**MANUAL DE PROTECCIÓN DE DATOS**

PARA EL RESPONSABLE DE TRATAMIENTO

**${razon}**

${fecha}

Contenido

[INTRODUCCIÓN 2](#_Toc488749531)

[1. RESPONSABILIDADES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO 4](#_Toc488749532)

[1.1 El deber de informar 4](#_Toc488749533)

[1.2 Derechos de los interesados 4](#_Toc488749534)

[1.2.1 Derecho de acceso 4](#_Toc488749535)

[1.2.2 Derecho de rectificación 5](#_Toc488749536)

[1.2.3 Derecho a la supresión 5](#_Toc488749537)

[1.2.4 Derecho a la Limitación del tratamiento 5](#_Toc488749538)

[1.2.5 Derecho a la Portabilidad de datos 6](#_Toc488749539)

[1.2.6 Derecho a la Oposición 7](#_Toc488749540)

[1.3 El destino de los datos al finalizar la prestación 7](#_Toc488749541)

[2. MEDIDAS DE RESPONSABILIDAD ACTIVA 8](#_Toc488749542)

[2.1 Análisis de riesgo 8](#_Toc488749543)

[2.1.1 Riesgos Generales 10](#_Toc488749544)

[2.1.2 Legitimación de los tratamiento y cesiones de datos personales 11](#_Toc488749545)

[2.1.3 Transferencias Internacionales 14](#_Toc488749546)

[2.1.4. Transparencia de los tratamientos 15](#_Toc488749547)

[2.1.5 Calidad de datos 16](#_Toc488749548)

[2.1.6 Datos especialmente protegidos 18](#_Toc488749549)

[2.1.7 notificación de los tratamientos 18](#_Toc488749550)

[2.1.8 Deber de secreto 19](#_Toc488749551)

[2.1.9 tratamientos por encargo 20](#_Toc488749552)

[2.1.10 Derechos ARCO 21](#_Toc488749553)

[2.1.11 Seguridad 21](#_Toc488749554)

[2.2 Registros de actividades de tratamiento 24](#_Toc488749555)

[2.3 Notificación de “violaciones de seguridad de los datos” 25](#_Toc488749556)

# INTRODUCCIÓN

El objeto de la normativa en protección de datos personales no es otro que garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, especialmente de su honor e intimidad personal y familiar.

**El Reglamento General de Protección de datos (RGPD) 2016/679 del Parlamento Europeo y del Consejo, entra en vigor desde el 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.** Este texto deroga la actual Directiva 95/46/CE de protección de datos y sustituye a las leyes de protección de datos nacionales existente (En España, la Ley 15/1999 de Protección de Datos). El texto será aplicable en todos los mercados de la Unión Europea de desde 25 de mayo de 2018. Hasta entonces se aplica la LOPD.

En el Reglamento General de Protección de Datos se unifica y moderniza la normativa europea sobre protección de datos, permitiendo a los ciudadanos un mejor control de sus datos personales y a las empresas aprovechar al máximo las oportunidades de un mercado único digital, reduciendo la burocracia y beneficiándose de una mayor confianza de los consumidores.

El Reglamento General de Protección de Datos adopta dos medidas fundamentales e innovadoras que son el principio de responsabilidad proactiva, donde existe 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. La otra medida sería el enfoque de riesgo, donde se debe 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.

En este manual se presentan de forma sistemática las principales cuestiones que las organizaciones deberán tener en cuenta de cara a la aplicación del RGPD. Está pensada para ayudar al responsable de **${razon}** y a los encargados a adaptarse a las nuevas obligaciones.

# RESPONSABILIDADES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

El responsable del tratamiento de **${razon}** aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento **General de Protección de datos**.

## El deber de informar

El encargado y responsable del tratamiento de **${razon}** garantizará que las personas autorizadas para tratar datos personales se han comprometido, de forma expresa, a respetar la confidencialidad o, en su caso, si están sujetas a una obligación de confidencialidad de naturaleza estatutaria; El cumplimiento de esta obligación debe quedar documentado.

## Derechos de los interesados

El responsable o encargado del tratamiento de **${razon}** debe cumplir con la obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III del RGPD:

### Derecho de acceso

El derecho de acceso es el derecho del titular de los datos a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos.

El responsable del tratamiento de **${razon}** facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

### Derecho de rectificación

El derecho de rectificación supone el derecho del afectado a que los datos almacenados en los ficheros del responsable sean veraces y exactos. Asimismo, expresa la obligación del responsable de mantener la veracidad y exactitud de sus ficheros.

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento de **${razon},** la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

### Derecho a la supresión

El derecho a la supresión o al olvido de los datos personales y, que permite, por ejemplo, que los interesados exijan la supresión, sin demora, de datos personales recogidos o publicados en una red social o en un motor de búsqueda.

El responsable del tratamiento de **${razon},** teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

Es una manifestación de los derechos de cancelación u oposición en el entorno online (según la jurisprudencia que el Tribunal de Justicia de la UE estableció en el caso Google Spain).

### Derecho a la Limitación del tratamiento

Este derecho consiste en reconocer la potestad de los interesados de solicitar y obtener del Responsable del tratamiento de **${razon}**, una limitación del tratamiento de sus datos personales cuando concurran los siguientes escenarios:

* **Inexactitud**: Cuando el interesado haya solicitado al Responsable del tratamiento la puesta al día de sus datos personales, por considerarlo inexactos. Esta limitación de tratamiento se realizará por parte del Responsable de fichero durante el plazo necesario para que este compruebe la exactitud de los mismos.
* **Ilicitud**: Cuando los datos sean ilícitos pero el interesado no desee cancelar los mismos. En estos supuestos se podrá solicitar por el interesado la limitación del tratamiento de sus datos, en vez de la supresión de los mismos.
* **Reclamaciones**: Cuando el interesado necesite que el Responsable siga tratando sus datos con el objeto de formular, ejercer o defender reclamaciones, a pesar de que el Responsable del fichero ya no necesite tratar los datos personales del interesado para la finalidad por la que fueron recabados.
* **Oposición**: Cuando el interesado lo solicite, como medida provisional, en el caso de haber ejercido el derecho de Oposición. La limitación de tratamiento operará durante el tiempo que emplee el Responsable del tratamiento en dilucidar si los argumentos que esgrime el interesado para oponerse el tratamiento de sus datos, son pertinentes.

La limitación de tratamiento consiste en que el Responsable de tratamiento de **${razon}** deberá reservar los datos y sólo utilizarlos en los siguientes supuestos:

* Cuando concurra el consentimiento del interesado.
  + Para la formulación, el ejercicio o la defensa de reclamaciones.
  + Para defender, en materia de Protección de Datos, los derechos de otra persona física o jurídica.
  + Por razones de interés público importante de la Unión Europea o de un determinado Estado miembro.

El Responsable de tratamiento de **${razon}** deberá informar, previamente, al interesado cuando vaya a tratar de nuevo sus datos personales y, por lo tanto, deje de aplicar la limitación de tratamiento sobre los mismos.

### Derecho a la Portabilidad de datos

Está estrechamente relacionado con el derecho de acceso. Este derecho a la portabilidad de datos personales permite a los individuos que han cedido sus datos al responsable del tratamiento de **${razon}** recibir estos mismos datos en un formato estructurado y que sea legible por parte de una máquina de modo que pueda transmitirlos fácilmente a otra empresa u organización

 En resumen, el derecho a la portabilidad permite a los individuos solicitar a una empresa sus datos personales en un formato digital estandarizado y**facilita en gran medida la transmisión de esos datos a otras empresas.**

### Derecho a la Oposición

El derecho de oposición puede ejercitarse en los casos en los que no es necesario el consentimiento del afectado para el tratamiento de sus datos de carácter personal. Siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable excluirá del tratamiento los datos relativos al afectado.

También puede ejercerse este derecho cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, y cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en el tratamiento automatizado de sus datos.

## 1.3 El destino de los datos al finalizar la prestación

Hay que prever si, una vez finalice la prestación de los servicios de tratamiento, el encargado del tratamiento de **${razon}** debe proceder a la supresión o a la devolución de los datos personales y de cualquier copia existente, ya sea al responsable o a otro encargado designado por el responsable.

El acuerdo debe establecer de forma clara cuál de las dos opciones es la elegida por el responsable, así como la forma y el plazo en que debe cumplirse. En todo caso, los datos deberán ser devueltos al responsable cuando se requiera la conservación de los datos personales, en virtud del Derecho de la Unión o de los Estados miembros.

No obstante, el encargado puede conservar una copia con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

# MEDIDAS DE RESPONSABILIDAD ACTIVA

El Reglamento General de Protección de Datos 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.

**${razon}** debe adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece. El Reglamento entiende que actuar sólo cuando ya se ha producido una infracción es insuficiente como estrategia, dado que esa infracción puede causar daños a los interesados que pueden ser muy difíciles de compensar o reparar. Para ello, el Reglamento prevé una batería completa de medidas:

* + - Protección de datos desde el diseño
    - Protección de datos por defecto
    - Medidas de seguridad
    - Mantenimiento de un registro de tratamientos
    - Realización de evaluaciones de impacto sobre la protección de datos
    - Nombramiento de un delegado de protección de datos
    - Notificación de violaciones de la seguridad de los datos
    - Promoción de códigos de conducta y esquemas de certificación

## Análisis de riesgo

El Reglamento General de Protección de Datos, 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).

Se debe hacer una evaluación del impacto de la protección de datos personales en la empresa, a través de la documentación “**Mapa de Riesgo”** donde se hace un seguimiento del ciclo de vida de los datos personales, sus usos previstos, las finalidades para las que se tratarán, las tecnologías utilizadas y la identificación de los usuarios que accederán a ella para, así, conocer los riesgos, reales y percibidos, existentes para la privacidad.

Los riesgos pueden ser de dos tipos. El primero y principal es el que afecta a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.

Pero tampoco hay que descuidar los riesgos que puede afrontar una empresa por no haber implantado una correcta política de protección de datos o por haberlo hecho de forma descui­dada o errática, sin poner en marcha mecanismos de planificación, implantación, verificación y corrección eficaces.

En este análisis de riesgo, se contemplan diversas opciones dependiendo del impacto que su materialización tendría para la empresa: evitarlo o eliminarlo, mitigarlo, transferirlo o aceptarlo. Una vez identificado cada riesgo, se procede a gestionarlos. A modo de ejemplo, a continuación se incluyen algunas medidas que se podrían adoptar para gestionar algunos riesgos que pueden haberse detectado en la fase anterior:

El responsable de tratamiento debe asegurarse de la monitorización continua de que las medidas de gestión del riesgo adoptadas son efectivas y cumplen el objetivo para el que fueron implantadas y, en caso de no ser así, introducir los cambios y modificaciones que resulten necesarias para conseguir los objetivos perseguidos.

### 2.1.1 Riesgos Generales

|  |  |
| --- | --- |
| RIESGOS GENERALES | |
| RIESGOS | **MEDIDAS** |
| Pérdidas económicas y daños reputacionales deriva­dos del incumplimiento de la legislación sobre protec­ción de datos personales | * Formación apropiada del personal sobre protección de datos * Comunicación auditable y clara de las responsabilida­des del personal en relación con el cumplimiento de las políticas de privacidad de la organización así como de las sanciones aparejadas al incumplimiento de las mismas |
| Pérdidas económicas y daños reputacionales deriva­dos del incumplimiento de legislaciones sectoriales con incidencia en la protección de datos personales a las que pueda estar sujeto el responsable del tra­tamiento | * Formación apropiada del personal sobre protección de datos en el sector específico de que se trate * Comunicación auditable y clara de las responsabili­dades del personal en relación con el cumplimiento de las políticas de privacidad de la organización re­lativas a las legislaciones sectoriales que afectan a la organización, así como de las sanciones aparejadas al incumplimiento de las mismas |
| Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de las mismas, en particular, cuando se producen pérdidas de datos personales | * Formación apropiada del personal sobre seguridad y uso adecuado de las TIC * Comunicación auditable y clara de las responsabili­dades del personal en relación con el cumplimiento de las políticas y las medidas de seguridad así como de las sanciones aparejadas al incumplimiento de las mismas |
| Pérdida de competitividad del producto o servicio de­rivada de los daños reputacionales causados por una deficiente gestión de la privacidad de las personas | * Formación apropiada del personal sobre protección de datos, seguridad y uso adecuado de las TIC |
| Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados | * Nombrar a una persona o departamento como responsable de la interlocución con los afectados en todo aquello relativo a la privacidad y la protección de datos personales, y comunicar claramente la forma de contactar con ella * Nombrar un Delegado de Protección de Datos o Data Protection Officer (que dependiendo del tamaño de la organización será una persona o un departamento interno o externo) para ocuparse de todas las cuestiones relativas a la privacidad dentro de la organización y contar con asesoramiento cualificado. Si se procede a este nombramiento, el Delegado de Protección de Datos puede hacerse cargo |
| Incorporación tardía de los expertos en protección de datos (en particular, del delegado de protección de datos o DPO) al proyecto o definición deficiente de sus funciones y competencias | * Incluir dentro de los procedimientos de diseño y desarrollo de nuevos productos y servicios la incorporación del DPO en las fases iniciales de los mismos * Establecer desde la dirección las funciones, competencias y atribuciones del DPO en el desarrollo y gestión de los proyectos |

### 2.1.2 Legitimación de los tratamiento y cesiones de datos personales

|  |  |
| --- | --- |
| LEGITIMACIÓN DE LOS TRATAMIENTOS Y CESIONES DE DATOS PERSONALES | |
| RIESGOS | **MEDIDAS** |
| Tratar datos personales cuando no es necesario para la finalidad perseguida | * Usar datos disociados siempre que sea posible y no implique un esfuerzo desproporcionado * Permitir el uso anónimo de los servicios y productos cuando no sea necesaria la identificación de las personas * Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso * Utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, sí que pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un número reducido de personas * Evitar el uso de datos biométricos salvo que resulte imprescindible o esté absolutamente justificado |
| Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales | * Formación adecuada del personal sobre protección de datos, seguridad y uso adecuado de las TIC * Revisar las posibilidades que ofrece la legislación de protección de datos para permitir el tratamiento de datos personales y asegurar que este encaja en alguna de ellas * Si es necesario, buscar asesoramiento experto * Si se ceden datos personales, establecer por escrito acuerdos que contemplen las condiciones bajo las que se produce la cesión y, en su caso, las relativas a cesiones ulteriores así como las posibilidades de supervisión y control del cumplimiento del acuerdo |
| Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales | * Asegurarse de que no existen otras causas de legitimación más adecuadas * Cuando el tratamiento de datos personales se legitime por una relación contractual, ofrecer siempre la posibilidad de consentimiento separado para tratar datos con finalidades que no son necesarias para el cumplimiento o perfeccionamiento de la misma, evitando incluirlas de forma indisoluble en las cláusulas del contrato. * Evitar condicionar el disfrute de un producto o servicio al consentimiento para finalidades diferentes * En el ámbito laboral, evitar basar los tratamientos de datos en el consentimiento de los trabajadores * Evitar forzar el consentimiento desde una posición de prevalencia del responsable o cuando existen otras causas legitimadoras suficientes y más adecuadas |
| Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión | * Establecer procedimientos claros para manifestar la revocación del consentimiento o la solicitud de oposición a un determinado tratamiento. Si la organización realiza acciones publicitarias, tener en cuenta las reglas especiales existentes para las comunicaciones comerciales y, en particular, cuando estas se llevan a cabo a través de comunicaciones electrónicas * Establecer los mecanismos necesarios para garantizar que se consultan los ficheros de exclusión de publicidad, tanto de la organización como externos, y que se tienen en cuenta los deseos de quienes se han inscrito en ellos |
| Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros | * Exigir garantías de que los datos personales provenientes de terceros se han obtenido y cedido legal y lealmente. * En la realización de campañas publicitarias con datos provenientes de terceros en las que se segmenta el público objetivo en función de parámetros determinados, exigir garantías de que las personas cuyos datos van a ser utilizados han dado su consentimiento para ello |
| Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardias necesarias | * Verificar que el tratamiento de datos especialmente protegidos es absolutamente imprescindible para la finalidad o finalidades perseguidas * Verificar si el tratamiento está amparado o es requerido por una ley * En caso contrario, establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él |
| Enriquecer los datos personales de forma no prevista en las finalidades iniciales y sin la información adecuada a los afectados al realizar una interconexión con otras bases de datos de la organización o de terceros, en particular, la re-identificación de información disociada | * Verificar la legitimidad de la interconexión de datos prevista * Definir claramente los datos personales resultantes del tratamiento y verificar tras el proceso que son los únicos que se han generado |
| Utilizar cookies de seguimiento u otros mecanismos de rastreo sin obtener un consentimiento válido tras una información adecuada | * Evitar el uso de cookies u otros mecanismos de rastreo y monitorización. En caso de que se utilicen, preferir las menos invasivas (cookies propias frente a cookies de terceros, cookies de sesión frente a cookies permanentes, periodos cortos de caducidad de las cookies, etc.) * Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas. * Respetar las preferencias establecidas por los afectados en sus navegadores sobre el rastreo de su navegación |
| Impedir la utilización anónima de un determinado producto o servicio cuando la identificación del usuario no resulta indispensable | * Permitir el uso anónimo de los servicios y productos cuando no sea necesaria la identificación de las personas |

### 2.1.3 Transferencias Internacionales

|  |  |
| --- | --- |
| TRANSFERENCIAS INTERNACIONALES | |
| RIESGOS | **MEDIDAS** |
| Acceso secreto a los datos personales por parte de autoridades de terceros países | * Incluir cláusulas de salvaguarda en las que se requiera información sobre el acceso a los datos personales transferidos por parte de autoridades de terceros países tan pronto como sea posible |
| Carencia de mecanismos de control de cumplimiento de las garantías establecidas para la transferencia | * Si existen transferencias internacionales a países fuera del Espacio Económico Europeo, implantar los procedimientos de control necesarios (incluidos los contractuales) para garantizar que se cumplen las condiciones bajo las que se llevó a cabo la transferencia. En este sentido, hay que prestar especial atención cuando se contraten servicios de cloud computing u hospedados en terceros |
| Impedimentos por parte del importador para el ejercicio de los procedimientos de supervisión y control pactados | * Asegurarse de la exigibilidad de mecanismos de control del importador tales como listas de encargados de tratamiento, países donde operan, posibilidad de revisar documentación y realizar auditorías, etc. |
| Incapacidad de ayudar a los ciudadanos en el ejercicio de sus derechos ante el importador | * Asegurarse de la definición y funcionamiento de un canal de comunicación entre exportador e importador para hacer llegar las solicitudes y reclamaciones de los afectados * Poner en marcha procedimientos que garanticen la adecuada atención de las demandas de los afectados |
| No obtención de las autorizaciones legales necesarias | * Solicitar la autorización del Director de la Agencia Española de Protección de Datos en aquellos casos que resulte necesario |

### 2.1.4. Transparencia de los tratamientos

|  |  |
| --- | --- |
| TRANSPARENCIA DE LOS TRATAMIENTOS | |
| RIESGOS | **MEDIDAS** |
| Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (cookies, ubicación geográfica, comportamiento, hábitos de navegación, etc.) | * Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas26. * Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrece la información adecuada |
| En el entorno web, ubicar la información en materia de protección de datos (políticas de privacidad, cláusulas informativas) en lugares de difícil localización o diseminada en diversas secciones y apartados que hagan muy difícil su acceso conjunto y detallado | * Estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles fácilmente accesibles por los afectados y valorar la utilización de iconos u otros sistemas gráficos para facilitar su comprensión * Verificar que la información que se ofrece en todos los lugares y situaciones es coherente y sistemática * Verificar que la información se ofrece en todos los formularios |
| Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer para que exista un tratamiento leal de sus datos personales | * Implantar políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización |

### 2.1.5 Calidad de datos

|  |  |
| --- | --- |
| CALIDAD DE DATOS | |
| RIESGOS | **MEDIDAS** |
| Solicitar datos o categorías de datos innecesarios para las finalidades del nuevo sistema, producto o servicio | * Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso |
| Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados con informaciones diferentes o contradictorias, lo que puede derivar en la toma de decisiones erróneas | * Establecer medidas técnicas y organizativas que garanticen que las actualizaciones de datos de los afectados se comunican a todos los sistemas de información y departamentos de la organización que estén autorizados a utilizarlos |
| Garantías insuficientes para el uso de datos personales con fines históricos, científicos o estadísticos | * Siempre que sea posible, utilizar datos anónimos o disociados * Utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, sí que pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un número reducido de personas * Garantizar que se aplican las medidas de seguridad adecuadas y correspondientes al nivel de seguridad de los datos utilizados |
| Utilizar los datos personales para finalidades no especificadas o incompatibles con las declaradas  –Datos transaccionales, de navegación o de geolocalización para la monitorización del comportamiento, la realización de perfiles y la toma de decisiones sobre las personas  –Toma de decisiones económicas, sociales, laborales, etc., relevantes sobre las personas (en particular las que pertenecen a colectivos vulnerables) especialmente si pueden ser adversas o discriminatorias, incluyendo diferencias en los precios y costes de servicios y productos o trabas para el paso de fronteras  –Toma de decisiones automatizadas con posibles consecuencias relevantes para las personas  –Utilización de los metadatos para finalidades no declaradas o incompatibles con las declaradas | * Suministrar información transparente y clara sobre las finalidades para las que se tratarán los datos personales, en particular, a través de una política de privacidad visible y accesible * Proporcionar información sobre los criterios utilizados en la toma de decisiones y permitir a los afectados impugnar la decisión y solicitar que sea revisada por una persona * Proporcionar información sobre las medidas que se han implantado para lograr el necesario equilibrio entre el interés legítimo del responsable y los derechos fundamentales de los afectados |
| Realizar inferencias o deducciones erróneas (y, en su caso, perjudiciales) sobre personas específicas mediante la utilización de técnicas de inteligencia artificial (en particular, minería de datos), reconocimiento facial o análisis biométricos de cualquier tipo | * Establecer mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer * Establecer posibilidades de impugnación ágiles para ofrecer vías de recurso adecuadas a los afectados * Establecer canales alternativos para tratar con los falsos negativos y falsos positivos en la identificación y autenticación de personas a través de datos biométricos |
| Carecer de procedimientos claros y de herramientas adecuadas para garantizar la cancelación de oficio de los datos personales una vez que han dejado de ser necesarios para la finalidad o finalidades para las que se recogieron | * Definir claramente los plazos de cancelación de todos los datos personales de los sistemas de información * Establecer controles automáticos dentro de los sistemas de información para avisar de la cercanía de los plazos de cancelación de la información * Implantar mecanismos para llevar a cabo y gestionar dicha cancelación en el momento adecuado incluyendo, si corresponde, el bloqueo temporal de los datos personales |

### 2.1.6 Datos especialmente protegidos

|  |  |
| --- | --- |
| DATOS ESPECIALMENTE PROTEGIDOS | |
| RIESGOS | **MEDIDAS** |
| Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso cuando éste sea la causa que legitima su tratamiento o cesión | * Evitar el uso de datos especialmente protegidos salvo que resulte absolutamente necesario * Establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él |
| Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos sensibles | * Nombrar un Delegado de Protección de Datos o Data Protection Officer (DPO) para contar con asesoramiento cualificado |
| Disociación deficiente o reversible que permita la re-identificación de datos sensibles en procesos de investigación que solo prevén utilizar datos anónimos | * Utilizar técnicas de disociación que garanticen el anonimato real de la información o, al menos, que el riesgo residual de re-identificación es mínimo |

### 2.1.7 Notificación y registro de las actividades de tratamiento

|  |  |
| --- | --- |
| NOTIFICACIÓN DE LOS TRATAMIENTOS | |
| RIESGOS | **MEDIDAS** |
| Carecer de los mecanismos y procedimientos necesarios para detectar cuándo debe  Registrarse la creación, modificación o cancelación de actividades de tratamiento. | Incluir en los procesos y metodologías de desarrollo de nuevos proyectos una fase o tarea relativa a la revisión de la necesidad de cumplimiento normativo. |
| Carecer de los mecanismos y procedimientos necesarios para detectar  cuando debe realizarse análisis de impacto en protección de datos y su consulta a la autoridad de control. | Incluir en los procesos y metodologías de desarrollo de nuevos proyectos una fase o tarea relativa a la revisión de la necesidad de cumplimiento normativo |

### 2.1.8 Deber de secreto

|  |  |
| --- | --- |
| DEBER DE SECRETO | |
| RIESGOS | **MEDIDAS** |
| Accesos no autorizados a datos personales | * Establecer mecanismos y procedimientos de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales * Establecer sanciones disciplinarias para quienes incumplan el deber de secreto y las políticas de confidencialidad de la organización * Establecer procedimientos que garanticen que se notifica formalmente a los trabajadores que acceden a datos personales de la obligación de guardar secreto sobre aquellos que conozcan en el ejercicio de sus funciones y de las consecuencias de su incumplimiento * Notificar que se dará traslado a las autoridades competentes de las violaciones de confidencialidad que puedan entrañar responsabilidades penales * Establecer procedimientos para garantizar la destrucción de soportes desechados que contengan datos personales |
| Violaciones de la confidencialidad de los datos personales por parte de los empleados de la organización | * Formación adecuada de los empleados sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información * Establecimiento de sanciones disuasorias para los empleados que violen la confidencialidad de los datos personales y comunicación clara y completa de las mismas |

### 2.1.9 tratamientos por encargo

|  |  |
| --- | --- |
| TRATAMIENTOS POR ENCARGO | |
| RIESGOS | **MEDIDAS** |
| Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas | * Establecer procedimientos que garanticen que siempre que se recurre a un encargado de tratamiento se firma el correspondiente contrato en los términos establecidos por la legislación de protección de datos |
| Falta de diligencia (o dificultad para demostrarla) en la elección de encargado de tratamiento | * Seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento de los contratos y de la adopción de las medidas de seguridad estipuladas a través, por ejemplo, de su adhesión a posibles códigos de conducta o a esquemas de certificación homologados y de acreditada solvencia * Establecer contractualmente mecanismos de supervisión, verificación y auditoría de los tratamientos encargados a terceros |
| No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos ARCO realizados ante los encargados de tratamiento | * Incluir en el contrato de encargo la obligación de comunicar al responsable las peticiones de ejercicio de los derechos ARCO * Definir los procedimientos operativos para que esta comunicación se lleve a cabo de forma ágil y eficiente |
| Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato | * Incluir la obligación de portabilidad en el contrato y en los acuerdos de nivel de servicio * Establecer medidas técnicas y organizativas que garanticen la portabilidad |

### 2.1.10 Derechos ARCO

|  |  |
| --- | --- |
| DERECHOS ARCO | |
| RIESGOS | **MEDIDAS** |
| Dificultar o imposibilitar el ejercicio de los derechos ARCO | * Implantar sistemas que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos ARCO * Evitar sistemas de ejercicio de los derechos ARCO que impliquen solicitar una remuneración * Evitar establecer procedimientos poco transparentes, complejos y laboriosos * Formar a todo personal para que conozca qué ha de hacer si recibe una petición de derecho ARCO o ha de informar a los afectados sobre cómo ejercerla * Definir qué personas o departamentos se ocuparán de gestionar los derechos ARCO y formarlos adecuadamente |
| Carencia de procedimientos y herramientas para la gestión de los derechos ARCO | * Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen que todos los empleados conocen cómo actuar ante un ejercicio de derechos ARCO y que pueden suministrar la información adecuada a los afectados * Formación de los empleados encargados de gestionar los ejercicios de derechos ARCO |
| Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales | * Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate * Establecimiento de acuerdos y procedimientos de gestión y comunicación con los cesionarios de la información que garanticen la correcta actualización de los datos personales cedidos * Formación de los empleados encargados de gestionar los ejercicios de derechos ARCO |

### 2.1.11 Seguridad

|  |  |
| --- | --- |
| SEGURIDAD | |
| RIESGOS | **MEDIDAS** |
| Inexistencia del responsable de seguridad o deficiente definición de sus funciones y competencias | * Nombramiento del responsable de seguridad y establecimiento por parte de la dirección de sus funciones, competencias y atribuciones en el desarrollo y gestión de los proyectos * Incluir dentro de los procedimientos de diseño y desarrollo de nuevos productos y servicios la incorporación del responsable de seguridad en las fases iniciales de los mismos |
| Deficiencias organizativas en la gestión del control de accesos | * Políticas estrictas de need to know (necesidad de conocer o acceder a la información) para la concesión de accesos a la información y de clean desks (escritorios limpios) para minimizar las posibilidades de acceso no autorizado a los datos personales * Establecer procedimientos que garanticen la revocación de permisos para acceder a datos personales cuando ya no sean necesarios (abandono de la organización, traslado, cambio de funciones, etc.) * Inventariar los recursos que contengan datos personales accesibles a través de redes de telecomunicaciones |
| Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales | * Instalar herramientas de hardware o software que ayuden a una gestión eficaz de la seguridad y los compromisos u obligaciones legales de la organización en el área de la protección de datos personales * En el caso de que pudiera resultar necesario, instalar herramientas de detección de intrusiones (Intrusion Detection Systems) y/o de prevención de intrusiones (Intrusion Prevention Systems) con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad * En la medida que pudiera resultar necesario, implantar sistemas de Data Loss Prevention o Prevención de Pérdida de Datos con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad |
| Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información | * Establecer mecanismos de registro de acciones sobre los datos personales o logging así como herramientas fiables y flexibles de explotación de los ficheros de auditoría resultantes |
| Uso de identificadores que revelan información del afectado | * Establecer políticas de asignación de códigos de usuario por parte de la organización que eviten datos triviales como fecha de nacimiento, nombre y apellidos, etc. * Evitar el uso de identificadores ligados a elementos de autenticación, como números de tarjetas de crédito o similares, ya que favorecen el fraude en la identificación e incluso la suplantación de identidad |
| Deficiencias en la protección de la confidencialidad de la información | * Adoptar medidas de cifrado –adecuadas al riesgo y al estado de la tecnología– de los datos personales almacenados y compartidos a través de redes de telecomunicaciones (en particular, si son públicas y/o inalámbricas) para minimizar el riesgo de que terceros no autorizados accedan a ellos ante un hipotético fallo de seguridad * Establecer procedimientos de notificación a las personas afectadas para el caso en que sus datos hayan podido ser accedidos o sustraídos por terceros no autorizados, informándoles de las medidas que pueden utilizar para minimizar los riesgos * Establecer procedimientos de notificación de quiebras de seguridad a la autoridad de control cuando ello sea legalmente exigible * Evitar, en general, las pruebas con datos reales y, en particular, cuando incluyan datos especialmente protegidos o un conjunto importante de datos que revelen aspectos relevantes de la personalidad de los afectados, cuando se empleen los de muchas personas o cuando participen en las pruebas un número elevado de usuarios * Construir canales seguros y con verificación de identidad para la distribución de información de seguridad (códigos de usuario, contraseñas, etc.) |
| Falta de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo | * Formación sobre la política de seguridad de la organización y, en particular, sobre las obligaciones de cada empleado * Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas y las medidas de seguridad, así como de las sanciones aparejadas al incumplimiento de las mismas |
| Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados | * En el caso de que pudiera resultar necesario, instalar herramientas de detección de intrusiones (Intrusion Detection Systems) y/o de prevención de intrusiones (Intrusion Prevention Systems) con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad * En la medida que pudiera resultar necesario, implantar sistemas de Data Loss Prevention o Prevención de Pérdida de Datos con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad |

## Registros de actividades de tratamiento

Si la empresa realiza algún tratamiento que pueda entrañar un riesgo para los derechos y libertades de los interesados, que no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales deberán realizar estos registros de actividades.

El Responsable y encargado deberá mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el Reglamento General de Protección de Datos 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

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.

## Notificación de “violaciones de seguridad de los datos”

El Reglamento General de Protección de Datos 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 **${razon}** (incluso del personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del Reglamento General de Protección de Datos y deben ser tratadas como el Reglamento establece.

Cuando se produzca una violación de la seguridad de los datos, el responsable de tratamiento de **${razon}** deberá 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

El responsable del tratamiento de **${razon}** documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto.

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 estos últimos. 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.

La valoración del riesgo de la quiebra es distinta del análisis de riesgos previo a todo tratamiento. 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.

La mínima 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.

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.

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.