Ley de protección de datos para entidades y colectivos ciudadanos

Contenidos **clave** para entidades y colectivos ciudadanos

Redconsultora Asociación

Edición para el Plan de formación de entidades y colectivos ciudadanos 2021.

Acciones formativas destinadas a formar y capacitar a personas vinculadas a las entidades y colectivos inscritos en el Censo Municipal de Entidades y Colectivos Ciudadanos, (CMECC).

MADRID

vicealcaldía
área delegada de
coordinación territorial,
transparencia y
participación ciudadana

Redconsultora Asociación

Fuente vectores: freepik.es

ÍNDICE

	Página
1. Tratamiento de datos personales	5
Datos personales y categorías	6
El deber de la información en el tratamiento de datos personales	10
Legitimización y consentimiento	14
2. Derechos ARCO	18
Derechos LOPDGDD (ARCO)	19
Ampliación de los derecho ARCO, derechos RGPD (POL)	23
Forma de ejercer los derechos	27
3. Privacidad y seguridad	31
Estudio del riesgo o nivel de seguridad	32
Deber de confidencialidad y secreto profesional	36
Medidas técnicas de seguridad	40
4. Brechas de seguridad	43
Incidentes de seguridad	44
Notificación a la autoridad de control	48
Comunicar a los afectados	52

Las normas de protección de datos de la UE garantizan la protección de los datos personales en todos los casos en que se recojan: por ejemplo, registrar a una persona usuaria en una actividad de la asociación, crear un libro de las personas socias de la organización, gestionar las personas asistentes a un evento, …

Estas normas se aplican tanto a empresas y organizaciones (públicas y privadas) con sede en la UE, así como a las que tienen su sede fuera de ella, y ofrecen bienes y servicios en la UE. La ley de protección de datos española y el Reglamento General de Protección de Datos (RGDP) europeo son de obligado cumplimiento para todas las asociaciones sin ánimo de lucro que recogen datos de ciudadanos españoles, europeos o residentes en territorio europeo.

Da igual el formato en que se recojan los datos (en línea, en un ordenador central, en papel o en un fichero estructurado); siempre que se almacene o se trate información que identifique directa o indirectamente a un individuo, deben respetarse sus derechos en materia de protección de datos.

1

"El tratamiento de los datos personales es 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."

DATOS PERSONALES Y CATEGORÍAS

Entendemos como datos personales toda información sobre una persona física identificada o identificable (persona interesada). Esta persona física es aquella cuya identidad pueda determinarse, directa o indirectamente; y en particular mediante un identificador (nombre, número de identificación, datos de localización, identificador en línea; uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social).

Son muy variadas las categorías de datos que nos identifican

La persona responsable del tratamiento de los datos es quien decide su finalidad y uso.

DATOS PERSONALES Y CATEGORÍAS

CATEGORIAS DE DATOS

> Los datos personales se refieren a cualquier información sobre una persona, donde está identificada o podría ser identificada. Pueden cubrir varios tipos de información, como el nombre, la fecha de nacimiento, la dirección de correo electrónico, el número de teléfono, la dirección postal, las características físicas o los datos de ubicación; una vez que esté claro con quién se relaciona esa información, o si es razonablemente posible averiguarlo.

Las categorías de datos más importantes son:

01 **DATOS DE CARÁCTER PERSONAL.**
Datos personales generales/ordinarios

02 **CATEGORÍAS DE DATOS ESPECIALMENTE PROTEGIDOS O SENSIBLES.** Datos de salud, origen étnico o racial, opiniones políticas, convicciones religiosas, afiliación sindical, datos genéticos, biométricos.

03 **DATOS DE NATURALEZA PENAL.** Denuncias, procedimientos o condenas penales.

DATOS PERSONALES Y CATEGORÍAS

INVENTARIO Y REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO

Cada responsable del tratamiento de datos, llevará un registro de las actividades de tratamiento efectuadas. Para llegar a un correcto registro de estas actividades, hay que inventariarlas.

***

El inventario tendrá la siguiente información:

- **Nombre de la actividad de tratamiento.**
- **Fecha de entrada en vigor.**
- **Breve descripción de la actividad de tratamiento.**
- **Observaciones.**

Estas actividades nacen de la revisión de los tratamientos de datos que la entidad o colectivo ciudadano tiene que realizar en correspondencia a las obligaciones que el RGPD impone.

También pueden partir de los ficheros que la organización describió con anterioridad ante la Agencia de Protección de Datos.

DATOS PERSONALES Y CATEGORÍAS

RESPONSABILIDAD SOBRE EL TRATAMIENTO

La persona responsable del tratamiento es quien decide la finalidad y uso de los datos, siempre desde la legitimación del tratamiento y el respeto por la normativa. Así mismo, es quien debe establecer las medidas técnicas y organizativas que garanticen la seguridad, privacidad y confidencialidad de los datos y quien tendrá que demostrar el cumplimiento de la ley ante las autoridades de control competentes.

El responsable puede ser tanto una persona física como una persona jurídica o una autoridad pública; y ser quién decide, solo o junto a otros, cómo y para qué se lleva a cabo el tratamiento de datos personales.

La diferencia entre responsable del tratamiento y encargado del tratamiento, está en que mientras que el primero es quién decide el uso y la finalidad de los datos personales, el segundo debe seguir sus instrucciones respecto a dicho uso y finalidad.

EL DEBER DE INFORMACIÓN EN EL TRATAMIENTO DE DATOS PERSONALES

Las entidades y colectivos ciudadanos que recogen datos personales, tienen la obligación de facilitar información a los titulares de dichos datos. Esta medida recibe el nombre de Deber de informar o Derecho a la información.

***

Las distintas entidades y colectivos ciudadanos, con motivo de su actividad diaria, pueden obtener datos personales por parte del propio interesado (formularios en papel, formularios web, navegación web (*cookies*); etc.); o por terceros (cesiones legítimas entre empresas, datos obtenidos desde fuentes de acceso público, etc.).

El RGPD establece la información que el responsable de tratamiento deberá proporcionarse a los interesados en todos los casos.

Cuando la persona interesada ya disponga de esta información, no es obligatorio cumplir con el deber de información nuevamente

EL DEBER DE INFORMACIÓN

OBLIGACIONES DE INFORMACIÓN

En el caso de que los datos sean **obtenidos del propio interesado**, hay que tener en cuenta lo siguiente: identidad y contacto del responsable, y en su caso, del representante; los fines del tratamiento de los datos y la base jurídica que los legitima, los intereses legítimos del responsable o del tercero, los destinatarios o categorías de destinatarios de los datos personales, la previsión de transferencias a terceros países, el plazo o criterios de conservación de tales datos, mencionar los derechos que asisten al interesado/a en el tratamiento, el derecho a retirar el consentimiento prestado, el derecho a presentar una reclamación ante la autoridad de control, la necesidad de comunicar los datos …

E informar de las consecuencias de no facilitar tales datos; y la existencia, en su caso, de decisiones automatizadas en el tratamiento de datos, incluida la elaboración de perfiles.

Cuando el Responsable haya **obtenido los datos de terceros**, hay que informar al interesado de los mismos extremos explicados anteriormente, añadiendo la fuente de procedencia de los datos y las categorías de datos que se van a tratar.

EL DEBER DE INFORMACIÓN

DISPOSICIÓN DE LA INFORMACIÓN

En el caso que la entidad o colectivo ciudadano sea **titular de los datos personales,** la información se pondrá a disposición de los interesados en el momento en que se soliciten los datos, previamente a la recogida o registro. Si el responsable decide posteriormente realizar un tratamiento de los datos de los que dispone, con un fin distinto para el que se recogieron, deberá proporcionar información al interesado sobre ese otro fin y el resto de información adicional según los puntos anteriormente detallados.

En el caso de que **los datos no se obtengan del propio interesado**, por proceder de alguna cesión legítima o de fuentes de acceso público, el deber de información deberá aportarse por parte del responsable del tratamiento dentro de un plazo razonable; y, en cualquier caso, antes de un mes desde la obtención de los datos personales, antes o en la primera comunicación que se realice con el interesado, o antes de comunicar los datos por primera vez a otros destinatarios.

EL DEBER DE INFORMACIÓN

MODELO DE INFORMACIÓN

La información por capas consiste en dividir la información facilitada a los usuarios en una primera capa más genérica y una segunda capa más detallada.

***

Los EPÍGRAFES sobre los que se informa son: responsable, finalidad, legitimización, destinatarios y derechos.

Los dos niveles de información son:

01

INFORMACIÓN BÁSICA O INFORMACIÓN DE PRIMERA CAPA. Se presenta una información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recogen los datos.

02

INFORMACIÓN ADICIONAL O INFORMACIÓN DE LA SEGUNDA CAPA. Se presentan detalladamente el resto de las informaciones, en un medio más adecuado para su presentación, comprensión y si el titular de los datos lo desea.

LEGITIMIZACIÓN Y CONSENTIMIENTO

El Reglamento General de Protección de Datos (RGPD) define consentimiento como "la manifestación de voluntad libre, específica, informada e inequívoca por la cual el interesado acepta, mediante una clara acción afirmativa, el tratamiento de sus datos personales".

La entidad o colectivo ciudadano responsable del tratamiento de datos personales, deberá ser capaz de demostrar que la persona dio tal consentimiento (consentimiento verificable).

El silencio, las casillas ya marcadas o la inacción, no constituirán prueba de consentimiento

LEGITIMIZACIÓN Y CONSENTIMIENTO

OTORGAMIENTO DEL CONSENTIMIENTO

El consentimiento se da en el contexto de una declaración escrita. La solicitud de consentimiento se presentará de tal modo que se diferencie cada consentimiento, de forma inteligible y de fácil acceso, y utilizando un lenguaje claro y sencillo (consentimiento inequívoco y explícito). Las prácticas de consentimiento tácito no serán aceptadas.

La edad en la que los niños y las niñas podrán prestar su consentimiento para el tratamiento de sus datos personales en el ámbito de los servicios de la sociedad de la información; será, como mínimo, de 14 años. Por debajo de esta edad, será preciso el previo consentimiento de padres, madres o personas tutoras

La persona interesada tendrá derecho a retirar su consentimiento en cualquier momento (debiendo ser informada la persona interesada antes de dar su consentimiento). Será tan fácil dar el consentimiento, como retirarlo

LEGITIMIZACIÓN Y CONSENTIMIENTO

LEGITIMIZACIÓN DEL TRATAMIENTO DE DATOS

La legitimación del tratamiento y las cesiones se consigue mediante la obtención del consentimiento previo e inequívoco del titular de los datos salvo en los casos siguientes:

Cuando se refieran a las partes de un contrato o precontrato de una negociación laboral o mercantil y sean necesarios para su mantenimiento o cumplimiento

Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del titular de los datos cuando esté física o jurídicamente incapacitado para dar su consentimiento.

Cuando los datos figuren en fuentes accesibles al público y el cesionario tenga interés legítimo para su tratamiento o conocimiento.

Cuando se trate de datos que revelen la ideología, afiliación sindical, religión y creencias, origen racial, salud y a la vida sexual

Cuando el tratamiento sea necesario para la prevención o para el diagnóstico médicos o la gestión de servicios sanitarios y se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente al secreto.

La organización requerirá el consentimiento en todos los formularios que esta diseñe para el desarrollo de su actuación.

El consentimiento se otorgará, tras la información, a través de una casilla que será marcada al efecto y que debe incluirse al final de cualquier formulario.

LEGITIMIZACIÓN Y CONSENTIMIENTO

BASES DE LEGITIMIZACIÓN PARA EL TRATAMIENTO DE LAS CATEGORÍAS DE DATOS

La regla general contemplada en el reglamento es la prohibición del tratamiento de categorías especiales de datos. No obstante, se recogen excepciones a esta regla general, como por ejemplo:

El tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a las personas actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados

El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento

O cuando la persona interesada dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada no puede ser levantada por el interesado

En cualquier caso, quienes traten categorías especiales de datos, sobre todo si es a gran escala, están obligados a realizar una evaluación de impacto.

2

"Con la entrada en vigor, y posterior aplicación, del Reglamento General de Protección de Datos, los derechos que los/as ciudadanos/as tenían reconocidos con la antigua Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), derechos ARCO, son ampliados y actualizados (derechos ARCO-POL).

Los derechos ARCO, son derechos cuyo ejercicio es personal. Solo pueden ser ejercidos por su titular."

Derechos LOPDGDD (ARCO)

Se denomina derechos ARCO a aquellos a través de los cuales una persona física puede ejercer el control sobre sus datos personales. La persona física podrá solicitar el acceso, rectificación, cancelación u oposición, sobre el tratamiento de sus datos, ante el sujeto obligado que esté en posesión de los mismos.

A=Acceso
R=Rectificación
C=Cancelación
O=Oposición

El derecho de cancelación ha sido sustituido por el de supresión en el contexto de los denominados derechos P.O.L.

DERECHOS LOPDGDD (ARCO)

DERECHO AL ACCESO

Es el derecho de las personas afectadas a obtener información sobre si los propios datos de carácter personal están siendo objeto de tratamiento; la finalidad del tratamiento que, en su caso, se esté realizando; así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

El derecho de acceso es gratuito

El ejercicio de este derecho de forma repetida en un plazo inferior a seis meses, o a través de medios que supongan un coste excesivo para el responsable del tratamiento, se puede considerar desproporcionado. En estos casos, se podría solicitar al interesado que corriese con los gastos derivados del ejercicio del derecho de acceso.

DERECHOS LOPDGDD (ARCO)

DERECHO DE RECTIFICACIÓN

Consiste en la potestad de las personas afectadas, a que se modifiquen los datos que resulten ser inexactos o incompletos, sin dilación indebida del responsable del tratamiento.

Teniendo en cuenta los fines del tratamiento, se tiene derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

En la Constitución Española, queda amparado por el artículo 20, donde se recogen los derechos a la libertad de expresión y a la información. Se regula y desarrolla en la Ley Orgánica 2/1984, que en su artículo 1 dice que «Toda persona natural o jurídica tiene derecho a rectificar la información difundida por cualquier medio de comunicación social de hechos que le aludan, que considere inexactos y cuya divulgación pueda causarle perjuicio».

DERECHOS LOPDGDD (ARCO)

DERECHO DE OPOSICIÓN

Consiste en el derecho de las personas afectadas a que no se lleve a cabo el tratamiento de sus datos de carácter personal, o se cese en el mismo, en los supuestos en que:

01 No sea necesario su consentimiento para el tratamiento.

02 Se trate de ficheros de prospección comercial.

03 Tengan la finalidad de adoptar decisiones referidas a las personas interesadas y basadas únicamente en el tratamiento automatizado de sus datos.

AMPLIACIÓN DE LOS DERECHOS ARCO, DERECHOS RGPD (POL)

Los derechos ARCO han sido ampliados con los derechos de Portabilidad, Oposición y Limitación del tratamiento (POL). El derecho de cancelación ha sido sustituido por el de supresión, por lo que a estos derechos ahora se les denomina ARCO-POL, o también derechos ARSULIPO (Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad y Oposición).

Sin embargo, por el uso y la costumbre, se sigue haciendo referencia a ellos como derechos ARCO.

No existe una Ley ARCO como tal, ya que estos derechos están recogidos tanto en el RGPD como en la LOPDGDD.

AMPLIACIÓN DE LOS DEREHCOS ARCO, DERECHOS RGPD (POL)

PORTABILIDAD

Las personas interesadas tendrán derecho a que el/la responsable transmita los datos a otro responsable del tratamiento o a las personas interesadas, mediante un formato estructurado de uso habitual y lectura mecánica, cuando el tratamiento se efectúe por medios automatizados y se base en:

- **El consentimiento de la persona interesada para fines específicos.**
- **La ejecución de un contrato o precontrato con la persona interesada.**

El derecho de portabilidad no se aplicará cuando:

- **Sea técnicamente imposible la transmisión.**
- **Pueda afectar negativamente a los derechos y libertades de terceros.**
- **El tratamiento tenga una misión de interés público fundamentado en la legislación vigente.**

AMPLIACIÓN DE LOS DEREHCOS ARCO, DERECHOS RGPD (POL)

OLVIDO O SUPRESIÓN

Es el derecho de las personas afectadas a que se supriman los datos que resulten ser inadecuados o excesivos.

Se podrá ejercitar este derecho ante el/la persona responsable, solicitando la supresión de los datos de carácter personal cuando concurra alguna de las siguientes circunstancias:

- **Los datos ya no son necesario para cumplir la finalidad para la cual fueron recabados.**
- La persona interesada retire su consentimiento.
- **La persona interesada se oponga al tratamiento y no existan motivos legítimos para llevarlo a cabo.**
- El tratamiento de la persona responsable se fundamentaba en el interés legítimo o en el cumplimiento de una misión de interés público, y no han prevalecido otros motivos para legitimar el tratamiento de los datos.
- **A que los datos personales sean objeto de mercadotecnia directa, incluyendo la elaboración de perfiles.**
- Los datos se hayan tratado de forma ilícita.
- **Por el cumplimiento de una obligación legal incluida en las normativas de los Estados miembros de la UE.**

Este derecho de supresión obliga a la persona responsable del tratamiento que haya hecho públicos los datos personales, a indicar a los responsables que estén tratando estos datos personales a suprimir todo enlace a ellos, o sus copias o réplicas.

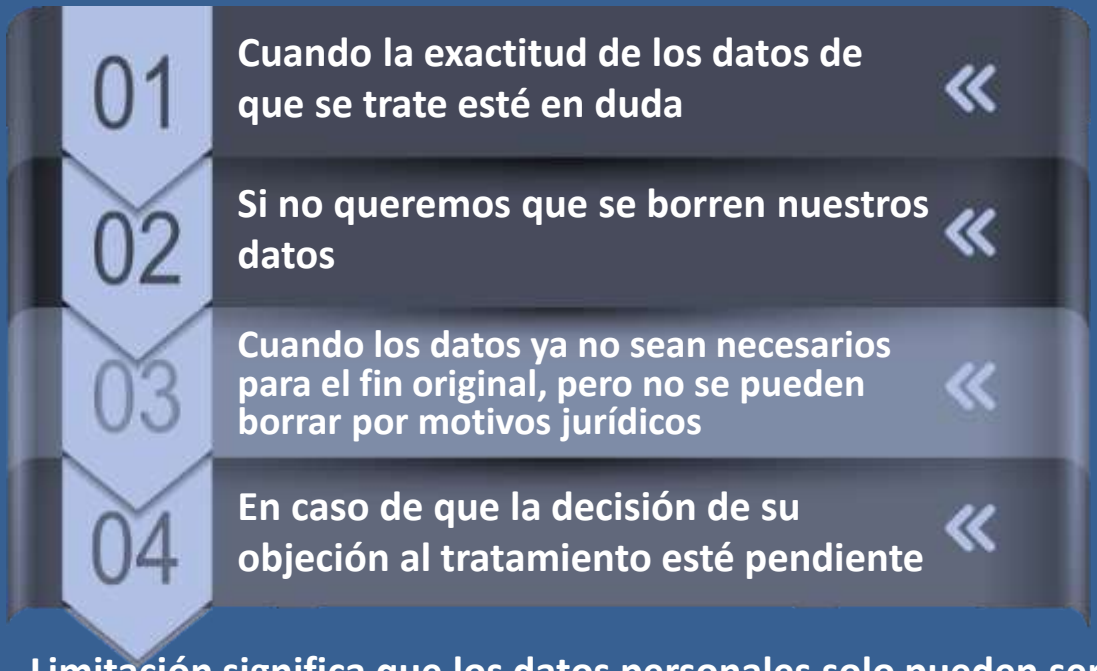
Este derecho establece que toda persona podrá solicitar la eliminación de sus datos personales de páginas web o motores de búsqueda, en caso de que la información esté desfasada, sea inexacta o pueda ocasionar un perjuicio a la persona.

AMPLIACIÓN DE LOS DEREHCOS ARCO, DERECHOS RGPD (POL)

LIMITACIÓN DE TRATAMIENTO

Se trata de un nuevo derecho, introducido por el RGPD, que supone que las personas afectadas puedan solicitar su derecho a la limitación del tratamiento de los datos personales.

Este derecho existe en los casos siguientes:



Limitación significa que los datos personales solo pueden ser tratados con el consentimiento para la formulación, el ejercicio o la defensa de reclamaciones, con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público.

FORMA DE EJERCER LOS DERECHOS

El/la responsable del fichero tiene obligación de facilitar el ejercicio de estos derechos a las personas afectas, y a responder a su solicitud en los plazos previstos legalmente. Se habrá de hacer con independencia del procedimiento utilizado por las personas interesadas, y aunque el/la responsable del fichero no posea sus datos personales.

El ejercicio de estos derechos debe realizarse mediante procedimientos sencillos y gratuitos, que quien es responsable del fichero debe poner a disposición de la ciudadanía.

Se limitará el ejercicio de estos derechos cuando sea una medida necesaria para la salvaguarda de la seguridad del Estado, la defensa y seguridad pública, y la prevención, averiguación, detección y castigo de infracciones penales.

FORMA DE EJERCER LOS DERECHOS

SOLICITUD DEL EJERCICIO DE UN DERECHO

El ejercicio de estos derechos ARCO sobre datos personales se ha de realizar mediante solicitud dirigida al responsable del fichero, que debe contener:

- **Nombre y apellidos de la persona interesada.**
- **Fotocopia del DNI, de su pasaporte u otro documento válido que permita identificarle; y, en su caso, de la persona que le represente.**
- **Petición en que se concreta la solicitud.**
- **Domicilio a efectos de comunicaciones.**
- **Documentos acreditativos de la petición que formula, en su caso. En el caso de que se desee acceder a bancos de datos de grabación de imágenes, es necesaria una fotografía reciente.**
- **Fecha y firma del solicitante.**

En función al tipo de derecho, la solicitud se motivará de la siguiente manera:

01

DERECHO DE ACCESO

No es necesaria la motivación, salvo si se ha ejercitado el derecho en los últimos doce meses.

02

DERECHO DE RECTIFICACIÓN

Debe indicarse a qué datos se refiere y la corrección que haya de realizarse, aportando documentación que justifique la inexactitud o el carácter incompleto de los datos.

03

DERECHO DE OPOSICIÓN

Concurrencia de motivos fundados y legítimos relativos a su concreta situación personal.

FORMA DE EJERCER LOS DERECHOS

SUBSANACIÓN DE LA SOLICITUD DEL EJERCICIO DE DERECHOS

En caso de que la solicitud no cumpla con los requisitos exigidos, la entidad o el colectivo ciudadano, en un plazo de cinco días hábiles, contado desde el día siguiente de la recepción de la solicitud, formulará las observaciones por incumplimiento que no puedan ser salvadas, invitando a la persona titular de los datos personales a subsanarlas dentro de un plazo máximo de cinco días hábiles. Transcurrido el plazo señalado sin que ocurra la subsanación, se tendrá por no presentada la solicitud.

En el caso de que la información proporcionada en la solicitud sea insuficiente o errónea, de forma que no permita su atención, la entidad o colectivo ciudadano podrá requerir dentro de los siete días siguientes de recibida la solicitud, documentación adicional al titular de los datos personales para atenderla. En un plazo de diez días de recibido el requerimiento, contado desde el día siguiente de la recepción del mismo, el titular de datos personales acompañará la documentación adicional que estime pertinente para fundamentar su solicitud. En caso contrario, se tendrá por no presentada dicha solicitud.

FORMA DE EJERCER LOS DERECHOS

RESPUESTA A LA SOLICITUD

Derecho de acceso

El/la responsable del fichero resolverá sobre la solicitud de acceso, en el plazo máximo de un mes a contar desde la recepción de la solicitud. El acceso podrá hacerse efectivo durante 10 días hábiles tras la comunicación de la resolución.

Si la solicitud fuera estimada y la entidad o colectivo ciudadano no acompañase a su respuesta la información solicitada, el acceso será efectivo dentro de los diez días siguientes a dicha respuesta.

Derecho de rectificación

10 días hábiles

Derecho de oposición

10 días hábiles

Derecho de información

8 días hábiles

Derecho de portabilidad

Un mes, exceptuando aquellos casos más complejos para los que se concede un plazo de tres meses, pero siempre informando dentro del primer mes de las razones para dicho retraso.

Olvido o suspensión

Un mes, salvo que sea una solicitud compleja o incluya a varios usuarios. En este caso, se indicará el motivo del retraso en esa respuesta.

Limitación del tratamiento

10 días hábiles.

Los plazos que correspondan para la respuesta o la atención de los referidos derechos, podrán ser ampliados una sola vez; y como máximo, por un plazo igual, siempre que las circunstancias lo justifiquen. La justificación de la ampliación del plazo será comunicada al titular del dato personal, dentro del plazo que se pretenda ampliar.

La entidad o colectivo ciudadano denegará la solicitud para el ejercicio de los derechos ARCO presentada por el titular de los datos personales, en los siguientes supuestos:

- **Si** la persona solicitante no es el titular de los datos personales, o el representante legal no se encuentra debidamente acreditado para ello.
- Si en los bancos de datos de la entidad o colectivo ciudadano, no se encuentran los datos personales del solicitante.
- Si existe un impedimento legal, o una resolución judicial o administrativa que restrinja el ejercicio de los derechos ARCO a la persona titular de los mismos.
- Cuando la persona titular de los datos personales ya ejerció alguno de sus derechos ARCO y pretende ejercerlo nuevamente, sin haber transcurrido el plazo que tiene la entidad o colectivo ciudadano para resolver su solicitud.

3

La seguridad de datos se refiere a las formas en que las entidades y colectivos ciudadanos protegen sus datos. Se incluyen las técnicas que ayudan a garantizar la confidencialidad, integridad y disponibilidad de los datos. La privacidad de los datos gira en torno al uso y administración de los datos personales. Esto puede incluir desde información personal identificable, hasta información financiera, información sobre la vida, educación, salud, familia o antecedentes penales de una persona.

ESTUDIO DEL RIESGO O NIVEL DE SEGURIDAD

El Reglamento General de Protección de Datos (RGPD) establece dos niveles de seguridad: el análisis de riesgo y la evaluación de impacto de protección de datos (EIPD). Uno de los principales objetivos de la nueva normativa es que la gestión de riesgos sea una prioridad para las organizaciones. Es necesario que las entidades y colectivos ciudadanos realicen un seguimiento continuado y regular de los potenciales riesgos asociados a la información que manejan, a través de las herramientas y procesos destinados a tal efecto.

El parámetro determinante para notificar una brecha de seguridad de datos personales a la Autoridad de Control o comunicarla a los afectados, es el nivel de riesgo.

No se trata de cualquier tipo de riesgo o de un riesgo para la organización, sino específicamente el riesgo para los derechos y libertades de las personas físicas afectadas por la brecha de seguridad.

ESTUDIO DEL RIESGO O NIVEL DE SEGURIDAD

ANÁLISIS DEL RIESGO

El análisis de riesgo está vinculado a la protección de la información. El análisis de riesgo se centra en tres aspectos relacionados con el buen uso de los datos personales: la alteración o modificación de los datos, la confidencialidad (el acceso sin autorización a los datos) y la disponibilidad (borrado o pérdida de los datos).

El principal objetivo del encargado de realizar un análisis de riesgos, debe ser velar por la seguridad y el control de las libertades y derechos de la ciudadanía, estableciendo las medidas pertinentes. Este análisis vendría a cubrir la capa más superficial de la protección de datos; y comenzaría, según apunta la Agencia Española de Protección de Datos (AEPD), con una correcta descripción de las actividades que una entidad realiza y que impliquen un tratamiento directo de la información de terceros.

ESTUDIO DEL RIESGO O NIVEL DE SEGURIDAD

EVALUACIONES DE IMPACTO DE PROTECCIÓN DE DATOS

Mientras que el análisis de riesgo está vinculado a la protección de la información; la evaluación del impacto, tiene que ver con los potenciales afectados.

La evaluación de impacto (EIPD), se realiza si el tratamiento de datos "entraña un alto riesgo para los derechos y libertades de las personas físicas". La nueva normativa establece ciertas categorías especiales, entre las que cabe destacar: los datos relacionados con la salud, las tendencias políticas y religiosas o la información biométrica.

Los/as responsables del tratamiento deberán realizar una evaluación de Impacto sobre la protección de datos, con carácter previo a su puesta en marcha. En particular si se utilizan nuevas tecnologías.

Esta obligación debe entenderse en el contexto de la responsabilidad proactiva y la obligación general de gestionar adecuadamente los riesgos, y demostrar que se han tomado las medidas adecuadas para garantizar el cumplimiento de los requisitos exigidos por el RGPD.

ESTUDIO DEL RIESGO O NIVEL DE SEGURIDAD

ADOPCIÓN DE MEDIDAS DE SEGURIDAD

La anterior Ley Orgánica de Protección de Datos determinaba con detalle y de forma exhaustiva las medidas de seguridad que debían aplicarse según el tipo de datos objeto de tratamiento.

Sin embargo, con la nueva normativa, quienes son 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 y tomando en cuenta más variables además del tipo de datos.

Las medidas de seguridad deberán ser implantadas en función al nivel adecuado del riesgo de los distintos tratamientos.

A partir de mayo de 2018, los responsables y encargados de tratamiento, deberán realizar su propio análisis de riesgo y evaluar qué medidas de seguridad técnica y organizativa consideran que deben de ser aplicables para garantizar la seguridad y confidencialidad en el tratamiento de los datos personales. Las conclusiones alcanzadas sobre qué medidas deben de ser aplicables, podrán o no coincidir total o parcialmente con las medidas de seguridad que establecía la LOPD. Se pasa de un modelo rígido de obligaciones a un modelo variable o dinámico, cuya aplicación o implantación dependerá del caso concreto y del análisis de riesgo que cada responsable o encargado realice, en función de los tratamientos de datos que deba realizar.

DEBER DE CONFIDENCIALIAD Y SECRETO PROFESIONAL

La LOPDGDD establece que la confidencialidad y el secreto profesional son dos derechos complementarios. Se puede entender el secreto profesional como la aplicación del principio de confidencialidad en el ámbito laboral.

El deber de confidencialidad es uno de los principios básicos de la normativa de protección de datos.

Es fundamental para garantizar la privacidad, seguridad e integridad de la información.

DEBER DE CONFIDENCIALIDAD Y SECRETO PROFESIONAL

CLAUSULA DE CONFIDENCIALIDAD

Para garantizar la privacidad de la información confidencial numérica, fotográfica, alfabética o acústica -contenida en diferentes formatos, ya sea en papel, soportes telemáticos, documentos electrónicos-, relativa a la organización, a las personas socias, usuarias, voluntarias o al personal trabajador; es frecuente que las entidades y colectivos ciudadanos, incluyan una cláusula de confidencialidad en los contratos de sus miembros y colaboradores, incluidos los trabajadores si procede. Dicha cláusula establece que las personas integrantes en la entidad o colectivo deben guardar secreto profesional respecto a los datos a los cuales tengan acceso, como consecuencia del ejercicio de sus funciones.

En las cláusulas de confidencialidad también se establece la obligación de cumplir con este principio, tras la extinción de la relación con la entidad o colectivo ciudadano, ya que la persona podría hacer un posterior uso malintencionado de los datos a los que tuvo acceso durante su relación con la entidad.

DEBER DE CONFIDENCIALIDAD Y SECRETO PROFESIONAL

EXCEPCIONES DE LA CONFIDENCIALIDAD

Existen casos en los que se puede anular la obligación de confidencialidad de la información:

En este sentido, el acceso a la información personal ha de ser pertinente y proporcionada.

DEBER DE CONFIDENCIALIDAD Y SECRETO PROFESIONAL

MEDIDAS ESPECÍFICAS DE SEGURIDAD

Debe impedirse el acceso a datos personales de personas no autorizadas. Para ello, no se dejan los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.). Esto incluye las pantallas que se utilicen para la visualización de imágenes del sistema de video vigilancia. Cuando alguien se ausenta de un equipo 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.

No se comunicarán datos personales o cualquier información personal a terceros. Ni se divulgan datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.

MEDIDAS TÉCNICAS DE SEGURIDAD

Las medidas organizativas (la gestión de la confidencialidad y secreto, la gestión de los derechos de las personas titulares de los datos y la gestión de las violaciones de seguridad de datos de carácter personal), son aquellas que afectan a la estructura y a la toma de decisiones para garantizar la reducción del riesgo de incumplimiento del RGPD, demostrando la efectividad de la gestión de la protección de datos.

Las medidas técnicas de protección de los datos personales pueden ser preventivas o reactivas, y siempre tienen como fin último asegurar la confidencialidad, la disponibilidad y la integridad de la información, además de obstaculizar una fuga de datos o brecha de seguridad.

Allí donde haya una medida técnica implantada, tiene que haber una política o procedimiento interno, aprobado por la dirección de la entidad o colectivo ciudadano.

El procedimiento, asignará los recursos económicos y humanos para su gestión, y establecerá precisamente cómo se va a configurar esta responsabilidad.

MEDIDAS TÉCNICAS DE SEGURIDAD

GESTIÓN DE USUARIOS/AS, ROLES Y PRIVILEGIOS

Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal, hay que disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Es importante separar los usos personales y profesionales en el ordenador.

Hay que tener perfiles con derechos de administración para la instalación y configuración del sistema, y perfiles de usuarios sin derechos de administración o privilegios 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. Las contraseñas deben contener números y letras, teniendo al menos 8 caracteres.

En caso de **acceso a los datos personales por varias personas**, cada una de ellas debe tener un usuario y contraseña específicos (identificación inequívoca).

Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso se compartirán las contraseñas, ni se dejarán anotadas en un lugar común, ni se permitirá el acceso de personas distintas al usuario/a.

MEDIDAS TÉCNICAS DE SEGURIDAD

SALVAGUARDA

En caso de acceso a los datos personales por varias personas, cada una de ellas tiene el deber de salvaguarda.
Las medidas técnicas mínimas para asegurar la salvaguarda de los datos personales, son:

01 MALWARE
Se dispondrá de un sistema de antivirus en los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales, que garantice la protección de la información. Este sistema deberá actualizarse periódicamente.

02 ACTUALIZACIÓN DE DISPOSTIVOS Y ORDENADORES
Los ordenadores y dispositivos usados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados.

03 CORTAFUEGOS O FIREWALL
Deberá existir un *firewall* activado en aquellos ordenadores y dispositivos en que se realice el almacenamiento y/o tratamiento de datos personales, para evitar accesos remotos indebidos.

04 CIFRADO DE DATOS
En caso de que sea necesario trasladar los 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 usar un proceso de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.

05 COPIA DE SEGURIDAD
Se efectuará de forma periódica 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, en caso de pérdida de la información, la recuperación de los datos personales.

Estas medidas de seguridad serán revisadas de forma periódica, y podrá realizarse por mecanismos automáticos (*software* o programas informáticos) o de forma manual.

4

Una brecha de seguridad es un incidente que permite el acceso no autorizado a datos informáticos, aplicaciones, redes o dispositivos. Es decir, permite acceder sin autorización a información. Normalmente, se produce cuando un intruso logra sortear los mecanismos de seguridad.

INCIDENTES DE SEGURIDAD

Una brecha de datos personales puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales, por lo que hay que intentar evitarlas; y en caso de que sucedan, gestionarlas adecuadamente, especialmente cuando puedan poner en riesgo los derechos fundamentales y libertades públicas de las personas.

Hay que estar preparados para mitigar y documentar una posible brecha de seguridad de datos personales.

Los datos de la brecha son objeto de tratamiento.

INCIDENTES DE SEGURIDAD

NO SON INCIDENTES

Todos los incidentes de seguridad, son necesariamente brechas de datos personales, y no solo los ciberincidentes pueden crear brechas de datos personales. A su vez, no toda acción que suponga una vulneración de la normativa de protección de datos, puede ser considerada una brecha de seguridad de datos personales.

No tendrán consideración de brecha de seguridad de datos personales, aquellos incidentes que:

- No afecten a datos personales; es decir, a datos que no sean de personas físicas identificadas o identificables.
- No afecten a tratamientos de datos personales llevados a cabo por un responsable o un encargado.
- Ocurran en tratamientos llevados a cabo por una persona física en el ámbito doméstico.

INCIDENTES DE SEGURIDAD

MITIGACIÓN DE LAS CONSECUENCIAS SOBRE LOS DATOS PERSONALES

Las entidades y colectivos ciudadanos que sufran una brecha de datos personales deben focalizar sus esfuerzos en evitar y mitigar las posibles consecuencias sobre los derechos fundamentales y libertades públicas de las personas afectadas.

La persona responsable de tratamiento debe estar preparada para esta posibilidad, debe establecer quién y qué acciones se ejecutarán en caso de producirse. Para ello, lo primero es ser consciente de qué datos personales se están tratando, con qué medios y los riesgos que puede haber. Así, una cuestión muy importante, es implementar mecanismos que permitan detectar las brechas de seguridad de datos de carácter personal.

Si sucede, la persona responsable de tratamiento debe poner en marcha el plan de actuación, concretando tareas específicas que permitan resolver la brecha, minimizar sus consecuencias y evitar que vuelva a suceder en el futuro.

INCIDENTES DE SEGURIDAD

DOCUMENTACIÓN DEL PROCESO

Durante su resolución, se debe documentar el proceso con toda la información que se vaya recopilando. Esta documentación será adjuntada al registro de incidentes, que deben mantener los responsables de los tratamientos. La información relativa a las decisiones tomadas sobre la notificación a la autoridad competente y la comunicación a los afectados (incluida una copia de la comunicación), debe recogerse también en este registro de forma detallada.

Cuando se sufre una brecha de seguridad, se recaba información para decidir qué medidas tomar y qué acciones se emprenderán para cumplir los objetivos anteriores y para valorar la necesidad de notificar a la autoridad de control y afectados:

Medio por el que se ha materializado la brecha; es decir, qué ha ocurrido: se ha perdido un dispositivo con datos personales, se ha producido un robo, se han publicado datos personales por error o se ha enviado a un destinatario/a equivocado, se ha producido una intrusión no autorizada en un sistema de información con datos personales, un colaborador/a ha sido víctima de *phishing*, etc.

Origen de la brecha: si ha sido interna o externa, y su intencionalidad

Categorías de datos: si son datos básicos, como credenciales o datos de contacto; o si bien son categorías especiales, como datos de salud.

Volumen de datos afectados: tanto en número de registros afectados, como en número de personas afectadas.

Categorías de afectados: clientes, empleados, estudiantes, abonados, pacientes, etc. Es importante identificar si se trata de colectivos vulnerables.

Información temporal de la brecha: cuándo se inició, cuándo se ha detectado y cuándo se resolvió o resolverá la brecha de seguridad.

> **La entidad o colectivo ciudadano deberá reflexionar sobre lo que ha sucedido, cuáles son las consecuencias para las personas cuyos datos se han visto afectados, qué medidas de seguridad técnicas u organizativas podrían haber evitado la brecha y la conveniencia de incorporarlas, y qué acciones tomar para evitar que las personas sufran los daños potenciales y evitar que el incidente se repita.**

> **No existe un modelo estándar de registro de incidentes. Cada organización debe utilizar el que considere más conveniente y que se integre en sus sistemas de gestión.**

NOTIFICACIÓN A LA AUTORIDAD DE CONTROL

El Reglamento (UE) 2016/679 General de Protección de Datos, establece la obligación para las organizaciones (públicas y privadas) que actúen como responsables de tratamiento, de notificar a la Autoridad de Control competente las brechas de datos personales, cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas.

Cuando la brecha de datos personales entrañe un alto riesgo para los derechos y libertades de las personas afectadas, además de la notificación a la Autoridad de Control, se deberá comunicar a los afectados sin dilación indebida.

La notificación de una brecha de datos personales a la Autoridad de Control, conforme al artículo 33 del RGPD; además de una obligación, es un ejercicio de responsabilidad proactiva.

NOTIFICACIÓN A LA AUTORIDAD DE CONTROL

CUÁNDO NOTIFICAR

Tan pronto como la persona responsable del tratamiento tenga conocimiento de que se ha producido una brecha de datos personales, debe efectuar la correspondiente notificación a la Autoridad de Control competente, cuando sea probable que la brecha constituya un riesgo para los derechos y libertades de las personas.

No es obligatorio notificar todas las brechas de datos personales, cuando conforme al principio de responsabilidad proactiva, el responsable pueda garantizar que es improbable que la brecha de datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

NOTIFICACIÓN A LA AUTORIDAD DE CONTROL

PLAZOS PARA NOTIFICAR

En su caso, debe notificarse sin dilación, y a más tardar en las 72 horas siguientes, computando también las horas trascurridas durante fines de semana y festivos.

El plazo empieza a calcularse desde el instante en que la persona responsable de tratamiento tenga constancia de que el incidente de seguridad ha afectado a datos personales, incluyendo las horas trascurridas durante fines de semana y días festivos.

NOTIFICACIÓN A LA AUTORIDAD DE CONTROL

QUIÉN DEBE NOTIFICAR

La notificación de una brecha de datos personales a la Autoridad de Control, conforme al artículo 33 del RGPD, corresponde al responsable del tratamiento. El responsable puede autorizar a una persona física, representante o entidad que ejerza su representación, para que realice la notificación de la brecha de datos personales ante la Autoridad de Control.

No obstante, el responsable de tratamiento debe ser previamente informado sobre la ocurrencia de la brecha de datos personales, y de todos los detalles relevantes.

COMUNICAR A LOS AFECTADOS

Las personas interesadas afectadas son las personas físicas cuyos datos personales se han visto aquejados por una brecha de seguridad, comprometiendo la confidencialidad, integridad y/o disponibilidad de esos datos, y son quienes pueden sufrir las consecuencias.

El proceso de gestión de brechas de datos personales establecido en la organización, deberá incluir un procedimiento para llevar a cabo su comunicación a las personas interesadas afectadas, concretando la información y estableciendo los plazos concretos adecuados.

La finalidad última de la notificación y comunicación de brechas de datos personales, es la protección efectiva de los derechos fundamentales y libertades de las personas físicas afectadas por la brecha.

COMUNICAR A LOS AFECTADOS

CUÁNDO NOTIFICAR

Cuando sea probable que la brecha de datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable de tratamiento lo comunicará a las personas afectadas, tan pronto como tenga constancia de que se ha producido.

Se deberá valorar el riesgo para las personas afectadas, y determinar la necesidad de comunicar la brecha a los afectados. En caso de que el riesgo se determine como alto, la comunicación a las personas afectadas deberá realizarse a la mayor brevedad posible.

COMUNICAR A LOS AFECTADOS

PLAZOS PARA COMUNICAR

El RGPD no establece un plazo concreto para la comunicación a las personas afectadas, pero sí indica que deberá realizarse sin dilación indebida. Cualquier dilación en la comunicación, le resta efectividad, por lo que una comunicación a destiempo puede llegar a tener el mismo efecto que una comunicación no realizada. Por tanto, todo retraso en la comunicación inmediata a las personas interesadas, ha de justificarse.

Cuando la comunicación a las personas afectadas se produzca como consecuencia de una orden emitida por la Agencia Española de Protección de Datos, deberá materializarse la comunicación a los afectados sin dilación indebida, y comunicar la confirmación de haber ejecutado la orden dentro del plazo de 30 días, salvo que se indique un plazo diferente en la orden.

COMUNICAR A LOS AFECTADOS

QUIÉN, CÓMO Y QUÉ SE DEBE COMUNICAR

> La persona responsable puede encomendarse a un tercero, en virtud de un contrato o vínculo legal, que actuará como encargado de tratamiento, para que realice la comunicación de la brecha de datos personales a las personas afectadas.

En todo caso, el responsable de tratamiento debe ser previamente informado sobre la ocurrencia de la brecha de datos personales, y sobre todos los detalles relevantes.

La comunicación preferentemente se deberá realizar de forma directa al afectado, ya sea por teléfono, correo electrónico, SMS, correo postal o a través de cualquier otro medio.

www.redconsultora.com

Ley de Protección de Datos para Entidades y Colectivos Ciudadanos

Contenidos **CLAVE** Para Entidades y Colectivos Ciudadanos

Redconsultora Asociación

madrid.es/espacioasociativo

MADRID