidas necesarias *después* de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

Por otra parte, el plan de contingencias y continuidad no debe limitarse a estas medidas organizativas. También debe expresar claramente:

1. Qué recursos materiales son necesarios.
2. Qué personas están implicadas en el cumplimiento del plan.
3. Cuáles son las responsabilidades concretas de esas personas y sus roles dentro del plan.
4. Qué protocolos de actuación deben seguir y cómo son.

13.3.3 Análisis de impacto en el negocio

El Análisis de Impacto en el Negocio (BIA) permite valorar las pérdidas que se pueden producir en caso de una interrupción en la actividad de la empresa, así como identificar las funciones críticas y su recuperación.

Los objetivos del Análisis de Impacto en el Negocio son:

- Identificar los impactos que generan las interrupciones y los desastres que pueden afectar a la organización.

- Determinar las funciones críticas del negocio y las prioridades de recuperación, de forma que se pueda establecer el objetivo de tiempo de recuperación.

Los impactos generados por la interrupción pueden ser:

- Impactos cuantificables:
  - Pérdidas económicas (activos).
  - Menos ingresos.
  - Multas económicas.
  - Pérdida de cuota de mercado.
  - Sanciones por incumplimiento de contratos.
  - Pérdidas de vidas humanas.

- Impactos cualitativos:
  - Pérdida de imagen.
  - Pérdida de credibilidad.
  - Incumplimiento legal.
  - Pérdida de capacidad operativa.

El principal elemento que se debe definir es: cuánto se puede permitir perder su organización.

13.3.4 El impacto en el tiempo

El impacto será mayor cuando, una vez sucedido algo, va transcurriendo el tiempo.

No es lo mismo una parada en la actividad de la empresa de una hora que una parada de una semana o un mes.

Seguramente, una parada de una hora ocasiona poco o ningún daño; en cambio, una parada de una semana supone una pérdida económica y de imagen importante, y una parada de un mes, la muerte del negocio.

En algunos casos críticos (navegación aérea), la criticidad es de minutos; en otros casos (comercio electrónico), de unas horas o días.

Es necesario determinar el máximo de tiempo que puede estar la organización sin el recurso o proceso.

En el análisis del impacto que se realice a la hora de realizar el plan de contingencias y continuidad de negocio se debe medir el impacto de lo largo del tiempo:

- Una hora.
- Tres horas.
- Doce horas.
- Un día.
- Dos días.
- Una semana.
- Dos semanas.
- Un mes.
- Dos meses o más.

Además, se deben considerar los momentos críticos del año (temporada alta, mucha producción, etc.).

El principal elemento que se debe definir es: cuánto se puede permitir perder su organización.

13.3.5 Revisión del plan

Cuántos planes se han realizado metódica y escrupulosamente, permaneciendo después olvidados en un cajón.

Y el día en que surge un imprevisto y es preciso poner en marcha el plan, comprobar que ya no se ajusta a la realidad *actual* de la organización, que los procesos y/o estructura han cambiado. Que ese plan *ya no vale*.

El plan de contingencias y continuidad de negocio es algo vivo, que hay que revisar periódicamente y mantener actualizado.

13.3.6 Prueba del plan

Cuando se confecciona —y siempre que se realice alguna modificación mayor en el plan—, es preciso probar su funcionamiento.

La verificación de los procedimientos del plan se debe realizar en los momentos o épocas que menos impacto cause a la empresa, simulando un incidente y verificando el desarrollo del plan, anotando las desviaciones que se producen sobre lo planeado para, posteriormente, ajustar los procedimientos.

Si esperamos a tener un incidente *real* para comprobar que el plan funciona, puede que nos llevemos una desagradable sorpresa.

13.3.7 Conclusiones en cuanto a la continuidad de negocio

Desastres como el del edificio Windsor nos demuestran que ninguna organización está libre del riesgo de perder todos sus activos de información a causa de una catástrofe.

En el caso del edificio Windsor, las empresas que disponían de un plan de contingencias y continuidad de negocio habían reanudado sus procesos de negocio en unos días.

Las que no disponían de plan, pero disponían de copias de seguridad externas, habían tardado más, pero pudieron continuar con su actividad.

Y las que no disponían de nada, o las que guardaban las copias de seguridad en el propio edificio, habían visto cómo perdían su negocio.

Un plan de contingencias y continuidad de negocio es la herramienta que permite recuperar la actividad de la empresa en el menor tiempo posible después de una interrupción no prevista en sus sistemas; y en el caso de un desastre mayor, la diferencia entre la vida y la muerte de las actividades de la empresa.

13.4 SGSI Y LA NORMA ISO 27001

La Norma ISO 27001 proporciona, a partir de un enfoque por procesos, un modelo para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI.

El éxito de este modelo radica en que se ha trasladado el modelo de gestión utilizado en las UNE-EN ISO 9001 y 14001 a la gestión de la seguridad de la información, permitiendo la integración de estos sistemas.

Esta norma es la definición de los procesos de gestión de la seguridad, por lo tanto, es una especificación para un SGSI y, en este momento, es la única norma certificable, dentro de la familia ISO 27000.

En su Anexo A aparecen los objetivos de control y los controles que se desarrollan con más profundidad en la Norma ISO 27002.

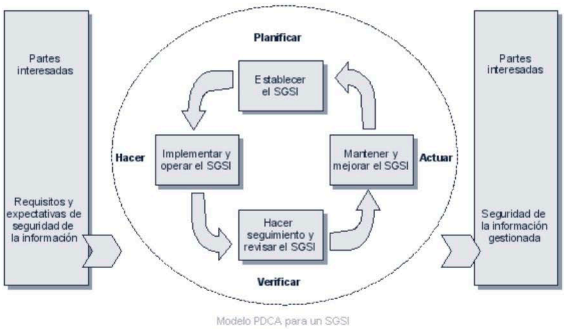


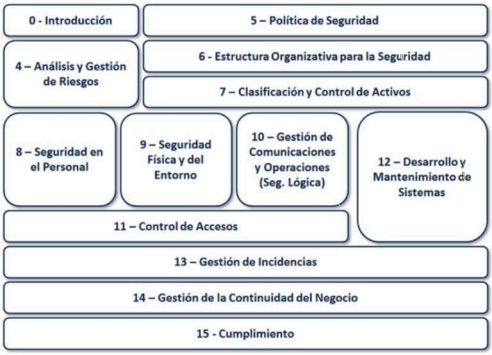
Figura 1.5. Fuente: Norma UNE-ISO/IEC 27001:2005

13.4.1 La norma ISO 27002

La ISO 27002 viene a ser un código de buenas prácticas en el que se recoge un catálogo de los controles de seguridad y una guía para la implantación de un SGSI.

Al igual que el Anexo A de la ISO 27001, se compone de 11 dominios, 39 objetivos de seguridad y 133 controles de seguridad.

Cada uno de los dominios conforma un capítulo de la norma y se centra en un determinado aspecto de la seguridad de la información. En el siguiente dibujo se muestra la distribución de dichos dominios y el aspecto de seguridad que cubren:



La pretensión de esta normativa es la elaboración de un SGSI que minimice los riesgos que se hayan detectado en los análisis de riesgos hasta un nivel asumible por la organización, con relación siempre a los objetivos de negocio.

Es importante destacar que cualquier medida de protección que se haya implantado debe quedar perfectamente documentada.

13.4.2 La certificación del SGSI

El diseño e implementación de un Sistema de Gestión de Seguridad de la Información conforme la Norma ISO 27001 permite su certificación por parte de un organismo certificador independiente.

La certificación del SGSI por parte de un organismo externo e independiente aporta las siguientes ventajas:

- Mejora la confianza con los clientes, proveedores y *partners*.
- Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación.
- Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.
- Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados, al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información.
- Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información.
- El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora.

13.4.3 Conclusiones

La Norma ISO 27001 proporciona una guía para construir un SGSI sólido, estable y reconocido a escala internacional.

Además, es posible certificar dicho SGSI, de forma que un organismo independiente certifique que, efectivamente, gestionamos la seguridad de la información y la continuidad del negocio.

Nos diferenciamos de esta forma con la competencia, incrementando la confianza de nuestros clientes, proveedores y *partners*.

14

IMPLANTACIÓN DE LA LOPD

«El secreto del éxito en la vida de un hombre está en prepararse para aprovechar la ocasión cuando se presente».

Benjamin Disraeli

14.1 IDENTIFICACIÓN Y NOTIFICACIÓN DE FICHEROS

En este capítulo vamos a aprender a identificar correctamente los ficheros con datos personales que se tratan en la organización y realizar su notificación al Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

14.1.1 Identificación de los ficheros

El primer paso para realizar la implantación es identificar correctamente los ficheros con datos personales que trata la organización y proceder a notificar su inscripción en el Registro General de Protección de Datos (RGPD).

Pero antes de meternos en faena, debemos aclarar una serie de conceptos.

14.1.2 ¿Qué es un fichero a nivel de inscripción?

Al principio, la respuesta a esta pregunta no es fácil: ¿son los ficheros de Excel donde almacenamos los presupuestos y facturas? ¿Es la base de datos, las tablas o los campos los que se han de notificar? ¿Y si el fichero está dividido, o se encuentra en varios sitios al mismo tiempo, debo notificar todos y cada uno de ellos?

Para contestar a estas preguntas correctamente no debemos pensar en términos de fichero informático, sino abstraernos de este concepto y pensar en términos de finalidad: ¿qué datos personales estoy tratando? ¿Cuál es la finalidad del tratamiento y qué departamentos o unidades de la empresa tienen acceso al fichero?

La respuesta a esta pregunta podría ser alguna de las siguientes:

- Gestión de servicios prestados a clientes.
- Gestión de nóminas y recursos humanos.
- Gestión de la prevención de riesgos laborales.
- Gestión del historial clínico del paciente.

En la inscripción del fichero en el RGPD debe hacerse considerando la entidad «fichero» como aquel conjunto de bases de datos, tablas, ficheros de texto, documentos en papel, etc., que están distribuidos en una o más localizaciones físicas, que están gestionados por un mismo departamento y cuya finalidad es la que nos interesa inscribir. Además, el nivel de medidas de seguridad que se deben aplicar —básico, medio o alto— deberá ser coherente para todos los componentes del fichero.

EJEMPLO

Veamos un ejemplo práctico para clarificar todo esto:

Una empresa que vende comida para perros quiere implantar la LOPD, y el primer paso que debe efectuar es identificar los ficheros que trata.

Para ello analiza los programas, ficheros y documentos en papel que maneja y que contienen datos personales. Del análisis surge lo siguiente:

- Trata datos de proveedores en la aplicación de gestión y en las facturas de compra en formato papel que tiene.
- Trata datos de clientes en la aplicación de gestión desde la que saca los albaranes y facturas, en los albaranes en papel de la entrega de la comida al cliente y en las facturas en papel que realiza a los clientes.
- Trata datos de trabajadores en las nóminas y contratos que almacena, así como para la documentación de la prevención de riesgos laborales.
- Almacena los *curriculum vitae* que le envían aquellas personas que optan a un puesto de trabajo.
- Dispone de dos cámaras de vigilancia, que graban cuanto ocurre a un aparato grabador.

¿Cuántos ficheros deben inscribirse?

La respuesta a esto, sobre la base del análisis realizado, es la siguiente:

Fichero	Finalidad	Tipo
PROVEEDORES	Gestión de proveedores fiscal, contable y administrativa.	Mixto
CLIENTES	Gestión de clientes fiscal, contable y administrativa.	Mixto
LABORAL	Gestión de recursos humanos, nóminas y prevención de riesgos laborales.	Mixto
VIDEOVIGILANCIA	Videovigilancia de las instalaciones.	Automatizado

Como puede apreciarse, a nivel de inscripción, hemos unido los ficheros informáticos con los ficheros en formato papel, resultando de todos ellos un único fichero. Debemos recordar que la agrupación siempre es sobre la base de su finalidad, independientemente del tipo de soporte en el que se encuentre el fichero —automatizado o manual— y su lugar o lugares de almacenamiento.

En el caso del fichero LABORAL, hemos incluido en él los *curriculum* que le llegan a la empresa, ya que la finalidad que vamos a declarar abarca la gestión de recursos humanos, y ésta incluye, a su vez, la selección de personal previa que

requiere. Además, dicha selección de personal la realiza el mismo departamento que se encarga del personal de la empresa.

14.1.2.1 SI UN FICHERO ESTÁ DISTRIBUIDO EN VARIOS SOPORTES, DOCUMENTOS Y UBICACIONES, ¿CÓMO ESCOGER CUÁNTOS FICHEROS NOTIFICAR?

Debe notificarse un único fichero, independientemente de los soportes, documentos y ubicaciones en que se encuentre, si concurren las siguientes circunstancias:

- Una misma finalidad (gestión de clientes, de personal, de expedientes, etc.).
- Gestionado por un mismo departamento o unidad (departamento de ventas, de recursos humanos, etc.).
- Aplicación de un mismo nivel de medidas de seguridad a todos los componentes del fichero (nivel básico, medio o alto).

14.1.2.2 ¿QUÉ OTROS DATOS NECESITO PARA NOTIFICAR LOS FICHEROS?

Para realizar la notificación de los ficheros debemos recabar, además, los siguientes datos:

- De dónde proceden los datos (del propio interesado, fuentes accesibles al público, etc.).
- Los colectivos y las categorías de interesados (clientes, trabajadores, etc.).
- Qué datos recogemos en cada uno de los ficheros (nombre y apellidos, teléfono, domicilio, datos bancarios, aficiones, edad, sexo, etc.).
- El servicio o unidad de acceso ante quien se deben ejercer los derechos legales de los afectados (acceso, rectificación, cancelación y oposición).
- Conocer qué nivel de medidas de seguridad son exigibles para cada uno de los ficheros (básico, medio o alto).

- Qué cesiones realizamos de los datos de esos ficheros (a otras entidades relacionadas con nosotros, administraciones, organismos, bancos y cajas de ahorros, etc.).

- Si se realizan transferencias internacionales de datos, el país al que se realizan y la categoría de los destinatarios de dichos datos, si es el caso.

- Si el fichero es tratado por algún encargado del tratamiento; en este caso, deberá inscribirse el encargado del tratamiento que realice más trabajo con el fichero o el que implique un nivel de riesgo mayor.

14.1.3 Notificación de los ficheros al RGPD

Una vez que hemos recabado todos los datos necesarios, debemos notificar los ficheros al RGPD a través del formulario NOTA que se encuentra en la web de la AEPD (www.agpd.es) o a través de algún *software* especializado que envíe la notificación al RGPD por Internet.

14.1.4 Registro de los ficheros en el RGPD

Si la inscripción enviada cumple con todos los requisitos exigidos, el RGPD resuelve favorablemente la petición e inscribe los ficheros, asignando a cada uno un código de inscripción.

La resolución favorable de inscripción, así como el número de inscripción asignado a cada fichero, nos es remitido por la AEPD.

Es muy importante conservar el número de inscripción que nos ha remitido la AEPD, ya que es necesario posteriormente para poder realizar modificaciones en el fichero o incluso la supresión completa del mismo.

Una vez recibido el identificador de todos y cada uno de los ficheros notificados, tendremos completada la legalización de los ficheros.

Es importante recordar que la inscripción de un fichero en el RGPD únicamente acredita que se ha cumplido con la obligación de notificación dispuesta por la LOPD, sin que de la inscripción realizada se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones previstas en la LOPD y su reglamento de desarrollo.

Además, esta inscripción deberá encontrarse actualizada en todo momento.

14.2 EL DOCUMENTO DE SEGURIDAD

El segundo paso que debemos efectuar es el de elaborar el Documento de Seguridad con el contenido exigido por el RD 1720/2007, y que describimos a continuación:

- Ámbito de aplicación, con especificación detallada de los recursos protegidos.
- Medidas, normas y procedimientos para garantizar el nivel de seguridad exigido.
- Funciones y obligaciones del personal.
- Estructura de los ficheros.
- Descripción de los sistemas de información que los tratan.
- Procedimientos de notificación, gestión y respuesta ante las incidencias.
- Procedimientos de realización de copias de respaldo y recuperación de los ficheros automatizados.
- Medidas que se deben adoptar para el transporte, destrucción y reutilización de soportes y documentos.
- Identificación del responsable o responsables de seguridad y controles periódicos que se deben efectuar en el caso de ficheros de nivel medio y alto.
- Identificación de los encargados del tratamiento, tratamientos realizados, las condiciones y la vigencia del encargo.
- Relación de personal autorizado para:
  - Otorgar autorizaciones.
  - Tratar datos personales fuera de las instalaciones.
  - Acceder a los ficheros, así como los accesos autorizados.
  - Conceder, modificar y anular accesos a otros usuarios.
  - Acceder al lugar donde se almacenan los soportes con datos personales.
  - Sacar datos personales fuera de las instalaciones.

- Es necesario elaborar y mantener los siguientes registros:
  - Inventario de soportes y documentos.
  - Registro de incidencias.
  - Registro de entrada y salida de soportes con datos automatiza-dos de nivel medio y alto.
  - Registro de accesos a la documentación que contenga datos de nivel alto y sea accedida por varias personas.

Dicho *Documento de Seguridad* debe *mantenerse en todo momento actualizado*, de forma que refleje fehacientemente la realidad de la organización.

14.2.1 Mantenimiento del Documento de Seguridad

Debemos tener en cuenta que, como hemos comentado anteriormente, el Documento de Seguridad tiene que estar en todo momento actualizado, de forma que refleje fehacientemente la realidad de la empresa y debiendo actualizarse siempre que se produzca algún cambio en:

- Los ficheros.
- Los sistemas de información.
- La organización.
- El personal con acceso a datos.
- El personal autorizado y/o las autorizaciones concedidas.
- Los encargados del tratamiento y/o el servicio prestado.
- Los controles periódicos efectuados.

14.2.1.1 IMPLANTAR LAS MEDIDAS RECOGIDAS EN EL DOCUMENTO DE SEGURIDAD

Este paso se completa realizando la implantación efectiva de las medidas de seguridad que se recogen en el Documento de Seguridad anteriormente elaborado.

En función de los datos personales tratados, se deberán implantar medidas de seguridad de nivel básico, medio y/o alto a los ficheros que contienen dichos datos.

Las medidas que se deben implantar son de dos tipos:

- **Medidas técnicas:** son las destinadas a conservar la integridad de la información —su no alteración, pérdida o robo— y la confidencialidad de los datos personales a través de medios o dispositivos técnicos. Ejemplo: instalación de un sistema de copia de respaldo, limitar el acceso al sistema a través de un nombre de usuario y contraseña, etc.

- **Medidas organizativas:** son aquellas medidas destinadas a establecer procedimientos, normas, reglas y estándares de seguridad, cuyos destinatarios son los usuarios que tratan los datos de los ficheros. Ejemplo: lista de usuarios y accesos autorizados, registro de incidencias, relación de personas autorizadas para sacar soportes fuera de las instalaciones del responsable, etc.

14.3 CLÁUSULAS LEGALES

Se deben elaborar e introducir las cláusulas informativas en todos los cuestionarios, formularios y/o contratos que la empresa utilice para la recogida de los datos personales.

La cláusula debe incorporar, al menos, los siguientes datos:

- Informar de la existencia de un fichero o tratamiento de datos personales.
- Finalidad de la recogida de los datos.
- Destinatarios de la información si los datos van a ser cedidos.
- De la identidad y dirección del responsable del fichero o tratamiento.
- De la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.

14.3.1 Cláusula informativa para recabar datos

Ésta es la cláusula más utilizada. Debe ir incluida en los documentos que se empleen para recoger los datos personales que son necesarios para prestar un servicio al afectado o durante la formalización de un contrato de la que sea parte el afectado y dichos datos sean necesarios para su mantenimiento o cumplimiento.

14.3.1.1 MODELO DE CLÁUSULA INFORMATIVA PARA RECABAR DATOS DE CLIENTES

CLÁUSULA

En cumplimiento de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD), le informamos de que los datos aportados serán incorporados en un fichero del que es titular LA EMPRESA S. L., y utilizados con la finalidad de prestarle los servicios solicitados. Puede ejercer sus derechos de acceso, rectificación, cancelación y oposición en el domicilio fiscal de LA EMPRESA S. L., sito en AVDA XXX, 34 XXX XXXXX

14.3.2 OTRAS CLÁUSULAS

Aunque la cláusula que más se utiliza es la informativa anterior, a veces puede ser necesario recurrir a otras cláusulas:

- Cláusula informativa para incluir en los documentos enviados al cliente que contienen datos personales (facturas, presupuestos, comunicados, etc.).

  Esta cláusula no es obligatoria, pero sí recomendable, ya que cumple una doble función: por un lado, cumplimos el principio de información que establece la LOPD; por otro lado, mejoramos nuestra imagen ante el cliente, que percibe nuestra preocupación por la privacidad de sus datos.

CLÁUSULA

En cumplimiento de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD), le informamos de que sus datos están incluidos en un fichero del que es titular LA EMPRESA S. L., y utilizados con la finalidad de prestarle los servicios solicitados. Puede ejercer sus derechos de acceso, rectificación, cancelación y oposición en el domicilio fiscal de LA EMPRESA S. L., sito en AVDA XXX, 34 XXX XXXXX.

- Cláusula para obtención de consentimiento para recabar datos personales de nivel alto o para una finalidad que no sea prestarle un servicio directo al titular de los datos.

CLÁUSULA

En cumplimiento de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD), consiente que los datos aportados sean incorporados en un fichero del que es titular LA EMPRESA S. L., y utilizados con la finalidad de DETALLAR FINALIDAD. Puede ejercer sus derechos de acceso, rectificación, cancelación y oposición en el domicilio fiscal de LA EMPRESA S. L., sito en AVDA XXX, 34 XXX XXXXX.

NOTA

En caso de que se recaben datos de ideología, afiliación sindical, religión o creencias, se deberá advertir al interesado de su derecho a no prestar dicho consentimiento.

- Cláusula para obtención de consentimiento para realizar una cesión de los datos personales a otra empresa.

CLÁUSULA

En cumplimiento de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD), consiente que sus datos personales, contenidos en un fichero del que es titular LA EMPRESA S. L., y utilizados con la finalidad de FINALIDAD, sean cedidos a empresas del sector XXXXXXX con la finalidad de DETALLAR FINALIDAD. Puede ejercer sus derechos de acceso, rectificación, cancelación y oposición en el domicilio fiscal de LA EMPRESA S. L., sito en AVDA XXX, 34 XXX XXXXX.

14.4 CONTRATOS

El cumplimiento de la LOPD exige firmar una serie de contratos entre las empresas que prestan un servicio que implica o pueda implicar el acceso a datos personales que se tratan en la otra empresa. Siempre que se produzca esta circunstancia, debe existir un contrato que regule dicho acceso y que se ajuste a lo dispuesto por el artículo 12 de la LOPD.

Por otra parte, el artículo 10 de la LOPD establece la obligación de secreto profesional respecto a la información a la que se tenga acceso en el ejercicio de las funciones propias del trabajo. Es conveniente articular esta obligación con la firma de un compromiso de confidencialidad y deber de secreto que deben suscribir los trabajadores que tratan datos personales dentro de la empresa.

A continuación, veremos los distintos tipos de contratos y compromisos que se deben formalizar.

14.4.1 Contratos de acceso a datos

Toda empresa externa que con objeto de prestarnos un servicio acceda a datos personales de los cuales nosotros somos responsables (ejemplo: asesoría fiscal, empresa de prevención de riesgos laborales) es considerada un encargado del tratamiento, y es preciso firmar un contrato de acceso a datos con la empresa que regule la prestación de los servicios.

Dicho contrato deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, así mismo, las medidas de seguridad que deberá cumplir el encargado del tratamiento.

NOTA

El contrato deberá detallar los servicios prestados por el encargado del tratamiento.

14.4.2 Prestaciones sin acceso a datos

Con las empresas externas que presten un servicio que no requiere acceso a datos, pero que pudiera darse el caso de que accedan a información de carácter personal, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Si el contrato de prestación de servicios existente no incluye esto, es necesario realizar y firmar un anexo al mismo que lo complete en este ámbito.

14.4.3 Compromisos de confidencialidad con los trabajadores

El artículo 10 de la LOPD establece que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Es decir, los trabajadores de una empresa que tengan acceso a datos están obligados al deber de secreto profesional con relación a los datos que traten en el desempeño de su trabajo.

Es conveniente para la empresa que este deber de secreto que debe respetar el trabajador sea puesto por escrito en lo que se denomina *Compromiso de confidencialidad y deber de secreto*, y que debe firmar el trabajador. De este modo, la empresa puede demostrar de forma fehaciente que ha cumplido con su obligación de informar al trabajador del deber de secreto al que le obliga la LOPD.

14.4.4 La LOPD y los trabajadores

La organización es responsable de las posibles vulneraciones que se produzcan en la normativa respecto a los datos personales que trata.

Entre sus obligaciones está la de formar y concienciar adecuadamente a sus trabajadores para que conozcan dicha normativa y sus obligaciones respecto al tratamiento de los datos personales, así como su deber de secreto profesional.

Es conveniente para cumplir esta obligación hacer entrega a cada trabajador —o, en su defecto, tener a disposición de todos ellos— de la Política de la empresa en Protección de Datos, una especie de Manual del empleado en este ámbito. En dicho documento debe explicarse la LOPD de un modo comprensible para los trabajadores, y sus funciones y obligaciones con respecto a dicha ley.

También es conveniente darles charlas de concienciación que eviten la vulneración de la normativa por desconocimiento de la misma.

14.5 PROTOCOLOS ARCO

Otra de las obligaciones que tiene la empresa es el deber de ejercitar los derechos legales de los afectados de forma ágil y efectiva.

Dichos derechos, como hemos visto en capítulos anteriores, son el acceso, rectificación, cancelación y oposición.

Para ello, la empresa debe disponer de plantillas ya preparadas de petición y respuesta de los derechos de acceso, rectificación, cancelación y oposición —también llamados derechos ARCO— que le permitan una rápida y eficaz respuesta a los afectados que quieran ejercer sus derechos.

La empresa debe ser especialmente cuidadosa y diligente en la atención de los derechos ARCO, ya que los afectados podrán solicitar la tutela de la AEPD en el caso de que la empresa no ejerza sus derechos en el plazo que marca la LOPD.

CONCLUSIONES FINALES

Estamos inmersos en la era de la información. Nunca antes en la historia de la humanidad la información ha sido tan valiosa como ahora.

Si aplicamos esto al *marketing*, el hecho de conocer los gustos, preferencias, inquietudes, lugares que frecuenta (*on* y *off line*), deseos, relaciones, nivel adquisitivo y demás información personal de los potenciales clientes es una clara ventaja competitiva a la hora de persuadir a una persona de que nuestra propuesta es la más idónea para él.

La proliferación de las redes sociales ha hecho este trabajo mucho más fácil. Ahora son los propios usuarios de las redes sociales los que cuelgan toda esta información de forma libre, y muchas veces sin ser muy conscientes de todo lo que muestran al resto del mundo. Como contrapartida, las redes sociales nos muestran publicidad dirigida especialmente a nosotros, sobre la base de toda esa información que hemos ido suministrando (a veces, sin ser conscientes de ello).

Y de la tasa de acierto que tienen sus anuncios (es decir, que hagamos clic en ellos), depende su cuenta de resultados.

¿No es éste suficiente aliciente para recoger cada vez más datos y, además, mejorar esa tasa de acierto?

Un ejercicio de reflexión

Normalmente, las cosas sólo se valoran cuando se pierden, así que le voy a pedir que imagine que no existe ninguna ley que proteja nuestra privacidad.

Imagine un mundo sin privacidad, donde los datos personales se pueden comprar, vender e intercambiar con total impunidad. Imagine una gran organización que sea la receptora final de todos esos datos dispersos —gracias a su poder de compra— y los unifique para crear un perfil único por cada persona —tengamos en cuenta que ese perfil incluiría nuestros datos identificativos, propiedades, informes médicos, ingresos, gastos, gustos, aficiones, hábitos de navegación, lugares que visita, etc., es decir, *todos, todos, todos* nuestros datos.

Y además, como nada lo impide, que cualquiera pueda —por un módico precio, claro— acceder al perfil de cualquier otra persona.

Cualquiera podría acceder a toda nuestra historia. Nuestras debilidades saldrían a la luz, y podríamos ser manipulados con relativa facilidad. Nuestro pasado condicionaría de forma fundamental nuestro futuro. Acabaríamos «etiquetados» y con un estrecho margen de maniobra.

¿Es ése el futuro que quiere para usted y los suyos?

ÍNDICE ALFABÉTICO

Protección de datos y seguridad de la información

4ª EDICIÓN ACTUALIZADA

Casi la totalidad de las empresas necesitan manejar datos personales para desarrollar su actividad (realizar la facturación, pagar las nóminas y seguros sociales, gestionar los clientes, lanzar campañas de marketing, etc.).

Estos datos están protegidos por la **Ley Orgánica de Protección de Datos de Carácter Personal (LOPD)**, de obligado cumplimiento para todas ellas.

Sin embargo, la mayoría de los ciudadanos desconocen los derechos que les asisten en este ámbito, los riesgos a los que se exponen sus datos personales en Internet o el modo de retirar una información personal que les perjudica.

¿Qué debo conocer cuando introduzco mis datos en un formulario?, ¿pueden ceder mis datos a otra empresa sin mi consentimiento?, ¿cómo puedo cancelar todos los datos que tiene una entidad sobre mí?, ¿cuáles son los riesgos cuando facilito datos en Internet?, **¿qué es el derecho al olvido?**

Estas y otras muchas cuestiones que nos suscitan a todos los ciudadanos son respondidas en esta obra de forma clara y sencilla.

Pero no podemos olvidar que un derecho para unos lleva parejo unas obligaciones para otros. En este caso, las obligaciones son para las entidades que recogen, almacenan y utilizan los datos (profesionales, empresas, asociaciones, administraciones, comunidades de propietarios, etc.).

En estas páginas también hemos dado respuesta a sus inquietudes: qué hay que hacer y cómo hay que hacerlo para cumplir perfectamente la normativa de protección de datos y tener segura la información que manejan.

9 788499 645605

ra-ma.es

Ra-Ma®