



# SEGURIDAD INFORMÁTICA

---

JOSÉ PABLO  
HERNÁNDEZ

# SEGURIDAD INFORMÁTICA

## 1.5.0. Capítulo 5

Protección de datos de carácter personal

JOSÉ PABLO HERNÁNDEZ

# 1. INTRODUCCIÓN

**La primera fuente para determinar los requisitos de seguridad, el primer criterio para elegir salvaguardas, y el primer objetivo que estas deben alcanzar, es el cumplimiento de la legislación que afecte a la empresa.**

# 1. INTRODUCCIÓN

La protección de datos carácter personal es un **derecho fundamental**.

La Constitución Española de 1978 (CE), establece en su artículo 18.4 que “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos, y el pleno ejercicio de sus derechos”.



# 1. INTRODUCCIÓN

**El Reglamento Europeo 2016/679 de Protección de Datos (RGPD) es el nuevo marco jurídico de la UE que rige el uso de los datos personales.**

**Deroga la Directiva 95/46/CE de protección de datos**

**Sustituye en aquello que lo contradiga a la LOPD y al RLOPD**

**Se aplica en toda la Unión Europea desde el 25 de mayo de 2018**

**Hasta el 25 de mayo de 2018 se aplicaba la LOPD y el RLOPD**



# 1. INTRODUCCIÓN

**El objetivo del RGPD es dar más control a los ciudadanos sobre su información privada en un mundo con cada vez más dependencia a los teléfonos inteligentes, a las redes sociales, a la banca por internet, al internet de las cosas, al big data y a las transferencias globales.**

## 2. ÁMBITO DE APLICACIÓN

- **Objetivo:** protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismos.
- **Material:** se aplica al tratamiento de datos personales, automatizados o no automatizados.
- **Territorial:** responsables o encargados del tratamiento establecidos en la Unión Europea

## 2. ÁMBITO DE APLICACIÓN

- **Responsables y encargados del tratamiento no establecidos en la Unión Europea, siempre que realicen tratamientos derivados de una oferta de bienes o servicios destinados a ciudadanos de la UE (redes sociales, buscadores o comercio electrónico) o como consecuencia de una monitorización y seguimiento de su comportamiento (cookies de seguimiento de navegación o tracking).**

**Para ello, estas organizaciones deberán nombrar un representante en la UE, que actuará como punto de contacto entre las Autoridades de Control (como la AEPD) y los ciudadanos**



## 2. ÁMBITO DE APLICACIÓN

### NO APLICA

- Tratamiento de datos por Estados Miembros en el ejercicio de actividades relacionadas con el **SEBC** (Sistema Europeo de Bancos Centrales).
- Tratamiento de datos por autoridades competentes para los fines de **prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales**, incluida la protección frente amenazas a la seguridad pública.
- Persona física en el ejercicio de actividades **exclusivamente personales o domésticas**. Sin embargo se aplica el Reglamento a los responsables de tratamiento que proporcionen los medios para tratar datos personales para actividades personales o domésticas (p.e. Facebook).

## 2. ÁMBITO DE APLICACIÓN

### NO APLICA

- Tratamiento de datos de **personas fallecidas**.
- Cuestiones de protección de los derechos y libertades fundamentales o la libre circulación de datos personales relacionadas con **actividades excluidas del ámbito del derecho de la Unión Europea** (p.ej., Actividades relativas a la Seguridad Nacional)
- Tratamiento de datos personales relativos a **personas jurídicas**, incluido el nombre y la forma de la persona jurídica

### 3. DATOS DE CARÁCTER PERSONAL

**¿Qué es un dato de carácter personal?**

**"Toda información sobre una  
persona física identificada o  
identificable"**

**Es importante apuntar que el afectado o titular del dato será calificado por el RGPD como  
"el interesado"**

### 3. DATOS DE CARÁCTER PERSONAL

#### ¿Qué es persona física identificada o identificable?

En el RGPD, la identificación de una persona a los efectos de protección de datos se realiza cuando puede determinarse la identidad directa o indirectamente a través de:

- **Elementos propios de la identidad** física, fisiológica, psíquica, económica y cultural o social, a los cuales añade el elemento genético:
  - «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.
- **Por identificadores**, como, por ejemplo, el nombre, un número de identificación, datos de localización o un identificador en línea.

Para conseguir identificar a una persona identificable, tener en cuenta: costes, tiempo, tecnología disponible...

### 3. DATOS DE CARÁCTER PERSONAL

#### Tipo de información

- **Alfabética:** nombre y apellidos, dirección de email...
- **Numérica:** DNI, IP, número de teléfono...
- **Fotográfica:** imágenes captadas por cámara o vídeo...
- **Acústica:** voz humana
- Datos **genéticos** y **biométricos** (ADN, huella digital)

## 3.1 CATEGORÍAS ESPECIALES DE DATOS

### Categorías especiales de datos

- **Origen racial** -> Origen étnico o racial
- **Ideología** -> Opiniones políticas
- **Religión o Creencias** -> Convicciones religiosas o filosóficas
- **Afiliación sindical** -> Afiliación sindical
- **Salud** -> Datos relativos a la Salud
- **Vida sexual** -> Datos relativos a la vida sexual o las orientaciones sexuales
- **Datos genéticos:** información única sobre su fisiología o salud obtenidos a partir de una muestra biológica (ej. ADN)
- **Datos biométricos:** obtenidos a partir de un tratamiento técnico específico (huella digital, el iris del ojo, etc.)

## 3.1 CATEGORÍAS ESPECIALES DE DATOS

**Se prohíbe el tratamiento de estos datos, salvo:**

- Consentimiento explícito
- Obligación legal: por ejemplo, en derecho laboral (accidentalidad / Mutuas)
- Interés vital del interesado: por ejemplo, en un hospital
- Fundaciones o asociaciones políticas, filosóficas, religiosas o sindicales
- Datos manifiestamente públicos
- Formulación, ejercicio o defensa de reclamaciones / tribunales
- Interés público en el ámbito de la salud pública, investigación científica, histórica... (Ley 14/2007 de investigación biomédica y el Real Decreto 1716/2011)

## 3.2 TRATAMIENTO DE DATOS

**Tratamiento de datos:** 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



## 3.2 TRATAMIENTO DE DATOS

**Responsable del tratamiento o Responsable:** la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros

## 3.2 TRATAMIENTO DE DATOS

**Encargado del tratamiento o Encargado:** la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento

## 4. PRINCIPIOS

### 1. Principio de licitud, lealtad y transparencia

El tratamiento deberá ser lícito, leal y transparente.

### 2. Principio de limitación de la finalidad

Los datos deberán ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines.

### 3. Principio de minimización de datos

Los datos deberán ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

## 4. PRINCIPIOS

### 4. Principio de exactitud

Los datos deberán ser exactos, y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

### 5. Principio de limitación del plazo de conservación

Los datos deberán ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento.

Plazos legales establecidos para la conservación de determinados datos y documentos por motivos fiscales, probatorios del cumplimiento de obligaciones, etc.

Excepción: fines de archivo, investigación científica, estadística etc., que podrán conservarse más tiempo

## 4. PRINCIPIOS

### 6. Principio de integridad y confidencialidad

Los datos serán tratados de manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

### 7. Principio de responsabilidad proactiva

El Responsable debe cumplir con el RGPD y debe ser capaz de demostrarlo.

## 5. PRIVACIDAD POR DEFECTO Y DESDE EL DISEÑO

**Privacidad desde el diseño:** en el momento de determinar los medios (soportes) para el tratamiento de los datos y también en el momento del tratamiento, así como a la hora de diseñar y desarrollar aplicaciones, servicios y productos, deberá tenerse en cuenta la protección de datos y considerarse la aplicación de medidas técnicas y organizativas adecuadas, como la seudonimización, el cifrado o la minimización de los datos.

## 5. PRIVACIDAD POR DEFECTO Y DESDE EL DISEÑO

**Privacidad por defecto:** sólo serán objeto de tratamiento:

- Los datos personales que sean necesarios
- Para cada uno de los fines específicos del tratamiento
- Se limitará la extensión del tratamiento (plazos de conservación)
- No deberán ser accesibles a un número indeterminado de personas físicas

## 5. PRIVACIDAD POR DEFECTO Y DESDE EL DISEÑO

### ¿Cómo cumplir con estos principios?

- Teniendo presentes todos los principios de protección de datos durante todo el ciclo de vida del tratamiento: desde el diseño, pasando por la puesta en práctica, hasta la supresión de los datos.
- Reduciendo al máximo el tratamiento de los datos personales: por ejemplo, utilizar una única aplicación y no muchos excel, no duplicar información, no recoger más datos de los necesarios...
- Dando acceso únicamente a las personas necesarias e imprescindibles para realzar el tratamiento
- Seudonimizar lo antes posible los datos personales; cifrar la información o las comunicaciones; otras medidas que ayuden a proteger los datos
- Dar transparencia al tratamiento de datos, permitiendo a los interesados supervisarlos



## 6. PRINCIPIO DE RESPONSABILIDAD PROACTIVA

**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.**

**Por ello, el Reglamento prevé una batería completa de medidas:**

## 6. PRINCIPIO DE RESPONSABILIDAD PROACTIVA

### **Medidas de responsabilidad proactiva**

- Mantener un registro de actividades de tratamiento
- Nombrar a un DPO
- Privacidad por defecto
- Privacidad desde el diseño
- Notificación de brechas de seguridad
- Aplicar medidas de seguridad adecuadas (enfoque del riesgo)
- Realizar Evaluaciones de impacto (EIPD o PIA)
- Promoción de códigos de conducta y esquemas de certificación, política y procedimientos de protección de datos
- Diligencia debida en la selección de los encargados del tratamiento
- Autorizaciones o consultas previas con la AEPD
- Formación

## 7. LICITUD DEL TRATAMIENTO

**El tratamiento de datos personales solo se considerará lícito si cumple una de las siguientes condiciones:**

- El interesado ha prestado su consentimiento.
- El tratamiento es necesario para:
  - La ejecución de un contrato.
  - Una obligación legal.
  - Proteger los intereses vitales del interesado o de otra persona física.
  - El cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
  - La satisfacción de un interés legítimo siempre que, sobre dichos intereses, no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales.

## 8. CONSENTIMIENTO

### Art. 4.11 RGPD

**Toda manifestación de voluntad, libre, específica, informada e inequívoca, por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.**

## 8. CONSENTIMIENTO

**El consentimiento debe ser "inequívoco"**

.

**El consentimiento Inequívoco es aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa.**

**A diferencia del RLOPD, el RGPD no admite formas de consentimiento tácito o por omisión, ya que se basan en la inacción.**

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

## 8. CONSENTIMIENTO

**Situaciones en las que el consentimiento, además de inequívoco, ha de ser explícito:**

- **Tratamiento de datos sensibles**
- **Adopción de decisiones automatizadas**
- **Transferencias internacionales de datos**

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

El interesado tiene derecho a retirar su consentimiento en cualquier momento.

## 8. CONSENTIMIENTO

### **Recogida de datos personales a través de páginas web (formularios)**

**La prestación del consentimiento por el interesado en un sitio web debe realizarse mediante una acción afirmativa:**

- **Marcar una casilla**
- **Seleccionar la configuración técnica de los servicios de sociedad de la información**
- **Cualquier otra declaración o conducta por la que el usuario acepta el tratamiento**

### **NO constituirá obtención del consentimiento:**

- **El silencio**
- **Las casillas premarcadas**
- **La inacción (p.ej., plazo de 30 días)**

## 8. CONSENTIMIENTO

**Carga de prueba en cuanto a la obtención del consentimiento.**

**Cuando el tratamiento se base en el consentimiento del interesado, corresponderá al responsable del tratamiento demostrar que el interesado prestó el consentimiento por cualquier medio de prueba admisible en derecho.**

**Por lo tanto, la carga de la prueba recae en el responsable del tratamiento.**



## 9. DERECHOS

**Cuando los datos se obtengan del interesado se deberá informar sobre:**

- la identidad y los datos de contacto del responsable y, en su caso, de su representante
- los datos de contacto del DPO, en su caso
- los fines del tratamiento a que se destinan los datos personales
- la base jurídica del tratamiento (fundamento: consentimiento, ley, contrato, interés legítimo...)
- los intereses legítimos del responsable o de un tercero;
- los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
- la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión
- el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinarlo
- la existencia de derechos de acceso, rectificación, supresión, limitación del tratamiento, oposición y portabilidad
- el derecho a retirar el consentimiento
- el derecho a presentar una reclamación ante la AEPD
- si el interesado está obligado a facilitar los datos o las consecuencias de no hacerlo
- la existencia de decisiones automatizadas, incluida la elaboración de perfiles

## 9. DERECHOS

**Cuando los datos no se obtengan del interesado se deberá informar también de:**

- la procedencia de los datos
- las categorías de datos

# 9. DERECHOS

## Derecho de acceso

**Comprende el acceso a la siguiente información:**

- Fines del tratamiento.
- Categoría de datos que se traten por la empresa.
- Los destinatarios de los datos en caso de comunicaciones y/o transferencias internacionales.
- El plazo de conservación de los datos cuando sea posible y/o de no ser posible los criterios utilizados para determinar este plazo.
- La existencia del derecho de rectificación, cancelación u oposición.
- Derecho a presentar reclamación ante una autoridad de control.
- En el caso de que los datos no se hayan obtenido del interesado, cualquier información sobre su origen.
- La existencia de decisiones automatizadas (incluye elaboración de perfiles).

## 9. DERECHOS

### Derecho de rectificación

**El derecho de rectificación es el derecho del interesado a que se modifiquen los datos que resulten ser inexactos o incompletos.**

**La solicitud de rectificación deberá indicar a qué datos se refiere, así como la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.**

**El responsable del tratamiento resolverá sobre la solicitud de rectificación sin dilación indebida o como máximo en el plazo de 1 mes a contar desde la recepción de la solicitud.**

**El responsable del tratamiento deberá conservar bloqueados los datos rectificados.**

## 9. DERECHOS

### Derecho de supresión

**Exige que los datos sean suprimidos en los siguientes supuestos:**

- **Dejen de ser necesarios**
- **El consentimiento haya sido retirado por el interesado**
- **El interesado se oponga al tratamiento**
- **Los datos hayan sido tratados ilícitamente**
- **Para el cumplimiento de un obligación legal**
- **Se hayan obtenido en relación a una oferta de servicios de la sociedad de la información efectuada a menores de edad**

**En determinados casos, el responsable del tratamiento deberá conservar bloqueados los datos afectados por la solicitud de supresión**

## 9. DERECHOS

### **Derecho al olvido**

El derecho al olvido o el derecho a la supresión de los datos en Internet es el derecho a solicitar que se bloqueen o eliminen en las listas de resultados de los buscadores los vínculos que conduzcan a informaciones que le afecten y que resulten obsoletas, incompletas, falsas o irrelevantes, y no sean de interés público, entre otros motivos.

Si el interesado ejerce un derecho de supresión y el responsable del tratamiento ha hecho públicos los datos en internet, debe solicitar a los buscadores correspondientes que eliminen los datos indexados.

El interesado puede ejercer este derecho ante los buscadores o ante el responsable del tratamiento

## 9. DERECHOS

### **Derecho la portabilidad de los datos**

El interesado tiene derecho a:

- recibir/recuperar los datos personas que previamente haya facilitado al responsable
- y los que se deriven directamente del uso del servicio prestado (los generados por su actividad)
- en un formato estructurado, de uso común y lectura mecánica
- así como a solicitar el traslado de dichos datos a otro responsable (siempre que sea técnicamente factible), cuando:
  - El tratamiento se basa en el consentimiento o en un contrato.
  - El tratamiento se haga a través de medios automatizados. No cubre los archivos en papel.

No se incluyen los datos inferidos o deducidos (ej. los resultados de un examen de salud, la elaboración de un perfil...)

## 9. DERECHOS

### **Derecho la limitación del tratamiento**

El interesado tendrá derecho al "bloqueo o marcado" de los datos por propia voluntad en los siguientes supuestos:

- Cuando el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos.
- En el caso de que el responsable ya no necesite los datos personales, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

El responsable podrá "bloquear o marcar " los datos para verificar la licitud del tratamiento en los siguientes supuestos :

- Cuando el interesado impugne la exactitud de los datos personales: para verificar la inexactitud
- Cuando el interesado se oponga al tratamiento: mientras se verifica el interés legítimo del responsable



## 9. DERECHOS

### **Derecho de oposición**

El interesado tendrá derecho a oposición, en cualquier momento, por motivos relacionados con su situación particular sobre aquellos datos personales suyos que sean objeto de un tratamiento basado en el interés público o en el interés legítimo del responsable, incluida la elaboración de perfiles.

El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones

# 10. SANCIONES

10.000.000 € o el 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior. Ej.: incumplimiento de obligaciones relacionadas con la seguridad de los datos.

20.000.000 € o el 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior. Ej.: incumplimiento de los principios de protección de datos y los derechos de los individuos.

Responsable de las sanciones: la empresa

Pero... existen procedimientos disciplinarios internos y la obligación de todo el personal con acceso a datos de carácter personal de conocer la política de seguridad de la empresa.

## 1 1. AUTORIDADES DE CONTROL

**Con el RGPD se mantienen, como es el caso de la AEPD (Agencia Española de Protección de Datos), las autoridades independientes de control y con competencia en el territorio de su Estado miembro.**

**Las autoridades de control supervisarán el cumplimiento de la normativa de protección de datos.**

# 12. CONTRATOS CON ENCARGADOS

**Contratos entre Responsables y Encargados de Tratamiento — art. 28 RGPD**

**Debe regirse por un contrato o acto jurídico, escrito (inclusive en formato electrónico)**

**Debe establecer:**

- **Objeto**
- **Duración**
- **Naturaleza y finalidad**
- **Tipo de datos personales**
- **Categorías de interesados**
- **Obligaciones y derechos del Responsable**
- **Obligaciones del Encargado del Tratamiento**

## 12. CONTRATOS CON ENCARGADOS

### Obligaciones del Encargado del Tratamiento

El contrato debe recoger las obligaciones del Encargado del Tratamiento

- **Seguir las instrucciones del responsable**
- **Confidencialidad de todas las personas con acceso**
- **Cumplir con las medidas de seguridad (conforme a art. 32 RGPD)**
- **Solicitar la autorización, específica o general para subcontratar.**
- **Si es general: informar previamente**
- **Asistir al responsable en el ejercicio de derechos**
- **Devolver o destruir los datos al fin de la prestación**
- **Poner a disposición del responsable la información necesaria para demostrar su cumplimiento, así como permitirle auditorías o inspecciones, o códigos de conducta...**



## 12. CONTRATOS CON ENCARGADOS

**Principio de responsabilidad proactiva**

**Diligencia debida en la selección de encargados**

**Los responsables habrán de elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento.**

**Esta previsión se extiende también a los encargados cuando subcontraten operaciones de tratamiento con otros subencargados.**



## 13. TRANSFERENCIAS INTERNACIONALES DE DATOS

- **TID basadas en una decisión de adecuación (Art. 45 RGPD):** podrá realizarse cuando Comisión haya decidido que garantiza nivel de protección adecuado, sin que requiera autorización específica
- **TID mediante garantías adecuadas:** a falta de decisión, solo cabe TID si ofreciera garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas

# 13. TRANSFERENCIAS INTERNACIONALES DE DATOS

**Nota:** las autorizaciones otorgadas con anterioridad a la entrada en vigor del RGPD seguirán siendo válidas hasta que sean derogadas, modificadas o sustituidas por la autoridad de control y la comisión

**Excepciones TID en ausencia de anteriores:**

- **Consentimiento explícito del interesado**
- **Necesario para ejecución contrato entre interesado y responsable**
- **Necesario para celebración o ejecución contrato en interés del interesado**
- **Interés público**
- **Formulación, ejercicio o defensa reclamaciones**
- **Proteger intereses vitales**
- **Registro Público determinadas condiciones**

**TID a EEUU:** permitidas TID con entidades certificadas en el marco del Escudo de Privacidad UE-EEUU



# 14. REGISTRO DE ACTIVIDADES DE TRATAMIENTO

## Contenido

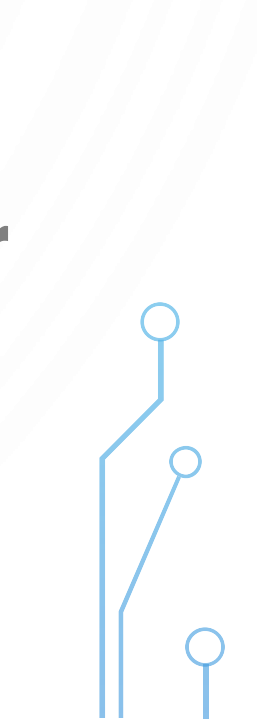

- **Nombre y datos de contacto del responsable y del DPO**
- **Finalidades del tratamiento**
- **Categorías de interesados**
- **Categorías de datos**
- **Categorías de destinatarios**
- **Transferencias internacionales de datos**
- **Plazos de conservación de los datos**
- **Descripción general de las medidas técnicas y organizativas de seguridad**



## 14. REGISTRO DE ACTIVIDADES DE TRATAMIENTO

**Los registros deberán constar por escrito, incluso en formato electrónico.**

**Se recomienda que los Departamentos correspondientes sean los responsables de mantener actualizado este RAT y comunicar al DPO las modificaciones que se realicen en el mismo.**



## 15. MEDIDAS TÉCNICAS Y ORGANIZATIVAS

**Art. 32 RGPD:** Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo

## 16. OBLIGACIONES DE LOS EMPLEADOS (CON ACCESO A DATOS)

- Llevar a cabo el Registro de Actividades de Tratamiento y mantenerlo actualizado.
- Comunicar las modificaciones realizadas en el registro al DPO.
- Comunicar al DPO los proyectos que implican tratamiento de datos personales
- Recoger el consentimiento siempre que sea necesario.
- Cumplir con el derecho de información, utilizando los modelos de cláusulas aprobados en la empresa.
- Seleccionar diligentemente a los encargados de tratamiento y firmar los modelos de contratos aprobados en la empresa.
- Atender y/o comunicar al DPO las solicitudes de ejercicio de derechos.
- Cumplir con los procedimientos de protección de datos y utilizar los modelos facilitados.
- Cumplir con las medidas de seguridad establecidas.
- Comunicar al DPO las brechas de seguridad.
- Guardar confidencialidad sobre toda la información con datos personales.
- Consultar al DPO siempre que tenga dudas en la aplicación de estas obligaciones.
- Guardar evidencias del cumplimiento de sus obligaciones.

# 17. MEDIDAS DE SEGURIDAD

## Enfoque de aproximación al riesgo

### ¿Qué medidas son adecuadas para garantizar un nivel adecuado de riesgo?

- Seudonimización y cifrado de datos
- Aquellas que garanticen confidencialidad, integridad, disponibilidad de los sistemas y servicios
- Aquellas que permitan recuperar la disponibilidad de los datos en caso de incidencia
- Establecer procesos de verificación, evaluación y valoración que midan la eficacia de las medidas técnicas y organizativas para garantizar el cumplimiento del RGPD
- Auditorías regulares de la eficacia de estas medidas
- Otras medidas: nombrar un DPO, registro de actividades de tratamiento...

## 18. SEUDONIMIZACIÓN Y ANONIMIZACIÓN

**Seudonimización:** es el tratamiento de datos de carácter personal, de manera que ya no puedan atribuirse a un interesado sin utilizar información adicional. Reduce el vínculo que existe entre los datos de carácter personal y la persona a la que identifican.

**Anonimización:** cuando en ningún caso es posible la vinculación del dato con la persona a la que hubiese identificado.

# 19. CIFRADO DE DATOS

**El cifrado de datos reduce el riesgo en el tratamiento de datos personales. No se establece en qué supuestos es obligatorio, pero sí se considera una buena práctica.**

Las medidas técnicas y organizativas deberán establecerse teniendo en cuenta:

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

## 20. EVALUACIÓN DE IMPACTO

- Los responsables de tratamiento deberán realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados.
- El RGPD establece un contenido mínimo de las Evaluaciones de Impacto sobre la Protección de Datos, aunque no contempla ninguna metodología específica para su realización.
- Cuando el análisis de riesgo que las organizaciones lleven a cabo sobre los tratamientos iniciados con anterioridad a la fecha de aplicación del RGPD indiquen que esos tratamientos presentan alto riesgo para los derechos o libertades de los interesados, los responsables deberán realizar una EIPD sobre esos tratamientos.
- En los casos en que las EIPD hayan identificado un alto riesgo que, a juicio del responsable de tratamiento no pueda mitigarse por medios razonables en términos de tecnología disponible y costes de aplicación, el responsable deberá consultar a la autoridad de protección de datos competente.



## 21. VIOLACIONES DE SEGURIDAD DE LOS DATOS

El RGPD define las violaciones de seguridad de los datos, más comúnmente conocidas como “quiebras de seguridad”, de una forma muy amplia, que incluye todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del RGPD y deben ser tratadas como el Reglamento establece.

## 21.1 NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

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

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

## 21.1 NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

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

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.

## 21.1 NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

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

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.

## 22. DELEGADO DE PROTECCIÓN DE DATOS

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

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

## 22. DELEGADO DE PROTECCIÓN DE DATOS

¿Qué funciones tiene un delegado de protección de datos?

- Informar y asesorar al responsable o al encargado y a los empleados sobre sus obligaciones.
- Supervisar el cumplimiento del RGPD:
  - Responsabilidades.
  - Concienciación y formación.
  - Auditorías
- Asesorar acerca de la evaluación de impacto.
- Cooperar con la autoridad de control.
- Ser un puente de comunicación entre la autoridad de control y la empresa.