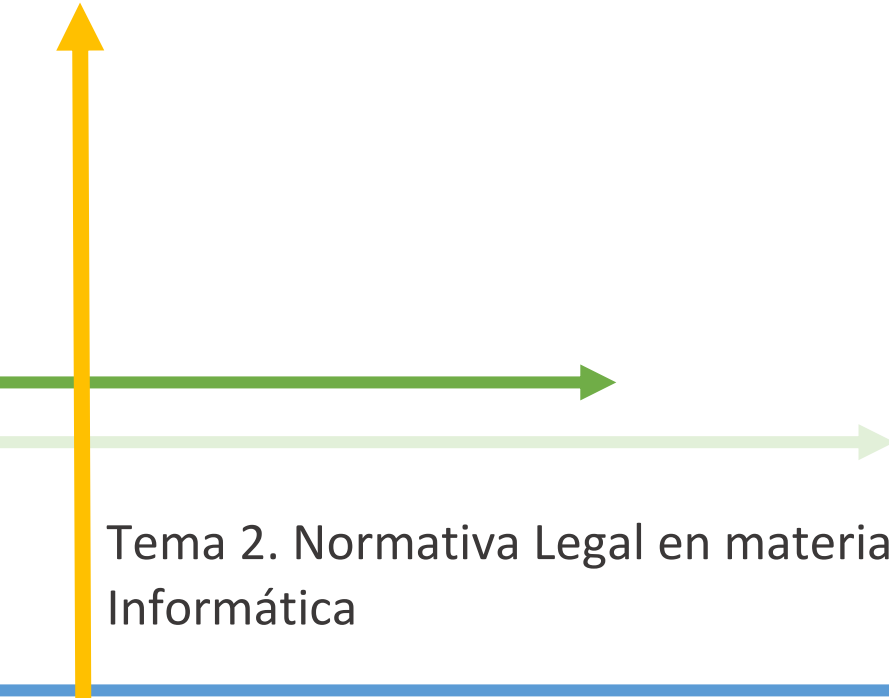




TEMA



Tema 2. Normativa Legal en material de Seguridad Informática

Administración de sistemas
informáticos en Red

Seguridad y alta disponibilidad

Autor/a: Joaquín Erencia

Tema 2: Normativa Legal en material de Seguridad Informática

¿Qué aprenderás?

- Qué es la Ley Orgánica de Protección de Datos
- Qué es la Ley sobre los Servicios de la Sociedad de la Información y el Correo Electrónico

¿Sabías que...?

- Eres responsable de la información que administras.
- Los usuarios tienen derechos sobre sus datos que la ley protege.
- Uno de los puestos de trabajo más demandados en las grandes empresas es el de delegado de Protección de Datos.



2.1. Introducción

En este tema vamos a tratar una de las partes que menos nos gusta como informáticos, la parte **legal**. No solemos ser un perfil que nos guste tener que conocer conceptos legales, normativas y reglamentos, pero resulta que no solo es uno de los campos con más presente laboral en la seguridad sino que tenemos una gran tarea como responsables de la informática de una empresa, pues nos debemos de regir por unos reglamentos a nivel nacional, europeo e internacional bastante estrictos, no solo a nivel interno, refiriéndonos a la información que almacenamos, sino a nivel externo, pues pocas empresas actualmente, no tienen movimientos comerciales por internet.

El objetivo de este tema no es conocer al detalle las legislaciones de las que vamos a hablar, Ley Orgánica de Protección de Datos y Ley Servicios de la Información y el Comercio Electrónico, pero sí conocer los elementos que más nos pueden influir, así como la responsabilidad e infracciones que podéis sufrir en caso de no cumplirlas.

2.2. Normativas

El **Sistema de Gestión de Seguridad de la Información** (SGSI) es el conjunto de políticas de administración de la información que se deben cumplir para considerar un sistema como seguro.

Ahora veamos las diferentes normativas que hay que lo componen.

2.2.1 El estándar iso/iec 27001

Esta normativa **Internacional** determina las especificaciones que deben cumplir los Sistemas de Gestión de la Seguridad de la Información, y que son los siguientes:

- Especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información de acuerdo con UNE-ISO 17799
- Define los controles de seguridad a revisar
- Define un marco general del Sistema de Gestión de la Seguridad de la Información
- Cómo se debe implantar el Sistema de Gestión de la Seguridad de la Información



- Cómo se realiza la explotación
- Cómo debe realizarse la revisión y mejora del Sistema de Gestión de la Seguridad de la Información

Esta normativa ha evolucionado con los años como podéis ver en la siguiente imagen, adecuándose a los diferentes elementos que han ido apareciendo:

Figura: Evolución Norma ISO 27001

ISO 27001-2005	ISO 27001-2013
<input type="checkbox"/> Manual del SGSI	<input type="checkbox"/> Políticas de seguridad
<input type="checkbox"/> Organización de la seguridad	<input type="checkbox"/> Organización de la seguridad de la información
<input type="checkbox"/> Gestión de Activos	<input type="checkbox"/> Seguridad de los RRHH
<input type="checkbox"/> Seguridad de RRHH	<input type="checkbox"/> Gestión de Activos
<input type="checkbox"/> Seguridad Física	<input type="checkbox"/> Control de acceso
<input type="checkbox"/> Gestión de comunicaciones y operaciones	<input type="checkbox"/> Criptografía
<input type="checkbox"/> Control de Acceso	<input type="checkbox"/> Seguridad física y ambiental
<input type="checkbox"/> Adquisición, desarrollo y mantenimiento de la información	<input type="checkbox"/> Operaciones de seguridad
<input type="checkbox"/> Gestión de incidentes	<input type="checkbox"/> Seguridad de las comunicaciones
<input type="checkbox"/> Continuidad del negocio	<input type="checkbox"/> Sistemas de adquisición, desarrollo y mantenimiento
<input type="checkbox"/> Cumplimiento	<input type="checkbox"/> Relaciones con proveedores
	<input type="checkbox"/> Gestión de incidentes
	<input type="checkbox"/> Seguridad de la información para la continuidad del negocio
	<input type="checkbox"/> Cumplimiento

2.2.2. Ley orgánica de protección de datos (LOPD)

Aparece en 1999 a nivel europeo, entrando en vigor en España desde el año 2000. Es revisada, siguiendo el Reglamento Europeo de Protección de Datos del 2016, y está en vigor la modificación desde el 25 de mayo del 2018.

Su objetivo es **proteger la privacidad de los datos de los ciudadanos** en lo relativo a seguridad de los datos personales que gestionan las empresas, ya sea en formato electrónico o papel.

Se aplica a empresas grandes, pymes y autónomos, ya que todos utilizan como mínimo datos de contacto del personal propio, clientes y proveedores.

¿Qué protegemos con esta ley? **El dato personal.**



Vamos a definirlo: *Toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultura, o social de dicha persona.*

Por lo tanto, consideraremos datos personales nuestros contactos en otras empresas, marcas, CIF, información corporativa, etc. En resumen, cualquier elemento que pueda ser útil para poder **identificar a alguna persona física**.

2.2.3 Reglamento general de protección de datos (rgpd)

Este reglamento define el concepto de **Tratamiento** como: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión, o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción

Además, determina cómo debemos recabar el **consentimiento** de los afectados para tratar sus datos. Las personas cuyos datos personales vayamos a tratar tienen que ser informados de que vamos a tratar su información, y de que tienen una serie de derechos, los **Derechos ARCOLP**: acceso, rectificación, cancelación, oposición al tratamiento, limitación y portabilidad.

Regula también el uso de datos personales en aspectos relacionados con el envío de publicidad, y determina cómo debemos actuar si vamos a transferir internacionalmente los datos a un tercero. Y, por último, pero no menos importante, las infracciones y sanciones a las que nos exponemos en caso de incumplimiento.

2.2.4. Conceptos importantes para tener en cuenta para entender la lpd y el rgpd

- **Interesado/a**: Es la persona a la cual pertenece el dato personal y, por lo tanto, su propietario/a. Esta persona tiene los siguientes derechos sobre su dato: acceso, rectificación, cancelación, oposición, portabilidad y olvido.



- **Responsable del tratamiento:** Es la persona física o jurídica que gestiona la información de un interesado. Lógicamente, cualquier mal uso es responsabilidad suya.
- **Encargado del tratamiento:** Es la empresa a la que entregamos, como responsable del tratamiento, el servicio de este. Esto se realiza por contrato entre responsable y Encargado, indicando las condiciones del tratamiento, las medidas de seguridad que se deben implantar y cómo se devolverán los datos al final del contrato.
- **Delegado de protección de datos o DPD (Ampliamos en el Anexo):** Es una persona con funciones de gestión y control de la protección de datos. Tendrá total autonomía en sus funciones. Podrá ser externa o interna. Esta figura se recomienda que tenga un perfil con formación específica en el tema o en derecho. Será obligatoria su existencia en las siguientes situaciones:
 - Operaciones de tratamiento que requieran una observación habitual y sistemática de personas a gran escala
 - Tratamiento a gran escala de datos de categorías especiales
 - No será obligatoria en empresas de menos de 250 empleados, salvo que realices tratamientos de riesgo para los derechos y libertades de las personas, no ocasionales o que incluyan categorías especiales de datos o datos relativos a condenas e infracciones penales
- **Niveles de Seguridad**
 - Básico: Se aplica a los ficheros que solo contengan datos identificativos y a todos los niveles medio y alto. Ejemplos: nombre, domicilio, teléfono, DNI, número afiliación a la seguridad social, fotografía, firma, correo electrónico, datos bancarios, edad, fecha de nacimiento, sexo, nacionalidad, etc.
 - Medio: Se aplica a los ficheros que contengan datos relativos a solvencia patrimonial, operaciones financieras y de crédito. Ejemplos: datos de personalidad, hábitos de consumo, hábitos de carácter, datos de seguridad social, solvencia patrimonial y crédito, antecedentes penales, sanciones administrativas, pruebas psicotécnicas, currículos, etc.
 - Alto: Se aplica a datos especialmente protegidos como los relativos a ideología, afiliación sindical y política, religión y creencias, origen racial, salud, alimentación, bajas laborales, vida y práctica sexual, etc.
- **Sanciones**
 - Leves: Se consideran faltas leves las siguientes:



- No realizar la solicitud de inscripción del fichero de datos en la Agencia Española de Protección de Datos (AEPD)
- La no información a la hora de recopilar datos personales
- No atender las consultas por parte de la AEPD
- No atender peticiones de rectificación o cancelación de datos por parte de un usuario
- Graves: Se consideran faltas graves las siguientes:
 - No inscribir los ficheros ante la AEPD
 - El uso de datos para finalidad diferente a aquella para la que fueron otorgados
 - Carecer del consentimiento necesario por parte del interesado para poder recopilar sus datos personales y disponer de ellos
 - Impedir o prohibir a los interesados el acceso a sus datos, aun cuando lo estén solicitando.
 - Mantener ficheros con datos que no son correctos o precisos y no hacer los cambios o las modificaciones que hayan sido solicitados por los usuarios.
 - El incumplimiento de los principios y garantías que vienen recogidos en la LOPD.
 - En el caso de tratamiento de datos especialmente protegidos y que no han sido autorizados por los afectados, se está cometiendo una infracción grave.
 - Si la empresa no envía o comunica a la AEPD las notificaciones que establece la regulación, estará incurriendo también en este tipo de infracción.
 - La falta de una seguridad suficiente en el mantenimiento de los ficheros en poder de la empresa.
- Muy Graves: Las sanciones consideradas como muy graves son las siguientes:
 - Crear ficheros que contemplen datos correspondientes a datos considerados como especialmente protegidos.
 - Recoger o recopilar datos de forma fraudulenta o mediante el uso de engaños.
 - Obtener datos con un alto nivel de protección sin tener, para ello, autorización de las personas afectadas.
 - Poner trabas o dificultar de manera continuada en el tiempo las peticiones o solicitudes de rectificación o cancelación de datos recibidas.
 - Vulnerar el secreto en el caso de los datos especialmente protegidos.



- Ceder o comunicar datos de terceros sin contar con permiso para ello es tipificado como una infracción muy grave.
- En el caso de que la AEPD lo pida, no acabar con el uso ilegítimo.
- Cualquier acción de tratamiento de datos que se lleve a cabo de manera ilegítima o no tenga en cuenta las garantías y los principios que se tengan que aplicar en cada caso.
- No hacer caso o no atender a los requerimientos que se reciban por parte de la AEPD.
- Llevar a cabo una transferencia, ya sea de manera temporal o definitiva, de datos personales dirigida a países en los que los niveles de protección no son los mismos o que no cuentan con autorización está considerado también como una falta muy grave.
- Las sanciones ante los anteriores incumplimientos pueden alcanzar entre los 10 y 20 millones de euros o entre el 2% y el 4% del volumen de negocio, en función de su gravedad.
- Gestión de riesgos

Es el conjunto de actividades y tareas que permiten controlar una amenaza mediante una secuencia de actividades que incluyen:

- Identificar la amenaza
- Evaluar los riesgos
- Tratar los riesgos
- Amenaza y Riesgo

Definimos amenaza como cualquier factor con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos de carácter personal se realiza un tratamiento.

Tipos de amenazas:

- Acceso ilegítimo a los datos. Ataque a la Confidencialidad
- Modificación no autorizada de los datos: Ataque a la Integridad
- Eliminación de los datos: Ataque a la Disponibilidad



En base a lo anterior, definimos también el concepto de riesgo como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas.

- Brecha de Seguridad: El Esquema Nacional de Seguridad o ENS define un “**incidente de seguridad**” como aquel suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

El RGPD la define como todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales, debe efectuar la correspondiente notificación a la autoridad de control competente, sin dilación y a más tardar en las 72 horas siguientes. Si la brecha entraña un alto riesgo para los derechos y libertades de los titulares de los datos, deberá comunicarla también a los afectados.

La comunicación se realiza a través del siguiente enlace:

<https://sedeagpd.gob.es/sede-electronica-web/>



*Esta foto de Autor desconocido está bajo
licencia [CC BY-SA](#)*



La excepción al párrafo anterior se determina cuando esta brecha no entraña un riesgo para los derechos y las libertades de las personas físicas.

El procedimiento para seguir ante una brecha es el siguiente:

- 1- Detección e identificación de la brecha.
- 2- Clasificación de la brecha
- 3- Plan de Actuación



- Comunicar a los medios internos/externos implicados
- Puesta en marcha del plan de respuesta
- Puesta en marcha del proceso de notificación
- Estudio y activación de las posibles medidas a adoptar

4- Seguimiento y cierre



Brechas de Seguridad: [Brechas de seguridad | AEPD](#)

2.2.4. Ley de servicios de la sociedad de la información y de comercio electrónico (Lssice)

Esta ley regula determinados aspectos jurídicos de los Servicios de la Sociedad de la Información, como:

- Comercio electrónico
- Contratación en línea
- Información y publicidad
- Servicios de intermediación

Pero siempre que constituya una actividad económica o lucrativa para el prestador del servicio.

2.2.4.1. Conceptos importantes para entender la Lssi

- Prestador: El Prestador es una figura que se aplica tanto a operadores de red y servicios de comunicaciones electrónica, como a empresas y ciudadanos que tengan su propia web.

Este debe indicar en su página web de forma permanente, fácil, directa y gratuita:

- Nombre o denominación social y datos de contacto
- Registro Mercantil o cualquier otro registro público
- Datos relativos a la autorización administrativa y el órgano de supervisión
- Datos de colegio profesional y número de colegiado
- NIF
- Precio de producto, indicando impuestos aplicables y los gastos de envío
- Los códigos de conducta a los que esté adherido y cómo consultarlos



- **Cookies:** Las cookies permiten a los prestadores de servicios almacenar y recuperar datos sobre los usuarios almacenados en sus equipos. Para usarlos deben recabar el consentimiento de los usuarios siempre que sean informados de manera clara y completa sobre su uso y finalidad.
- **Política de seguridad:** Los proveedores de acceso a internet están obligados a informar a sus usuarios sobre los medios técnicos que permitan la protección frente a las amenazas de seguridad en Internet. Igualmente deben informar a sus clientes sobre las responsabilidades en que pueden incurrir por el uso de internet con fines ilícitos. Los proveedores de servicios de correo electrónico están obligados a informar a sus clientes sobre las medidas de seguridad que aplican.
- **Contratación electrónica:** La LSSI asegura la validez y eficacia de los contratos que se celebren por vía electrónica, aunque no consten en soporte de papel.
- **Publicidad:** La LSSI determina que la publicidad debe presentarse de manera que no pueda confundirse con otra clase de contenido, identificando claramente al anunciante. Las ofertas promocionales, concursos o juegos deben mostrar también de forma clara las condiciones de acceso y participación. En el caso de comunicaciones comerciales a un usuario debe estar solicitado o autorizado por el propio usuario con carácter previo. En este caso, el proveedor podrá enviar publicidad sobre productos o servicios similares a los contratados por el cliente. El destinatario siempre tendrá la opción de oponerse al tratamiento de sus datos tanto en el momento de recogida de sus datos como en cada una de las comunicaciones comerciales que se le dirijan. El proceso será sencillo y gratuito.
- **Infracciones y sanciones**

Los tipos de infracciones y sus sanciones son los siguientes:

 - Infracción leve: Multa de hasta 30.000 euros
 - Infracción grave: Multa de hasta 150.000 euros
 - Infracción muy grave: Multa de hasta 600.000 euros



2.3. Anexos para profundizar (contenido informativo)

2.3.1. Funciones y Obligaciones del Personal Informático - Administradores de Sistemas

1. Funciones: Se encarga de administrar y monitorizar el correcto funcionamiento del sistema incluyendo cambios de versiones, administración de acceso y realización de copias de respaldo.

2. Obligaciones

- Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal. Dicha normativa puede consistir en normas, procedimientos, reglas y estándares, así como posibles guías.
- Cumplir lo dispuesto en la normativa interna vigente en cada momento.
- Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.
- Utilizar los controles y medios que se hayan establecido para proteger tanto los datos de carácter personal como los propios sistemas de información y sus componentes: los ficheros automatizados, los programas, los soportes y los equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.
- No intentar vulnerar los mecanismos y dispositivos de seguridad, evitar cualquier intento de acceso no autorizado a datos o recursos, informar de posibles debilidades en los controles, y no poner en peligro la disponibilidad de los datos, ni la confidencialidad o integridad de los mismos.
- Guardar secreto sobre los datos que pueda conocer, así como sobre controles y posibles debilidades, incluso después de haber causado baja en la Universidad.
- Usar de forma adecuada según la normativa los mecanismos de identificación y autenticación ante los sistemas de información, tanto sean contraseñas como sistemas más avanzados, como biométricos u otros, y en ambos casos; mediante acceso local o a través de redes de comunicaciones, cuando esté así previsto. En el caso de contraseñas cumplir lo recogido en la normativa, especialmente en cuanto a asignación, sintaxis, distribución, custodia y almacenamiento de estas, así como el cambio con la periodicidad que se determine.



- No ceder ni comunicar a otros las contraseñas, que son personales, que no estarán almacenadas en claro, y que serán transmitidas por canales seguros. Los usuarios serán responsables ante la Universidad de todos los accesos y actividades que se puedan haber realizado utilizando su código de usuario y contraseña.
- Evitar transmitir o comunicar datos considerados sensibles por medios poco fiables sin protección (telefonía de voz, correo electrónico, fax)
- Realizar las copias de los datos que en cada caso se establezcan en la normativa, así como proteger las copias obtenidas.
- Cumplir la normativa en cuanto a gestión de soportes informáticos que contengan datos de carácter personal, así como tomar precauciones en el caso de soportes que vayan a desecharse o ser reutilizados, mediante la destrucción, inutilización o custodia. En el caso de averías que requieran su transporte fuera de las instalaciones se intentará borrar previamente su contenido o se exigirán garantías escritas de que se hará así.
- No sacar equipos o soportes de las instalaciones sin la autorización necesaria, y en todo caso con los controles que se hayan establecido.

2.3.2. Delegado de Protección de Datos (DPD o DPO)

Será una persona con conocimiento especializado en Derecho y en la práctica en materia de protección de datos. Estos conocimientos serán exigibles en relación con los tratamientos que se realicen, así como las medidas que deban adoptarse para garantizar un tratamiento adecuado de los datos personales objeto de esos tratamientos.

El delegado de Protección de Datos debe desempeñar sus tareas y funciones con total independencia. Las funciones del delegado se encuentran especificadas en el artículo 39 del RGPD, siendo las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones del RGPD y demás normativa aplicable en protección de datos.
- Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.



- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al artículo 35 del RGPD.
- Cooperar con la Autoridad de control.
- Actuar como punto de contacto de la Autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.



Fuente: [wp243 rev.01 es \(aepd.es\)](https://wp243.rev.01.es/aepd.es)

2.3.3. Derechos de los Titulares de los Datos Personales

Cualquier persona, en tanto que titular de datos personales tiene reconocidos los derechos de acceso, rectificación, cancelación, oposición, limitación del tratamiento, olvido y portabilidad (derechos ARCOLP) a los mismos. Seguidamente se describe el modo en que puede ejercitar los mencionados derechos, así como alguna información que puede ser de su interés respecto a ellos.

El afectado también tiene derecho, con carácter previo a la presentación de una reclamación contra la Universidad de Almería ante la Agencia Española de Protección de Datos, a dirigirse al delegado de protección de datos de la Universidad de Almería. En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

1. Ejercitación de los derechos de ARCOLP

Los requisitos para ejercitar los mencionados derechos son:

- **Acreditación de la identidad** del interesado mediante cualquier documento válido, adjuntando una fotocopia en la solicitud.
- **Presentación de una solicitud dirigida a la Secretaría General de la UAL** indicando:
 - Nombre y apellidos del interesado o, cuando corresponda, de la persona que le represente, así como el documento acreditativo de 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, si corresponde.



- En caso de la rectificación o cancelación, indicación del dato a rectificar o cancelar y la causa que lo justifica.
- El interesado deberá usar cualquier medio que permita acreditar el envío y recepción de la solicitud y, por lo tanto, utilizar cualquiera de los procedimientos previstos para la presentación de solicitudes ante la Administración pública.

2. El derecho de Acceso

Es el derecho del interesado a solicitar y obtener del responsable del tratamiento gratuitamente información sobre el tratamiento de sus datos de carácter personal (Art. 15 RGPD). El afectado delimita con gran libertad el alcance del derecho de acceso, ya que puede optar a obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero o a la totalidad de sus datos sometidos a tratamiento.

El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, así como la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. El solicitante tiene derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en caso de que se confirme el tratamiento, el acceso a los datos y la siguiente información:

- Los fines del tratamiento.
- Las categorías de datos personales de que se trate.
- Los destinatarios o las categorías de destinatarios a quienes han sido o serán comunicados los datos personales, en particular los destinatarios establecidos en terceros países o las organizaciones internacionales.
- El plazo previsto durante el cual se conservarán los datos personales, cuando esto no sea posible, los criterios utilizados para determinar este plazo.
- La existencia del derecho a solicitar del responsable del tratamiento la rectificación o supresión de datos personales o la restricción del tratamiento de los datos personales relativos al interesado o a oponerse al tratamiento de dichos datos.
- El derecho a presentar una reclamación ante una autoridad de control.
- Cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen.



- En el caso de las decisiones basadas en un tratamiento automatizado que comprenda la elaboración de perfiles, información sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento la importancia y las consecuencias previstas de dicho tratamiento
- Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías apropiadas.

El responsable del tratamiento deberá proporcionar una copia de los datos de carácter personal objeto de tratamiento a través de alguna de las múltiples formas previstas en el listado orientativo del artículo 28 del RDLOPD:

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

3. El Derecho de Rectificación

Es el derecho que tiene el interesado a rectificar sus datos cuando sean inexactos. Habida cuenta de los fines para los cuales hayan sido tratados los datos, el interesado tendrá derecho a que se completen los datos personales cuando estos resulten incompletos, en particular por medio de la entrega de una declaración (Art. 16 RGPD).

4. El Derecho a la Supresión y Olvido

Derecho de Supresión

El Derecho a la Supresión no está considerado un derecho autónomo o diferenciado de los derechos ARCOL, sino es la consecuencia de la aplicación del derecho al borrado. Es una manifestación de los derechos de cancelación u oposición en el entorno on-line (Art. 17 RGPD).

Derecho del interesado a solicitar la supresión de sus datos, sin perjuicio del deber de bloqueo.

El responsable del tratamiento tendrá la obligación de borrar los datos personales sin demora injustificada cuando concurra alguna de las circunstancias siguientes:



- Los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados.
- El interesado ha retirado el consentimiento en que se basa el tratamiento y no exista otro fundamento jurídico para el tratamiento de los datos.
- El interesado se oponga al tratamiento de datos personales y no prevalezca otro motivo legítimo para el tratamiento.
- Los datos han sido tratados ilícitamente.
- Los datos deban suprimirse para el cumplimiento de una obligación legal de la Unión o Estados miembros, a la que esté sujeto el responsable del tratamiento.
- Los datos han sido recogidos en relación con la oferta de servicios de la sociedad de la información y no prevalezcan otros motivos legítimos para el tratamiento.

El Derecho al Olvido

Cuando el responsable del tratamiento haya hecho públicos los datos personales y esté obligado a suprimir dichos datos, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que traten los datos de que el interesado les solicita que supriman cualquier enlace a esos datos personales, o cualquier copia o réplica de estos. No es necesario que el interesado sufra un perjuicio para que ejerza el derecho al olvido.

Limitaciones en la supresión de datos.

El derecho a la supresión (u olvido) no será de aplicación, si el tratamiento de los datos personales es necesario:

- Para el ejercicio del derecho a la libertad de expresión e información
- Para el cumplimiento de una obligación legal que requiera el tratamiento de datos personales impuesta por el Derecho de la Unión o de un Estado miembro a la que esté sujeto el responsable del tratamiento o para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento
- Por motivos de interés público en el ámbito de la salud pública
- Con fines de archivo en interés público o de investigación científica e histórica, propósitos o fines estadísticos, en la medida en que el derecho de supresión haga imposible o



perjudique seriamente la consecución de los objetivos de los fines de archivo en el interés público, o de investigación científica e históricos o los fines estadísticos

- Para el reconocimiento, ejercicio o defensa de demandas judiciales.

5. El Derecho de Limitación de tratamiento

Derecho del interesado a obtener del responsable del tratamiento la limitación del tratamiento de los datos personales cuando:

- El interesado impugne la exactitud de los datos, durante un plazo que permita al responsable del tratamiento verificar la exactitud de los mismos;
- El responsable del tratamiento ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; o
- El interesado se ha opuesto al tratamiento mientras se verifica si los motivos legítimos del responsable del tratamiento prevalecen sobre los del interesado.

6. Derecho de Oposición

Derecho del interesado a oponerse, en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento (Art. 21 RGPD). Ante el ejercicio del derecho de oposición el responsable del tratamiento dejará de tratar los datos personales.

El derecho de oposición no aplicará cuando el responsable del tratamiento acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

Marketing directo

Cuando el tratamiento de datos personales tenga por objeto el marketing directo, el interesado tendrá derecho a oponerse en cualquier momento al tratamiento de los datos personales que le conciernan destinados a dicha comercialización, que incluye perfiles en la medida en que se relaciona con el marketing directo.

Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.



Tratamiento a efecto de investigación científica e histórica, o estadísticos

Cuando los datos personales se traten a efectos de investigación científica e histórica, o estadísticos, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de los datos personales que le conciernan, salvo que el tratamiento sea necesario para realizar una tarea efectuada por motivos de interés público.

Derecho de oposición a decisiones basadas únicamente en tratamiento automatizado

Derecho del interesado a no ser objeto de una decisión que evalúe aspectos personales relativos a él fundada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que tenga efectos jurídicos que le conciernan o que le afecte de modo significativo.

7. Derecho de Portabilidad de los datos

Derecho del interesado a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado y de uso habitual y de lectura mecánica y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable del tratamiento al que se hubieran facilitado los datos (Art. 20 RGPD).

Este derecho se podrá ejercitar en los siguientes casos:

- El tratamiento esté basado en el consentimiento o en un contrato.
- El tratamiento se efectúe por medios automatizados.

El ejercicio de este derecho se entenderá sin perjuicio del ejercicio del derecho a la supresión.

Supuestos en los que no se aplicará este derecho:

1. Al tratamiento necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento.
2. Cuando la revelación de los datos personales vulnere los derechos de propiedad intelectual respecto del tratamiento de dichos datos personales.



Recursos y enlaces

- Agencia Española de Protección de Datos <https://www.aepd.es/>



- [LOPD](#)



- [RGPD](#)



- [LSSICE](#)



- Portal ISO 27001 <http://iso27000.es/iso27002.html>



- Asociación Usuarios Internet <http://www.aui.es/>



- Asociación Internautas <https://www.internautas.org/>





Test de autoevaluación

1. La Agencia a quien tenemos que informar en caso de disponer de un fichero con información de clientes de nuestra empresa es:

- a) LSSICE
- b) LOPD
- c) ENS
- d) AEPD

2. Vamos a crear una tienda virtual para vender los productos de nuestra empresa. ¿Qué normativa he de cumplir?

- a) LSSICE
- b) LOPD
- c) ENS
- d) AEPD

3. La figura responsable del tratamiento de la información es:

- a) Delegado de Protección de Datos
- b) Encargado del tratamiento
- c) Responsable del tratamiento
- d) Administrador de Sistemas

4. ¿Qué derecho gestiona la opción que tiene un usuario de que sus datos se eliminen de una base de datos?

- a) Acceso
- b) Rectificación
- c) Limitación tratamiento
- d) Olvido



Solucionarios

Test de autoevaluación

1. La Agencia a quien tenemos que informar en caso de disponer de un fichero con información de clientes de nuestra empresa es:
 - a) LSSICE
 - b) LOPD
 - c) ENS
 - d) **AEPD**

2. Vamos a crear una tienda virtual para vender los productos de nuestra empresa. ¿Qué normativa he de cumplir?
 - a) **LSSICE**
 - b) LOPD
 - c) ENS
 - d) AEPD

3. La figura responsable del tratamiento de la información es:
 - a) Delegado de Protección de Datos
 - b) **Encargado del tratamiento**
 - c) Responsable del tratamiento
 - d) Administrador de Sistemas

4. ¿Qué derecho gestiona la opción que tiene un usuario de que sus datos se eliminen de una base de datos?
 - a) Acceso
 - b) Rectificación
 - c) Limitación tratamiento
 - d) **Olvido**