Política de Protección de Datos

ALFISA ASESORES Y CONSULTORES, S.L.U.

Reglamento General de Protección de Datos - Ley Orgánica 3/2018

ÍNDICE DE CONTENIDO

· INTRODUCCIÓN

El Reglamento General de Protección de Datos (RGPD) entró en vigor en mayo de 2016 y es aplicable desde mayo de 2018.

La adaptación al Reglamento general de protección de datos requiere la elaboración de una nueva ley orgánica que sustituya a la actual.

El objeto de la **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales** es adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.

En el RGPD se amplían los derechos de los ciudadanos y se aplica al tratamiento de datos personales de ciudadanos que residan en la Unión Europea por parte de un responsable o encargado no establecido en la Unión, es decir, aquellas empresas situadas fuera de la Unión que ofrezcan sus servicios o productos a través de internet a los europeos deberán cumplir con el RGPD.

Dos elementos de carácter general constituyen la mayor innovación del RGPD para los responsables y se proyectan sobre todas las obligaciones de las organizaciones:

El principio de responsabilidad proactiva.

El RGPD describe este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.

En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión. Este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

El enfoque de riesgo.

El RGPD señala que las medidas dirigidas a garantizar su cumplimiento deben tener 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.

De acuerdo con este enfoque, algunas de las medidas que el RGPD establece se aplicarán sólo cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten. La aplicación de las medidas previstas por el RGPD debe adaptarse, por tanto, a las características de las organizaciones. Lo que puede ser adecuado para una organización que maneja datos de millones de interesados en tratamientos complejos que involucran información personal sensible o volúmenes importantes de datos sobre cada afectado no es necesario para una pequeña empresa que lleva a cabo un volumen limitado de tratamientos de datos no sensibles.

LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS

Todo tratamiento de datos necesita apoyarse en una base jurídica que lo legitime:

· Consentimiento

· Relación contractual.

· Intereses vitales del interesado o de otras personas.

· Obligación legal para el responsable.

· Interés público o ejercicio de poderes públicos.

· Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

El consentimiento debe ser "inequívoco" El consentimiento inequívoco es aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa, no se admiten formas de consentimiento tácito o por omisión, ya que se basan en la inacción.

Hay situaciones en las que el consentimiento inequívoco, ha de ser **"explícito"**:

· Tratamiento de datos sensibles.

· Adopción de decisiones automatizadas.

· Transferencias internacionales.

El consentimiento puede ser inequívoco y otorgarse de forma **"implícita"** cuando se deduzca de una acción del interesado, por ejemplo, cuando el interesado continúa navegando por una web y acepta así el que se utilicen cookies para monitorizar su navegación.

Los tratamientos iniciados con anterioridad al inicio de la aplicación del RGPD sobre la base del consentimiento seguirán siendo legítimos siempre que ese consentimiento se hubiera prestado del modo en que prevé el propio RGPD, es decir, mediante una manifestación o acción afirmativa.

RGPD establece lo siguiente respecto al tratamiento de determinadas categorías especiales de datos:

Regla general: Prohibición de tratamiento de datos que revelen el origen étnico o racial, las opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, así como el tratamiento de datos genéticos, biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud, vida sexual u orientaciones sexuales de una persona física.

Excepciones a la regla general:

· Consentimiento del titular de los datos, excepto que por el Derecho de la Unión o Estados miembros no se pueda levantar la prohibición.

· Tratamiento necesario para que el responsable cumpla con obligaciones de Derecho laboral, seguridad y protección social, si así lo autoriza el Derecho de la Unión o convenio colectivo.

· Tratamiento necesario para proteger el interés vital del interesado u otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para prestar su consentimiento.

· Tratamiento realizado por una fundación, asociación u otra entidad sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera a sus miembros (antiguos o actuales) o personas que mantengan contactos regulares, y que los datos no se cedan a terceros sin consentimiento.

· Tratamiento referido a datos que el interesado ha hecho manifiestamente públicos.

· Tratamiento necesario para la formulación, ejercicio o defensa de reclamaciones o

cuando los tribunales actúen en ejercicio de su función.

· Tratamiento necesario en base al interés público esencial, sobre la base del Derecho (UE o Estados miembros), debiendo ser proporcional al objetivo perseguido, respetando la protección de datos y estableciendo medidas para proteger los intereses y derechos fundamentales del interesado.

· Tratamiento para fines de medicina (preventiva/laboral), evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación/tratamiento sanitario o social o gestión de sistemas y servicios de asistencia sanitaria.

· Tratamiento necesario por razones de interés público en el ámbito de la salud pública o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos/productos sanitarios, sobre la base del Derecho (UE o Estados miembros), adoptando medidas adecuadas para proteger los derechos y libertades del interesado, en particular el secreto profesional.

· Tratamiento con fines de archivo en interés público, investigación científica, histórica o estadística, respetando la protección de datos y estableciendo medidas para proteger los intereses y derechos fundamentales del interesado.

INFORMACIÓN A LOS INTERESADOS

La información a los interesados, tanto respecto a las condiciones de los tratamientos que les afecten como en las respuestas a los ejercicios de derechos, deberá proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

Se establece una lista exhaustiva de la información que debe proporcionarse a los interesados, pudiendo distinguir entre una información básica (primer nivel) y una información adicional (segundo nivel):

· Identidad del responsable del tratamiento

· Descripción de los fines del tratamiento, incluso elaboración de perfiles

· Base jurídica del tratamiento

· Intención de realizar transferencias internacionales

· Referencia al ejercicio de derechos

· Fuente de los datos (cuando no proceden del interesado)

· Datos del Delegado de Protección de Datos (si lo hubiere)

La información a los interesados deberá facilitarse por escrito, incluidos los medios electrónicos cuando sea apropiado.

DERECHOS

Los responsables deben facilitar a los interesados el ejercicio de sus derechos, los

procedimientos deben ser visibles, accesibles y sencillos.

Se requiere que los responsables posibiliten la presentación de solicitudes por medios electrónicos, especialmente cuando el tratamiento se realiza por estos medios.

El ejercicio de los derechos será gratuito para el interesado, excepto en los casos en que se formulen solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas, el responsable podrá cobrar un canon que compense los costes administrativos de atender a la petición o negarse a actuar (el canon no podrá implicar un ingreso adicional para el responsable, sino que deberá corresponderse efectivamente con el verdadero coste de la tramitación de la solicitud).

El responsable debe:

- Articular procedimientos que permitan fácilmente que los interesados puedan acreditar que han ejercido sus derechos por medios electrónicos.
- Demostrar el carácter infundado o excesivo de las solicitudes que tengan un coste para el interesado.
- Informar al interesado sobre las actuaciones derivadas de su petición en el plazo de un mes (podrá extenderse dos meses más cuando se trate de solicitudes especialmente complejas y deberá notificar esta ampliación dentro del primer mes).
- Si el responsable decide no atender una solicitud, deberá informar de ello, motivando su negativa, dentro del plazo de un mes desde su presentación.
- Tomar medidas para verificar la identidad de quienes soliciten acceso y de quienes ejerzan los restantes derechos ARCO.
- El responsable que trate una gran cantidad de información sobre un interesado podrá pedir a éste que especifique la información a que se refiere su solicitud de acceso.
- El responsable podrá contar con la colaboración de los encargados para atender al ejercicio de derechos de los interesados, pudiendo incluir esta colaboración en el contrato de encargo de tratamiento.

Derecho de acceso

Se reconoce como el derecho a obtener una copia de los datos personales objeto del tratamiento.

A través del ejercicio de este derecho el interesado conocer qué datos de carácter personal son tratados por parte del responsable, la finalidad de este tratamiento, el origen de los citados datos y si se han comunicado o se van a comunicar a un tercero.

Una vez ejercitado el derecho de acceso, se deben de contestarte en el plazo máximo de un mes, y en caso de estimar el derecho, el acceso se hará efectivo en el plazo máximo de diez días hábiles, pudiendo elegir la forma por la cual se va a recibir la información a través de alguno de los siguientes medios:

- Visualización en pantalla.
- Escrito, copia o fotocopia remitida por correo, certificado o no.
- Telecopia.
- Correo electrónico u otros sistemas de comunicación electrónica.
- Cualquier otro sistema adecuado ofrecido por quien posee tus datos personales (responsable del fichero).

Derecho de rectificación

Consiste en la posibilidad de que se modifiquen los datos del interesado que sean inexactos o incompletos, debiendo en la solicitud de rectificación indicar qué datos deseas que se modifiquen. A esta solicitud se deberá acompañar la documentación justificativa correspondiente

Cuando se ejercita este derecho, se debe contestar en el plazo máximo de 10 días hábiles. Si los datos hubieran sido comunicados a un tercero, el responsable deberá comunicarle los datos rectificados para que a su vez este tercero los rectifique.

Derecho de oposición

Mediante el ejercicio de este derecho puede oponerse el afectado a que no se realice el tratamiento de sus datos personales en los siguientes supuestos:

- Cuando no siendo necesario el consentimiento del afectado para el tratamiento de sus datos, exista un motivo legítimo y fundado referente a su concreta situación personal (salvo que una Ley establezca lo contrario).
- Cuando estemos ante tratamientos de datos personales cuya finalidad sea la realización de actividades de publicidad y prospección comercial.
- Cuando el tratamiento tenga como fin la adopción de una decisión referida al afectado basada únicamente en un tratamiento automatizado de sus datos personales.

Derecho de cancelación

Este derecho permite la cancelación de los datos personales que sean inadecuados o excesivos. No obstante, se conservarán bloqueados de manera que se impida su tratamiento, sin perjuicio de su puesta a disposición de las administraciones públicas, jueces y tribunales, para la atención de las posibles responsabilidades que hayan surgido del tratamiento durante su plazo de prescripción.

Cumplido este plazo se procederá a la supresión de los mismos.

Cuando se soliciten la cancelación de los datos personales, se deberá indicar a qué datos se refieren, aportando la documentación que justifique tal pretensión.

Se deben contestar en el plazo máximo de 10 días hábiles. Si los datos hubieran sido comunicados a un tercero, el responsable deberá comunicarle los datos cancelados para que, a su vez, este tercero los cancele.

Derecho al olvido

El tratamiento de datos que realizan los motores de búsqueda de internet, como Google, Bing o Yahoo, está sometido a las normas de protección de datos de la Unión Europea, y los ciudadanos pueden solicitar que los enlaces a sus datos personales no aparezcan en los resultados de una búsqueda realizada por su nombre y apellidos, cuando la información es obsoleta o no tiene relevancia ni interés público

Es la consecuencia de la aplicación del derecho al borrado de los datos personales, es una manifestación de los derechos de cancelación u oposición en el entorno online.

Limitación del tratamiento

Supone que, a petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían.

Se puede solicitar la limitación cuando:

- El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender a la solicitud.
- El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello.
- Los datos ya no son necesarios para el tratamiento, que también determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

En el tiempo que dure la limitación, el responsable sólo podrá tratar los datos afectados, más allá de su conservación:

- Con el consentimiento del interesado.
- Para la formulación, el ejercicio o la defensa de reclamaciones.
- Para proteger los derechos de otra persona física o jurídica.

· Por razones de interés público importante de la Unión o del Estado miembro correspondiente.

Portabilidad

El derecho a la portabilidad de los datos es una forma avanzada del derecho de acceso por el cual la copia que se proporciona al interesado debe ofrecerse en un formato estructurado, de uso común y lectura mecánica.

Este derecho sólo puede ejercerse:

· Cuando el tratamiento se efectúe por medios automatizados.

· Cuando el tratamiento se base en el consentimiento o en un contrato.

· Cuando el interesado lo solicita respecto a los datos que haya proporcionado al responsable y que le conciernan, incluidos los datos derivados de la propia actividad del interesado.

El derecho a la portabilidad implica que los datos personales del interesado se transmiten directamente de un responsable a otro, sin necesidad de que sean transmitidos previamente al propio interesado, siempre que ello sea técnicamente posible.

No es aplicable:

· A los datos de terceras personas que un interesado haya facilitado a un responsable.

· En caso de que el interesado haya solicitado la portabilidad de datos que le incumban pero que hayan sido proporcionados al responsable por terceros.

ENCARGADO DE TRATAMIENTO

La responsabilidad última sobre el tratamiento sigue estando atribuida al responsable, que es quien determina la existencia del tratamiento y su finalidad.

En determinadas materias los encargados tienen obligaciones propias que establece el RGPD, que no se circunscriben al ámbito del contrato que los une al responsable, y que pueden ser supervisadas separadamente por las autoridades de protección de datos. Por ejemplo:

· Deben mantener un registro de actividades de tratamiento.

· Deben determinar las medidas de seguridad aplicables a los tratamientos que realizan.

· Deben designar a un Delegado de Protección de Datos en los casos previstos por el RGPD.

Los responsables habrán de **elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento.** Esta previsión se extiende también a los encargados cuando subcontraten operaciones de tratamiento con otros subencargados.

Las relaciones entre el responsable y el encargado deben formalizarse en un contrato o en un acto jurídico que vincule al encargado respecto al responsable.

Se regula de forma minuciosa el contenido mínimo de los contratos de encargo, debiendo preverse aspectos como:

· Objeto, duración, naturaleza y la finalidad del tratamientos.

· 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…

MEDIDAS DE RESPONSABILIDAD ACTIVA

El RGPD establece un catálogo de las medidas que los responsables, y en ocasiones los encargados, deben aplicar para garantizar que los tratamientos que realizan son conformes con el Reglamento y estar en condiciones de demostrarlo.

Análisis de riesgo

El RGPD condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados.

Se maneja el riesgo de dos maneras:

- En algunos casos, prevé que determinadas medidas solo deberán aplicarse cuando el tratamiento suponga un alto riesgo para los derechos y libertados (por ejemplo, Evaluaciones de impacto sobre la Protección de Datos).
- En otros casos, las medidas deberán modularse en función del nivel y tipo de riesgo que el tratamiento conlleve (por ejemplo, con las medidas de Protección de Datos desde el Diseño o con las medidas de seguridad).

Todos los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo.

El tipo de análisis variará en función de:

- Los tipos de tratamiento.
- El número de interesados afectados.
- La cantidad y variedad de tratamientos que una misma organización lleve a cabo.

Registro de actividades de tratamiento

Responsables y encargados deberán mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el RGPD y que contenga cuestiones como:

- Nombre y datos de contacto del responsable o corresponsable y del Delegado de Protección de Datos si existiese.
- Finalidades del tratamiento.
- Descripción de categorías de interesados y categorías de datos personales tratados.
- " Transferencias internacionales de datos...

Están exentas las organizaciones que empleen a menos de 250 trabajadores, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

Las posibilidades para organizar el registro de actividades de tratamiento son:

- Partir de los ficheros que actualmente tienen notificados los responsables en el Registro General de Protección de Datos, detallando todas las operaciones que se realizan sobre cada conjunto estructurado de datos.
- En torno a operaciones de tratamiento concretas vinculadas a una finalidad básica común de todas ellas (por ejemplo, "gestión de clientes", "gestión contable" o "gestión de recursos humanos y nóminas") o con arreglo a otros criterios distintos.

Protección de Datos desde el Diseño y por Defecto

Estas medidas se incluyen dentro de las que debe aplicar el responsable con anterioridad al inicio del tratamiento y también cuando se esté desarrollando.

Este tipo de medidas reflejan muy directamente el enfoque de responsabilidad proactiva. Se trata de pensar en términos de protección de datos desde el mismo momento en que se diseña un tratamiento, un producto o servicio que implica el tratamiento de datos personales.

Desde el inicio, los responsables deben tomar medidas organizativas y técnicas para integrar en los tratamientos garantías que permitan aplicar de forma efectiva los principios del RGPD.

Los responsables deben adoptar medidas que garanticen que solo se traten los datos necesarios en lo relativo a la cantidad de datos tratados, la extensión del tratamiento, los periodos de conservación y la accesibilidad a los datos.

Medidas de seguridad

El Reglamento de Desarrollo de la LOPD determinaba con detalle y de forma exhaustiva las medidas de seguridad que debían aplicarse según el tipo de datos objeto de tratamiento.

En el RGPD, los responsables y encargados establecerán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo.

Las medidas técnicas y organizativas deberán establecerse teniendo en cuenta:

- El coste de la técnica.
- Los costes de aplicación.
- La naturaleza, el alcance, el contexto y los fines del tratamiento.
- Los riesgos para los derechos y libertades.

En algunos casos los responsables podrán seguir aplicando las mismas medidas que establece el Reglamento de la LOPD si los resultados del análisis de riesgos previo concluye que las medidas son realmente las más adecuadas para ofrecer un nivel de seguridad adecuado. En ocasiones será necesario completarlas con medidas adicionales o prescindir de alguna de las medidas.

Notificación de violaciones de seguridad de los datos

El RGPD define las violaciones de seguridad de los datos, más comúnmente conocidas como "quiebras de seguridad", de una forma muy amplia, que incluye todo incidente que ocasione 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. Sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del RGPD y deben ser tratadas como el Reglamento establece.

Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

La notificación de la quiebra a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.

La notificación ha de incluir un contenido mínimo:

- La naturaleza de la violación.
- Categorías de datos y de interesados afectados.
- Medidas adoptadas por el responsable para solventar la quiebra.
- Si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados.

Los responsables deben documentar todas las violaciones de seguridad.

En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con una notificación dirigida a los interesados.

El objetivo de la notificación a los afectados es permitir que puedan tomar medidas para protegerse de sus consecuencias. Por ello, el RGPD requiere que se realice sin dilación indebida, sin hacer referencia ni al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas. El propósito es siempre que el interesado afectado pueda reaccionar tan pronto como sea posible.

El RGPD añade a los contenidos de la notificación las recomendaciones sobre las medidas que pueden tomar los interesados para hacer frente a las consecuencias de la quiebra.

La valoración del riesgo se trata de establecer hasta qué punto el incidente, por sus características, el tipo de datos a los que se refiere o el tipo de consecuencias que puede tener para los afectados puede causar un daño en sus derechos o libertades.

Los daños pueden ser materiales o inmateriales, e ir desde la posible discriminación de los afectados como consecuencia de su uso por quien ha accedido a ellos de forma no autorizada hasta usurpación de identidad, pasando por perjuicios económicos o la exposición pública de datos confidenciales.

Se considera que se tiene constancia de una violación de seguridad cuando hay una certeza de que se ha producido y se tiene un conocimiento suficiente de su naturaleza y alcance.

La mera sospecha de que ha existido una quiebra o la constatación de que ha sucedido algún tipo de incidente sin que se conozcan mínimamente sus circunstancias no deberían dar lugar, todavía, a la notificación, dado que en esas condiciones no sería posible, en la mayoría de los casos, determinar hasta qué punto puede existir un riesgo para los derechos y libertades de los interesados.

En casos de quiebras que por sus características pudieran tener gran impacto, sí podría ser recomendable contactar con la autoridad de supervisión tan pronto como existan evidencias de que se ha producido alguna situación irregular respecto a la seguridad de los datos, sin perjuicio de que esos primeros contactos puedan completarse con una notificación formal más completa dentro del plazo legalmente previsto.

Puede haber casos en que la notificación no pueda realizarse dentro de esas 72 horas, por ejemplo, por la complejidad en determinar completamente su alcance. En esos casos, es posible hacer la notificación con posterioridad, acompañándola de una explicación de los motivos que han ocasionado el retraso.

La información puede proporcionarse de forma escalonada cuando no sea posible hacerlo en el mismo momento de la notificación.

El criterio de alto riesgo debe entenderse en el sentido de que sea probable que la violación de seguridad ocasione daños de entidad a los interesados. Por ejemplo, en casos en que se desvele información confidencial, como contraseñas o participación en determinadas actividades, se difundan de forma masiva datos sensibles o se puedan producir perjuicios económicos para los afectados.

La notificación a los interesados no será necesaria cuando:

- El responsable hubiera tomado medidas técnicas u organizativas apropiadas con anterioridad a la violación de seguridad, en particular las medidas que hagan ininteligibles los datos para terceros, como sería el cifrado.
- Cuando el responsable haya tomado con posterioridad a la quiebra medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice.
- Cuando la notificación suponga un esfuerzo desproporcionado, debiendo en estos casos sustituirse por medidas alternativas como puede ser una comunicación pública.

Evaluación de Impacto

Cuando el **análisis de riesgo** que las organizaciones lleven a cabo sobre los tratamientos iniciados con anterioridad a la fecha de aplicación del RGPD indiquen que esos tratamientos presentan alto riesgo para los derechos o libertades de los interesados, los responsables deberán realizar una EIPD sobre esos tratamientos, a fin de estar en condiciones de poder adoptar las medidas adecuadas para adecuar esos tratamientos a las exigencias del RGPD.

Los responsables de tratamiento deberán realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados.

El RGPD establece un contenido mínimo de las Evaluaciones de Impacto sobre la Protección de Datos, aunque no contempla ninguna metodología específica para su realización

En los casos en que las EIPD hayan identificado un alto riesgo que, a juicio del responsable de tratamiento no pueda mitigarse por medios razonables en términos de tecnología disponible y costes de aplicación, el responsable deberá **consultar a la autoridad de protección de datos competente**. La consulta debe ir acompañada de la documentación que prevé el RGPD, incluyendo la propia Evaluación de Impacto, y la autoridad de supervisión puede emitir **recomendaciones** o ejercer cualquier otro de los poderes que el RGPD le confiere, entre ellos el de prohibir la operación de tratamiento.

Lista indicativa de supuestos en que se considera que los tratamientos conllevan un alto riesgo:

- Elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos sobre los interesados o que les afecten significativamente de modo similar.
- Tratamientos a gran escala de datos sensibles:
- Para valorar si un tratamiento se realiza a gran escala debe tenerse en cuenta:
    - El número de interesados afectados, bien en términos absolutos, bien como proporción de una determinada población.
    - El volumen de datos y la variedad de datos tratados.
    - La duración o permanencia de la actividad de tratamiento.
    - La extensión geográfica de la actividad de tratamiento.
- Observación sistemática a gran escala de una zona de acceso público.

Las autoridades de protección de datos están obligadas a confeccionar listas adicionales de

tratamientos que requerirán una EIPD.

También está previsto que las autoridades puedan elaborar listas de tratamientos en los que no se precisa EIPD.

La existencia de los listados no excluye el que los responsables deban realizar el correspondiente análisis de riesgo y, en caso de que concluyan que existe un alto riesgo para los derechos y libertades de los interesados, lleven a cabo una EIPD, aun cuando el tratamiento en cuestión no esté incluido en ninguna de las dos listas mencionadas. Como se ha dicho, el RGPD se basa en un principio de responsabilidad activa del responsable y es siempre en último extremo el responsable el que debe decidir qué medidas aplicar y cómo hacerlo. La intervención de las autoridades de supervisión o las previsiones del propio RGPD aclaran sus disposiciones o las especifican, pero no sustituyen la responsabilidad de quienes tratan los datos.

Es posible realizar una única EIPD para varios tratamientos similares que entrañen altos riesgos también similares.

Puede ser necesario llevar a cabo una nueva evaluación cuando cambien las condiciones del tratamiento o cuando varíen los riesgos asociados al mismo.

Delegado de Protección de Datos

El artículo 37.1 del RGPD establece la figura del Delegado de Protección de Datos (DPD), que será obligatorio en:

- Autoridades y organismos públicos.
- Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala.
- Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles.

El artículo 34 de la Ley Orgánica 3/2018 de Protección de datos estipula la designación de un delegado de protección de datos:

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, **en todo caso, cuando se trate de las siguientes entidades:**

- Los colegios profesionales y sus consejos generales.
- Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
- Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
- Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
- Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
- Los establecimientos financieros de crédito.
- Las entidades aseguradoras y reaseguradoras.
- Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
- Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
- Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.
- Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

- Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.
- Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.
- Las empresas de seguridad privada.
- Las federaciones deportivas cuando traten datos de menores de edad.

El DPD ha de ser nombrado atendiendo a sus cualificaciones profesionales y, en particular, a su conocimiento de la legislación y la práctica de la protección de datos. Aunque no debe tener una titulación específica, en la medida en que entre las funciones del DPD se incluya el asesoramiento al responsable o encargado en todo lo relativo a la normativa sobre protección de datos, los conocimientos jurídicos en la materia son sin duda necesarios, pero también es necesario contar con conocimientos ajenos a lo estrictamente jurídico, como por ejemplo en materia de tecnología aplicada al tratamiento de datos o en relación con el ámbito de actividad de la organización en la que el DPD desempeña su tarea.

La designación del DPD y sus datos de contacto deben hacerse públicos por los responsables y encargados y deberán ser comunicados a las autoridades de supervisión competentes.

DPD en las organizaciones tiene que cumplir los requisitos establecidos:

- Total autonomía en el ejercicio de sus funciones.
- Necesidad de que se relacione con el nivel superior de la dirección.
- Obligación de que el responsable o el encargado faciliten al DPD todos los recursos necesarios para desarrollar su actividad.

Se permite nombrar un solo DPD para un grupo empresarial siempre que sea accesible desde cada establecimiento del grupo. La accesibilidad debe entenderse en un sentido amplio. Incluye la accesibilidad física para el propio personal del grupo y también la posibilidad de que los interesados contacten con el DPD en su lengua, aun cuando el DPD esté adscrito a un establecimiento en otro Estado Miembro.

Se permite que el DPD mantenga con responsables o encargados una relación laboral o mediante un contrato de servicios, permite que pueda contratarse el servicio de DPD con personas físicas o jurídicas ajenas a la organización.

Está permitido que el DPD desarrolle sus funciones a tiempo completo o parcial. En este último caso, es preciso evitar que existan conflictos de intereses, que pueden surgir cuando el DPD, en su tarea de supervisión de las actividades de tratamiento de datos llevadas a cabo por la organización, debe valorar su propio trabajo dentro de ella, como sucede si se designa DPD al responsable de tecnologías de la información (cuando estas tecnologías se emplean para el tratamiento de datos) o al responsable de un área de negocio que decide sobre determinados tratamientos.

El RGPD prevé también el catálogo de funciones del DPD, entre las que se incluyen las relativas a actuar como punto de contacto para los interesados en todo lo que tenga relación con el tratamiento de sus datos personales.

RÉGIMEN SANCIONADOR

La normativa europea contempla sanciones muy elevadas ya que, según la infracción, las multas administrativas pueden alcanzar entre 10 y 20 millones de euros, o entre el 2 y el 4% del volumen de negocio anual global.

La Ley Orgánica 3/2018 mantiene la clasificación del antiguo articulado entre muy grave, grave y leve, según el grado de afectación de los datos.

El régimen español de infracciones se divide en:

- **Muy graves:** las que supongan una vulneración sustancial del tratamiento y tengan quever con el uso de los datos para una finalidad diferente de la anunciada, la omisión del deber de informar al afectado, la exigencia de un pago para poder acceder a los datos propios almacenados, transferencia internacional de información sin garantías...

  Este tipo de infracción prescribe a los 3 años.

- **Graves:** las que supongan una vulneración sustancial del tratamiento y tengan que ver con datos de un menor recabados sin consentimiento, falta de adopción de medidas técnicas y organizativas necesarias para la efectiva protección de datos o, por ejemplo, el incumplimiento de la obligación de nombrar responsable o encargado de tratamiento de datos.

  Este tipo de infracción prescribe a los 2 años.

- **Leves:** las restantes que no queden contempladas en los grupos anteriores y se refieren a casos como la no transparencia de la información, el incumplimiento de no informar al afectado cuando lo haya solicitado o, por ejemplo, el incumplimiento por parte del encargado de sus obligaciones.

  Este tipo de infracción prescribe al año.

Además, para aplicar una u otra sanción también se tendrán en cuenta circunstancias como el carácter continuado de la infracción, la vinculación de la actividad del infractor con el tratamiento, la afectación a los derechos de los menores, etc.

TRANSFERENCIAS INTERNACIONALES

Los datos solo podrán ser comunicados fuera del Espacio Económico Europeo:

- A países, territorios o sectores específicos (el RGPD incluye también organizaciones internacionales) sobre los que la Comisión haya adoptado una decisión reconociendo que ofrecen un nivel de protección adecuado.
- Cuando se hayan ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino.
- Cuando se aplique alguna de las excepciones que permiten transferir los datos sin garantías de protección adecuada por razones de necesidad vinculadas al propio interés del titular de los datos o a intereses generales.

Las decisiones de adecuación que la Comisión ha adoptado con anterioridad a la aplicación del RGPD seguirán siendo válidas, y por tanto, podrán seguir realizándose transferencias basadas en ellas, en tanto la Comisión no las sustituya o derogue.

Las decisiones de la Comisión estableciendo cláusulas tipo para los contratos en los que se establecen garantías para las transferencias internacionales seguirán siendo válidas hasta que la Comisión las sustituya o derogue.

Las autorizaciones de transferencias que las autoridades nacionales de protección de datos hayan otorgado sobre la base de garantías contractuales seguirán siendo válidas en tanto las autoridades no las revoquen.

Las garantías sobre la protección que recibirán los datos en destino las debe ofrecer el exportador, que podrá ser tanto un responsable como un encargado de tratamiento.

Se amplía la lista de posibles instrumentos para ofrecer garantías, incluyéndose expresamente, entre otros, las Normas Corporativas Vinculantes para responsables y encargados, los códigos de conducta y esquemas de certificación, así como los cláusulas contractuales modelo que puedan aprobar las autoridades de protección de datos.

En los casos de Normas Corporativas Vinculantes, cláusulas contractuales estándar, códigos de conducta y esquemas de certificación, la transferencia no requerirá la autorización de las autoridades de supervisión.

Se añade una excepción al listado que en su momento estableció la Directiva 95/46, se trata de la posibilidad de que el responsable pueda transferir datos a un país sin nivel adecuado de protección cuando esa transferencia sea necesaria para satisfacer intereses legítimos imperiosos del responsable y la transferencia no es repetitiva y afecta sólo a un número limitado de interesados. En todo caso, la transferencia solo será posible si no prevalecen los derechos, libertades e intereses de los afectados y deberá comunicarse a la autoridad de protección de datos.

TRATAMIENTOS DE DATOS DE MENORES

El RGPD prevé para la obtención del consentimiento en el ámbito de la oferta directa de servicios de la sociedad de la información, que solo será válido a partir de los 16 años, debiendo contar con la autorización de los padres o tutores legales por debajo de esa edad.

En España, el Reglamento de Desarrollo de la LOPD fija la edad a partir de la que el consentimiento de los menores es válido en los 14 años con carácter general. El RGPD permite a los estados miembros establecer una edad inferior, siempre que no sea menor de 13 años. La Ley 3/2018 de Protección de Datos Personales y garantías de los derechos digitales, fija en **14 años la edad** a partir de la cual se puede prestar consentimiento de manera autónoma. También se regula expresamente el derecho a solicitar la supresión de los datos facilitados a redes sociales u otros servicios de la sociedad de la información por el propio menor o por terceros durante su minoría de edad.

El RGPD especifica el tratamiento de datos de menores en la regulación de los intereses legítimos del responsable como base legal para el tratamiento, señalándose que no será aplicable cuando prevalezcan los derechos, libertades o intereses de los interesados que requieran protección de datos personales, especialmente cuando esos interesados sean niños.

Lo mismo ocurre al señalar que la información que se ofrece a los interesados en relación con el tratamiento o con el ejercicio de derechos deberá ser especialmente concisa, transparente, inteligible y proporcionada con lenguaje claro y sencillo cuando los interesados sean niños.

El RGPD requiere que los responsables hagan esfuerzos razonables, teniendo en cuenta la tecnología disponible, para verificar que, para los niños menores de la edad que se fije como límite, el consentimiento sea dado o sea autorizado por los padres o tutores del menor (no es una obligación en sí, sino tan sólo de medios o procedimientos razonables para establecer la intervención real de padres o tutores).

VIDEOVIGILANCIA

La imagen de una persona en la medida que identifique o pueda identificar a la misma constituye un dato de carácter personal, que puede ser objeto de tratamiento para diversas finalidades. Si bien la más común consiste en utilizar las cámaras con la finalidad de garantizar la seguridad de personas, bienes e instalaciones, también pueden usarse con otros fines, como la investigación, la asistencia sanitaria o el control de la prestación laboral por los trabajadores. Al suponer un tratamiento de datos de carácter personal, salvo la excepción doméstica, este tratamiento debe ajustarse a los principios y obligaciones que establece la normativa de protección de datos.

La videovigilancia sólo debe utilizarse cuando no sea posible acudir a otros medios que causen menos impacto en la privacidad.

Además, no se podrá captar imágenes de la vía pública con fines de seguridad, ya que es competencia de las Fuerzas y Cuerpos de Seguridad, salvo el caso que:

- Resulte imprescindible para la finalidad que se pretende.

- Resulte imposible evitarlo por razón de la ubicación de las cámaras.

En todo caso, deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida. Está prohibida la instalación en baños, vestuarios, o lugares análogos.

El tratamiento de las imágenes con fines de seguridad mediante la videovigilancia debe adecuarse al RGPD, de manera que, en primer lugar, hay que configurar el registro de actividades de tratamiento.

Asimismo, se tiene que dar cumplimiento al derecho de información:

- Colocar un cartel donde aparezca que es una zona videovigilada, la identidad del responsable y la posibilidad del ejercicio de los derechos.

- Mantener a disposición de los afectados el resto de información referida en el artículo 13. También se deberán adoptar las medidas de seguridad, teniendo en cuenta lo siguiente:

-El artículo 32 del RGPD determina que se establezcan las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo.

La implementación de las medidas de seguridad cuando se lleve a cabo un tratamiento de datos mediante el uso de la videovigilancia dependerá del análisis de riesgo llevado a cabo previamente.

Si se encarga a un tercero la gestión de las cámaras, estaremos ante la figura del encargado del tratamiento, quién deberá cumplir los requisitos que regula el artículo 28 del RGPD.

ANEXO

El artículo 5.1.f del Reglamento General de Protección de Datos (en adelante, RGPD) determina la necesidad de establecer garantías de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de los datos personales, la destrucción o el daño accidental. Esto implica el establecimiento de medidas técnicas y organizativas encaminadas a asegurar la integridad y confidencialidad de los datos personales y la posibilidad de demostrar, tal y como establece el artículo 5.2, que estas medidas se han llevado a la práctica (responsabilidad proactiva).

Se deberá establecer mecanismos visibles, accesibles y sencillos para el ejercicio de derechos y tener definidos procedimientos internos para garantizar la atención efectiva de las solicitudes recibidas.

ATENCIÓN DEL EJERCICIO DE DERECHOS

El responsable del tratamiento informará a todos los trabajadores acerca del procedimiento para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos (medios electrónicos, referencia al Delegado de Protección de Datos si lo hubiera, dirección postal, etc.) y teniendo en cuenta lo siguiente:

· Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento. El ejercicio de los derechos es gratuito.

· El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida y de forma concisa, transparente, inteligible, con un lenguaje claro y sencillo y conservar la prueba del cumplimiento del deber de responder a las solicitudes de ejercicio de derechos formuladas.

· Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo.

· Las solicitudes deben responderse en el plazo de 1 mes desde su recepción, pudiendo prorrogarse en otros dos meses teniendo en cuenta la complejidad o el número de solicitudes, pero en ese caso debe informarse al interesado de la prórroga en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación.

DERECHO DE ACCESO: En el derecho de acceso se facilitará a los interesados copia de los datos personales de los que se disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación previstos o el criterio utilizado para determinarlo, la existencia del derecho a solicitar la rectificación o supresión de datos personales así como la limitación o la oposición a su tratamiento, el derecho a presentar una reclamación ante la Agencia Española de Protección de Datos y si los datos no han sido obtenidos del interesado, cualquier información disponibles sobre su origen. El derecho a obtener copia de los datos no puede afectar negativamente a los derechos y libertades de otros interesados.

DERECHO DE RECTIFICACIÓN: En el derecho de rectificación se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento. El interesado deberá indicar en la solicitud a qué datos se refiere y la corrección que haya de realizarse, aportando, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento. Si los datos han sido comunicados por el responsable a otros responsables, deberá notificarles la rectificación de estos salvo que sea imposible o exija un esfuerzo desproporcionado, facilitando al interesado información acerca de dichos destinatarios, si así lo solicita.

DERECHO DE SUPRESIÓN: En el derecho de supresión se eliminarán los datos de los interesados cuando estos manifiesten su negativa al tratamiento y no exista una base legal que lo impida, no sean necesarios en relación con los fines para los que fueron recogidos, retiren el consentimiento prestado y no haya otra base legal que legitime el tratamiento o éste sea ilícito. Si la supresión deriva del ejercicio del derecho de oposición del interesado al tratamiento de sus datos con fines de mercadotecnia, pueden conservarse los datos identificativos del interesado con el fin de impedir futuros tratamientos. Si los datos han sido comunicados por el responsable a otros responsables, deberá notificarles la supresión de estos salvo que sea imposible o exija un esfuerzo desproporcionado, facilitando al interesado información acerca de dichos destinatarios, si así lo solicita.

DERECHO DE OPOSICIÓN: En el derecho de oposición, cuando los interesados manifiesten su negativa al tratamiento de sus datos personales ante el responsable, este dejará de procesarlos siempre que no exista una obligación legal que lo impida. Cuando el tratamiento esté basado en una misión de interés público o en el interés legítimo del responsable, ante una solicitud de ejercicio del derecho de oposición, el responsable dejará de tratar los datos salvo que se acrediten motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado o sean necesarios para la formulación, ejercicio o defensa de reclamaciones. Si el interesado se opone al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para estos fines.

DERECHO DE PORTABILIDAD: En el derecho de portabilidad, si el tratamiento se efectúa por medios automatizados y se basa en el consentimiento o se realiza en el marco de un contrato, los interesados pueden solicitar recibir copia de sus datos personales en un formato estructurado, de uso común y lectura

mecánica. Asimismo, tienen derecho a solicitar que sean transmitidos directamente a un nuevo responsable, cuya identidad deberá ser comunicada, cuando sea técnicamente posible.

DERECHO DE LIMITACIÓN AL TRATAMIENTO: En el derecho de limitación del tratamiento, los interesados pueden solicitar la suspensión del tratamiento de sus datos para impugnar su exactitud mientras el responsable realiza las verificaciones necesarias o en el caso de que el tratamiento se realice en base al interés legítimo del responsable o en cumplimiento de una misión de interés público, mientras se verifica si estos motivos prevalecen sobre los intereses, derechos y libertades del interesado. El interesado también puede solicitar la conservación de los datos si considera que el tratamiento es ilícito y, en lugar de la supresión, solicita la limitación del tratamiento, o si aun no necesitándolos ya el responsable para los fines para los que fueron recabados, el interesado los necesita para la formulación, ejercicio o defensa de reclamaciones. La circunstancia de que el tratamiento de los datos del interesado esté limitado deberá constar claramente en los sistemas del responsable. Si los datos han sido comunicados por el responsable a otros responsables, deberá notificarles la limitación del tratamiento de estos salvo que sea imposible o exija un esfuerzo desproporcionado, facilitando al interesado información acerca de dichos destinatarios, si así lo solicita.

Si no se da curso a la solicitud del interesado, el responsable del tratamiento le informará, sin la debida dilación y a más tardar transcurrido un mes desde la recepción de esta, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante la Agencia Española de Protección de Datos y de ejercitar acciones judiciales.

MEDIDAS DE SEGURIDAD

A tenor del tipo de tratamiento que ha puesto de manifiesto cuando ha cumplimentado este formulario, las medidas de seguridad mínimas que debería tener en cuenta son las siguientes:

MEDIDAS ORGANIZATIVAS

INFORMACIÓN QUE DEBERÁ SER CONOCIDA POR TODO EL PERSONAL CON ACCESO A DATOS PERSONALES

Todo el personal con acceso a los datos personales deberá tener conocimiento de sus obligaciones con relación a los tratamientos de datos personales y serán informados acerca de dichas obligaciones. La información mínima que será conocida por todo el personal será la siguiente:

DEBER DE CONFIDENCIALIDAD Y SECRETO

· Se deberá evitar el acceso de personas no autorizadas a los datos personales. A tal fin se evitará dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.). Esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia. Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.

· Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.

· No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción efectiva.

· No se comunicarán datos personales o cualquier otra información de carácter personal a terceros, prestando especial atención a no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.

· El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la empresa.

VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL

· Cuando se produzcan violaciones de seguridad de datos de carácter personal como, por ejemplo, el robo o acceso indebido a los datos personales se notificará a la Agencia Española de Protección de Datos en término de 72 horas acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso

indebido a los datos personales. La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos. Si se dispone de Delegado de Protección de Datos, se le comunicará dicha violación con la mayor celeridad posible para que éste actúe en consecuencia comunicándolo a la autoridad competente y a los afectados/interesados, si fuera necesario.

MEDIDAS TÉCNICAS

IDENTIFICACIÓN

· Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.

· Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.

· Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.

· Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).

· Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. Para la gestión de las contraseñas puede consultar la guía de privacidad y seguridad en internet de la Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

DEBER DE SALVAGUARDA

A continuación, se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

· **ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS:** Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.

· **MALWARE:** En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.

· **CORTAFUEGOS O FIREWALL:** Para evitar accesos remotos indebidos a los datos personales se velará por garantizar la existencia de un firewall activado y correctamente configurado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.

· **CIFRADO DE DATOS:** Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.

· **COPIA DE SEGURIDAD:** Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

CAPTACIÓN DE IMÁGENES CON CÁMARAS Y FINALIDAD DE SEGURIDAD (VIDEOVIGILANCIA)

La imagen de una persona, en la medida que la identifique o la pueda identificar, constituye un dato de carácter personal que puede ser objeto de tratamiento para diversas finalidades. Si bien la más común consiste en utilizar las cámaras para garantizar la seguridad de personas, bienes e instalaciones, también pueden usarse con otros fines como el control de la prestación laboral de los trabajadores. A continuación, se incluyen las directrices básicas a respetar para que el tratamiento de las imágenes obtenidas a partir de cámaras de videovigilancia sea conforme a la normativa de protección de datos.

UBICACIÓN DE LAS CÁMARAS: Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores, así como la captación de la vía pública si se utilizan cámaras exteriores, estando únicamente permitido la captación de la extensión mínima imprescindible para preservar la seguridad de las personas, bienes e instalaciones.

UBICACIÓN DE MONITORES: Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros. A las imágenes grabadas sólo accederá el personal autorizado.

CONSERVACIÓN DE IMÁGENES: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que acrediten la comisión de actos que atenten contra la integridad de personas, bienes e instalaciones. En ese caso las imágenes deben ser puestas a disposición de la autoridad competente en un plazo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación.

DEBER DE INFORMACIÓN: Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo colocado en un lugar suficientemente visible donde se identifique, al menos, la identidad del responsable y la posibilidad de los interesados de ejercer sus derechos en materia de protección de datos. En el propio pictograma se podrá incluir también un código de conexión o dirección de internet en la que se muestre esta información. Dispone de modelos, tanto del pictograma como del texto, en la página web de la Agencia.

CONTROL LABORAL: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador y a sus representantes sindicales por cualquier medio que garantice la recepción de la información acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.

DERECHO DE ACCESO A LAS IMÁGENES: Para dar cumplimiento al derecho de acceso de los interesados a las grabaciones del sistema de videovigilancia se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado para comprobar su identidad, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso. No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se le facilitará un documento en el que se confirme o niegue la existencia de imágenes del interesado.