CUMPLIMIENTO LEGAL

Colección

PROTEGE TU EMPRESA

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
protege tu empresa

ÍNDICE

1- INTRODUCCIÓN 03
2- LEYES QUE HAN DE CUMPLIR PYMES Y AUTÓNOMOS 05
3- LOPDGDD Y RGPD 10
3.1. ¿QUÉ SON DATOS PERSONALES? 12
3.2. ACTORES PRINCIPALES 14
3.3. ¿CUÁLES SON LOS PRINCIPIOS EN LOS QUE SE BASA EL NUEVO RGPD? 16
3.4. RESPONSABILIDAD PROACTIVA: PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO 18
3.5. ¿CUÁLES SON LOS RIESGOS DE PRIVACIDAD? 19
3.6. ¿CÓMO SE HACE UN ANÁLISIS DE RIESGOS DE PRIVACIDAD? 21
3.7. ¿QUÉ TENGO QUE HACER PARA CUMPLIR CON EL NUEVO RGPD? 22
3.8. ¿QUÉ PASA SI NO CUMPLO? 23
3.9. SINERGIAS ENTRE LA GESTIÓN DE LA SEGURIDAD Y EL CUMPLIMIENTO DEL RGPD ... 24
4- LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN 27
4.1. ¿QUÉ TENEMOS QUE HACER PARA CUMPLIRLA? 28
4.2. ¿QUÉ TENEMOS QUE CONOCER COMO USUARIOS DE SERVICIOS DE INTERNET? 30
5- LEY DE PROPIEDAD INTELECTUAL 31
6- PROPIEDAD INDUSTRIAL Y MARCAS 33
7- NOMBRES DE DOMINIO 34
8- REFERENCIAS 36

ÍNDICE

ÍNDICE DE FIGURAS

Ilustración 1: Desarrollo legal en materia de ciberseguridad **09**

Ilustración 2: ¿Qué regula la LOPDGDD y el RGPD? **11**

Ilustración 3: Diagrama de flujo del tratamiento de datos **21**

Ilustración 4: *Checklist* para cumplir el RGPD con el Plan Director de Seguridad..... **26**

1. INTRODUCCIÓN

Todas las empresas están obligadas a cumplir la legislación. La finalidad de las leyes es garantizar y proteger los derechos de ciudadanos y empresas también en el entorno digital de la sociedad de la información. Algunas leyes regulan las actividades de las personas y los negocios a través de Internet como el comercio electrónico o las relaciones con la administración.

En general, estas son las ventajas de observar la ley:

- Demostrar respeto por los clientes, su privacidad y sus derechos como consumidores.
- Mostrar transparencia y respeto por el resto del comercio al acatar las reglas del juego.
- Evitar sanciones y problemas con terceros.
- Mejorar nuestra imagen, pues seremos más confiables.

En la Unión Europea, una de las prioridades de la Comisión Europea es la construcción de un **mercado único digital** **[1]**, **libre y seguro** en el que las empresas puedan vender en todo el territorio de la UE, y los ciudadanos puedan comprar en línea a través de las fronteras. Para ello, se desarrolla la **estrategia** para un mercado único digital europeo **[2]**, introduciendo **cambios** legislativos que afectan a los estados miembros para armonizar la legislación en todo el territorio. En particular, se han publicado directivas y reglamentos para regular el comercio electrónico, la protección de datos personales, la identificación electrónica y los servicios de confianza digital (sellos de tiempo, correo electrónico certificado o certificados de sitios web). La estrategia del mercado único digital europeo está produciendo algunos cambios:

- **Fin del bloqueo geográfico injustificado** que impide la práctica discriminatoria por razones de nacionalidad, lugar de residencia o establecimiento que impedía a los clientes acceder a productos y servicios y adquirirlos en un sitio web alojado en otro Estado miembro.
- **Fin de las tarifas de itinerancia** *(roaming)* que nos permite viajar por la UE y utilizar nuestros dispositivos móviles con las mismas tarifas de las que disfrutamos en nuestro país de origen.
- **Portabilidad transfronteriza de los contenidos en línea** que nos permite acceder a servicios en línea como películas, emisiones o juegos que hubiéramos contratado en nuestro país, cuando viajamos por la UE.
- **Modernización de la protección de datos** con el Reglamento General de Protección de Datos o RGPD **[4]** y la propuesta de reglamento de ePrivacy **[7]** actualmente en desarrollo.

- Transparencia en las tarifas y aumento de las competencias de supervisión de los reguladores en los **servicios de paquetería transfronterizos.**
- Creación de normas armonizadas en materia de **contratos y protección de los consumidores** en la compraventa online, tanto de bienes físicos como de contenidos digitales (libros electrónicos o aplicaciones para móviles, por ejemplo).
- Desarrollo de nuevas disposiciones para la eliminación de los obstáculos a la libre circulación de datos no personales para **impulsar la economía de datos** y crear un mercado único de servicios de almacenamiento y tratamiento de datos.
- El **pago y factura online** con el Reglamento de intercambio para pagos con tarjeta **[32]** y la Directiva de medios de pago **[33]**. Estas normas favorecen la transparencia, la seguridad y la armonización de las legislaciones nacionales.

La estrategia también facilita el desarrollo de nuevos servicios digitales, como el *cloud computing*, a través de la certificación de servicios en la nube, regulando los contratos, el cambio de proveedor y fomentando la creación de una nube abierta para la investigación científica.

2. LEYES QUE HAN DE CUMPLIR PYMES Y AUTÓNOMOS

Estas son algunas de las leyes que afectan a pymes y autónomos desde el punto de vista de la seguridad de la información:

- **La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales**, o LOPDGDD **[3]** vela por la privacidad de los ciudadanos en lo relativo a seguridad de los datos personales que gestionan las empresas, ya sea en formato electrónico o papel. Aplica a empresas grandes, pymes y autónomos, ya que todos ellos utilizan como mínimo datos de contacto del personal propio, clientes y proveedores.

  En 2016, la Unión Europea aprobó el Reglamento General de Protección de Datos Personales, el RGPD **[4]**, que entró en vigor en los países miembros el 25 de mayo de **2018**. Esta normativa, que se traspone en la legislación española en la citada LOPDGDD, tiene por objetivo reforzar los derechos de los ciudadanos, a la vez que favorece la creación de nuevos modelos de negocio que aprovechan los avances tecnológicos (como *big data* o IoT). Los cambios aprobados afectan a las empresas, en líneas generales, de la siguiente forma:

  - Se obliga a ciertas empresas a disponer de un **Delegado de Protección de Datos.**
  - Se elimina la necesidad de inscribir los ficheros en la Agencia Española de Protección de Datos (AEPD) **[5]**.
  - Se incorpora el principio de **«rendición de cuentas»**, por el cual las empresas tendrán que implantar mecanismos para garantizar el cumplimiento de sus responsabilidades de protección de datos.
  - Aumenta las sanciones.

  Con esta normativa, se introduce un estándar único europeo de protección de datos. Esto supone beneficios tanto para las empresas, que no tendrán que enfrentarse a distintas leyes en los países de la Unión cuando realicen tratamientos de datos personales, como a los consumidores, que verán sus derechos (consentimiento expreso, derecho al olvido, etc.) protegidos de igual forma en toda la UE.

- **La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico**, o LSSI-CE **[6]** y, cuando se apruebe, la propuesta de Reglamento ePrivacy **[7]** que ofrecen garantías de seguridad en el comercio electrónico, las comunicaciones electrónicas y las transacciones online. La LSSI-CE afecta a aquellas empresas que realicen actividades lucrativas o económicas en Internet:
  - comercio electrónico;
  - contratación en línea;
  - información y publicidad;
  - servicios de intermediación (ISP o proveedores de acceso a Internet, alojamiento y almacenamiento, y enlaces a contenidos);
  - prestadores de servicios de correo electrónico y similares;
  - registros de dominio y agentes registradores de dominio.

Los requisitos de cumplimiento legal nos obligan a incluir información sobre la empresa y los servicios que ofrecemos en la página web, la aplicación móvil, los perfiles en redes sociales y en las comunicaciones electrónicas, para proteger los derechos de los consumidores.

El reglamento de ePrivacy afectará a los prestadores de servicios de comunicaciones electrónicas, incluyendo los proveedores de servicios de acceso a Internet, de comunicaciones interpersonales y de transporte de señales.

- **La Ley de Propiedad Intelectual, o LPI [8]**, crea un marco de protección legal para las obras intelectuales. Para ello, define el concepto de «obra intelectual», crea un registro de obras y regula en qué términos se pueden o no utilizar estas obras según el criterio del autor. Son obras intelectuales las obras literarias, artísticas o científicas en cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro:
  - libros, folletos, impresos, escritos, discursos, conferencias y similares;
  - proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería;
  - gráficos, mapas y diseños relativos a la topografía, la geografía y, en general, a la ciencia;
  - obras fotográficas;
  - programas de ordenador.

La LPI protege los derechos morales (art. 14) y patrimoniales (explotación y copia) de los autores. En la legislación española, los derechos morales (relativos al reconocimiento de la autoría, divulgación, integridad, etc.) son inalienables e irrenunciables.

En 2019, en el marco de la estrategia del mercado único digital europeo, se ha adaptado a la era digital la normativa europea sobre **derechos de autor [34]**, para mejorar el acceso de los ciudadanos a los contenidos culturales (películas, músicas, etc.) en línea y ofrecer nuevas oportunidades a los creadores y a la industria de contenidos. Los países miembros tendrán que transponer esta directiva a sus ordenamientos jurídicos nacionales en un plazo de 2 años desde su firma.

Además de estas leyes, debemos tener en cuenta que en función de nuestro sector de negocio y clientes, debemos cumplir otros aspectos regulatorios adicionales que podrían afectarnos, por ejemplo:

- **Ley 11/2022 de 28 de Junio,** General de Telecomunicaciones y otra normativa del Código de las Telecomunicaciones, en el caso de que nos dediquemos a la prestación de servicios de comunicaciones electrónicas.
- **Ley 8/2011,** por la que se establece medidas para la protección de infraestructuras críticas para mejorar la prevención, preparación y respuesta del Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas.
- **Ley 25/2013** de impulso de la Factura electrónica y creación del registro contable de facturas en el Sector Público, y su desarrollo. Esta ley obliga, desde el 15/01/2015 a las empresas que tienen relación comercial con la Administración Pública a emitir facturas electrónicas.
- **Ley 6/2020, de 11 de noviembre,** reguladora de determinados aspectos de los servicios electrónicos de confianza y la **Ley 39/2015, de 1 de octubre,** del Procedimiento Administrativo Común de las Administraciones Públicas.
- **Ley 17/2001,** de Marcas y la **Ley 24/2015** de Patentes y otras leyes del Código de Propiedad Industrial, si nuestra actividad implica la gestión de patentes y marcas. Si tenemos un marco o logotipo corporativos tendremos en cuenta la Ley de Marcas.
- **Ley 13/2011,** de Regulación del Juego, si nuestra actividad tiene relación con el sector del juego online.

En particular, si eres autónomo o pyme, puedes hacer uso de los distintos servicios online de la administración **[9]**, por ejemplo:

- En la sede de la Agencia Tributaria **[10]**: presentar la declaración de la renta, cambios de domicilio fiscal, pagar impuestos, apoderar y otorgar representación, obtener certificaciones tributarias, participar en subastas o consultar deudas.
- En la sede de la Seguridad Social **[11]**: pedir la vida laboral, realizar los trámites de afiliación a la Seguridad Social, solicitar la situación de cotización/deuda de trabajadores, cambios de base de cotización (autónomos) o devolución de cuotas y pensiones.

- En la sede electrónica del Ministerio de Trabajo y Economía Social **[12]**: envío de los datos del certificado de empresa de tus trabajadores contratados, cuando finalice o se suspenda o reduzca su relación laboral; trámites relativos a prestaciones; publicar y gestionar ofertas de empleo.
- Sede del Punto de Acceso General (PAG) **[13]**: punto único de acceso para el ciudadano y empresas a trámites y servicios electrónicos agrupados por materias y a las sedes electrónicas de los Departamentos ministeriales, organismos autónomos, Comunidades Autónomas y Entidades Locales.
- En la sede de la Oficina Española de Patentes y Marcas **[14]**: solicitud de marca o nombre comercial y solicitud de registro del diseño industrial.

En los últimos años, como consecuencia de los cambios tecnológicos y los nuevos modelos de interacción entre ciudadanos, empresas y administración, se han promulgado y revisado leyes relacionadas con la seguridad de la información:

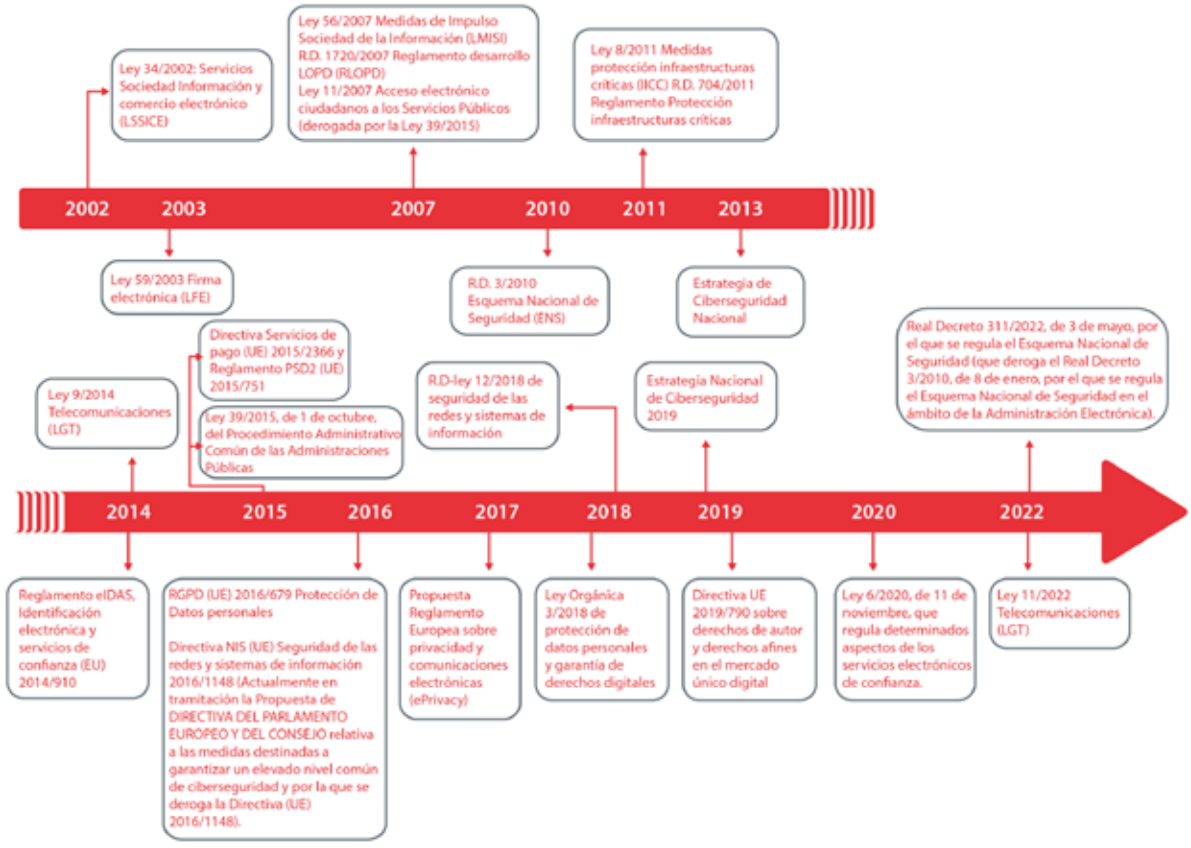


Ilustración 1
Desarrollo legal en materia de ciberseguridad

3. LOPDGDD Y RGPD

La LOPDGDD y el RGPD son las **normas que velan por la protección de los datos de carácter personal,** es decir, por la privacidad de las personas ya sean clientes, empleados o proveedores.

> Un **dato personal** es según el RGPD: «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, cultural, o social de dicha persona».

También son datos personales nuestros contactos con otras empresas, aunque quedan fuera del ámbito personal los datos corporativos: marcas, CIF, información corporativa, etc.

Estas normas deben cumplirse siempre que como empresa tratemos datos personales, aunque solo sean correos electrónicos o números de teléfono. La mayoría de empresas tratan con datos de clientes, proveedores y empleados por lo que, esta normativa siempre será de aplicación.

Las empresas, sociedades, comunidades, asociaciones y autónomos que han de cumplir el RGPD son:

- los establecidos en la UE, independientemente de si el tratamiento se hace o no en la UE;
- los que ofrecen bienes o servicios a personas que se encuentren en la UE;
- los que monitorizan el comportamiento de personas que se encuentren en la UE.

> El RGPD **[15]** define **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 de los principios de privacidad y derechos de los individuos sobre sus datos personales, en esta normativa se tratan los siguientes aspectos:

INFORMAR	OBTENER CONSENTIMIENTO	GARANTIZAR DERECHOS	NOTIFICAR VIOLACIONES
Tratamiento	Inequívoco	Que puedan ejercerlos	Que supongan riesgo para la privacidad
Decisiones automatizadas	No tácito		
Perfiles	Expreso en caso de datos de especial protección	Según los plazos RGPD	A la autoridad
Transferencias internacionales			A los usuarios

Ilustración 2
¿Qué regula la LOPDGDD y el RGPD?

3.1. ¿QUÉ SON DATOS PERSONALES?

Un **dato personal** es cualquier dato que identifique o que pueda ser asociado a una persona identificada o identificable.

Los datos personales son tanto aquellos que nos identifican (nombre, apellidos, DNI) como los que tienen que ver con nuestra situación laboral, financiera o de salud. También se incluyen ahora los datos biométricos y los biológicos, es decir, cualquier información con la que se nos identifique o se nos pueda identificar. Algunos como los relativos a salud, ideología, religión, origen racial, vida sexual y comisión de infracciones penales y administrativas, están **especialmente protegidos** en el RGPD y la LOPDGDD.

> Por ejemplo, un DNI es un dato personal. La talla del pie no es un dato personal por sí sola, pero sí cuando va asociada al DNI o a cualquier otro dato que ayude a identificar unívocamente a una persona, es decir, cuando sabemos que una persona utiliza una determinada talla del pie, es un dato de carácter personal.

Un dato personal no deja de serlo por estar en ficheros separados ni cuando están seudonimizados.

Según el RGPD seudonimizada está «aquella información que, sin incluir los datos denominativos de un sujeto, permiten identificarlo mediante información adicional, siempre que esta figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.»

> Por ejemplo, supongamos que tenemos dos hojas de cálculo en dos directorios separados a los que tenemos acceso. En una de ellas aparece el código de empleado y su DNI. En otra hoja, el código de empleado y la talla del pie. Es evidente que teniendo acceso a ellos, podremos saber la talla del pie de una persona.
>
> Los datos estarían seudonimizados si por ejemplo, cifráramos los datos relativos al DNI. Aun así seguirían siendo datos personales pues existe la posibilidad de volver a asociarlos a la persona.

Los datos personales que recojamos durante nuestras actividades deben ser adecuados, pertinentes, exactos y limitados a la finalidad del tratamiento.

> Por ejemplo, si estamos en las primeras fases de un proceso de selección, sería excesivo solicitar el historial médico del candidato o sus datos bancarios.

El RGPD indica que, en base a un **análisis de riesgos** de privacidad, debemos aplicar las medidas adecuadas de seguridad, técnicas y organizativas, para abordar los riesgos de:

- destrucción, pérdida o alteración accidental o ilícita de los datos personales cuando se transmiten, conservan o tratan de alguna otra forma;
- la comunicación o acceso no autorizado a dichos datos.

En un mundo donde los datos circulan de manera global, las empresas tenemos que prestar atención a la protección de la privacidad pues todas en mayor o menor medida, tratamos con datos personales, ya sean de clientes o de empleados, es decir, tratamos datos que deben ser protegidos.

Los datos personales que nuestros clientes nos dan al cumplimentar los pedidos o durante el curso de nuestros servicios, si caen en manos de delincuentes pueden ser utilizados en fraudes, extorsiones y suplantación de identidad. Protegerlos, evitando fugas y brechas de datos es un deber y una necesidad. Las pérdidas económicas y de imagen pueden ser cuantiosas.

3.2. ACTORES PRINCIPALES

Estos son algunos de los actores:

- **Afectado o interesado** es la persona a la cual pertenece el dato personal. Es el propietario de sus datos personales.
- **Responsable del tratamiento** es la persona física o jurídica que decide los fines y medios para tratar datos personales, es decir, cuando una empresa comienza a gestionar información de una persona (un cliente, un proveedor, un empleado, un paciente, etc.), se convierte en responsable de esa información de carácter personal. De **esta forma, cualquier mal uso de dicha información es responsabilidad suya.**
- **Un encargado del tratamiento** es aquella empresa a la que le «encargamos» un determinado tratamiento de datos. Por ejemplo, una gestoría que elabora las nóminas de nuestros empleados es un encargado del tratamiento, dado que realiza ese trabajo por encargo nuestro. En este caso, se ha realizar un **contrato** con el encargado, estipulándose las condiciones del tratamiento, las medidas de seguridad que debe implantar y cómo se devolverán los datos al final del contrato.
- **Delegado de protección de datos o DPD** es una nueva figura que aparece en el RGPD con funciones de gestión y control de la protección de datos dentro de la empresa, contacto con el nivel superior de dirección y total autonomía en sus funciones. Puede ser una persona de la empresa o externa. Actuará como punto de contacto entre la empresa y la AEPD.

Será obligatorio que nombren un DPD las empresas que realizan:

a. Operaciones de tratamiento que requieran una observación **habitual y sistemática** de personas a **gran escala.**

Según el RGPD las operaciones de tratamiento a gran escala son las «[...] que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, [...]»

b. Tratamiento **a gran escala de datos de categorías especiales.** Por ejemplo, datos que revelan ideología, afiliación sindical, opiniones políticas, creencias religiosas, origen racial o étnico, salud, vida sexual y orientación sexual, datos genéticos y biométricos, y datos de condenas penales o administrativas.

No será obligatorio en el caso de que tengas 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.

Además de lo expuesto, la LOPDGDD determina, en su **artículo 34**, las entidades que estarían obligadas a designar un Delegado de Protección de Datos.

3.3. ¿CUÁLES SON LOS PRINCIPIOS EN LOS QUE SE BASA EL NUEVO RGPD?

El nuevo reglamento aplica y extiende los principios en los que se basa la protección de datos personales:

1. **Principio de licitud, lealtad y transparencia**, es decir, los datos personales no pueden ser recogidos de forma fraudulenta, desleal o ilícita. El tratamiento será lícito si cumple con alguna de las condiciones del art. 6 del RGPD **[4]**. Además, el responsable debe facilitar al interesado toda la información sobre el tratamiento de forma concisa, transparente, inteligible y de fácil acceso.
2. **Principio de limitación de la finalidad.** Los fines para los que se recogen los datos personales deben ser determinados, explícitos y legítimos, y no serán tratados ulteriormente de forma incompatible con esos fines. No son fines incompatibles: el archivo en interés público, la investigación científica e histórica o los estadísticos, aunque podrán aplicarles garantías específicas, como anonimizarlos o, en algunos, casos seudonimizarlos.
3. **Principio de minimización de datos.** Los datos deben ser adecuados, pertinentes y limitados a los fines para los que se recogen. En este sentido, se podrán seudonimizar, es decir, tratar de manera que ya no puedan atribuirse al interesado, sin utilizar información adicional que estará separada y protegida.
4. **Principio de exactitud de datos.** Los datos han de ser exactos, correctos y completos, suprimiéndose o rectificándose, sin dilación, los que no estén actualizados o sean inexactos. El interesado tiene derecho a solicitar la rectificación de sus datos al responsable, que tendrá 1 mes para hacerlo.
5. **Principio de limitación del plazo de conservación de los datos,** es decir, solo deben ser mantenidos, de forma que se permita la identificación, durante el tiempo necesario para los fines del tratamiento. Además, se ha de informar al interesado, al tiempo de recoger los datos, de este plazo de conservación o de los criterios para determinarlo.
6. **Principio de integridad y confidencialidad,** es decir, los tratamientos han de garantizar la seguridad adecuada de los datos, aplicando medidas técnicas u organizativas (en base a un análisis de riesgos) apropiadas para:
   - la protección contra el tratamiento no autorizado o ilícito;
   - la protección contra su pérdida, destrucción o daño accidental.

A esto hay que añadir que el responsable del tratamiento será también responsable del cumplimiento de los principios anteriores. Esta **responsabilidad proactiva** implica realizar una **evaluación de riesgos de privacidad** que servirá de base para implantar las medidas técnicas y organizativas adecuadas para evitar que los datos caigan en manos de terceros no autorizados o sean accedidos por ellos, se pierdan o se traten posteriormente para fines no autorizados y para que las autoridades puedan verificarlo, es decir, las empresas deben controlar los datos personales en todo momento y poder demostrarlo.

3.4. RESPONSABILIDAD PROACTIVA: PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

Es evidente que la tecnología permite el seguimiento del rastro que las personas dejamos en Internet y en nuestro uso de dispositivos móviles. Esto es posible gracias a las *cookies* de los navegadores, los dispositivos RFID, las apps o los GPS de los móviles, etc., lo que permite, por ejemplo, personalizar la publicidad o la oferta de productos. Es lo que se denomina **«elaboración de perfiles»**, es decir, el tratamiento automatizado de datos personales para analizar o predecir: preferencias o intereses personales, el comportamiento, la situación económica, la fiabilidad o la salud (créditos bancarios, seguros,...), el rendimiento profesional (candidatos a empleos), la ubicación o los movimientos de las personas físicas.

Protección y explotación de datos personales son por ello para la empresa dos caras de una misma moneda. Por esto, la nueva legislación europea exige una mayor **proactividad** a las empresas y las insta a que **valoren sus riesgos** e incorporen mecanismos para minimizarlos, garantizando entre otros la **privacidad desde el diseño y por defecto** hasta la concepción de sus productos o servicios. Este tipo de medidas pueden ser controles técnicos o políticas proactivas que se aplican desde el principio, pensando en todo el ciclo de vida del proyecto y centrados en garantizar la privacidad del usuario.

Si tu empresa realiza tratamientos con datos personales tendrá que adoptar medidas al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos para el tratamiento de manera que respeten la privacidad. Es lo que se conoce como privacidad desde el diseño y por defecto.

- Los sistemas que incorporan privacidad **desde el diseño** han sido **construidos** teniendo en cuenta la protección de la privacidad. Algunas técnicas que pueden adoptarse desde el diseño son: anonimización, cifrado, control de accesos (autenticación) y trazabilidad.
- Los sistemas que incorporan privacidad **por defecto** están **configurados** por defecto de forma que ofrecen la mayor privacidad y garantizan la confidencialidad.

Las técnicas que deben aplicarse por defecto son: sobre la cantidad de datos personales recogidos, sobre la extensión del tratamiento y periodo de conservación del mismo, así como sobre la accesibilidad de los datos.

3.5. ¿CUÁLES SON LOS RIESGOS DE PRIVACIDAD?

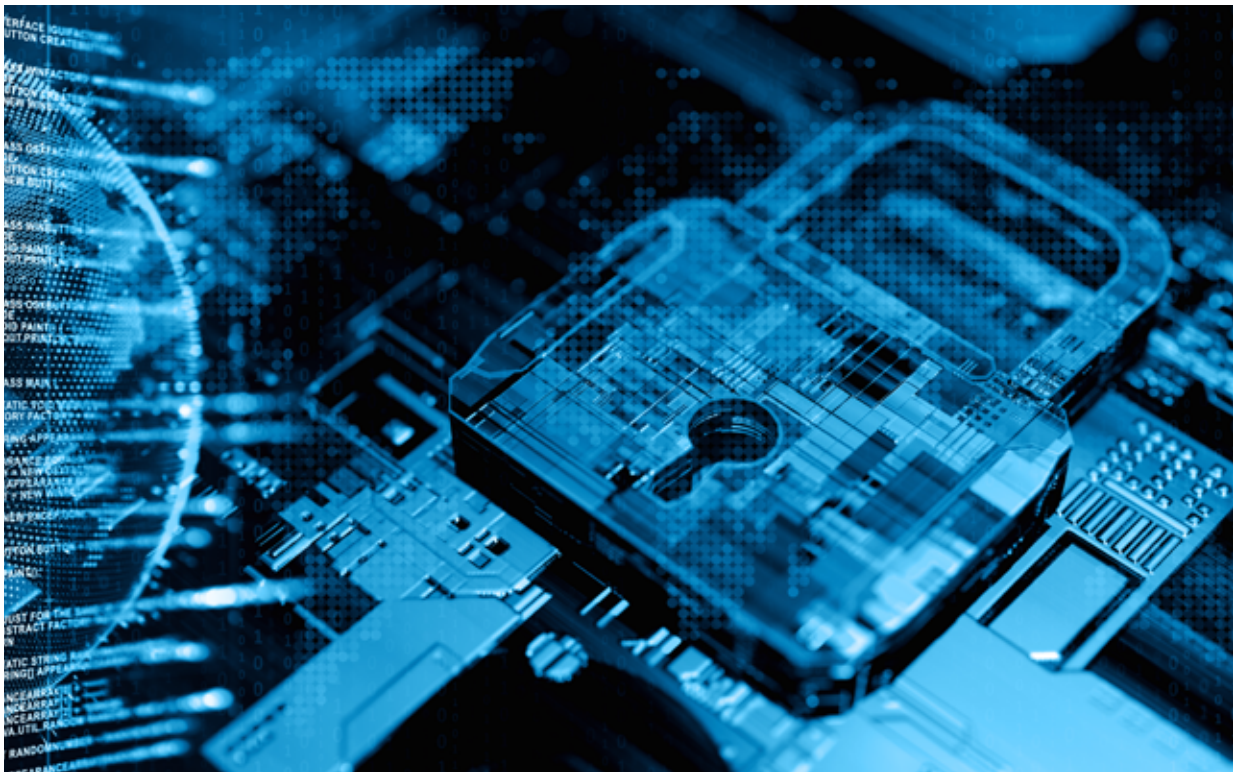
El objetivo de la evaluación de riesgos es determinar si el tratamiento de la información tiene consecuencias negativas para las personas, por ejemplo: marginación, exclusión social, dificultades de acceso a un puesto de trabajo, etc. Por ello, velar por la privacidad de nuestros clientes, proveedores y empleados es algo que puede favorecer la confianza en nuestro negocio.

En la empresa los riesgos para la privacidad, los que debemos evaluar, derivan fundamentalmente de:

- No ser transparentes al **informar** sobre tratamiento y no pedir el **consentimiento** adecuado.

> Ya no es válido el consentimiento tácito, es decir, basado en inacción u omisión.

- Tratar más datos de los necesarios o tomar datos cuya recogida no es legítima, para los que no estamos autorizados.



- No permitir o impedir a los propietarios de los datos ejercer sus **derechos**:
  - derecho a ser informado;
  - derecho de acceso;
  - derecho de rectificación;
  - derecho a supresión (derecho al olvido);
  - derecho a la limitación del tratamiento;
  - derecho a la portabilidad;
  - derecho de oposición (o a la exclusión voluntaria);
  - derecho a no someterse a la toma de decisiones automatizadas, incluyendo la elaboración de perfiles.
- Procesar los datos personales de forma descuidada o sin tener en cuenta los efectos para las personas que puedan derivarse de su mal uso.
- Difundirlos, derivarlos a terceros o utilizarlos para usos no autorizados.
- No eliminarlos de forma adecuada una vez ya no son necesarios.
- Realizar tratamientos de datos sin una base de legitimación lícita.
- Realizar transferencias internacionales de datos sin las garantías adecuadas.
- No adoptar las medidas técnicas y organizativas necesarias que garanticen la seguridad del tratamiento de datos realizado.
- No disponer de los contratos específicos en materia de protección de datos con aquellos proveedores que tengan acceso a datos personales de la entidad.

Las empresas grandes, pymes, micropymes y autónomos, hemos de cumplir con el RGPD, pero esto puede servir para reforzar también la seguridad en general de nuestro negocio, desde un punto de vista organizativo y tecnológico. Esto es posible si aprovechamos el momento para hacer una buena gestión de la seguridad, que incluya todos los aspectos de la privacidad mencionados.

3.6. ¿CÓMO SE HACE UN ANÁLISIS DE RIESGOS DE PRIVACIDAD?

Para comenzar con el análisis de riesgos de privacidad debemos:

- Identificar todas las **fuentes** de datos personales de nuestros tratamientos, catalogar todos los **agentes** responsables y los tipos de **operaciones** que se hacen con esos datos durante todo su ciclo de vida: captura, clasificación y almacenamiento, uso, cesión o transferencia y destrucción.
- Ser **exhaustivos** con los datos que se recogen: ¿dónde se almacenan?, ¿durante cuánto tiempo?, ¿en un fichero o en una base de datos?, ¿en qué equipos? ¿siguen los principios del tratamiento del RGPD?
- Hacer un **diagrama de flujo de datos del tratamiento**, es decir, desde que se recogen hasta que se utilizan o desechan con las transformaciones intermedias.

Ilustración 3
Diagrama de flujo del tratamiento de datos

- Priorizar y analizar en primer lugar a los agentes involucrados en el tratamiento y las acciones problemáticas sobre los datos, es decir, aquellas que pueden tener un **efecto adverso** sobre la privacidad de las personas.

3.6. ¿CÓMO SE HACE UN ANÁLISIS DE RIESGOS DE PRIVACIDAD?

Además, la evaluación de riesgo asociado a un tratamiento se podrá dividir en las siguientes etapas:

- Identificación de amenazas.
- Análisis y evaluación de los riesgos, en su impacto y probabilidad, para poder llevar acabo la evaluación del riesgo inherente.
- Tratamiento del nivel global del riesgo.

En la gestión del riesgo es necesario continuar con la observación del tratamiento y auditar de manera periódica los resultados obtenidos. Serán los responsables del tratamiento los encargados de realizar dicha evaluación creada por sus actividades de tratamiento con el fin de detectar cuando un tratamiento atañe un alto riesgo para los derechos y libertades de las personas físicas.

Para ello, la Agencia Española de Protección de Datos ha publicado en junio de 2021 la Guía sobre **"Gestión del riesgo y evaluación de impacto en tratamientos de datos personales"** en la que aúna todas las guías anteriores relativas a la realización de análisis de riesgos y eva- luacio- nes de impacto".

3.7. ¿QUÉ TENGO QUE HACER PARA CUMPLIR CON EL NUEVO RGPD?

Comienza con responder a estas preguntas:

- **¿Realizas una actividad comercial en la UE o tratas datos personales en la UE o sobre residentes en la UE?** Si es así, esto te afecta, has de ser responsable proactivamente, es decir, hacer un análisis de riesgos de privacidad **[5]**, tomar las medidas adecuadas y verificar que puedes demostrar que garantizas la privacidad.
- **¿Tratas datos de categorías especiales o a gran escala, es decir, son tratamientos de alto riesgo?** Sigue la guía para verificar si tratas datos de categorías especiales o a gran escala. Si es así, debes seguir la guía de la AEPD para realizar una Evaluación de Impacto en la protección de datos personales **[5]**.
- **¿Tienes menos de 250 empleados y no realizas tratamientos de alto riesgo?** Si es así cumple con FACILITA **[5]**, en caso contrario, tanto si tienes más de 250 empleados, como si realizas tratamientos de alto riesgo, has de llevar un Registro de actividades **[5]**.

> Tendrás que llevar un **Registro de actividad del tratamiento** si empleas a más de 250 personas o realizas tratamientos de datos personales de forma no ocasional o que pueda entrañar riesgos para su privacidad o con categorías especiales de datos.

- **¿Haces tratamientos a gran escala?** Si la respuesta es afirmativa: nombra un DPD, es decir, un Delegado de Protección de Datos y firma con él un contrato **[5]**. También has de firmar contratos con terceros si les encargas el tratamiento en todo o en parte.
- **¿Estás preparado por si tienes una brecha de seguridad con riesgo para la privacidad?** Actualiza tus procedimientos para **notificar**, en un plazo máximo de 72 horas a las autoridades y sin dilación a los interesados.

Consulta el documento **«Ganar en competitividad y cumplir el RGPD: Una guía de aproximación para el empresario» [31]**, si quieres conocer las medidas que has de aplicar para proteger la privacidad según el RGPD.

3.8. ¿QUÉ PASA SI NO CUMPLO?

Cualquier ciudadano de la UE tiene derecho a **presentar reclamaciones de forma individual o colectiva** si considera que el tratamiento de sus datos personales vulnera el RGPD. También, al ser la privacidad un derecho fundamental, tendrá derecho a la **tutela judicial efectiva** y **a la indemnización** por los **daños y perjuicios** sufridos a consecuencia de una infracción del RGPD.

Las autoridades podrán investigar y corregir las infracciones. Para ello, estarán en disposición de ordenar al responsable o al encargado **que facilite información, lleve a cabo auditorías u obtenga acceso a los datos, locales y equipos.**

Las sanciones por infracción podrán ir, desde advertencias si la infracción es posible, apercibimientos y limitaciones temporales, hasta prohibir el tratamiento, ordenar supresión de datos e imponer multas.

> Recuerda que la protección de datos personales de tus clientes, usuarios, colaboradores o empleados según el RGPD, no solo sirve para evitar las sanciones, sino que es además un importante **factor de competitividad y fidelización.**

3.9. SINERGIAS ENTRE LA GESTIÓN DE LA SEGURIDAD Y EL CUMPLIMIENTO DEL RGPD

Tener un Plan Director de Seguridad o PDS en tu empresa va a servir para cumplir con el RGPD. El PDS tiene entre sus objetivos reducir los riesgos para las personas y las organizaciones del mal uso de los datos personales.

El PDS, nuestro plan de seguridad, nos ayudará a tener un sistema de gestión de la seguridad de la información adecuado a nuestra organización, en continua mejora y actualización. El RGPD obliga a las empresas a analizar los riesgos contra la privacidad y a mantener registros de sus tratamientos de datos personales. Por esto, PDS y RGPD se solapan en estas áreas:

- seguridad de los datos personales,
- notificación de brechas de privacidad,
- gestión de contratos con encargados del tratamiento,
- registro de actividades de los tratamientos,
- privacidad por diseño y por defecto,
- derechos de los propietarios de datos.

Tanto si tenemos ayuda externa para las tareas técnicas, como si tenemos personal en plantilla, la siguiente tabla muestra algunas de las cuestiones que se han de tratar al poner el marcha el PDS para abordar a la vez el RGPD.

Seguridad de los datos personales	▶ ¿Qué tipos de datos personales se recogen, tratan y almacenan? ¿Son datos especialmente protegidos? ¿Protegemos estos últimos con seudonimización y cifrado? ▶ ¿Están documentados los controles y protocolos que aplican a datos personales? ¿Existen controles técnicos y organizativos específicos para cada categoría de datos y tratamiento? ▶ ¿Cómo se determinan las pérdidas de confidencialidad, integridad y disponibilidad? ¿Se realiza una evaluación de los riesgos para la privacidad? ▶ ¿Se cifran los datos personales en el almacenamiento y cuando se transmiten? ¿Tenemos capacidad de anonimizar y seudonimizar los datos personales?
Notificación de brechas de privacidad	▶ Para cada tratamiento de datos: ¿somos responsables o encargados? ▶ Los registros de los tratamientos, los inventarios de datos personales y sus métricas, ¿nos permiten identificar brechas de datos? ▶ Si tenemos DPO, ¿está incluido en los planes y procedimientos de gestión de incidentes? ▶ En caso de incidente, ¿tenemos controles específicos para mitigar los riesgos de las personas afectadas por brechas de datos personales? ▶ ¿Se ha incluido en los planes de respuesta a incidentes la notificación en 72 horas a las autoridades de control?
Gestión de encargados/ responsables del tratamiento	▶ ¿Tenemos los datos y contactos de todos los encargados de tratamiento? Y si somos encargados de los tratamientos de otros ¿tenemos los datos y contactos de los responsables de estos tratamientos? ▶ Nuestra evaluación de riesgos, ¿contiene cuestiones sobre las medidas técnicas y organizativas para la protección de privacidad dirigidas a los encargados del tratamiento? ▶ ¿Hemos redactado las cláusulas contractuales que incluiremos en los contratos con terceros que vayan a actuar de encargados del tratamiento de datos personales? ▶ ¿Hemos revisado los contratos existentes con responsables de tratamiento anteriores para que incluyan estas cláusulas? ▶ Para cada tratamiento del que seamos responsables ¿requerimos a los encargados que nos pidan autorización antes de subcontratar a su vez el tratamiento? ▶ Para cada tratamiento del que seamos encargados ¿incluyen nuestras políticas de seguridad los requisitos del artículo 32 del RGPD **[4]**

Registro de actividades de tratamiento	▶ Para cada tratamiento sabemos: » ¿Qué tipo de datos personales recogemos? » ¿Cómo y desde dónde se recogen los datos? » ¿Cómo y dónde se realiza cada parte del tratamiento? » ¿Cómo y a dónde se transfieren? » ¿Cómo y dónde se almacenan, protegen y borran? » ¿Qué políticas de retención y destrucción tenemos en marcha? ¿se siguen y revisan?
Privacidad por diseño y por defecto	▶ ¿Qué datos personales son necesarios para cada tratamiento que gestionamos como responsables o encargados? ▶ Nuestras políticas actuales, ¿limitan la cantidad de datos personales que se pueden recoger, bien sea por diseño de los formularios o por otras medidas de seguridad? ▶ Si contratamos un equipo de desarrollo o adquirimos nuevas aplicaciones, ¿incorporan los principios de privacidad en los requisitos de diseño de nuevas aplicaciones?
Derechos de los propietarios de datos	▶ ¿Hemos actualizado nuestros protocolos para informar a los propietarios de los datos y para recabar su consentimiento? ▶ ¿Tenemos procedimientos para clasificar e inventariar los datos de carácter personal y poder responder a las solicitudes de los usuarios sobre su información personal? ▶ Nuestros procedimientos actuales, ¿permiten a los propietarios de los datos acceder de forma segura a los datos personales que tenemos de ellos?, ¿tenemos otros datos personales a los que los propietarios no pueden acceder directamente?, ¿cómo se generan los informes sobre estos últimos y cómo se comunican de forma segura a los propietarios de los datos que lo soliciten? ▶ ¿Incluyen en nuestras políticas chequeos u otros procedimientos para revisar y corregir datos personales incorrectos o desactualizados? ▶ ¿Tenemos en marcha mecanismos para notificar a los propietarios cuando se modifican o se borran sus datos personales? Art. 19 RGPD **[4]** ▶ ¿Utilizamos perfilado o toma de decisiones automatizadas basados en datos personales y los tratamos conforme al Art. 22 RGPD? **[4]** ▶ ¿Tenemos en marcha procedimientos para no retener los datos personales más allá del tiempo necesario para el tratamiento o si el propietario decide ejercer su derecho de supresión? ¿Cómo se ejecutan y revisan estos procedimientos? ▶ ¿Disponen los encargados de la seguridad de la información y contactos actualizados sobre los terceros a quienes se transfieren los datos?

Ilustración 4
Checklist para cumplir el RGPD con el Plan Director de Seguridad

4. LEY DE SERVICIO DE LA SOCIEDAD DE LA INFORMACION

La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico **[16]** se publicó en 2002 y ha sido revisada posteriormente varias veces. Su finalidad es la protección de los derechos de los consumidores de servicios contratados a través de Internet. Es previsible que la legislación de esta materia se vea modificada debido a la tramitación de la Propuesta de Reglamento de privacidad electrónica (*ePrivacy*) de la Unión Europea **[7]**.

Actualmente, la ley impone una serie de obligaciones tanto a las empresas que prestan servicios en Internet como a los que venden productos. Para ello, distingue entre:

- Prestadores de servicios de intermediación que son las empresas que brindan conexión a Internet a sus clientes (ISP o *Internet Service Providers*), los prestadores de servicios de alojamiento de datos y los buscadores y proveedores de enlaces.
- Empresas y ciudadanos que utilicen la red para fines comerciales o lucrativos.

Actualmente, afecta, por tanto, a empresas y autónomos, ubicados en España, que utilicen las redes para alguna actividad económica o lucrativa. Se excluyen los notarios, los registros mercantiles y de la propiedad, en su función pública; y los abogados y procuradores, en sus funciones de representación y defensa en un juicio. Afecta, por tanto, a las empresas y autónomos con páginas web, tiendas online o que realicen contratos de servicios con clientes, siempre y cuando estas actividades tengan fines lucrativos. También afecta a toda actividad económica que utilice Internet de alguna forma, por ejemplo: páginas financiadas con publicidad, patrocinios, comunicaciones comerciales, buscadores y páginas de enlaces.

4.1. ¿QUÉ TENEMOS QUE HACER PARA CUMPLIRLA?

Si realizamos **comunicaciones comerciales** a través de Internet, ya sea por correo electrónico, SMS, redes sociales u otros medios, la LSSI-CE indica que debemos cumplir con la legislación de protección de datos informando sobre el tratamiento, recabando el consentimiento de los destinatarios y facilitándoles que puedan ejercer sus derechos.

En la LSSI-CE se indica que si lanzamos comunicaciones con publicidad, los mensajes deben estar identificados como tal con palabras como publi o publicidad. Además del RGPD, en la Comisión Europea se está tramitando una propuesta de Reglamento de privacidad electrónica (ePrivacy) que será de aplicación directa en todos los países miembros. El Reglamento ePrivacy aplicará a todos los datos de comunicaciones electrónicas sean o no datos personales e introducirá **un consentimiento más estricto** para la publicidad digital.

Si realizamos marketing directo vía SMS, correo electrónico o llamadas automatizadas, también tendremos que recabar el consentimiento del usuario a no ser que la legislación nacional permita registrarse en alguna lista para evitar ese tipo de marketing. Las llamadas de marketing directo se identificarán con un prefijo común.

Por otra parte, si tenemos **una página web o un blog**, con fines comerciales o si en ella incluimos publicidad de terceros para financiarnos o tomamos algún dato personal de nuestros usuarios (por ejemplo, el correo electrónico o usuario y contraseña) para enviarles un boletín o suscribirse a algún servicio también tenemos que cumplir la legislación de protección de datos como en el caso anterior y con la LSSI-CE como se indica a continuación.

En el caso de que tengamos un portal (extranet o intranet) o una **tienda online**, la mayoría de requisitos que establece la ley tienen que ver con la identificación del prestador de servicios. Debemos incluir la siguiente información en nuestra página web, generalmente en un aviso legal o similar:

- denominación social, NIF, domicilio social, correo electrónico de contacto y datos de inscripción registral;
- cuando existan o sean necesarios: códigos de conducta a los que estemos adheridos, datos de colegiación o titulación académica;
- si vendemos productos: los precios de los productos, especificando impuestos y gastos de envío.

El artículo 22 de la LSSI-CE es el que regula la utilización de las *cookies* en las páginas web **[6]**. Las *cookies* son unos ficheros de texto que se almacenan en los navegadores de los usuarios y sirven para facilitar el

acceso y registro de los usuarios en nuestra web y recabar información estadística o de uso de los servicios. Las *cookies* permiten, por ejemplo, que el usuario llene la cesta de la compra, mostrarle las páginas en su idioma, que podamos analizar sus preferencias de compra o que pueda entrar en nuestra tienda con su usuario de redes sociales. Algunas *cookies* tienen una vida limitada, no obstante los usuarios pueden desactivar en los navegadores su uso o eliminarlas.

En general, si nuestra página web utiliza ***cookies*** propias o de terceros, debemos pedir el consentimiento previo del usuario para poder instalarlas en su equipo, salvo que se utilicen *cookies* técnicas las cuales se encuentran exentas de consentimiento, además de informarles en caso de utilizar cookies de terceros (por ejemplo *Google Analytics*). Una buena práctica es incluir la Política de *Cookies* **[18]** o un apartado en el Aviso Legal.

Con la entrada en vigor del Reglamento de ePrivacy los usuarios tendrán control sobre toda la información cuya pérdida o alteración pueda producir daños que afecten a su privacidad que se almacene en sus dispositivos, sin tener que hacer clic en un banner para dar su consentimiento cada vez que visite una página. Se prevé que las opciones de los navegadores dispongan de una forma sencilla de aceptar o rechazar las *cookies*. Las *cookies* que no afecten a la privacidad no necesitarán consentimiento. Este Reglamento no solo aplicará a las *cookies* sino también a otras herramientas de rastreo, como por ejemplo: direcciones MAC, número del dispositivo o IMEI y direcciones IP.

En los casos que sea necesario recabar el consentimiento del usuario, este será explícito, más riguroso y para cada uno de los usos que se vaya a hacer de los datos.

Adicionalmente, si tenemos una página web a través de la cual se permita la **contratación de servicios online**, debemos también informar de los siguientes puntos, previamente al contrato:

- los trámites a seguir por el usuario para «celebrar» el contrato;
- si almacenaremos el documento electrónico y si estará disponible posteriormente para su descarga por parte de nuestro cliente;
- los medios técnicos disponibles para corregir datos erróneos durante la contratación;
- las lenguas en las que podrá formalizarse el contrato;
- las condiciones generales a que debe sujetarse el contrato.

4.2. ¿QUÉ TENEMOS QUE CONOCER CÓMO USUARIOS DE SERVICIOS DE INTERNET?

Como empresas o autónomos que contratamos servicios a proveedores de Internet (conexión, alojamiento, buscadores y proveedores de datos) y a otros proveedores tecnológicos (redes sociales, correo electrónico, servicios en la nube, etc.) somos consumidores de los mismos y tenemos que conocer también nuestros derechos.

Los proveedores de servicios de interconexión, además de otros requisitos particulares (colaboración con las autoridades), han de cumplir con los requisitos anteriores relativos a la identificación y a la contratación.

Los proveedores de acceso a Internet deberán:

- Informar a sus usuarios sobre los medios técnicos que permitan la protección frente a las amenazas de seguridad en Internet (virus informáticos, programas espías, *spam*) y sobre las herramientas para el filtrado de contenidos no deseados.
- Informar a sus clientes sobre las medidas de seguridad que apliquen en la provisión de sus servicios.
- Informar a sus clientes sobre las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos.

Los prestadores de servicios de correo electrónico:

- Informar a sus clientes sobre las medidas de seguridad que apliquen en la provisión de sus servicios.

Ambos deberán informar a los usuarios en la web acerca de las exigencias reflejadas en la LSSI, tales como: nombre o denominación social y datos de contacto; número de inscripción en los registros correspondientes, NIF o CIF, información sobre el precio de productos, códigos de conducta a los que se encuentre adherida la entidad, etc.

5. LEY DE PROPIEDAD INTELECTUAL

Esta ley, regulada en el Real Decreto Legislativo 1/1996 **[19]**, nace de la necesidad de proteger las obras de propiedad intelectual abarcando cualquier tipo de creación literaria, artística o científica fruto de nuestra actividad empresarial.

Debido a la gran expansión de Internet y a la posibilidad de digitalizar y compartir de forma gratuita la gran mayoría de obras, esta ley se encuentra en constante evolución tratando de contener la distribución masiva de copias ilegales de obras intelectuales protegidas.

No se trata de una ley con puntos concretos que deban cumplir las empresas españolas sino que, por un lado, establece un marco para que empresas y ciudadanos puedan registrar sus obras, y por otro proporciona herramientas para perseguir las actividades delictivas sobre estas obras.

La LPI protege los derechos morales (art. 14) y los patrimoniales (explotación y copia) de los autores. En la legislación española los derechos morales (relativos al reconocimiento de la autoría, divulgación, integridad, etc.) son inalienables e irrenunciables.

En cuanto a los derechos patrimoniales como empresa, tendremos que:

- No utilizar obras protegidas sin pagar los derechos a los autores, esto afecta tanto al software que utilicemos como a textos, imágenes, videos y otras creaciones. También incluye a las creaciones que contratemos a terceros (creativos, desarrolladores, etc.) mediante contratos mercantiles.
- Proteger como empresa los derechos de las creaciones propias o de los empleados en virtud de su relación según contrato laboral (art. 51). Los contratos con empleados han de celebrarse por escrito, respetando siempre el derecho del creador de reconocerse como autor real de la obra. Si no hubiera contrato se supone una cesión tácita del empleado de la explotación por dos años y sólo para la actividad empresarial de la empresa.

Para evitar que en nuestra empresa existan copias ilegales de material protegido, como software o material multimedia, debemos tomar las medidas oportunas entre las que destacamos las siguientes:

- Documentar en la normativa interna la prohibición de utilizar software sin la adecuada licencia, así como el compromiso de la dirección de velar por su cumplimiento.
- Proporcionar a los empleados todo aquel software (con sus licencias pertinentes) que necesiten para desarrollar su trabajo. No tiene sentido que exija-

mos a nuestros empleados que no instalen software ilegal si en ocasiones les proporcionamos copias de programas de los que no tenemos licencia.

- Disponer de un inventario automatizado de software instalado en los equipos de los usuarios para revisar periódicamente que no existe software ilegal o que no se excede del número de licencias instaladas.
- Revisar las licencias de uso de los distintos programas para asegurarse de que no se están utilizando licencias destinadas al uso doméstico en un entorno laboral.
- Restringir la instalación de software por parte de los usuarios.
- Monitorizar las cuotas de disco en busca de ficheros y carpetas especialmente grandes (música o películas).
- Monitorizar la red y su ancho de banda para detectar el uso de programas de compartición de ficheros no autorizados.
- Filtrar las páginas web de descarga directa.
- Limitar el uso de puertos USB para conectar memorias externas.
- Monitorizar el uso que se haga de impresoras, fotocopiadoras y unidades de grabación de discos compactos (CD, DVD, *BluRay,* etc.).
- Guardar en lugar seguro las licencias del software adquirido.
- Pagar los derechos (*copyright*) y reconocer la autoría en cualquier caso por los textos, imágenes y documentos multimedia que utilicemos si no son propios ni están sujetos a licencias *Creative Commons* **[20]**.

6. PROPIEDAD INDUSTRIAL Y MARCAS

La Propiedad Industrial **[30]** otorga, mediante varias leyes, derechos sobre ciertas creaciones inmateriales que se protegen como si fueran derechos de propiedad. Según la legislación en esta materia **[21]**, en España hay varios tipos de derechos de Propiedad Industrial: diseños industriales, marcas y nombres comerciales, patentes y modelos de utilidad (invenciones), y topografías de semiconductores (circuitos integrados).

Los derechos de Propiedad Industrial permiten a quien los ostenta decidir quién puede usarlos y cómo puede usarlos. Se otorgan mediante un procedimiento a través de la Oficina Española de Patentes y Marcas y la protección se extiende a todo el territorio nacional. Para las invenciones, diseños industriales o circuitos integrados nos remitiremos a la legislación particular **[21]**. Con la facilidad e impunidad que permite Internet se puede dar el caso de que empleados descontentos puedan divulgar elementos fundamentales para el negocio, como patentes o secretos industriales. También estos datos están a riesgo, accidental o no, de **fuga de datos [22]**.

Por otra parte, las empresas tienen también marcas y nombres comerciales. En realidad son combinaciones gráficas o denominativas que ayudan a distinguir en el mercado unos productos o servicios de otros similares ofertados por otras empresas. Están regulados por la Ley 17/2001 de 7 de diciembre de Marcas.

La marca y el nombre comercial son parte de nuestra **identidad digital [23]** y puede ser objeto de abuso, que ocurre cuando alguien utiliza una grafía, logo o imagen corporativa o de algún producto con un gran parecido a nuestra marca. Esto supone un riesgo para la identidad y reputación de una empresa asociado con el uso por terceros no autorizados de los derechos de propiedad industrial. En caso de conflicto, siempre que hayamos registrado la marca, podemos acudir a los tribunales.

7. NOMBRES DE DOMINIO

Los nombres de dominio son la dirección de una empresa, organización, asociación o persona en Internet. Tienen una doble utilidad:

- Identificarnos en Internet, como empresa o a nuestros productos y servicios en la red.
- Ser nuestra dirección en la red, siendo la forma más fácil, rápida e intuitiva para localizarnos.

Existen tres niveles de nombres de dominio:

- Los que acaban en com, gob, edu, org (entre otros) que son asignados por instituciones designadas por el ICANN **[24]**, que también registra los nuevos dominios de primer nivel libres (gTLD).
- Los nombres de dominio de segundo nivel son los que identifican el país y en España los asigna a Red.es **[25]**.
- Los nombres de dominio de tercer nivel como «.com.es», «.nom.es», «.org.es», «.gob.es» y «.edu.es», que también los asigna en España Red.es.

El registro de nombres de dominio se rige por su propia legislación nacional e internacional (en función del tipo de dominio) y **no es competencia de la Oficina Española de Patentes y Marcas.** Los conflictos que entre ambas modalidades pudieran surgir deben dirimirse ante Organismos Internacionales de Arbitraje o ante los Tribunales.

El nombre de dominio también forma parte de nuestra **identidad digital** como empresa. Existe el riesgo de registro abusivo de nombre de dominio, cuando alguien registra un nombre parecido al nuestro, como se indica en la «Guía de Identidad digital» **[23]**. Esto puede afectar negativamente a nuestra imagen.

En caso de que un tercero haya ocupado un dominio sin autorización debe procederse a su reclamación. Para ello, se contemplan diferentes vías:

- En primer lugar, respecto de los dominios «.es» existe un procedimiento de resolución extrajudicial de conflictos desarrollado y coordinado por la Entidad Pública Empresarial Red.es **[26]**. Para poder iniciar esta reclamación arbitral es necesario acreditar estar en posesión de derechos previos sobre la denominación y justificar la mala fe del dominio registrado en lugar del que reivindicamos.

- En segundo lugar, existe un procedimiento equivalente de la ICANN, denominado política uniforme de resolución de conflictos (UDRP) **[27]**, que contempla una serie de entidades internacionales acreditadas para realizar el arbitraje.
- También es posible acudir ante la jurisdicción ordinaria invocando la legislación sobre competencia desleal **[28]** además de la Ley de Marcas **[29]**. La ley tiene por objeto la protección de la competencia en interés de todos los que participan en el mercado, y a tal fin establece la prohibición de los actos de competencia desleal, como es en algunos casos la utilización fraudulenta de nombres de dominio.

8. REFERENCIAS

[Ref - 1]. UE, Comisión Europea «Digital Single Market» - https://www.consilium.europa.eu/es/policies/digital-single-market/

[Ref - 2]. UE, Consejo Europeo «Mercado único digital de Europa» - http://www.consilium.europa.eu/es/policies/digital-single-market/

[Ref - 3]. BOE, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales - https://www.boe.es/eli/es/lo/2018/12/05/3/con

[Ref - 4]. UE, Reglamento 2016/679 Reglamento General de Protección de Datos - http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES

[Ref - 5]. Agencia Española de Protección de Datos - https://www.aepd.es

[Ref - 6]. BOE, Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico LSSI-CE - https://www.boe.es/eli/es/l/2002/07/11/34/con

[Ref - 7]. UE, Propuesta de Reglamento de privacidad electrónica (ePrivacy) de la Unión Europea - https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010

[Ref - 8]. BOE, Código de la propiedad intelectual - https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=087_Codigo_de_Propiedad_Intelectual_&tipo=C&modo=2

[Ref - 9]. Gobierno de España, Sedes electrónicas - https://sede.agenciatributaria.gob.es/Sede/inicio.html

[Ref - 10]. Agencia Tributaria - http://www.agenciatributaria.es/AEAT.internet/Inicio/_Segmentos_/Empresas_y_profesionales/Empresas_y_profesionales.shtml

[Ref - 11]. Seguridad Social - http://www.seg-social.es/wps/portal/wss/internet/Inicio

[Ref - 12]. Sede electrónica del Ministerio de Trabajo y Economía Social - https://sede.mites.gob.es/

[Ref - 13]. Gobierno de España, Sede electrónica del Punto de Acceso General - https://sede.administracion.gob.es/PAG_Sede/HomeSede.html

[Ref - 14]. Oficina española de patentes y marcas - https://sede.oepm.gob.es/eSede/es/index.html

[Ref - 15]. INCIBE, Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario - https://www.incibe.es/empresas/guias/ganar-competitividad-cumpliendo-el-rgpd-guia-aproximacion-el-empresario

[Ref - 16]. BOE, Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico - https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

[Ref - 17]. Gobierno de España, Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico - www.lssi.gob.es

[Ref - 18]. AEPD, Guía sobre el uso de las cookies - https://www.aepd.es/guias/guia-cookies.pdf

[Ref - 19]. BOE, Ley de Propiedad Intelectual - https://www.boe.es/diario_boe/txt.php?id=-BOE-A-1996-8930

[Ref - 20]. Creative Commons - https://creativecommons.org/licenses/?lang=es_ES

[Ref - 21]. BOE, Códigos Ley de propiedad industrial - https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=067_Propiedad_Industrial&tipo=C&modo=2

[Ref - 22]. INCIBE, Cómo gestionar una fuga de información - https://www.incibe.es/empresas/guias/guia-fuga-informacion

[Ref - 23]. INCIBE, Ciberseguridad en la identidad digital y la reputación online - https://www.incibe.es/empresas/guias/guia- ciberseguridad-identidad-online

[Ref - 24]. ICANN - https://www.icann.org/es

[Ref - 25]. Dominios.es - https://www.dominios.es/es

[Ref - 26]. Red.es - https://www.red.es/es

[Ref - 27]. ICANN, UDRP - https://www.icann.org/resources/pages/enforcing-udrp-2013-07-16-es

[Ref - 28]. BOE, Ley 3/1991, de 10 de enero, de Competencia desleal - https://www.boe.es/buscar/act.php?id=BOE-A-1991-628

[Ref - 29]. Oficina Española de Patentes y Marcas, LEY 17/2001, de 7 de diciembre, de Marcas - http://www.oepm.es/cs/OEPMSite/contenidos/NORMATIVA/NormasSobreMarcas-YOtrosSignosDistintivos/NSMYOSD_Nacionales/LEY_172001_de_7_de_diciembre_de_Marcas.htm

[Ref - 30]. Ministerio de Industria y Turismo, Oficina Española de Patentes y Marcas, Propiedad Industrial - https://www.oepm.es/es/conoce-la-propiedad-industrial/

[Ref - 31]. INCIBE, Ganar en competitividad y cumplir el RGPD: una guía de aproximación para el empresario - https://www.incibe.es/empresas/guias/ganar-competiti-vidad-cumpliendo-el-rgpd-guia-aproximacion-el-empresario

[Ref - 32]. UE, Reglamento (UE) 2015/751 sobre las tasas de intercambio aplicadas a las operaciones de pago con tarjeta - https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=-CELEX%3A32015R0751

[Ref - 33]. UE, Directiva 2015/2366 sobre servicios de pago en el mercado interior - https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A32015L2366

[Ref - 34]. UE, Directiva 2019/790 sobre los derechos de autor y derechos afines en el mercado único digital - https://www.boe.es/doue/2019/130/L00092-00125.pdf


Financiado por
la Unión Europea
NextGenerationEU


Plan de
Recuperación,
Transformación
y Resiliencia

España | digital 2026

incibe_

protege
tuempresa