Ganar en competitividad cumpliendo el RGPD:

guía de recomendaciones para empresas

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

ÍNDICE

1 PROTEGE LA PRIVACIDAD Y GANARÁS EN COMPETITIVIDAD

La ciberseguridad en general, y la protección de datos personales en particular, adquieren cada día más importancia para la **mejora de la competitividad** en el mundo de los negocios arrastrado por las **ventajas** en conectividad, inmediatez y ubicuidad a la inevitable transformación digital. Tanto es así que en los últimos años la ciberseguridad se ha convertido en una **prioridad**. Prueba de ello son los cambios que se están produciendo en las normativas que a su vez implican importantes **desafíos** para las organizaciones.

En el ámbito internacional se ha incrementado en los últimos años la importancia que se concede a la **transformación digital** como elemento fundamental para conseguir un crecimiento económico inclusivo y sostenible. Los esfuerzos de la UE se han centrado en conseguir **un entorno digital más equitativo, abierto y seguro.**

Para ello, en el seno de la Comisión Europea han entrado en vigor en los últimos años, entre otras, unas normativas relativas a la ciberseguridad que afectan en mayor o menor medida a las empresas, ya sean proveedoras o clientes de otras empresas, y cuyo plazo de transposición finaliza en el año 2018.

- **La Directiva de Servicios de Pago (PSD2)** [1] para el desarrollo del mercado interior de pagos electrónicos que aplica a los proveedores de servicios de pago electrónico, es decir, al sector de las entidades financieras y al comercio electrónico, con importantes mejoras para la protección de los consumidores.

1

"Ante esta perspectiva, es importante que las empresas **examinen su situación** en cuanto a la seguridad de la información en sus organizaciones, además de la que les ofrecen sus proveedores de servicios digitales, **pues la confianza de sus clientes, y con ella su propia competitividad, está en juego"**

- **El Reglamento sobre identificación electrónica y servicios de confianza (eIDAS)** [2] También relacionado con el comercio y las transacciones electrónicas.
- La elaboración de la **Directiva NIS1** [3], **relativa a las medidas destinadas a garantizar un elevado nivel de seguridad de las redes y sistemas de información en el marco de la UE** resultó necesaria debido a la creciente amenaza de los ciberataques, así como la inexistencia de un marco legal que promoviera la seguridad cibernética dentro de la UE.

  La Directiva insta a los Estados miembros a estar dotados de una serie de medidas de prevención, detección, respuesta y mitigación de los incidentes y riesgos que afecten a las redes y sistemas de información, resultando aplicable a los operadores de servicios esenciales (energía, transporte, banca, mercados financieros, sanidad, suministro y distribución de agua potable e infraestructura digital) y a los proveedores de servicios digitales (mercados online, motores de búsqueda online y servicios *cloud*). Esta directiva ha llevado a la reciente asociación de las entidades expertas en la respuesta ante incidentes de ciberseguridad en España: **CSIRT.es** [4] «*computer security incident response teams*»

  Debido a la creciente sofisticación de las amenazas cibernéticas, se vio necesario establecer un nuevo marco regulatorio, cuyo objetivo fuese fortalecer la seguridad cibernética dentro de la UE. Es por ello por lo que en diciembre de 2022 se aprobó la Directiva (UE) 2022/2555, de 14 de diciembre de 2022 (**Directiva NIS2**) [5], actualizando así la Directiva NIS1.

  La **Directiva NIS2** establece requisitos más rigurosos en materia de seguridad cibernética y amplía su alcance para abarcar sectores y servicios de vital importancia económica y social. Esta normativa considera esenciales o importantes a las entidades en función de la crítica de sus sectores, tamaño o servicios prestados, eliminando la categorización previa de la NIS1. Además, refuerza los estándares de seguridad, detalla el proceso de notifi-

1

cación de incidentes, aborda la seguridad en la cadena de suministro, fortalece el intercambio de información y establece una red europea de crisis (EU-CYCLONe). De igual modo, promueve la colaboración público-privada, facilita el intercambio de datos sobre amenazas y vulnerabilidades, y fomenta la confianza y la implementación de mejores prácticas en ciberseguridad en toda la UE.

- Y finalmente la relativa a la protección de datos personales, que se concreta en el **Reglamento General de Protección de datos, RGPD** [6], también llamado GDPR por sus siglas en inglés, y que aplica a todas las empresas que realicen tratamientos de datos personales.

"Podríamos decir que el **RGPD** es de amplio espectro, al verse afectadas empresas de todos los sectores y tamaños"

Ante esta perspectiva, es importante que las empresas **examinen su situación** en cuanto a la seguridad de la información en sus organizaciones —y, en particular, en cuanto a sus políticas de privacidad—, además de la que les ofrecen sus proveedores de servicios digitales, **pues la confianza de sus clientes, y con ella su propia competitividad, está en juego.**

Podríamos decir que el RGPD es de amplio espectro, al verse afectadas empresas de todos los sectores y tamaños. Es un hecho que los usuarios, al relacionarse con las empresas emplean cada vez más la tecnología, por ejemplo redes sociales, aplicaciones móviles y tiendas online. En estas interacciones intercambian gran cantidad de información personal (identificación, gustos, hábitos de compra, preferencias,...) que, a su vez, resulta esencial para el éxito y la estrategia de las empresas. Pero los usuarios son **cada vez más conscientes del valor de su privacidad**, y no están dispuestos por ejemplo: a verse avasallados por publicidad, a ser localizados cuando no lo esperan o a ser discriminados por su perfil; ni mucho menos a resultar víctimas indirectas de una fuga masiva de datos de sus proveedores o tiendas de confianza, o a ser víctimas de un robo de identidad.

1

"Esta guía trata de la protección de datos personales y del **cumplimiento** del nuevo Reglamento, el **RGPD**, en las empresas"

Esta guía trata de la protección de datos personales y del cumplimiento del nuevo Reglamento, el RGPD, en las empresas, no sólo para evitar las temidas y cuantiosas sanciones por incumplimiento, sino porque la protección de sus clientes, usuarios, colaboradores o empleados es, además de una responsabilidad, un importante factor de competitividad y fidelización.

2 ¿QUÉ ES EXACTAMENTE EL RGPD?

La importancia del uso de los datos para crear nuevos servicios y dar soporte a los existentes está en continuo crecimiento. El **dato es el combustible o la nueva materia prima del siglo XXI** e incluso podemos hablar de la «economía del dato», aunque sin olvidar en ningún momento los derechos de los ciudadanos en el mundo digital, en concreto a la protección de la intimidad, y al mismo tiempo el libre flujo de datos personales.

Además los avances tecnológicos y la reducción de los costes de almacenamiento están permitiendo, junto con el desarrollo de las técnicas estadísticas, **el análisis de datos masivos.** Estos datos en grandes cantidades, en su mayoría datos personales que vienen de distintas fuentes, son heterogéneos y varían rápidamente. Es lo que se conoce como *Big Data*. Algunos ejemplos de *Big Data* son los datos de nuestra actividad en las redes sociales, tráfico web, transacciones en tiendas online, sensores en ***wearables*** y móviles, datos con geoposicionamiento, datos científicos, financieros, de salud o los de las ciudades inteligentes o ***smartcities***, etc.

La analítica de estos *Big Data* permite descubrir **tendencias**, mostrar el comportamiento de los usuarios y realizar **pronósticos**. Los clientes desvelan, con sus datos de uso, sus **necesidades**, cómo utilizan productos y servicios, los **patrones de compra o de comportamiento** y anticipan los posibles **cambios en la demanda**. Con la analítica de *Big Data* las empresas pueden optimizar la toma de decisiones, sus estrategias de marketing, su eficiencia interna y adaptar sus productos y servicios a los gustos y necesidades de perfiles de consumidores.

Pero la retención masiva de datos de carácter socioeconómico, demográfico, de comportamiento (búsquedas, compras, comentarios,...) y financiero con propósitos analíticos puede **afectar a los derechos de los consumidores** al suponer pérdidas en su privacidad y libertad individual. Los legisladores, los tecnólogos y las empresas se enfrentan al reto, desde una perspectiva de **seguridad y privacidad**, de garantizar que los consumidores tengan el suficiente control sobre sus datos para prevenir el uso indiscriminado de estos a la vez que se mantiene su utilidad para extraer conocimiento, patrones y, en resumen, valor.

2

"Toda persona tiene derecho a la **protección de los datos de carácter personal** que la conciernan"

Al margen de los posibles aspectos éticos que se derivan de los usos abusivos, como por ejemplo la vigilancia a la que podemos estar sometidos y la discriminación o control social, existen otros retos de seguridad y privacidad, como la falta de transparencia al solicitar el consentimiento, la pérdida de control del usuario sobre sus datos, la reusabilidad de los mismos más allá de su consentimiento o la fuga de datos sensibles, por citar algunos.

Pero la preocupación por la privacidad no es nueva. Ya en enero de 1981 el **Consejo Europeo** [7] adoptó el **Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.** Desde entonces, el Convenio, conocido como Convenio 108, se ha ampliado para incluir cuestiones como la protección en las redes sociales, la elaboración de perfiles o el ámbito laboral. Desde 2006 se celebra el 28 de enero, en conmemoración de la firma de este Convenio, como Día de la protección de datos en Europa. Pero, a pesar de la existencia del Convenio, los países miembros no contaban con una normativa armonizada en esta materia.

Avanzando en este sentido, en el año 2000, la **Carta de Derechos Fundamentales** [8] de la UE incluía en su artículo 8 la «Protección de datos de carácter personal»:

1. ***Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.***
2. ***Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.***
3. ***El respeto de estas normas quedará sujeto al control de una autoridad independiente.***

Más adelante, con la entrada en vigor del **Tratado de Lisboa** [9] en diciembre de 2009, la Carta de Derechos Fundamentales de la UE pasó a ser jurídicamente vinculante y, con ello, se

2

elevó el derecho a la protección de los datos personales a la **categoría de derecho fundamental independiente del derecho a la intimidad**. O lo que es lo mismo:

> ***«La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede al ámbito propio del derecho fundamental a la intimidad y que se traduce en el derecho de control sobre los datos relativos a la propia persona.»***

La estrategia del Consejo Europeo **Europa 2020** [10] está planteada en torno a 7 pilares, uno de los cuales es la **Agenda digital para Europa** que promueve la creación de un **Mercado Único Digital Europeo** [11] 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. La estrategia para un **mercado único digital** fue adoptada en mayo de 2015.

"La Agenda digital para Europa que promueve la creación de un **Mercado Único Digital Europeo** libre y seguro en el que las empresas puedan vender en todo el territorio de la UE"

En el marco de esta estrategia se ha impulsado la armonización de las normativas que antes mencionamos, entre ellas la de privacidad de datos personales, con el objetivo de **crear un marco de confianza** para que pueda desarrollarse un **mercado digital** interior con seguridad jurídica para los usuarios y transparencia. Estos esfuerzos culminaron en el nuevo **Reglamento General de Protección de Datos** [12] que es de **obligado cumplimiento desde el 25 de mayo de 2018.**

Esta normativa europea, se convierte por tanto en la sucesora de la actual normativa de protección de datos de **todos los países miembros.** En España actualmente se está tramitando un **proyecto de ley** [13] para ajustar nuestro ordenamiento al nuevo Reglamento.

2

Las principales modificaciones del Reglamento frente a la actual legislación en cuanto a su aplicación en las empresas se pueden resumir en:

A lo largo de la guía trataremos de aclarar qué empresas están obligadas a realizar estas acciones y en qué circunstancias.

3 DATOS PERSONALES: ¿QUÉ DERECHOS RECONOCE EL RGPD?

En primer lugar, tenemos que tener claro qué son los datos personales y qué derechos tienen los ciudadanos sobre ellos con la nueva normativa.

Los datos personales son aquellos que están relacionados con una persona **identificada o identificable,** es decir, son datos personales los identificadores online como direcciones IP, nombre de usuario, correo electrónico, las cookies en las páginas web, etiquetas RFID, datos de localización, etc.

En general son datos personales los que nuestros clientes nos dan, por ejemplo, al cumplimentar los pedidos o durante el curso de nuestros servicios: su nombre y apellidos, direcciones, datos de facturación, datos de solvencia económica, DNI, datos biométricos o de salud, edad, estado civil, números de teléfono, correo electrónico, localización, etc. También son datos personales los análogos de nuestros empleados[1] incluidos los datos profesionales o de formación y los de nuestros contactos en proveedores. Si estos datos 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 para la empresa pueden ser cuantiosas, además de enfrentarnos a sanciones por incumplimiento legal.

Una persona es **identificable** si puede obtenerse, sin tener que realizar un esfuerzo desproporcionado, Información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Por ejemplo, esto es posible mediante fotografías o videos digitales, datos como la fecha y lugar de nacimiento, datos biométricos, huellas dactilares o la matrícula de vehículos de su propiedad. Por ello, se han de anonimizar los datos cuando se van a utilizar para estadísticas y otros análisis, ya que realizar tratamientos masivos indiscriminadamente con datos no anonimizados atenta contra la privacidad.

Por otra parte, en el RGPD se definen unas **categorías especiales de datos**[2], los antes denominados datos sensibles, que exigen una protección

1. El Art. 88 del RGPD establece la posibilidad de que los Estados miembros legislen de forma específica el tratamiento en el ámbito laboral.

2. El Art. 9 del RGPD especifica cómo han de tratarse los datos de categorías especiales.

3

reforzada y que, por lo tanto, están sujetos a un régimen jurídico especial. Son datos de este tipo:

1. ***datos personales que revelan ideología, afiliación sindical, opiniones políticas, creencias religiosas y otras creencias;***
2. ***datos personales que revelan el origen racial o étnico y los relativos a la salud o la vida sexual y orientación sexual, y ahora también datogenéticos[3] y datos biométricos[4] ;***
3. ***datos de condenas penales o administrativas[5].***

Esta protección reforzada se manifiesta por ejemplo en que el tratamiento de los primeros requiere el consentimiento expreso y por escrito de la persona; los segundos requieren el consentimiento expreso o que haya razones de interés general según una ley; y los terceros sólo podrán ser tratados por las administraciones públicas competentes en los supuestos previstos en sus normas reguladoras.

"Todos estos son los datos que tenemos que proteger de **clientes, empleados y proveedores**, porque es un derecho que tienen, y porque son un factor de competitividad"

Todos estos son los datos que tenemos que proteger de clientes, empleados y proveedores, porque es un derecho que tienen, y porque son un **factor de competitividad** para la empresa, lo que se evidencia, como comentábamos, al diversificarse y potenciarse con la tecnología los posibles usos de los mismos (perfilado, análisis de sentimiento, fidelización,...) en los nuevos modelos de negocio.

3.1. Nuevos derechos y no tan nuevos

Estamos acostumbrados a los tradicionales **derechos ARSOPOL** [14] que tienen los usuarios y que están recogidos en

3. Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionan una información única sobre la fisiología o la salud de esa persona, obtenidos en particular de una muestra biológica.

4. Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de esta persona (imágenes del rostro, huellas digitales, etc.)

5. El Art. 10 del RGPD limita el tratamiento de este tipo de datos.

3

la legislación anterior al RGPD, es decir, al acceso, rectificación, cancelación y oposición. Estos derechos se revisan con el nuevo Reglamento[6] y se añaden alguno más: la portabilidad para que puedan dárselos a otras empresas, el derecho al olvido y el derecho a la limitación del tratamiento.

Los dueños de los datos personales, pueden ejercer, según el RGPD, sus derechos. Estos son los **derechos [14]** que pueden ejercer los interesados:

1. **Derecho de acceso** a los propios datos personales: a ser informados de los datos, de los fines del tratamiento, del plazo de conservación, de las garantías existentes en caso de transferencia internacional[7] y de la existencia de decisiones automatizadas (incluida la elaboración de perfiles) y también el derecho a obtener una copia de los datos.
2. **Derecho de rectificación** si los datos son inexactos o incompletos.
3. **Derecho de supresión** (derecho al olvido) si se tratan de forma ilegal o ya no son necesarios para la finalidad con que se recogieron, siempre que no se ponga en riesgo la libertad de expresión o la capacidad para investigar, por ejemplo para exigir la supresión de eliminación de datos en redes sociales o buscadores de internet.
4. **Derecho a la limitación del tratamiento,** es decir, a solicitar que se suspenda si existen controversias sobre su licitud, y derecho al bloqueo para que no eliminen los datos personales si interesa su mantenimiento y conservación, por ejemplo para reclamar ante la autoridad competente.
5. **Derecho a la portabilidad** de los datos para poder cambiar o transmitirlos a otro responsable si es técnicamente posible en un formato estructurado y de

"Los dueños de los datos personales, pueden ejercer, según el RGPD, sus **derechos**"

6. El Capítulo III del RGPD (Art. 12 a 23) trata los Derechos del interesado, tiene 5 secciones: transparencia y modalidades, información y acceso a los datos personales, rectificación y supresión, derecho de oposición y decisiones individuales automatizadas, y limitaciones.

7. El Capítulo V del RGPD trata de las transferencias de datos personales a terceros países u organizaciones internacionales.

3

"¿Qué **derechos** tendré cuando se aplique el nuevo Reglamento?"

uso común. Por ejemplo, la portabilidad de un proveedor de servicios de internet a otro.

6. **Derecho de oposición** al tratamiento y a un uso posterior con fines de prospección comercial (marketing directo), investigación científica o histórica, o fines estadísticos (salvo que quien trate los datos acredite un interés legítimo). Derecho a optar a no recibir publicidad directa.

7. **Derecho a no ser objeto de decisiones individuales automatizadas**, incluida la elaboración de perfiles para el tratamiento de solicitudes de acuerdos jurídicamente vinculantes.

> ***«Elaboración de perfiles:*** *toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dichas personas.**» Art. 4 RGPD***

Para una descripción completa y detallada de los Derechos de los usuarios en el nuevo Reglamento consulta estos artículos de la Agencia Española de Protección de Datos, en adelante AEPD: **¿Qué derechos tendré cuando se aplique el nuevo Reglamento?** y **Protección de datos: guía para el ciudadano [15]** donde detalla los derechos y la forma de ejercitarlos, además de casos específicos como videovigilancia, ficheros de morosos, comunidades de propietarios, publicidad o telecomunicaciones.

> *También tienen derecho a que les notifiques[8] de forma clara y sencilla y sin dilación cuando hayas sufrido una **violación de seguridad**[9] que entrañe alto riesgo para sus derechos y libertades,*

8. Art. 34 RGPD.

9. «Violación de seguridad de los datos personales: toda violación de seguridad que ocasione 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.» Art. 4 RGPD

3

indicándole un contacto para obtener más información, las consecuencias de la violación y las medidas que pueden tomar.

"Los usuarios podrán denunciar **de forma individual o a través de asociaciones** de usuarios y exigir indemnizaciones de daños y perjuicios por el tratamiento ilícito de sus datos personales"

Informar

- Tratamiento.
- Decisiones automatizadas.
- Perfiles.
- Transferencias internacionales.

Obtener Consentimiento

- Inequívoco.
- No tácito.
- Expreso en caso de datos de especial protección.

Garantizar Derechos

- Que puedan ejercerlos.
- Según los plazos RGPD.

Notificar violaciones

- Que supongan riesgo para la privacidad.
- A la autoridad.
- A los usuarios.

Los usuarios **podrán denunciar**[10] de forma individual o a través de asociaciones de usuarios y exigir indemnizaciones de daños y perjuicios por el tratamiento ilícito de sus datos personales.

3.2. ¿Cómo facilito a los usuarios que puedan ejercer sus derechos?

El RGPD obliga a los responsables[11] a facilitar a los usuarios el ejercicio de sus derechos **mediante procedimientos y**

10. El Capítulo VIII trata de los recursos, responsabilidad y sanciones.

11. El Responsable del tratamiento o responsable es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento;[...] según el Art. 4 del RGPD.

3

"El RGPD obliga a los responsables a facilitar a los usuarios el ejercicio de sus derechos mediante procedimientos y formas que sean **visibles, accesibles y sencillos"**

formas que sean visibles, accesibles y sencillos. Si el tratamiento se realiza por medios electrónicos, también deben poder ejercer sus derechos por los mismos medios. Con carácter general, no se puede cobrar al usuario por ejercer sus derechos, salvo en casos infundados o excesivos, para los cuales se podrá fijar un canon que no puede superar los costes administrativos de realizar lo solicitado.

También se ha de verificar la identidad de los solicitantes y se les pide que especifiquen los datos a los que se refiere su solicitud si tienen muchos datos del usuario.

El responsable debe informar al que lo haya solicitado en el **plazo de un mes**, que en algunos casos complejos puede prorrogarse, sobre las actuaciones que ha realizado a raíz de su solicitud, o si no accede a ella (indicando el motivo) o si prorroga el plazo.

Si se encarga el tratamiento relativo al ejercicio de los derechos a algún encargado se debe firmar con él un **contrato** de encargo del tratamiento. Sigue las **Directrices para la elaboración de contratos entre responsables y encargados del tratamiento** [16] de la AEPD.

3.3. ¿Qué cambia en el deber de informar?

Si cumplías con la LOPDGDD seguro que cuando tomabas datos personales facilitabas a las personas a las que solicitabas sus datos la siguiente información:

- que tienes un fichero o tratamiento, para qué lo tienes y quién lo utiliza,
- que su aceptación es obligatoria o no lo es y las consecuencias de no aceptar,
- que puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición,
- quién es el responsable del tratamiento y cómo contactar.

A partir del día 25 de mayo, se generaliza el término **tratamiento** (ya no se utiliza el término fichero, ni habrá que inscribirlos en la AEPD):

3

> ***«Tratamiento:** 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.»* **Art. 4 RGPD**

"A partir del día 25 de mayo, se generaliza el término tratamiento"

Además, el responsable del tratamiento ha de informar — en un lenguaje claro y sencillo, de forma transparente, concisa, inteligible y de fácil acceso—, de:

- los datos de contacto del Delegado de protección de datos o DPO, (si tienes que nombrar uno como veremos más adelante) o del responsable,
- la finalidad y la base jurídica o legitimación para realizar el tratamiento,
- el plazo o los criterios de conservación de la información,
- la existencia de decisiones automatizadas o elaboración de perfiles,
- la previsión de transferencias a terceros países,
- el modo en que el usuario podrá ejercitar sus derechos ARSOPOL y que tiene derecho a presentar una reclamación ante las autoridades de control si entiende que sus derechos han sido vulnerados o que no se cumple el RGPD.

Y si los datos no se obtienen del interesado, es decir, de la persona a la que pertenecen, se tiene que informar antes de un mes o antes de la primera comunicación o de su comunicación a otros destinatarios:

- del origen de los datos, por ejemplo una cesión legítima o de fuentes de acceso público,
- de las categorías de los datos.

3

La **Guía para el cumplimiento del deber de informar de la AEPD** [17] recomienda una información por capas o niveles para que sea a la vez concisa y comprensible. En una primera capa se presentará la información básica resumida. En la segunda capa, la información adicional detallada, de manera que se pueda descargar.

3.4. ¿Cómo debo tomar su consentimiento?

Una de las condiciones para que un tratamiento sea lícito es que el propietario de los datos dé su consentimiento para el tratamiento de sus datos para uno o varios fines específicos.

Las empresas deben proveer mecanismos para que los interesados acepten el tratamiento y puedan ejercer sus derechos. Al tomar los datos deben recabar el consentimiento. Hasta ahora bastaba con el consentimiento libre, específico e informado del interesado.

Ahora según la AEPD debe ser:

- **Libre**, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento por falta de conocimiento o de libertad en los términos regulados por el Código Civil.
- **Específico**, es decir, referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento.
- **Informado,** es decir, que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce.
- **Inequívoco**, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

"Una de las condiciones para que un tratamiento sea lícito es que el propietario de los datos dé su **consentimiento"**

3

"Ahora según la AEPD debe ser:
Libre, Específico, Informado e Inequívoco"

Y además puede ser retirado en cualquier momento por el usuario.

En el nuevo RGPD, el consentimiento **ya no puede ser tácito** o por omisión, es decir, ya no podemos decir al usuario que si no dice lo contrario, suponemos que consiente con el tratamiento. Todos los consentimientos deben ser inequívocos y hay que poder demostrarlo.

> *El **consentimiento inequívoco** es «aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa.»*

Sólo en el caso de que se deduzca de una **acción** del interesado, (como por ejemplo cuando al seguir navegando en una web, acepta que se utilicen cookies para monitorizar su navegación) podrá otorgarse de forma **implícita** (consentimiento inferido).

> ***Si se tratan datos especialmente protegidos o se van a utilizar para decisiones automatizadas o para transferencias internacionales, además de ser inequívoco ha de ser expreso, es decir, no podrá ser inferido.***

En caso **de menores de 13 años**[12] en relación de la oferta de servicios de la sociedad de la información, como por ejemplo redes sociales o tiendas online, se requiere el consentimiento de los padres o tutores.

Por ello, si tu empresa ya cumple con la LOPDGDD —y no es necesario el consentimiento expreso—, en los tratamientos que hayas hecho con datos personales, **si has recabado el consentimiento inequívoco** de los usuarios, no se tiene que volver a pedir.

Si utilizas el consentimiento tácito debes **revisar cuanto antes los consentimientos así obtenidos para adecuarlos a este nuevo requisito o no se podrá utilizar.**

12. El RGPD indica que consentimiento será legal siempre y cuando estos tengan más de 16 años. Sin embargo, permite rebajar esta edad y que cada Estado miembro establezca la suya propia, con un límite inferior de 13 años. En el caso de España, esta edad está fijada actualmente en 14 años, pero con la entrada en vigor de la nueva Ley de Protección de datos se reducirá desde los 14 a los 13 años.

3

Si ha cambiado el tipo de datos o tus usuarios son menores, tienes que revisarlo bien solicitando, de nuevo y en adelante, el consentimiento inequívoco o expreso, según corresponda al tipo de datos; bien informando a los usuarios si así lo permite la base legal del tratamiento.

*Si el **consentimiento** obtenido es **tácito** debes modificarlo cuanto antes pues **ya no es válido** y no podrás utilizar los datos así obtenidos. **Debes recabar siempre el consentimiento inequívoco o expreso** según el tipo de datos de tus tratamientos.*

"En caso de **menores** en relación de la oferta de servicios de la sociedad de la información, como por ejemplo redes sociales o tiendas online, se requerirá el **consentimiento de los padres o tutores**"

4 ¿CÓMO AFECTA EL RGPD A MI EMPRESA?

Las empresas, sociedades, comunidades, asociaciones y autónomos a los que aplica 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 encuentran en la UE;
- los que monitorizan el comportamiento de las personas que se encuentren en la UE.

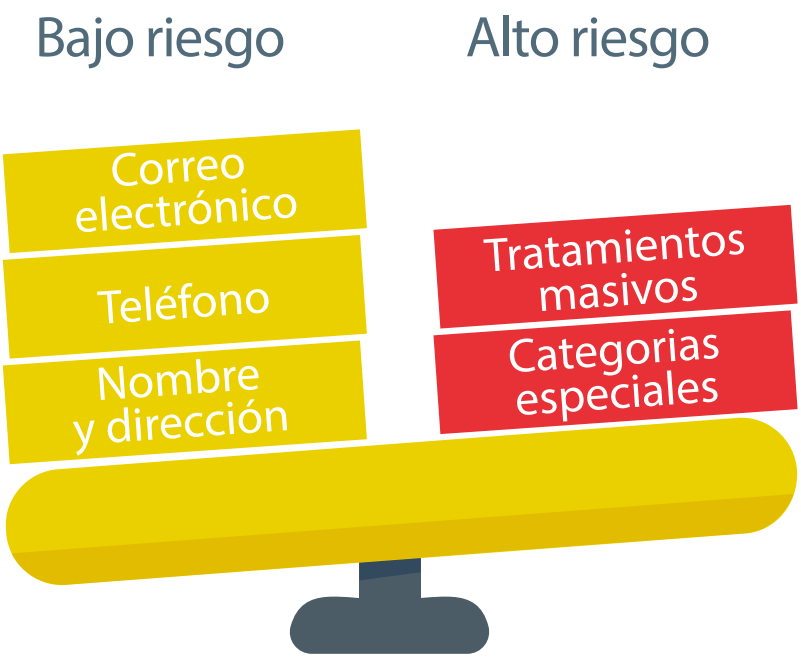
Por lo que, tanto si cumples con la LOPDGDD como si vas a realizar una actividad comercial en la UE o para la que tienes que tratar algún dato personal en la UE o sobre datos de las personas que se encuentren en la UE, tienes que cumplir con el nuevo Reglamento.

4.1. ¿Tratamiento de alto o de bajo riesgo?

Para saber cómo te afecta tienes que determinar si tu tratamiento es de alto o de bajo riesgo para los derechos y libertades de las personas.

4

"Para saber cómo te afecta tendrás que determinar si tu tratamiento **es de alto o de bajo riesgo** para los derechos y libertades de las personas"



Son de alto riesgo por ejemplo:

- los que tratan **datos de categorías especiales** como los que realizan las empresas:
  - del sector sanitario o legal,
  - de seguros,
  - de servicios sociales,
  - de actividades políticas, sindicales o religiosas,
  - de solvencia patrimonial y crédito,
  - videovigilancia en centros comerciales o en estaciones de ferrocarril.
- los que realizan **tratamientos masivos** de datos como por ejemplo las empresas de:
  - servicios de telecomunicaciones,
  - entidades bancarias y financieras,
  - generación y uso de perfiles,
  - publicidad.

Son de **bajo riesgo** los tratamientos que sólo traten:

- datos personales de contacto de clientes o proveedores;
- datos básicos de recursos humanos.

4

4.2. Bajo riesgo: cumple con FACILITA

Si los tratamientos que realizas son de **bajo riesgo** puedes utilizar la herramienta **Facilita de la AEPD** [18] que en base a los datos que proporciones, generará:

- la información que debes incluir en los formularios de recogida de datos personales tanto de clientes como de proveedores;
- las cláusulas contractuales que debes anexar a los contratos de encargado de tratamiento por ejemplo si contratas una gestoría o si contratas un proveedor para tu web;
- un modelo de Registro de actividades[13] de tratamiento y
- un anexo con medidas de seguridad orientativas consideradas mínimas.

"Si los tratamientos que realizas son de bajo riesgo puedes utilizar la herramienta **FACILITA de la AEPD"**

4.3. ¿Qué es el Registro de actividades?

Hasta que sea de obligado cumplimiento el nuevo Reglamento, para cumplir con la LOPDGDD, y antes con la LORTAD, las empresas tenían que inscribir el fichero en la AEPD que era una forma de notificar que realizaban un tratamiento de datos con una descripción del mismo. En adelante ya no será necesario inscribir el fichero.

Desde el 25 de mayo de 2018, el responsable del tratamiento, y el encargado[14], deben llevar sendos **Registros de actividades de tratamiento** que se realicen bajo su responsabilidad. Este registro contiene en caso del responsable:

- nombre y datos de contacto del responsable o corresponsable y del Delegado de Protección de Datos si existiese,
- finalidades o motivos del tratamiento,

13. En el art. 30 del RGPD se especifica cómo ha de ser el Registro de actividades de tratamiento en cuanto a contenido y forma, quién es el que debe mantenerlos y qué empresas están exentas.

14. El encargado del tratamiento o encargado es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento, según el art. 4 del RGPD.

4

"A partir del 25 de mayo de 2018, el responsable del tratamiento, y el encargado, deben llevar sendos **Registros de actividades de tratamiento** que se realicen bajo su responsabilidad"

- descripción de categorías de interesados y datos personales tratados,
- categorías de los destinatarios a quienes se comunican los datos personales, incluso si están en otros países o son organizaciones internacionales,
- transferencias de datos a otro país u organización,
- cuando sea posible, el plazo previsto para eliminar los datos,
- cuando sea posible, una descripción de las medidas de seguridad utilizadas durante el tratamiento.

> *Pero **no es 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.*

Si ya tenías notificado el fichero de tu empresa en la AEPD puedes utilizarlo de base para hacer el Registro general de actividades, incluyendo detalle sobre las operaciones que se realizan sobre cada conjunto de datos. La AEPD te facilita una **copia de la inscripción de Ficheros.**

4.4. Responsables, encargados[15] y ¿ahora un delegado?

El **responsable** es el que determina por qué hace falta el tratamiento y para qué, el que realiza el análisis de riesgos del tratamiento y también el responsable último del mismo. Toda empresa debe tener uno o varios. También, en el nuevo Reglamento, el responsable es quien debe elegir a los **encargados que ofrezcan garantías suficientes** para aplicar medidas técnicas y organizativas de manera que el tratamiento se realice conforme a los requisitos del reglamento. Los encargados pueden adherirse a códigos de conducta o certificarse[16] para ofrecer esas garantías suficientes.

15. El Capítulo IV Sección 1 del RGPD trata de las obligaciones de los responsables y encargados del tratamiento.

16. Consulta la sección 5 del capítulo IV del RGPD para saber más de los códigos de conducta y de la certificación.

4

"El **responsable** es el que determina por qué hace falta el tratamiento y para qué, el que realiza el análisis de riesgos del tratamiento y también el responsable último del mismo"

Los encargados son por ejemplo el soporte tecnológico o jurídico, interno o externo, que contratamos para cumplir con el Reglamento. La relación entre Responsable y Encargado debe formalizarse

en un **contrato o acto jurídico vinculante**. Recomendamos seguir las **Directrices para la elaboración de contratos entre responsables y encargados del tratamiento** [16] que ofrece la AEPD que incluye un ejemplo de cláusulas contractuales que este contrato debe contener. El contenido mínimo de este contrato ha variado respecto a la normativa anterior, por lo que los contratos actuales deben modificarse para incluir:

4

"La relación entre Responsable y Encargado debe formalizarse en un **contrato o acto jurídico vinculante"**

- objeto, duración, naturaleza y finalidad del tratamiento,
- tipo de datos personales y categorías de interesados,
- obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable
- condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones
- asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados.

Si el encargado está **establecido en la UE**, aunque los tratamientos no se realicen aquí, está también sujeto al RGPD. Y de igual forma en caso de que el encargado **no esté establecido en la UE** y los tratamientos que se realicen en la UE sean de:

a. oferta de bienes o servicios a residentes en la UE, independientemente de si se les requiere su pago;
b. control de su comportamiento, en la medida en que tenga lugar en la UE.

A estos casos les aplicará el RGPD como si se tratara de **transferencias internacionales**[17] de datos, teniendo en cuenta que en ningún caso debe suponer una reducción del nivel de protección de las personas, por lo que el encargado debe ofrecer, en cualquier caso, garantías suficientes.

4.4.1 Delegado de Protección de Datos

El **Delegado de Protección de Datos DPD**[18], o DPO por sus siglas en inglés, es una nueva figura que sólo es obligatoria si realizas:

a. operaciones de tratamiento que requieran una observación habitual y sistemática de personas a gran escala;
b. tratamiento a gran escala de datos de categorías especiales.

17. Puedes leer más sobre este tema en el artículo El nuevo reglamento y las transferencias internacionales de la AEPD https://www.agpd.es/blog/el-nuevo-reglamento-y-las-transferencias-internacionales-ides-idPhp.php

18. La Sección 4 del Capítulo IV del RGPD trata la designación, posición y funciones del DPD.

4

"El Delegado de Protección de Datos **DPD**, o DPO por sus siglas en inglés, es una nueva figura"

*Según el Art. 91 RGPD las operaciones de tratamiento **a gran escala** «[...] 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, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala y a otras operaciones de tratamiento que entrañan un alto riesgo para los derechos y libertades de los interesados, en particular cuando estas operaciones hacen más difícil para los interesados el ejercicio de sus derechos»*

Para determinar si el tratamiento es a gran escala se recomienda considerar estos factores:

- el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;
- el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento;
- la duración, o permanencia, de la actividad de tratamiento de datos;
- el alcance geográfico de la actividad de tratamiento.

Son algunos ejemplos de tratamientos a gran escala los relativos a: pacientes de un hospital, desplazamiento de usuarios de tarjetas de transporte, geolocalización de clientes en tiempo real, clientes de compañías de seguros o de banca, publicidad según comportamiento en motores de búsqueda o los de proveedores de servicios de telefonía.

Nombrar un DPD será obligatorio (según el art. 34.1 del **Proyecto de Ley Orgánica de Protección de Datos [15]**) por ejemplo, para:

- entidades con actividades de publicidad y prospección comercial si se basan en preferencias de los usuarios

4

"Nombrar un DPD será **obligatorio en algunos casos**, según el art. 34.1 del Proyecto de Ley Orgánica de Protección de Datos"

o elaboran perfiles y entidades que emitan informes comerciales referidos a personas físicas,

- colegios profesionales y sus consejos generales,
- colegios e institutos y universidades públicas,
- centros sanitarios obligados por ley a mantener historias clínicas,
- entidades que exploten redes y presten servicios de comunicaciones electrónicas que traten datos a gran escala,
- prestadores de servicios de la sociedad de la información que elaboren perfiles a gran escala,
- operadores de juego a través de canales electrónicos, informáticos, telemáticos e interactivos,
- entidades de crédito, establecimientos financieros y empresas de servicios de inversión,
- entidades responsables de ficheros comunes para la evaluación de solvencia patrimonial y crédito o la gestión y prevención del fraude, incluidas las de prevención de blanqueo de capitales y financiación del terrorismo,
- entidades aseguradoras y reaseguradoras,
- distribuidores y comercializadores de energía eléctrica,
- empresas de seguridad privada y despachos de detectives privados.

En estos casos, y si realizas este tipo de tratamientos a gran escala, debes **nombrar un DPD cualificado**, —contratándolo como empleado o contratando sus servicios—, con conocimientos en la legislación y la práctica de la protección de datos, cuyos datos de contacto se tienen que comunicar a las autoridades de supervisión competentes. El responsable o encargado deben facilitar al DPO todos los recursos necesarios para desarrollar su actividad y hacer públicos sus datos de contacto. Esta figura, el DPD:

- Tiene total autonomía en el ejercicio de sus funciones y contacto directo con el nivel superior de dirección;
- Tiene funciones de gestión y control de la protección de datos dentro de la empresa;

4

"El DPO tendrá **total autonomía** en el ejercicio de sus funciones y contacto directo con el nivel superior de dirección"

» Actúa como punto de contacto entre la empresa y la AEPD.

Si contratas los servicios de un DPD externo, persona física o jurídica, tienes que considerarlo encargado del tratamiento y por tanto firmar un contrato de servicios siguiendo las **Directrices para la elaboración de contratos entre responsables y encargados del tratamiento** [16] que ofrece la AEPD.

Si tu empresa no realiza ese tipo de tratamientos a gran escala no es obligatorio que nombres un DPD.

4.5. Responsabilidad no sólo activa, también proactiva

El RGPD se basa en los mismos principios que la legislación anterior, pero se diferencia de la misma en que se desarrolla además en torno la responsabilidad proactiva y el enfoque de riesgo.

» La **responsabilidad proactiva** implica que el responsable del tratamiento debe aplicar **medidas técnicas y organizativas** apropiadas a fin de **garantizar y poder demostrar** que el tratamiento es conforme al Regla-

4

"El RGPD se basa en los mismos principios de la legislación anterior pero se diferencia de la misma en que se desarrolla además en torno **la responsabilidad proactiva y el enfoque de riesgo"**

mento. En la práctica supone analizar los datos, las finalidades y las operaciones de los tratamientos, para determinar de forma explícita la aplicación de las medidas que el RGPD prevé, para proteger la privacidad y poder demostrarlo.

» Para aplicar las medidas de responsabilidad proactiva se ha de utilizar un **enfoque de riesgos** teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas. En la práctica esto supone que algunas medidas (por ejemplo, evaluación de impacto o el nombramiento del DPD) se aplicarán sólo cuando exista un alto riesgo y el resto (por ejemplo, privacidad desde el diseño) serán adaptadas al nivel y tipo de riesgo que los tratamientos presenten.

4.5.1. Responsabilidad proactiva

La responsabilidad proactiva se concreta en las siguientes medidas:

a. llevar un Registro de operaciones de tratamiento en los casos en los que estés obligado;

b. adoptar y adaptar las distintas medidas en base a un análisis de los riesgos del tratamiento para los derechos y libertades de las personas;

c. aplicar la protección de la privacidad desde el diseño y por defecto para garantizar que los usuarios puedan ejercer sus derechos y la seguridad de sus datos personales;

d. notificar las violaciones de seguridad de los datos a la autoridad de protección de datos competente y a las personas afectadas, salvo que sea improbable que suponga un riesgo para los derechos y libertades de los afectados;

e. llevar a cabo una evaluación de impacto sobre la protección de datos en aquellos tratamientos que conlleven un alto riesgo para los derechos y libertades de las personas;

f. nombrar a un DPD cuando sea necesario.

Ya hemos hablado de los casos en los que has de llevar un Registro de operaciones de tratamiento o nombrar un DPO. Veamos ahora

4

con más detalle a quién afecta el resto de medidas proactivas.

4.5.2. Análisis de riesgos y en algunos casos análisis de impacto

Para saber si estás obligado a llevar un Registro de operaciones de tratamiento o a nombrar un DPD y a realizar una evaluación de impacto, es necesario que el responsable haga una **valoración continua de los riesgos** que entrañan los tratamientos a los derechos y libertades de los usuarios. Este análisis también servirá para establecer el resto de medidas de responsabilidad proactiva.

Si eres una gran empresa seguro que ya sigues alguna metodología propia o estándar para el análisis de riesgos de la seguridad de la información. Algunos estándares generales para gestión de riesgos en seguridad de la información son: ISO/IEC27005, Magerit, NIST SP 800-30 u Octave. Y más específicamente para riesgos de privacidad **ISO/IEC 29100/2011** [19] y **NISTR 8062** [20].

Para empezar a realizar 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.
- Ser exhaustivos con los datos que se recogen: ¿dónde se almacenan?, ¿durante cuánto tiempo?, ¿en un fichero o en una base de datos?, ¿siguen los principios del tratamiento del RGPD[19]?
- Hacer un diagrama con el flujo de datos del tratamiento, es decir, desde que se recogen hasta que se utilizan o desechan con las transformaciones intermedias.
- 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.

"Una medida de responsabilidad proactiva es llevar un **Registro de operaciones de tratamiento** en los casos en los que estés obligado"

19. El RGPD en el Art. 5 define los principios que debe cumplir el tratamiento: licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, y responsabilidad proactiva para cumplir todos los anteriores.

4

"Es necesario que el responsable haga una **valoración continua de los riesgos** que entrañan los tratamientos a los derechos y libertades de los usuarios"

Para la protección de la privacidad, el objetivo del análisis de riesgos es determinar si el tratamiento tiene consecuencias negativas para las personas como por ejemplo, marginación, exclusión social, dificultades para acceder a un puesto de trabajo, problemas para contratar servicios, etc.

Si tu empresa es una pyme o no realiza tratamientos masivos u orientados a una explotación que invada notablemente la privacidad[20], puedes seguir una metodología que se adapte mejor a tu circunstancia. Para conocer cómo hacer un análisis de riesgos de forma general puedes utilizar estos recursos:

- **Gestión de riesgos: una guía de aproximación para el empresario** [21]
- **¿Conoces tus riesgos?** [22]

Ten en cuenta, de cara a la análisis de riesgos de privacidad, las siguientes equivalencias:

- los activos de información son en este caso los datos personales a proteger;
- los incidentes de seguridad incluyen las violaciones de la privacidad;
- los riesgos, son riesgos de privacidad;
- y los objetivos de la gestión de riesgos, son objetivos de la gestión de riesgos de privacidad.

Más específicamente la AEPD publica una **Guía para la Gestión del riesgo y evaluación de impacto en tratamientos de datos personales** [23] con varias plantillas para la Gestión de Riesgos: análisis de la necesidad de la realización de una evaluación de impacto, descripción de las actividades de tratamiento, otra para documentar el análisis básico de riesgos y para el registro de actividades de tratamiento para el responsable y el encargado. Para empezar puedes verificar si respondes afirmativamente a estas preguntas:

20. Por ejemplo la monitorización del comportamiento o publicidad basada en comportamiento, elaboración de perfiles, verificación de la idoneidad para determinadas tareas, evaluación de la personalidad o de la situación financiera o laboral, social, familiar, formación, gustos o aficiones y las que impliquen tratamiento de datos especialmente protegidos.

4

"Los objetivos de la gestión de riesgos, son objetivos de gestión de **riesgos de privacidad"**

1. ¿se tratan datos especialmente protegidos de forma sistemática y masiva?
2. ¿se incluyen datos de gran cantidad de personas o gran cantidad de datos de los usuarios?
3. ¿se tratan datos de menores de forma significativa o no incidental?
4. ¿está destinado el tratamiento a evaluar o predecir aspectos personales de los usuarios[21] o su comportamiento?
5. ¿incluye el tratamiento la elaboración de perfiles con cualquier finalidad, incluido el envío de publicidad personalizada?
6. ¿se cruzan datos obtenidos de los usuarios con otros disponibles en otras fuentes?
7. ¿se pretende utilizar los datos obtenidos para una finalidad para nuevas finalidades más intrusivas?
8. ¿se están tratando grandes volúmenes de datos con técnicas de análisis masivo tipo *Big Data*?
9. ¿se utilizan tecnologías especialmente invasivas para la privacidad, como las drones o las relativas a geolocalización, videovigilancia, minería de datos, biometría, RFID o ciertas aplicaciones del internet de las cosas y las ciudades inteligentes o *smartcities*?
10. ¿se van a ceder o comunicar los datos a terceros que antes no tenían acceso a ellos?
11. ¿se van a transferir los datos a países fuera del EEE (Espacio Económico Europeo) que no tengan declaración de adecuación[22]?
12. ¿se va a contactar con las personas de forma especialmente intrusiva?
13. ¿se van a utilizar los datos personales no disociados o no anonimizados de forma irreversible para fines estadísticos, históricos o de investigación científica?
14. ¿existen riesgos específicos que puedan comprometer la confidencialidad, la integridad o la disponibilidad de los datos personales?

21. Como por ejemplo estado de salud, fiabilidad o adecuación para determinadas tareas, situación financiera, laboral, social, familiar, su ideología, creencias, formación, gustos, aficiones, compras, etc.

22. Consulta en la AEPD (Agencia Española de Protección de Datos) los países con un nivel adecuado de protección https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php

4

"¿está destinado el **tratamiento** a evaluar o predecir aspectos personales de los usuarios o su comportamiento?"

Si has respondido afirmativamente a una o varias de ellas tu empresa es de las que debería hacer una **evaluación de impacto y consultar** previamente a la autoridad de protección de datos[23]. Si es así sigue la Guía para la Gestión del riesgo y evaluación de impacto en tratamientos de datos personales **[23]** en la que se analizan los distintos riesgos: acceso no autorizado, uso ilegítimo, modificación no autorizada, perfilado de datos y pérdida de datos.

*Una **evaluación de impacto** se puede definir como «una metodología para evaluar el impacto en la privacidad de un proyecto, política, programa, servicio, producto o cualquier iniciativa que implique el tratamiento de datos personales y,*

23. La Sección 3 del Capítulo IV del RGPD describe la evaluación de impacto relativa a la protección de datos y consulta previa.

4

tras haber consultado con todas las partes implicadas, tomar las medidas necesarias para evitar o minimizar los impactos negativos. Una evaluación de impacto en la privacidad es un proceso que debería comenzar en las etapas más iniciales que sea posible, cuando todavía hay oportunidades de influir en el resultado del proyecto[24]»

El **análisis de riesgos** dará como resultado la adopción de las medidas necesarias para eliminar o mitigar los riesgos que el producto o servicio pueda entrañar para la protección de datos de las personas. La evaluación de impacto permitirá aplicar la privacidad desde el diseño, evitando costes de mitigación de riesgos a posteriori.

"Sigue la Guía para la Gestión del riesgo y evaluación de impacto en tratamientos de datos personales"

4.5.3. Protección de datos desde el diseño y por defecto

Protección y explotación de datos personales son 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** desde 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 es de las que tiene que hacer una evaluación de impacto, con él tendrás identificados los riesgos del tratamiento con lo que podrás adoptar medidas en su fase de diseño.

» *Los sistemas **privacidad desde el diseño** han sido construidos teniendo en cuenta la protección de la privacidad. Para ello «el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización[25], y otras*

24. Weight, D., De Hert, P, Privacy Impact Assessment Springer (2012)

25. Seudonimización: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional 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. RGPD Art. 4

4

concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento [...]»

» *Los sistemas que incorporan **privacidad por defecto** están configurados por defecto de forma que ofrecen la mayor privacidad y garantizan la confidencialidad. En particular «deben garantizar que los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.»*

"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. También son medidas técnicas: protección perimetral, VPN, redes inalámbricas seguras, etc. Algunas medidas organizativas son: formación y concienciación, definición y comunicación de políticas, separación de funciones, etc.

» Si utilizas tecnologías de **tratamiento masivo** de datos consulta el **Código de Buenas prácticas en protección de datos para proyectos Big Data** [24] de ISMS y AEPD y el documento **Orientaciones y garantías en los procedimientos de ANONIMIZACIÓN de datos personales** [25] de la AEPD.

4.5.4. Notificar las violaciones de seguridad

El RGPD obliga a notificar[26] las violaciones de datos que podamos sufrir en la empresa a la autoridad de protección de datos competente y a las personas afectadas, salvo que sea improbable que suponga un riesgo para los derechos y libertades de los afectados. Por ejemplo, estarías exento si los datos afectados estaban cifrados.

La notificación a la autoridad debe incluir como mínimo:

» la naturaleza de la violación, y cuando sea posible las categorías y número de afectados aproximados;

26. Art. 33 del RGPD

4

- el nombre y los datos de contacto del DPD o de otro punto dónde obtener más información;
- las consecuencias posibles de la violación;
- las medidas adoptadas o propuestas para remediar los efectos negativos.

¿?

Has sufrido una brecha de seguridad con riesgo para la privacidad

SI

NOTIFICA A LA AEPD Y A LOS AFECTADOS

"Si has sufrido una brecha con riesgo para la privacidad notifica a la autoridad y a los afectados"

5 ¿QUÉ MEDIDAS DE SEGURIDAD DEBO TOMAR?

La protección de la privacidad en el nuevo Reglamento ha de hacerse de forma proactiva adoptando precauciones para garantizar los derechos y libertades de los usuarios con respecto a sus datos personales. Por ejemplo, proporcionándoles información sobre el tratamiento, recabando su consentimiento inequívoco o expreso, o habilitando formas sencillas para que puedan ejercer sus derechos ARSOPOL, portabilidad, derecho al olvido y limitación del tratamiento.

Pero estas no son las únicas medidas que hemos de tomar en la empresa para proporcionar las garantías a los usuarios, proveedores y empleados sobre sus datos personales. Todo el personal que intervenga en el tratamiento está involucrado en la seguridad de los datos y en garantizar los derechos y libertades de los dueños de los mismos. Por eso:

- su soporte tecnológico y el área legal de su empresa tendrán que **revisar contratos, adecuar políticas y ajustar procedimientos** para hacer que los tratamientos sean confiables,
- el resto de personal debe **entender los cambios y ser capaces de ejecutarlos.**

Además, no sólo hemos de poder proporcionar las garantías sobre los datos a las personas, debemos estar preparados para **poder demostrar** que lo hacemos correctamente.

5

"Tras realizar una evaluación de los riesgos de nuestros tratamientos para la privacidad de las personas, tendremos que adoptar o adecuar también distintas **medidas técnicas"**

En las empresas y dependiendo de su tamaño, de los tipos de tratamientos[27] que realicemos y de las categorías de datos que tratamos, tendremos que tomar distintas **medidas organizativas** como por ejemplo, nombrar un DPD o hacer un análisis de impacto. También tendremos que cambiar las políticas y procedimientos internos para entre otras cosas, conocer cómo actuar en caso de incidente o hacer que todos los implicados en el tratamiento sean conscientes de las garantías que debemos ofrecer y de cómo aplicar seguridad en los tratamientos.

En cualquier caso, **y tras realizar una evaluación de los riesgos** de nuestros tratamientos para la privacidad de las personas, tendremos que adoptar o adecuar también distintas **medidas técnicas**. Son ejemplos de estas medidas la seudonimización, el cifrado, los mecanismos para garantizar confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios dedicados al tratamiento, o para restaurar el acceso en caso de incidente y, en cualquier caso, para verificar la eficacia de las mismas.

5.1. Medidas organizativas

Durante la guía hemos visto algunas medidas organizativas que se deben tomar en la empresa y en qué casos son obligatorias:

- Registros de actividad, cuando sea necesario[28];
- Contratos entre responsable y encargado, si encargas el tratamiento a terceros;
- Nombramiento de un DPD[29], en su caso, con sus responsabilidades organizativas de asesoramiento, supervisión,

27. El Proyecto de ley, en su título IV indica disposiciones aplicables a tratamientos concretos como: datos de contacto de empresarios individuales, los relacionados con la realización de algunas operaciones mercantiles, los que tienen fines de videovigilancia, los sistemas de exclusión publicitaria, sistemas de información de denuncias internas en el sector privado, y otros tratamientos estadísticos o de archivo en el sector público.

28. Recuerda que no es 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.

29. Si realizas tratamientos a gran escala de forma sistemática o con datos especiales.

5

comunicación, punto de contacto con la autoridad de control y cooperación.

También son medidas organizativas las responsabilidades asignadas al responsable o al encargado en su caso:

- Determinar la **existencia de datos personales, clasificarlos** y documentar su existencia, revisar que no sean incorrectos y si se han compartido datos incorrectos informar de ello para su corrección.
- Identificar los tratamientos de los datos personales, documentarlos y **verificar la base legal** en la que se justifican, entre otros, **revisar la forma en la que tomaste el consentimiento** y cómo garantizas los derechos.
- **Analizar los riesgos** que entrañan los tratamientos para los derechos y libertades de los usuarios **de forma continua**, para garantizar un nivel de seguridad adecuado en extensión y profundidad en función de la naturaleza de los datos, tipos de tratamiento, número de afectados y otros tratamientos que realice la empresa.
- Implementar **evaluaciones de impacto** si realizas tratamientos de alto riesgo.
- **Establecer un procedimiento**, formando parte de un plan de respuesta a incidentes, **para comunicar las violaciones de seguridad** a la autoridad nacional, sin dilación y antes de 72 h, y a los usuarios afectados si entraña alto riesgo para su privacidad.
- Poner los medios para aplicar **medidas de protección de datos desde el diseño y por defecto**, como por ejemplo reducir los datos personales a tratar al mínimo, seudonimizar lo antes posible y dotar de transparencia al tratamiento para permitir la supervisión.
- Elaborar o revisar y poner los medios para aplicar las **políticas internas** de protección de datos, incluidas las políticas relativas **asignación de responsabilidades, concienciación y formación y auditorías.**
- **Formar** a todos los empleados que participen en el tratamiento:

"**Analizar los riesgos** que entrañan los tratamientos para los derechos y libertades de los usuarios de forma continua"

5

"En cualquier caso deben contemplar el conocimiento de los derechos y de los requisitos de **transparencia** del RGPD"

- → en los derechos y libertades de los cuales han de informar y en los procedimientos para atender a dichos derechos;
- → en el deber de confidencialidad y secreto, haciéndoles partícipes de las políticas para que eviten el acceso de terceros a los datos y la divulgación accidental, apliquen las medidas para el correcto almacenaje y destrucción segura de soportes y firmen acuerdos de confidencialidad que se extiendan más allá de la finalización de sus contratos;

» Elaborar y difundir **procedimientos internos** para empleados que intervengan en el tratamiento que en cualquier caso deben contemplar el conocimiento de los derechos y de los requisitos de transparencia del RGPD.

» Si tus tratamientos incluyen **transferencias internacionales** a países fuera de la UE o con los que no haya convenio:

- → Elaborar o revisar y poner los medios para aplicar las **políticas** relativas a las transferencias internacionales dentro del grupo empresarial o unión de empresas.
- → Poner en marcha **auditorías o inspecciones** para garantizar el cumplimiento de las normas vinculantes relativas a protección de datos dentro de un grupo empresarial o unión de empresas y métodos para garantizar acciones correctivas para proteger los derechos de las personas.
- → Establecer un **punto centralizado** para tratar con una autoridad nacional, por ejemplo para gestionar quejas de usuarios, en caso de que tu empresa esté establecida en varios países.

5

Consulta y descarga las **Políticas de seguridad para la pyme**[30], que contienen listas de verificación de las acciones que has de tomar para poner en marcha o mejorar la seguridad en distintos aspectos. En particular para la protección de datos personales son interesantes las relativas a almacenamiento, cumplimiento legal, borrado seguro, copias de seguridad, uso de técnicas criptográficas y respuesta a incidentes.

5.2. Medidas técnicas

Los procedimientos, las políticas y la formación son indispensables para cumplir con el RGPD, pero la técnica puede ayudar en todo el proceso, desde la toma de datos hasta su destrucción final.

Por eso además de implementar las medidas en los procedimientos técnicos utilizados para notificar en caso de violaciones y para informar a los dueños de los datos sobre los tratamientos, obtener su consentimiento y garantizarles que pueden ejercitar sus derechos (acceso, borrado de sus datos, portabilidad, oponerse, objetar al marketing directo y a la elaboración de perfiles,...), en este apartado identificaremos qué tipos de herramientas[31] son las más adecuadas **para garantizar la seguridad de los datos personales** y con ello, el cumplimiento del RGPD. Para ello utilizaremos como referencia la Taxonomía de soluciones de seguridad:

"Consulta y descarga las **Políticas de seguridad para la pyme**, que contienen listas de verificación de las acciones que has de tomar para poner en marcha o mejorar la seguridad en distintos aspectos"

30. Incibe Políticas de seguridad para la pyme https://www.incibe.es/protege-tu-empresa/herramientas/politicas

31. Para conocer más sobre esto revisa la Taxonomía de soluciones de seguridad de INCIBE de 2016 que puedes descargar en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/taxonomia_ciberseguridad.pdf

CATEGORÍA DE PRODUCTO	ÁMBITO DE APLICACIÓN				
	Gestión de acceso e identidad	Seguridad en el puesto de trabajo	Seguridad en aplicaciones y datos	Seguridad en los sistemas	Seguridad en la red
Anti-fraude Anti-*phising*, Anti-spam, Herramientas de filtrado de navegación, UTM, *Appliance*		✓	✓	✓	✓
Anti-malware Anti-virus, Anti-*Adware*, Anti-*spyware*, UTM, *Appliance*		✓	✓	✓	✓
Auditoría técnica Análisis de logs y puertos, vulnerabilidades, Auditoría de contraseñas, Auditoría de sistemas y ficheros	✓		✓		✓
Certificación normativa SGSI, Análisis de riesgos, Planes y políticas de seguridad, Normativas de seguridad		✓	✓	✓	✓
Contingencia y continuidad H. de gestión de planes de contingencia y continuidad, Copias de seguridad, Infraestructura de respaldo, Virtualización, *Cloud*		✓	✓	✓	✓
Control de acceso y autenticación Control de acceso a red, NAC, Gestión de identidad y autenticación, *Single Sign-On,* Certificados digitales, Firma electrónica	✓				
Cumplimiento legal Herramientas de cumplimiento legal (LOPD, LSSI,...), Borrado seguro, Destrucción documental	✓	✓	✓		
Inteligencia de seguridad Gestión de eventos de seguridad, SIM/SIEM, *Big Data,* Herramientas de monitorización y *reporting*			✓	✓	✓
Prevención de fuga de información Control de contenidos confidenciales, Gestión del ciclo de vida de la información, Herramientas de cifrado		✓	✓		✓
Protección de las comunicaciones Cortafuegos *(firewall)*, VPN, IDS, IPS, UTM, *Appliance,* Filtro de contenidos, P2P, Gestión y control de ancho de banda		✓	✓	✓	✓
Seguridad en dispositivos móviles Seguridad para dispositivos móviles, Seguridad para redes inalámbricas, BYOD		✓			✓

5.2.1. ¿Cómo garantizo la seguridad de los tratamientos?

Si tu empresa trata datos de carácter personal debes adoptar las medidas de seguridad necesarias para evitar[32] 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.

32. El RGPD en el Art. 32 hace referencia en particular a los riesgos derivados de «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.

5

"Para garantizar la seguridad de los datos en cuanto a su **confidencialidad, integridad y disponibilidad**, aplicaremos herramientas tecnológicas"

Además, las empresas deben controlar los datos personales en todo momento y poder demostrarlo. Esto implica que debes conocer y asegurar en todo momento, durante todo el tratamiento, las ubicaciones de los datos es decir dónde están en los sistemas, ordenadores, discos duros, dispositivos móviles, servidores y en los servicios externos que contrates, así como en los servicios de proveedores web o servicios de almacenamiento, correo y todo tipo de aplicaciones en la nube, o tránsito en los servicios de comunicaciones.

Para determinar dónde están ubicados los ficheros que contienen datos personales, clasificarlos según su criticidad, monitorizar su uso, conocer quién accede, cuando se borran y cifrarlos cuando sea necesario se pueden utilizar soluciones de almacenamiento de datos, gestores documentales e incluso soluciones de BI (*Business Intelligence*) si los datos están en formatos y fuentes variadas. También son adecuadas para esta funcionalidad las herramientas de las categorías de **Prevención de fuga de información** y las de **Cumplimiento legal** como las de borrado seguro.

Para garantizar la seguridad de los datos en cuanto a su confidencialidad, integridad y disponibilidad, aplicaremos herramientas tecnológicas que permitan:

- Evitar accesos no autorizados y restringir el acceso a los datos aplicando principios de mínimos privilegios mediante sistemas de **Gestión de identidad y Autenticación** de la categoría de Control de accesos y autenticación. Aquellos servicios que sean críticos deben tener doble factor de autenticación para acceder a ellos.
- Realizar backups mediante herramientas específicas para hacer **Copias de seguridad** que son herramientas propias de planes de contingencia y continuidad.
- Seudonimizar[33] (tratarlos de manera que no puedan

33. El tratamiento de grandes volúmenes de datos (big data) nos permite descubrir tendencias, el comportamiento de los usuarios o sus patrones de compra. También nos permiten realizar pronósticos y anticiparnos a cambios en la demanda. Pero estos tratamientos suponen grandes retos a la hora de garantizar la privacidad. Con la anonimización se elimina o reduce al mínimo el riesgo de reidentificacion de las personas y estos datos podrían almacenarse o tratarse, por ejemplo para fines estadísticos. En este sentido la AEPD publica Orientaciones y garantías en los procedimientos de anonimización de datos personales. Los datos son anonimizados si no incluyen identificadores y son seudonimizados si estos, los identificadores, están cifrados.

5

"Realizar backups mediante herramientas específicas para hacer **copias de seguridad** que son herramientas propias de planes de contingencia y continuidad"

atribuirse a una persona física identificada o identificable) y cifrar los datos, para lo cual se utilizarán **herramientas de cifrado** que pertenecen a la categoría de Prevención de fuga de información. El cifrado garantiza la confidencialidad y la integridad. Además **reduce el riesgo de sanciones** y evita que tengamos que informar a los usuarios en caso de brecha de seguridad.

- Controlar el almacenamiento, los soportes y el acceso a los datos con herramientas como las mencionadas de Prevención de fuga de información y si utilizas para los tratamientos **dispositivos móviles** también las análogas para estos dispositivos. De igual forma, tendremos controlados todos los dispositivos y **soportes** con herramientas que nos permitan hacer inventarios de los mismos y del software instalado verificando a su vez que sea legítimo y esté actualizado.
- Para proteger los datos en los dispositivos, en el puesto de trabajo, en el correo electrónico y en las comunicaciones utilizaremos también herramientas **Antifraude y Antimalware.**
- Además, utilizaremos los mecanismos adecuados para **Protección de las comunicaciones tanto por cable como inalámbricas.** Estas herramientas, y en particular los cortafuegos, van a permitirnos segmentar y restringir las partes de nuestra red dónde se tratan datos personales, para evitar que puedan estar accesibles a terceros no autorizados. Igualmente tendremos que asegurar las comunicaciones con redes privadas virtuales o VPN.

Si ya cumplías con la LOPDGDD, revisa que las medidas que tomabas están acordes con el nuevo Reglamento, pues no tienen el mismo tratamiento. El RGPD indica que la adopción de estas medidas debe tener una **base en el análisis de riesgos para los derechos y libertades** y considerar además:

- el coste de la técnica a emplear,
- los costes de aplicación,
- la naturaleza, el alcance, el contexto y los fines del tratamiento.

5

"Si ya cumplías con la LOPDGDD, revisa que las medidas que tomabas están acordes con el nuevo Reglamento, pues no tienen el mismo tratamiento"

5.2.2 Rendición de cuentas

Desde el 25 de Mayo de 2018 también se tiene que tener en cuenta que el responsable y el encargado del tratamiento deben establecer las medidas técnicas y organizativas apropiadas para **garantizar** el nivel de seguridad[34] adecuado al riesgo existente. Además de los procedimientos del apartado anterior, a nivel técnico:

a. para demostrar la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento utilizaremos herramientas que nos permitan mantener actualizados y vigilados los sistemas como las de Auditoría técnica y, dependiendo de la complejidad de los tratamientos, herramientas de Inteligencia de seguridad;

b. y para demostrar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico utilizaremos como mencionamos planes y herramientas de Contingencia y continuidad.

34. El art. 32 del RGPD trata del nivel de seguridad del tratamiento

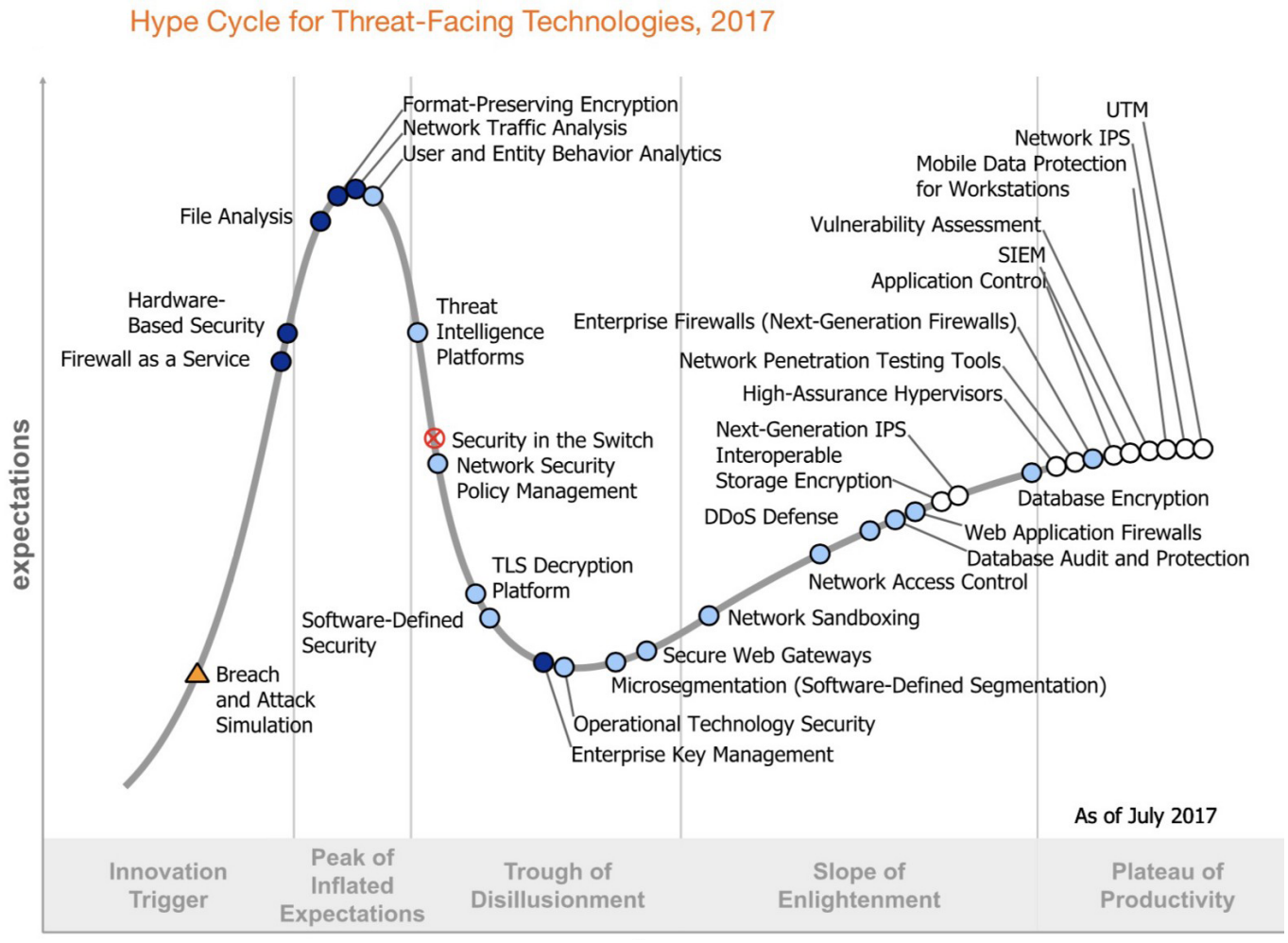
5

CONTINGENCIA Y CONTINUIDAD

AUDITORÍA TÉCNICA E INTELIGENCIA DE SEGURIDAD

Además, dispondremos de un **proceso de verificación, evaluación y valoración** regular de la eficacia de las medidas técnicas y organizativas que hayamos aplicado para garantizar la seguridad del tratamiento. Esto puede automatizarse dependiendo del tratamiento con las herramientas mencionadas o con nuevas herramientas como las de **Simulación de ataques y brechas de seguridad** que muestra la curva de Gartner que algunos fabricantes empiezan a ofrecer.

Adicionalmente para monitorizar la actividad de los usuarios autorizados se pueden implementar herramientas que incluyan técnicas de IA (Inteligencia artificial) como las indicadas en la curva de Gartner con el nombre ***User and Entity Behaviour Analytics.***



5

"El responsable y el encargado del tratamiento deben establecer **las medidas técnicas y organizativas** apropiadas para **garantizar** el nivel de seguridad adecuado al riesgo existente"

Estas medidas han de proteger los datos personales de manera que sean tratados con garantías de seguridad incluyendo protección contra el procesamiento no autorizado o ilegal, y para evitar la pérdida accidental, su destrucción o que sufran daños, **tanto si la infraestructura para el tratamiento está en local como si está externalizada o en la nube.**

Si utilizas servicios en la nube como Office 365, Dropbox o algún CRM/ERP online tienes que confirmar que en ellos puedes aplicar **los mismos requisitos de seguridad para los datos de tus tratamientos** que los que tendrías en local. Una buena medida si utilizas servicios ***cloud*** para almacenar los datos de tus tratamientos es que cifres, y a ser posible anonimices, todos los datos personales que vayas a subir. En cualquier caso es una buena práctica revisar la seguridad que le pides a tu proveedor ***cloud***[35] y elegir **servicios cloud certificados** o los servicios de intermediarios de seguridad en la nube o CSAB[36] ***(Cloud Security Access Brokers)***.

Siempre puedes optar por apoyarte en tu proveedor tecnológico[37] para que te ayude con la gestión de riesgos de privacidad y a determinar las medidas técnicas y organizativas necesarias para obtener las garantías que el RGPD demanda.

35. ¿Qué seguridad le pides a tur proveedor cloud? https://www.incibe.es/protege-tu-empresa/blog/seguridad-le-pides-tu-proveedor-cloud o Pasos a seguir antes de subir en la nube https://www.incibe.es/protege-tu-empresa/blog/pasos-seguir-subir-nube

36 Lee el artículo de M.A. Mendoza en Welivesecurity de ESET Seguridad en la nube para empresas: ¿Qué son los CASB? https://www.welivesecurity.com/la-es/2014/09/24/seguridad-nube-empresas-que-son-casb/

37. Consulta el Catálogo de empresas y soluciones de seguridad para encontrar el proveedor adecuado https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad

6 ¿QUÉ PASA SI NO CUMPLO?

Los ciudadanos de la UE tienen derecho a **presentar reclamaciones** ante las autoridades de control si consideran que el tratamiento de sus datos personales infringe el RGPD.

También al ser la privacidad un derecho fundamental tienen derecho a la **tutela judicial efectiva:**

- contra las decisiones jurídicamente vinculantes de las autoridades de control que le afecten, por ejemplo si no dan curso a su reclamación o no le informan del resultado en el plazo de tres meses;
- contra un responsable o encargado del tratamiento cuando considere que sus derechos han sido vulnerados como consecuencia de un tratamiento de sus datos personales.

Así mismo, tienen **derecho a indemnización** por el responsable o el encargado del tratamiento por los **daños y perjuicios** sufridos a consecuencia de una infracción del RGPD.

Estos derechos podrán ejercitarlos **de forma individual o colectiva**, a través de organizaciones o asociaciones sin ánimo de lucro constituidas para la protección de estos derechos y libertades.

Por otra parte, las autoridades de control pueden investigar y corregir las infracciones[38]. Para las investigaciones podrán ordenar al responsable o al encargado **que facilite información, llevar a cabo auditorías y obtener acceso a los datos, locales y equipos.** Para corregir las infracciones podrá, entre otros, sancionar con advertencias si consideran que la infracción es posible, sancionar con apercibimientos si se ha infringido el RGPD, limitar temporalmente o prohibir el tratamiento, ordenar supresión de datos e imponer multas[39].

Las multas administrativas por las infracciones del RGPD, se establecen en dos niveles de acuerdo con criterios de proporcionalidad, responsabilidad, intencionalidad, carácter continuado, beneficios obtenidos y, en particular por las conductas que supongan una vulneración:

38. Artículo 58 RGPD Poderes.

39. Artículo 83 del RGPD.

6

- de hasta 10 millones de euros, o si es una empresa del equivalente al 2% del volumen de negocio total anual global del ejercicio financiero anterior, la mayor de las dos;
- de hasta 20 millones de euros, o si es una empresa del equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior, la mayor de las dos;

El **Proyecto de Ley** [13] establece una distinción entre infracciones muy graves, graves y leves a los solos efectos de determinar los plazos de prescripción. Las muy graves prescribirán a los tres años, las graves a los dos años y las leves al año. Esta clasificación incluye casos particulares de lo que se considera infracciones de cada tipo. Por ejemplo:

- es una infracción leve, el incumplimiento de la obligación de informar al usuario, si así lo ha solicitado, de los destinatarios a los que se ha comunicado la rectificación, supresión o limitación del tratamiento de sus datos personales;
- es una infracción grave, el incumplimiento del deber del encargado del tratamiento de notificar al responsable de las violaciones de seguridad de que tuviera conocimiento;
- es una infracción muy grave, la transferencia internacional de datos cuando no se cumplen las garantías, requisitos y excepciones establecidas.

"La protección de datos personales de tus clientes, usuarios, colaboradores o empleados es un importante **factor de competitividad y fidelización"**

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

7 REFERENCIAS

[1] Unión Europea, Síntesis de la Directiva de Servicios de Pago (PSD2)
http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=LEGISSUM:2404020302_1&from=EN&isLegissum=true

[2] Reglamento sobre identificación electrónica y servicios de confianza (eIDAS)
https://www.boe.es/doue/2014/257/L00073-00114.pdf

[3] Unión Europea, La Directiva NIS para la seguridad en las redes y sistemas de información
http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016L1148&from=ES

[4] Foro CSIRT.es
https://www.csirt.es/index.php/objetivos

[5] Directiva NIS2
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32022L2555

[6] Reglamento General de Protección de Datos, RGPD
https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=es

[7] Unión Europea, Consejo Europeo
http://www.consilium.europa.eu/es/european-council/

[8] Unión Europea, 2000 Carta de Derechos Fundamentales de la UE
https://www.europarl.europa.eu/charter/pdf/text_es.pdf

[9] Tratado de Lisboa en diciembre de 2009,
http://www.europarl.europa.eu/ftu/pdf/es/FTU_1.1.5.pdf

[10] Unión Europea, Estrategia del Consejo Europeo Europa 2020,
https://eur-lex.europa.eu/ES/legal-content/summary/europe-2020-the-european-union-strategy-for-growth-and-employment.html

[11] Unión Europea Comisión Europea, Mercado Único Digital Europeo,
https://ec.europa.eu/commission/priorities/digital-single-market_es

[12] España, BOE (2016) Reglamento General de Protección de Datos
https://www.boe.es/doue/2016/119/L00001-00088.pdf

[13] España, Congreso de los Diputados (2017) Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal.
http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF

[14] AEPD, Canal del ciudadano, Derechos, Principales Derechos
https://www.aepd.es/derechos-y-deberes/conoce-tus-derechos

7 REFERENCIAS

[15] AEPD, Protección de datos: guía para el ciudadano
https://www.aepd.es/documento/guia-ciudadano.pdf

[16] AEPD, Directrices para la elaboración de contratos entre responsables y encargados del tratamiento de la AEPD.
https://www.aepd.es/documento/guia-directrices-contratos.pdf

[17] AEPD, La Guía para el cumplimiento del deber de informar de la AEPD
https://www.aepd.es/documento/guia-modelo-clausula-informativa.pdf

[18] AEPD, Herramienta Facilita
https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

[19] Acosta, D. Blog (2017) ISO/IEC 29100/2011 Una introducción al marco de trabajo de privacidad para la protección de información de identificación personal (PII)
https://www.deacosta.com/isoiec-291002011-una-introduccion-al-marco-de-trabajo-de-privacidad-para-la-proteccion-de-informacion-de-identificacion-personal-pii/

[20] EEUU, National Institute of Standards and Technology NIST, (2017) NISTR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems
https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

[21] Incibe, Gestión de riesgos: una guía de aproximación para el empresario
https://www.incibe.es/empresas/guias/gestion-riesgos-guia-empresario

[22] Incibe, ¿Conoces tus riesgos?
https://www.incibe.es/empresas/herramientas/conoces-tus-riesgos

[23] AEPD Guía para la Gestión del riesgo y evaluación de impacto en tratamientos de datos personales
https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

[24] ISMS y AEPD Código de Buenas prácticas en protección de datos para proyectos Big Data
https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

[25] AEPD (2016) Orientaciones y garantías en los procedimientos de ANONIMIZACIÓN de datos personales de la AEPD
https://www.aepd.es/sites/default/files/2019-12/guia-orientaciones-procedimientos-anonimizacion.pdf

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa