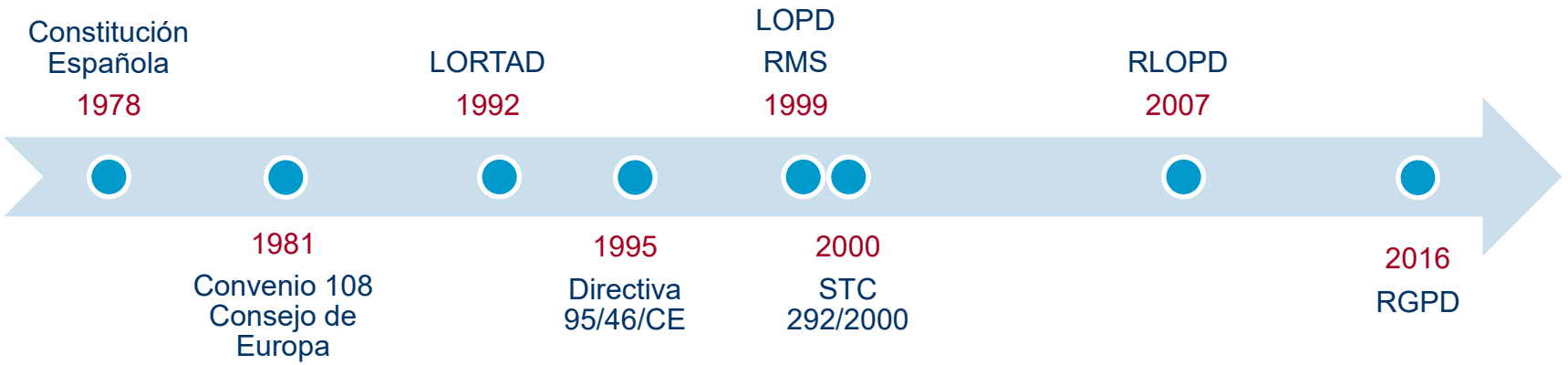
PROTECCIÓN DE DATOS PERSONALES

JORNADA DE LAS TIC

Cualquier entidad está obligada a cumplir, entre otras, obligaciones:

1. **Las obligaciones contables**
    - 1.1. Cuentas anuales
2. **Las obligaciones formales**
    - 2.1. Sujetos pasivos del Impuesto sobre Sociedades
    - 2.2. Sujetos pasivos del Impuesto sobre la Renta de las Personas Físicas
3. **Las obligaciones fiscales**
    - 3.1. Impuesto de la renta de las personas físicas
    - 3.2. Impuesto sobre sociedades
    - 3.3. Impuesto sobre el Valor Añadido
4. **Obligaciones Laborales**
5. **Obligaciones Varias**
    - 5.1. Obligaciones en materia de Prevención de Riesgos Laborales
    - 5.2. Obligaciones en materia de **Protección de Datos**
6. **Otras**

Antecedentes Normativos



Legislación Aplicable

Agencia Española de Protección de Datos – LEGISLACIÓN

¿Qué son los datos de carácter personal?

Cualquier información concerniente a **personas físicas identificadas o identificables**, tanto la relativa a su identidad (nombre, apellidos, dirección, teléfono …) a sus ocupaciones (estudio, trabajo …) datos bancarios, datos relativos a la salud, afiliación sindical y creencias, entre otros

¿Qué es el tratamiento de datos personales?

*"*Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas interconexiones y transferencias*"*

Las operaciones más frecuentes son:

- La *recogida organizada* de datos
- La *conservación y mantenimiento*
- La *cesión de los datos* a otras personas y/o entidades

Ámbito de aplicación.

El **ámbito material**, se aplica al tratamiento de datos personales, total o parcialmente de forma automatizada, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

El Reglamento amplía el **ámbito** de aplicación **territorial** a los responsables y los encargados del tratamiento no establecidos en la UE cuando las actividades tratamiento están relacionadas con la oferta de bienes o servicios o con el control del comportamiento de las personas, si tienen lugar en la UE.

- **Oferta de bienes o servicios:** Para determinar si dicho responsable o encargado ofrece bienes o servicios a **interesados que residan en la Unión**, debe determinarse **si es evidente** que el responsable o el encargado pueda ofrecer servicios al interesado en uno o varios de los Estados Miembros de la Unión (p.e tener la página web traducida en la lengua del Estado Miembro o el teléfono de contacto del Estado Miembro).
- **Monitorizar comportamientos** si, el mismo, tiene lugar dentro de la UE: para considerar que se está monitorizando se **deberá evaluar** si la persona física es objeto de un seguimiento, o análisis de comportamiento en Internet o el potencial uso posterior de técnicas que consistan en la elaboración de un perfil con el fin de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

Principios.

El Reglamento prevé que los responsables aplicarán las **medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el Reglamento**.

En términos prácticos, este principio requiere que las organizaciones analicen **que datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo.**

En síntesis, **este principio exige una actitud consciente, diligente, y proactiva por parte de las organizaciones** frente a todos los tratamientos de datos personales que lleven a cabo.

El RGPD, señala que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta **la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas**

Privacy by design

- En el momento de diseñar y desarrollar aplicaciones, servicios y productos que permitan o realicen un tratamiento de datos personales, **deberá tenerse en cuenta el derecho a la protección de datos desde el momento del diseño**.
- Las empresas también deberán aplicar este principio **al seleccionar, adquirir y usar aplicaciones**, servicios y productos para el tratamiento de datos personales.
- Por defecto, **sólo serán objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento**. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

¿Se realiza tratamiento de datos personales?.

- ¿Algún departamento de la empresa recoge o registra datos personales?
- ¿Algún departamento de la empresa organiza o estructura datos personales?
- ¿Algún departamento de la empresa conserva datos personales aunque no los utilice?
- ¿Algún departamento de la empresa adapta o modifica datos personales?
- ¿Algún departamento de la empresa extrae, consulta o utiliza datos personales?
- ¿Algún departamento de la empresa comunica, transmite, difunde o facilita el acceso a datos personales?
- ¿Algún departamento de la empresa extrae, consulta o utiliza datos personales?
- ¿Se utilizan los datos personales para evaluar, analizar o predecir el rendimiento profesional de un empleado?
- ¿Se utilizan los datos personales para evaluar, analizar o predecir la situación económica de una persona?
- ¿Se utilizan los datos personales para evaluar, analizar o predecir la salud de una persona?
- ¿Se utilizan los datos personales para evaluar, analizar o predecir la preferencias personales de una persona?
- ¿Se utilizan los datos personales para evaluar, analizar o predecir los intereses de una persona?
- ¿Se utilizan los datos personales para evaluar, analizar o predecir la fiabilidad de una persona?
- ¿Se utilizan los datos personales para evaluar, analizar o predecir el comportamiento de una persona?
- ¿Se utilizan los datos personales para evaluar, analizar o predecir la ubicación de una persona?
- ¿Se utilizan los datos personales para evaluar, analizar o predecir los movimientos de una persona?

Tratamientos excluidos

Actividades no comprendidas en el ámbito de aplicación del **Derecho UE**.

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).

Tratamientos excluidos

Tratamiento de datos de **personas fallecidas**

Tratamiento de Datos personales relativos a **personas jurídicas**, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.

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 UE** (p.e. Actividades relativas a la Seguridad Nacional).

El tratamiento de datos por los Estados Miembros en el ejercicio de las actividades relacionadas con la **política exterior y seguridad común de la Unión.**

Bases de legitimación para el tratamiento de datos.

El RGPD mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos necesita apoyarse en una base que lo legitime. También recoge las mismas bases jurídicas que contenía la Directiva y que reproduce la LOPD:

- **Consentimiento.**
- **Relación contractual.**
- **Intereses vitales del interesado o de otras personas.**
- **Obligación legal para el responsable.**
- **Interés público o ejercicio de poderes públicos.**
- **Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.**

Documentar e identificar claramente la base legal sobre la que se desarrollan los tratamientos

El consentimiento.

Libre, específico, informado e "**inequívoco**" A través de **declaraciones** o "**claras acciones afirmativas**"

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

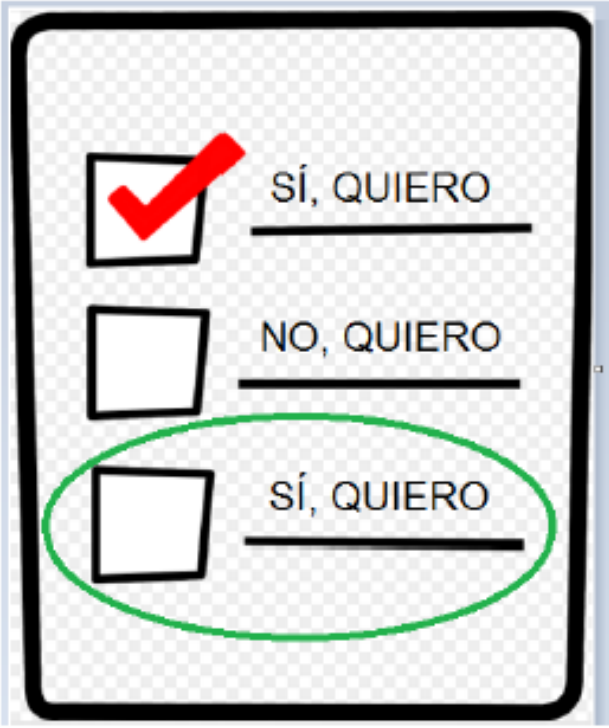
A diferencia del Reglamento de Desarrollo de la LOPD, **NO SE ADMITEN formas de consentimiento tácito o por omisión**, ya que se basan en la inacción.

Se contemplan situaciones en las que **el consentimiento, además de inequívoco, ha de ser explícito:**

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

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 consentimiento.



Supuestos en los que no se requiere consentimiento.

Ejercicio de las **funciones propias de las Administraciones públicas** en el ámbito de su competencia

Cuando se refiera a las **partes de un contrato o precontrato** de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento

Cuando el tratamiento de los daos tenga por finalidad **proteger un interés vital del interesado.**

Cuando los datos figuren en **fuentes accesibles al público** y su tratamiento sea necesario para la satisfacción de un interés legitimo, siempre que no se vulneren los derechos y libertades fundamentales del interesado

Datos especialmente protegidos

Está prohibido el tratamiento de datos personales que revelen:

- Origen étnico o racial.
- Opiniones políticas.
- Convicciones religiosas o filosóficas.
- Afiliación sindical.

NOVEDAD

- Datos genéticos.
- Datos biométricos dirigidos a identificar a una persona.
- Datos relativos a la salud.
- Vida u orientación sexual.

- **Datos genéticos**: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionan una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica.
- **Datos biométricos**: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de esta persona (imágenes faciales, datos dactiloscópicos, etc.).

Datos especialmente protegidos

No existirá la prohibición para el tratamiento de datos sensibles en los siguientes supuestos:

- El interesado **haya dado el consentimiento** explícito al tratamiento.
- El **tratamiento sea necesario para el cumplimiento de obligaciones y/o el ejercicio de derechos específicos** del responsable del tratamiento o del interesado en el ámbito del **Derecho laboral** y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados Miembros.
- El tratamiento sea **necesario para proteger los 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.
- El tratamiento sea 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 y/o sindical.
- El tratamiento se refiera a datos personales que el **interesado haya hecho manifiestamente públicos.**
- El tratamiento es necesario para la **formulación, el ejercicio o la defensa de reclamaciones** o cuando los tribunales actúen en ejercicio de su función judicial.
- El tratamiento es necesario por **razones de un interés público esencial**.
- El tratamiento es necesario para **fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social.**
- El tratamiento es necesario por **razones de interés público en el ámbito de la salud pública**, como la protección frente a amenazas transfronterizas graves para la salud.
- El tratamiento es necesario con **fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.**

Deber de informar.

- Los datos de contacto del Delegado de Protección de Datos, en su caso,
- La base jurídica o legitimación para el tratamiento,
- El plazo o los criterios de conservación de la información,
- La existencia de decisiones automatizadas o elaboración de perfiles,
- La previsión de transferencias a Terceros Países
- El derecho a presentar una reclamación ante las Autoridades de Control

Y además, en el caso de que los datos no se obtengan del propio interesado:

- El origen de los datos
- Las categorías de los datos

El **Derecho de transparencia** exige a los responsables del tratamiento a tomar las medidas pertinentes para proporcionar toda la **información en una forma concisa, transparente, comprensible y de fácil acceso, utilizando un lenguaje claro y sencillo**, y especialmente, para cualquier información dirigida a un menor.

¿Quién y cuándo debe informar?.

- La obligación de informar a las personas interesadas sobre las circunstancias relativas al tratamiento de sus datos **recae sobre el Responsable** del Tratamiento.
- La información se debe poner a disposición de los interesados **en el momento en que se soliciten los datos**, previamente a la **recogida o registro**, si es que los datos se obtienen directamente del interesado.
- 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 Responsable informará a las personas interesadas **dentro de un plazo razonable**, pero en cualquier caso:
  - antes de un mes desde que se obtuvieron los datos personales,
  - antes o en la primera comunicación con el interesado,
  - Antes de que los datos, en su caso, se hayan comunicado a otros destinatarios
- Esta obligación se debe cumplir **sin necesidad de requerimiento** alguno, y el responsable deberá **poder acreditar** con posterioridad que la obligación de informar ha sido satisfecha

¿Cuándo NO es preciso informar?

Únicamente no será necesario informar **cuando el interesado ya disponga de la información**, ni tampoco, en el caso de que los datos no procedan del interesado, cuando:

- la comunicación resulte imposible o suponga un esfuerzo desproporcionado,
- el registro o la comunicación esté expresamente establecido por el Derecho de la Unión o de los Estados miembros,
- cuando los datos deban seguir teniendo carácter confidencial por un deber legal de secreto

¿Dónde y cómo informar?

Los procedimientos de recogida de información son muy variados y en consecuencia, los modelos de informar a las personas interesadas deben adaptarse a las circunstancias de cada uno de los medios empleados para la recopilación o registro de datos.

- Formularios en papel.
- Navegación o formularios web
- Datos de actividad personal.
- Entrevista telefónica.
- Registro de aplicaciones móviles
- Datos de sensores

En cualquier caso, la información a las personas interesadas deber proporcionarse:

- con un lenguaje **claro y sencillo**,
- de forma **concisa, transparente, inteligible y de fácil acceso.**

¿Dónde y cómo informar?

Información básica sobre Protección de Datos	
Responsable	Ediciones Warren&Brandeis, S.A.
Finalidad	Gestión de la suscripción
Legitimación	Ejecución de un contrato
Destinatarios	No se cederán datos a terceros, salvo obligación legal
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web: http://www.warrenbrandeis.com/protecciondatos

¿Dónde y cómo informar?

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

Inscripción y notificación de ficheros.

El RGPD **suprime**, a partir del 25 de mayo de 2018, la necesidad de crear formalmente los ficheros y notificarlos al Registro de protección de datos de las autoridades de control.

Registro de actividades de tratamiento.

Los responsables y encargados del tratamiento tienen que llevar un **registro de las actividades (debe tener documentadas y a "DISPOSICIÓN" de la AEPD)** de tratamiento que lleven a cabo. Este registro debe contener, respecto de cada actividad, la información que establece el artículo 30 del RGPD.

Esta información incluye cuestiones como:

- **Nombre y datos de contacto del responsable y, en su caso, corresponsable, así como 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.**
- **Cuando sea posible, plazos previstos para la supresión de los datos.**
- **Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.**

Los **registros** deberán **constar por escrito, incluso en formato electrónico**. Asimismo, el encargado o el responsable del tratamiento deberán poner a disposición de la autoridad de control tales registros en el caso de que lo solicite.

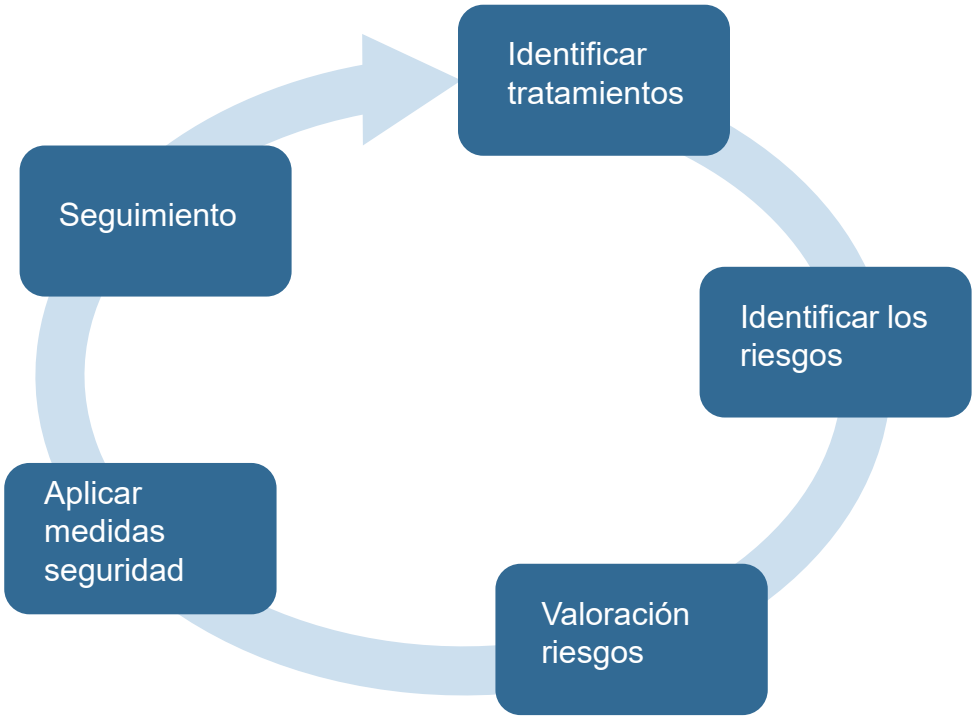
Medidas de seguridad.

ANTES

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

AHORA

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

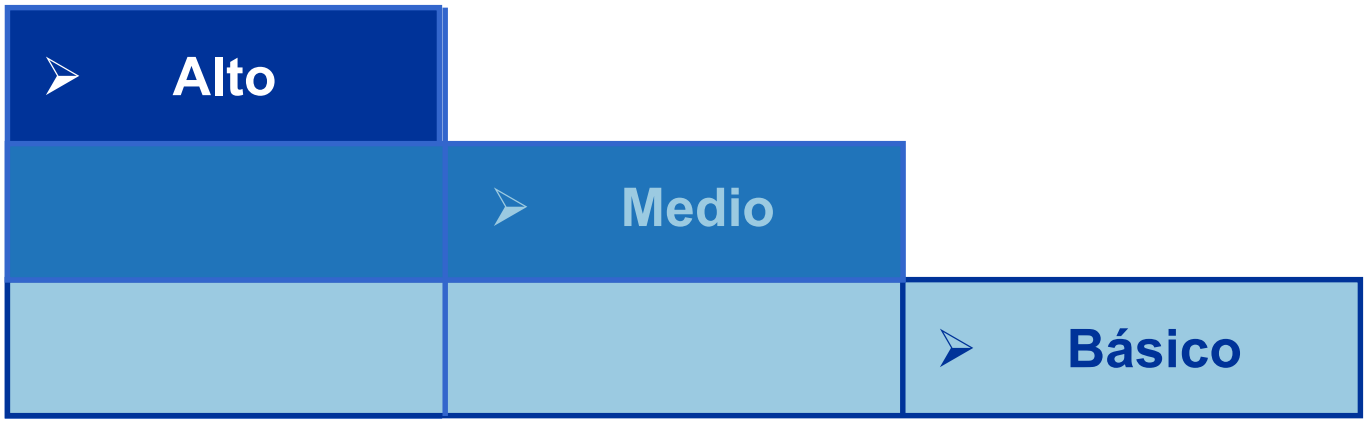


1.Calendario anual de revisiones y controles
2.Calendario anual de evaluaciones
3.Calendario anual de reuniones con los departamentos
4.Calendario anual de recogida de evidencias
5.Calendario anual de formación

ANTES

Niveles de Seguridad

La normativa clasifica las medidas de seguridad que debe adoptar su empresa en tres niveles según el tipo de datos que se traten :



9.- Requisitos organizativos de cumplimiento

ANTES

NIVEL	BASICO	MEDIO	ALTO
Naturaleza de los Datos	• Nombre • Apellidos. • Direcciones de contacto (físicas y electrónicas) • Teléfono (fijo o móvil) • Otros	• Infracciones penales. • Infracciones administrativas. • Información de hacienda pública. • Información de servicios financieros • Otros	• Ideología • Religión. • Creencias. • Origen racial. • Salud. • Vida sexual • Otros
Medidas de Seguridad	• Documento de seguridad • Régimen de funciones y obligaciones del personal • Registro de incidencias • Identificación y autenticación de usuarios • Control de acceso • Gestión de soportes • Copias de respaldo y recuperación	• Medidas de seguridad de nivel básico • Responsable de Seguridad • Auditoria bienal • Medidas adicionales de Identificación y autenticación de usuarios • Control de acceso físico	• Medidas de seguridad de nivel básico y medio • Seguridad en la distribución de soportes • Registro de accesos • Medidas adicionales de copias de respaldo • Cifrado de telecomunicaciones

Medidas de seguridad.

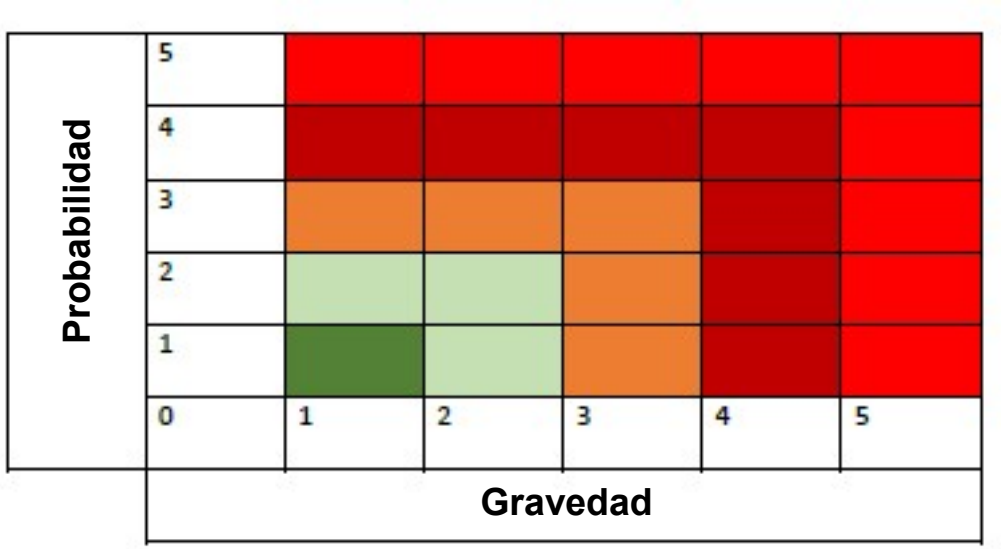
https://adl.incibe.es/

TRATAMIENTO	RIESGO INHERENTE	CONTROL	RIESGO RESIDUAL
	Riesgo que entraña el tratamiento si no hay ningún tipo de control	Efecto mitigador que genera la existencia de un control	Riesgo que permanece tras la aplicación del control

Medidas de seguridad.

probabilidad	
Descripción	nivel
inminente	5
muy probable	4
probable	3
poco probable	2
improbable	1

gravedad	
Descripción	nivel
extremadamente grave	5
significativamente grave	4
grave	3
leve	2
irrelevante	1



- Análisis de probabilidad de que se materialice el riesgo.
- Análisis del impacto económico que tendría el riesgo en caso de materializarse.
- Análisis del impacto en el negocio en caso de materializarse el riesgo.
- Análisis del impacto reputacional.

Medidas de seguridad.

- Mecanismos de **seudonimización y de cifrado de datos personales.**
- Sistemas que garanticen la **confidencialidad, integridad, disponibilidad y resistencia permanentes de los sistemas y servicios de tratamiento.**
- Sistemas que ayuden **a restaurar la disponibilidad y el acceso a los datos** personales de forma rápida en caso de accidente físico o técnico.
- Establecer **procesos de verificación, evaluación y valoración que midan la eficacia de las medidas técnicas y organizativas** para garantizar la seguridad del tratamiento.

Obligaciones del responsable del tratamiento.

- El responsable deberá **aplicar las medidas técnicas y organizativas apropiadas** a fin de que se pueda garantizar y acreditar que el tratamiento es acorde al Reglamento.
- Para ello, el responsable deberá tener en cuenta la **naturaleza, el ámbito, el contexto y los fines del tratamiento que se llevan a cabo en la empresa.**
- El responsable, cuando aplique tales medidas técnicas y organizativas, deberá considerar los **riesgos de diversa probabilidad y gravedad que puede entrañar el tratamiento de los datos para los derechos y libertades de las personas**.
- Tales medidas deberán ser **revisadas y actualizadas periódicamente.**
- El responsable deberá **cooperar con la autoridad de control** que lo solicite en el desarrollo de sus funciones.
- El responsable del tratamiento deberá **elaborar y mantener actualizadas las políticas de protección de datos**, como otra medida más, siempre que sean proporcionadas en relación con las actividades de tratamiento.
- El responsable, a pesar de no ser obligatorio, para **acreditar el cumplimiento de las obligaciones**, podrá adherirse a:
  - Códigos de conducta.
  - Cualquier mecanismo de certificación contemplado en el Reglamento.
- Cuando el tratamiento no requiera de identificación, el responsable no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir con el Reglamento.
- Cuando el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado le informará de ser posible.

Relaciones Responsable - Encargado.

ANTES

La Directiva 95/46 y en general las leyes nacionales de trasposición se centran en la actividad de los responsables.

AHORA

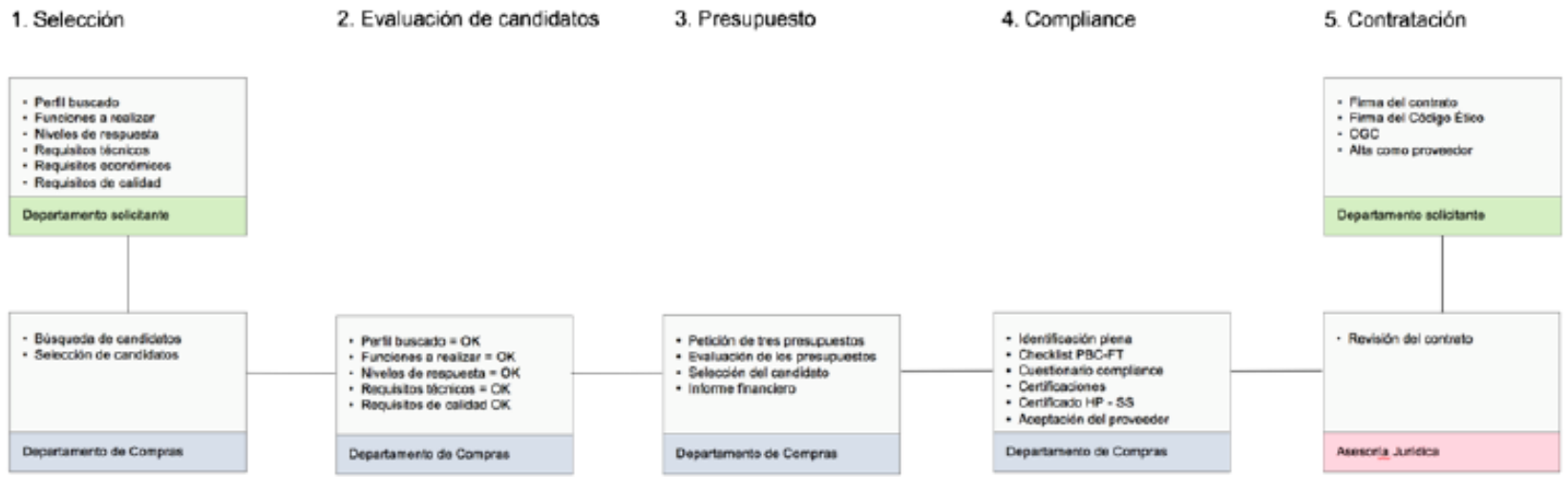
El RGPD, por el contrario, **contiene obligaciones expresamente dirigidas a los encargados**

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

- En determinadas materias **los encargados tienen obligaciones propias** que establece el RGPD, que no se circunscriben al ámbito del contrato que los une al responsable, y que pueden ser supervisadas separadamente por las autoridades de protección de datos. Por ejemplo:
  - Deben mantener un registro de actividades de tratamiento.
  - Deben determinar las medidas de seguridad aplicables a los tratamientos que realizan.
  - Deben designar a un Delegado de Protección de Datos en los casos previstos por el RGPD.

- Los encargados **pueden adherirse a códigos de conducta o certificarse** en el marco de los esquemas de certificación previstos por el RGPD.

Relaciones Responsable - Encargado.



Contenido del contrato de encargado

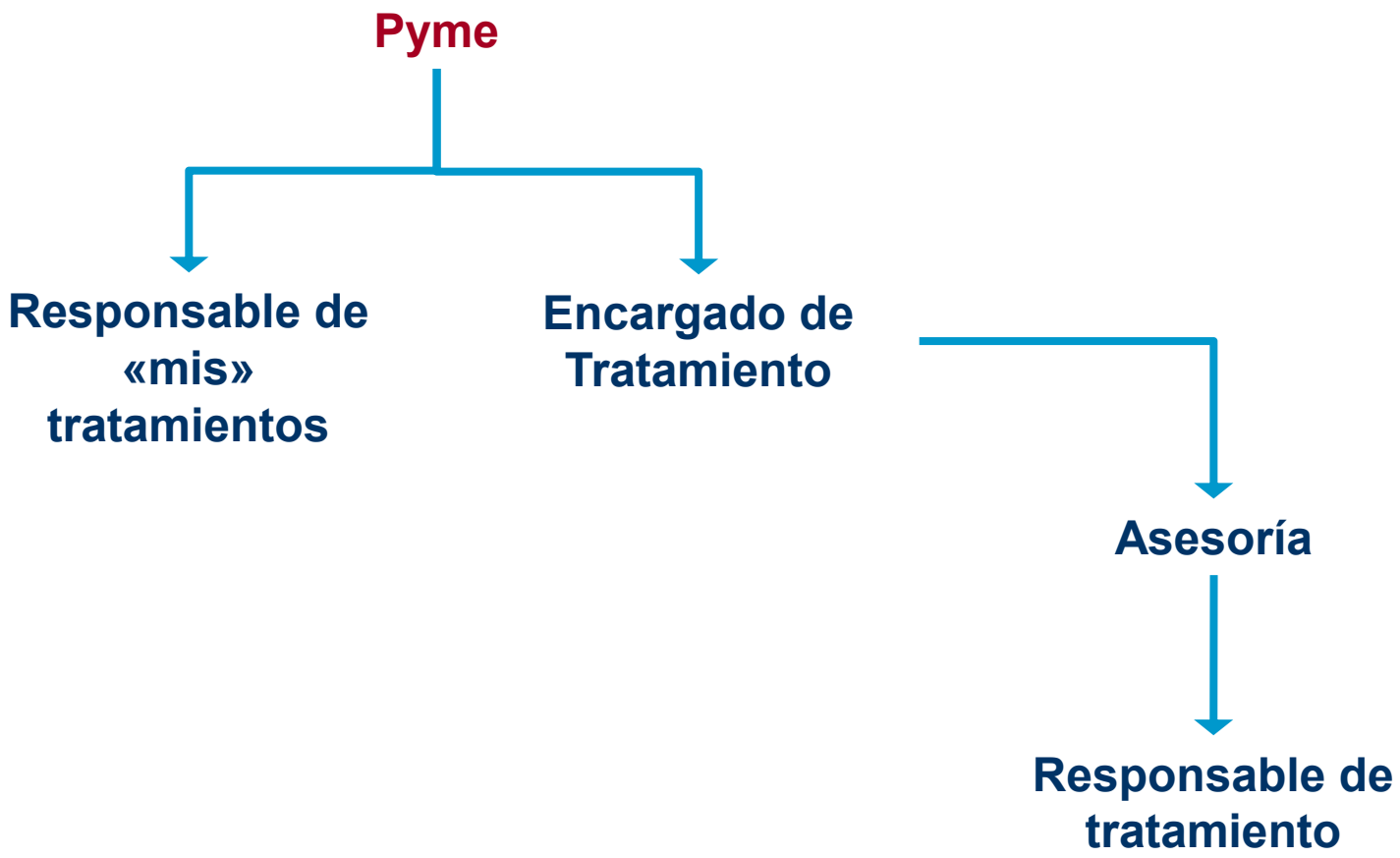
Las relaciones entre el responsable y el encargado deben formalizarse en un **contrato o en un acto jurídico** que vincule al encargado respecto al responsable.

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

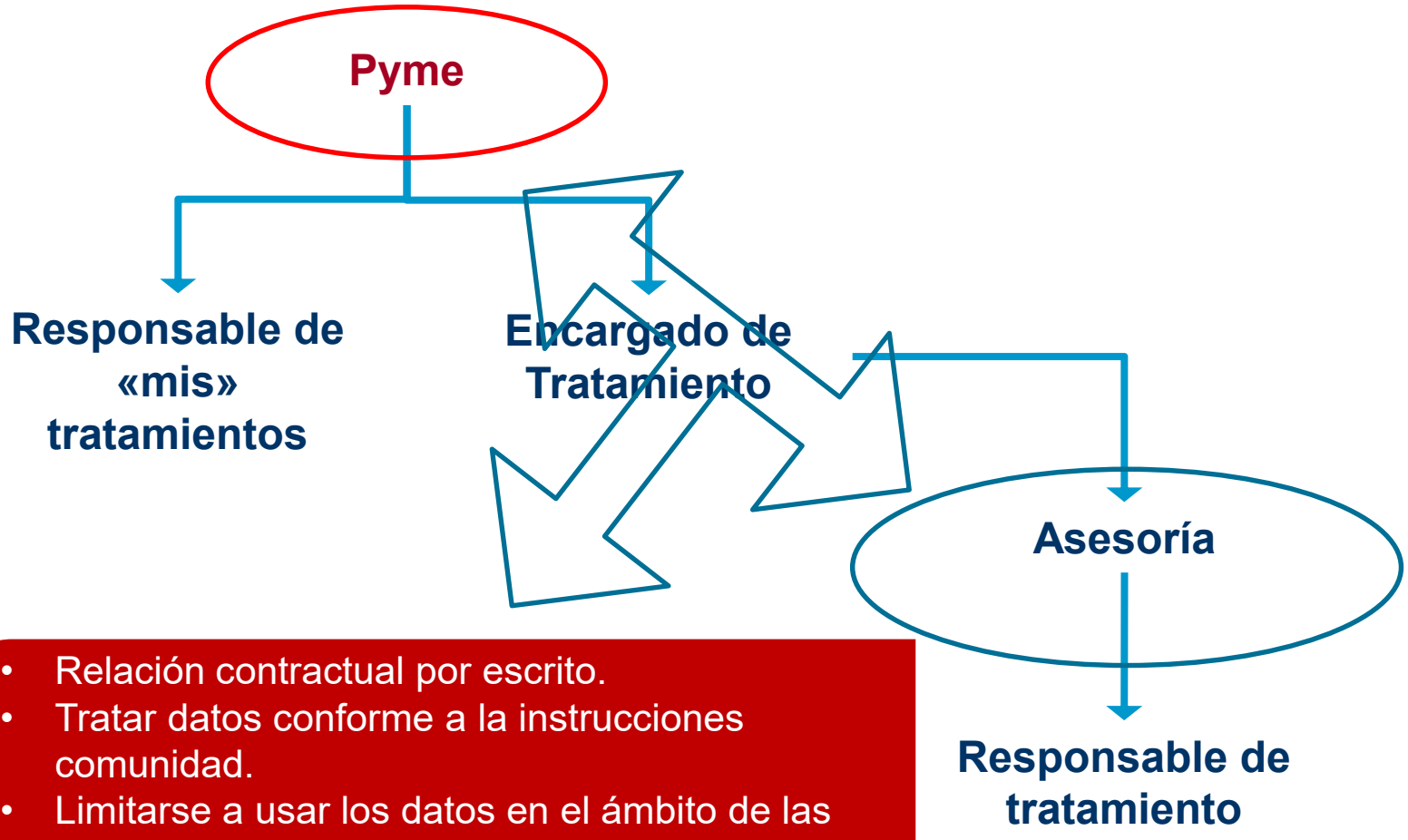
- Objeto del tratamiento.
- Duración del tratamiento.
- Naturaleza del tratamiento.
- Finalidad del tratamiento.
- Tipo de datos personales.
- Categoría de interesados.
- Obligaciones y derechos del responsable.

Los **contratos de encargo concluidos con anterioridad a la aplicación del RGPD en mayo de 2018 deben modificarse y adaptarse para respetar este contenido**, sin que sean válidas las remisiones genéricas al artículo del RGPD que los regula.

¿Cuál es mi figura?



¿Cuál es mi figura?



- Relación contractual por escrito.
- Tratar datos conforme a la instrucciones comunidad.
- Limitarse a usar los datos en el ámbito de las funciones de la comunidad.
- Devolver los datos al finalizar la relación.
- Aplicar medidas de seguridad.
- Secreto / confidencialidad

Derecho de los interesados.

Catalogo tradicional con tres novedades.

- Acceso.
- Rectificación.
- Derecho al borrado y **al "olvido".**
- **Limitación del tratamiento.**
- **Portabilidad.**
- Oposición

Información y Transparencia

Acceso, rectificación y oposición

Supresión/Olvido

Portabilidad de los datos

Limitación del tratamiento

Derecho al olvido.

- No está considerado un derecho autónomo o diferenciado de los clásicos derechos ARCO, sino la consecuencia de la aplicación del derecho al borrado de los datos personales.

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

- Datos que ya no son necesarios en relación con la finalidad que fueron recogidos.
- El interesado retira el consentimiento del tratamiento con base a que dicho consentimiento fue prestado de forma voluntaria, mediante consentimiento expreso y ahora tiene el mismo derecho de retirarlo.
- Oposición al tratamiento de datos personales.
- Que los datos personales hayan sido tratados ilegalmente.
- Datos borrados por el cumplimiento de una obligación legal en Derecho de la UE o del Estado Miembro al que esté sujeto el responsable.
- Los datos de un menor de 16 años recogidos con la autorización de los padres.

Limitación de tratamiento

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

- **Se puede solicitar la limitación cuando:**

  - Cuando el interesado **impugne la exactitud** de los datos personales.
  - 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**.

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

  - Con el consentimiento del interesado
  - Para la formulación, el ejercicio o la defensa de reclamaciones
  - Para proteger los derechos de otra persona física o jurídica.
  - Por razones de interés público importante de la Unión o del Estado miembro correspondiente

Portabilidad

El interesado tiene derecho a **transmitir sus datos a otro responsable sin obstáculos** por parte del responsable al cual le han sido proporcionados, cuando:

- El tratamiento se basa en el consentimiento.
- El tratamiento se haga a través de medios automatizados.

En el ejercicio de su derecho a la portabilidad de los datos, el interesado tiene derecho a que los datos se transmiten directamente desde el responsable al otro responsable, siempre que sea técnicamente factible

Notificación de “violaciones de seguridad de los datos”.

- **Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.**
- La **notificación de la quiebra** a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.
- La notificación ha de incluir un contenido mínimo:
  - la naturaleza de la violación.
  - categorías de datos y de interesados afectados.
  - medidas adoptadas por el responsable para solventar la quiebra.
  - si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados
- **Los responsables deben documentar todas las violaciones de seguridad.**
- En los casos en que sea probable que la **violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados**, la notificación a la autoridad de supervisión deberá complementarse con una **notificación dirigida a 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.
- El RGPD añade a los contenidos de la notificación **las recomendaciones sobre las medidas que pueden tomar los interesados** para hacer frente a las consecuencias de la quiebra.

DOCUMENTO DE SEGURIDAD

Es el núcleo central de toda política de protección de datos de carácter personal, pues **contiene políticas, normas y procedimientos** por los cuales se va a regir la organización en el tratamiento de los datos de carácter personal.

Es un manual que debe reflejar la realidad de los procedimientos de una organización en relación con el tratamiento de los datos de carácter personal.

En el mismo se ***recogen todas aquellas medidas de carácter técnico, jurídico y organizativo*** que una organización adopta con el objeto de proteger o garantizar la seguridad de los datos personales que puedan existir, tanto en sus sistemas de información como en sus ficheros manuales o no automatizados.

Ha de ser un documento cuya ***vigencia*** esta relacionada con el ***funcionamiento diario*** *de la organización* y en las personas que la conforman.

Es decir, que sea un documento ***vivo, actualizado y revisado***
a efectos de contemplar las nuevas situaciones con respecto al uso de la información.

Algunos procedimientos básicos a tener en cuenta:

PROCEDIMIENTOS RELATIVOS A FICHEROS AUTOMATIZADOS

- Control de Acceso Lógico
- Copias de Seguridad
- Correo Electrónico

PROCEDIMIENTOS RELATIVOS A FICHEROS AUTOMATIZADOS

- Criterios de archivo
- Dispositivos de almacenamiento
- Custodia de soportes
- Medidas de Traslado de documentación
- Control de Copia y/o Reproducción (nivel alto)
- Áreas Restringidas (nivel alto)

Algunos procedimientos básicos a tener en cuenta:

PROCEDIMIENTOS COMUNES A AMBOS TIPOS DE FICHEROS

- Gestión de Usuarios
- Gestión de Incidencias
- Gestión de Soportes y Documentos
- Desechado y Reutilización de Soportes y Documentos
- Gestión de ficheros temporales o copias de trabajo de
- documentos
- Medidas de Seguridad Adicionales
- Control de lo dispuesto en el Documento de Seguridad:
- AUDITORÍA.
- **Atención al ejercicio de los derechos A.R.C.O.**

¿Influye la ubicación del fichero?

- Normalmente, es el propio administrador de fincas quién se encarga de la custodia de la información, tanto por disponibilidad como por disponibilidad a la hora de prestar los servicios contratados.

Administradores de Fincas

→ **Custodian la información**

- **Recoger en un contrato las obligaciones de custodia INCLUYENDO la llevanza del documento de seguridad si así se estableciese.**
- **Implementar las medidas de seguridad adecuadas al nivel requerido por el fichero**

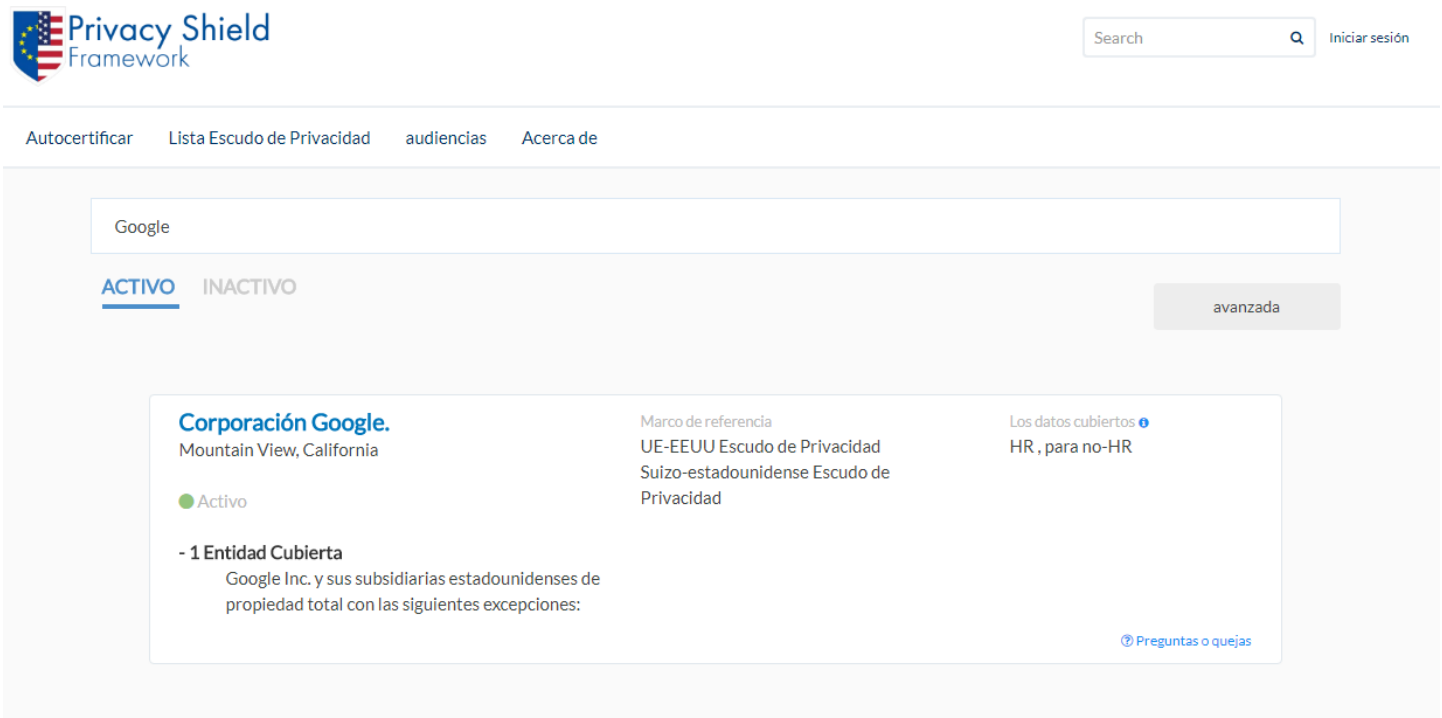
Transferencia internacional de datos

- Se **mantienen las transferencias de datos en aquellos países** en los que la **Comisión**, haya decidido que se garantiza un nivel de protección adecuado, sin que dicha transferencia **requiera ninguna autorización específica.**
- La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una **lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales**, respecto de los cuales haya decidido que se garantiza, o ya no, un **nivel de protección adecuado**.
- A **falta de decisión**, el responsable o el encargado del tratamiento sólo podrá transmitir datos a un tercer país u organización internacional si hubiera ofrecido **garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.**

Transferencia internacional de datos

Transferencia internacional de datos a EEUU

Puedes acceder a la lista de empresas que ya se han adherido al Privacy Shield a través del siguiente enlace: https://www.privacyshield.gov/welcome



Delegado de Protección de Datos (DPO)

Deberá existir en responsables y encargados cuando:

- tratamiento se realice por **autoridad u organismo público.**
- las actividades principales de responsable o encargado consistan en operaciones de tratamiento que **requieran una observación habitual y sistemática de interesados a gran escala.**
- las actividades principales de responsable o encargado consistan en el **tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales**

También habrán de designarlo cuando así lo establezca el derecho de la Unión o de los Estados Miembro.

El delegado de protección de datos tendrá entre otras las siguientes funciones:

- **Informar y asesorar al responsable o al encargado** y a los trabajadores sobre las **obligaciones** que impone la normativa de protección de datos.
- **Supervisar el cumplimiento de la normativa.**
- **Asesorar** respecto de la **evaluación de impacto** relativa a la protección de datos.
- **Cooperar con la autoridad de control.**
- Prestar la debida **atención a los riesgos asociados a las operaciones de tratamiento**, teniendo en cuanta la naturaleza, el alcance, el contexto y fines del tratamiento.
- **Atender a los interesados.**
- **Mantener el secreto o la confidencialidad** en lo que respecta al desempeño de sus funciones.

Delegado de Protección de Datos (DPO)

- Nombramiento basado en:

  - **Cualidades profesionales**
  - **Conocimientos especializados** del Derecho
  - **Práctica en materia de protección de datos.**
  - **Capacidad para desempeñar las tareas** que tiene designadas en el Reglamento.

- Relación **laboral** o mediante **contrato de servicios**
- Podrá desempeñar **otras funciones**, si no hay conflicto de intereses
- No podrá recibir **ninguna instrucción** en lo que respecta al desempeño de dichas funciones
- No podrá ser destituido ni sancionado por desempeñar sus funciones
- **Rendirá cuentas** directamente al **más alto nivel jerárquico**
- Podrá ser **contactado por interesados y APD**

¿Qué entendemos por "tratamiento a gran escala"?

Los tratamientos a gran escala son aquellas **operaciones de tratamiento que persiguen tratar una cantidad considerable de datos personales que afectan a un gran número de ciudadanos** con la probabilidad de existir un alto riesgo para los derechos y libertades de los mismos.

¿Cuándo se considera un "tratamiento habitual y sistemático?

Cuando se realiza un **seguimiento frecuente y repetitivo de personas** mediante un método de organización, clasificación u ordenación de sus datos.

Ejemplos de empresas afectadas:

Banca, aseguradoras, empresas de vigilancia que traten datos directamente como encargadas del tratamiento, empresas dedicadas a la elaboración de perfiles (ETT, marketing directo, Apps, etc.), medios de comunicación, etc.

Carga de la prueba

- Los responsables y encargados de tratamiento tienen la obligación de **demostrar que cumplen las disposiciones del Reglamento**. Se les atribuye la carga de la prueba en cualquier situación que se ponga en duda el cumplimiento de la normativa.
- El legislador hace referencia a demostrar la voluntad de cumplimiento **a través de políticas de cumplimiento normativo o de controles.**
- Es recomendable ante este tipo de obligaciones legales seguir el siguiente modelo de estructura normativa de tres niveles: políticas, normas y procedimientos.

Carga de la prueba

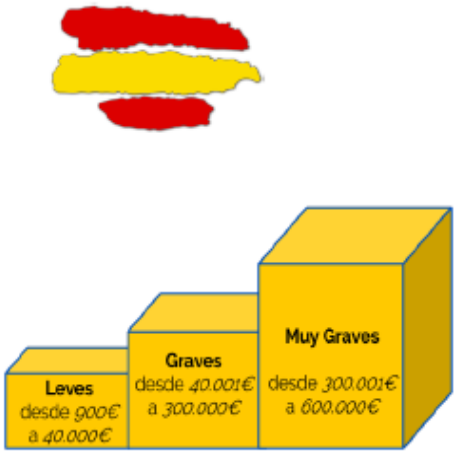
Fase del ciclo de vida de una evidencia	Ejemplo
Aplicación de un control	Control de acceso a una base de datos médica
Comprobación de la eficacia del control	Intento de acceso con una contraseña incorrecta
Obtención de la evidencia de la eficacia del control	Captura de la pantalla de denegación de acceso
Sellado de tiempo de la evidencia	Sellado de tiempo del PDF con la captura de pantalla
Introducción de la evidencia en el repositorio	Introducción en el sistema de gestión documental
Custodia de la evidencia	Conservación por parte de la empresa o de un tercero
Actualización del repositorio con nuevas versiones de la evidencia	
Aportación de la evidencia a un procedimiento judicial	

Carga de la prueba

1	Asegurar que en todos los tratamientos de datos se apliquen, desde la fase del diseño y por defecto, las medidas técnicas y organizativas adecuadas para cada tratamiento.
2	Revisar y garantizar la efectiva aplicación de las políticas, normas y procedimientos establecidos.
3	Identificar las políticas, normas y procedimientos que se encuentren desactualizados.
4	Coordinar con recursos humanos las sanciones a aplicar a aquellos empleados que no cumplan con las normas internas de protección de datos establecidas por la empresa.
5	Crear y gestionar un repositorio de evidencias.
6	Realizar formaciones a los distintos departamentos en relación al tratamiento de datos que realice cada uno de ellos.
7	Solicitar la adhesión a un código de conducta o certificación, en el caso de que una asociación sectorial suficientemente representativa lo haya desarrollado.

- Cantidad deberá modularse atendiendo a circunstancias del caso
- Aplicables a responsables y encargados
- Esquema básico de infracciones y sanciones
  - Multa hasta 10 M € o para empresas, optándose por la de mayor cuantía, hasta el 2 % de volumen de negocio anual a nivel mundial
    - Obligaciones de responsable o encargado
    - Obligación de organismos de certificación
    - Obligaciones de organismos de supervisión de códigos de conducta
  - Multa hasta 20 M € o hasta el 4%
    - Principios básicos
    - Derechos
    - Transferencias internacionales..
    - Incumplimiento de resoluciones de APD

Sanciones



- **NO contempla una graduación de sanciones (leve, grave y muy grave).**

10 millones de euros	2% Volumen negocio
20 millones de euros	4% Volumen negocio

Naturaleza

Ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada. Actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones.

Funciones

De forma general se puede decir que la principal función de la APD es: **velar por el cumplimiento de la legislación** sobre protección de datos y **controlar su aplicación**, en especial **en lo relativo a los derechos** de información, acceso, rectificación, oposición y cancelación de datos.

Sus funciones en **relación a quién trata los datos** son:

- Emitir autorizaciones previstas en la Ley.
- **Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos.**
- Requerir medidas de corrección.
- **Ejercer la potestad sancionadora.**
- Recabar ayuda e información que precise.
- Autorizar las transferencias internacionales de datos.

ZONA VIDEOVIGILADA

LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS

PUEDE EJERCITAR SUS DERECHOS ANTE:

❑ **Instalación.**

Las cámaras **sólo podrán captar imágenes de interior o de zonas privadas**. No podrán captarse imágenes de la vía pública a excepción de una franja mínima de los accesos al inmueble. Tampoco podrán captarse imágenes de terrenos y viviendas colindantes o de cualquier otro espacio ajeno.

La contratación de un servicio de videovigilancia externo o la instalación de las cámaras por un tercero **no exime del cumplimiento de la legislación de protección de datos.**

❑ **Sistema de grabación**.

El sistema de grabación se ubicará en un lugar vigilado o de acceso restringido. A las imágenes grabadas accederá sólo el personal autorizado, que deberá introducir un código de usuario y una contraseña.

Las imágenes serán conservadas durante un **plazo máximo de un mes** desde su captación.

Calidad de los datos.

- Que se deben recoger sólo los datos personales **estrictamente necesarios** para las finalidades de que se trate relativas a la gestión ordinaria de asuntos de la comunidad de propietarios.
- Que se deben recabar los datos de los comuneros de forma leal y transparente.
- Que **no se deben usar los datos para finalidades distintas** con las establecidas y comunicadas a los copropietarios afectados.
- Que deberán establecerse **mecanismos de actualización** de la información y de verificación de dicha actualización.
- Que habrán de **cancelarse los datos personales de los comuneros de oficio, cuando ya no sean necesarios** para la finalidad o finalidades para las que se recogieron.

Conservación de datos.

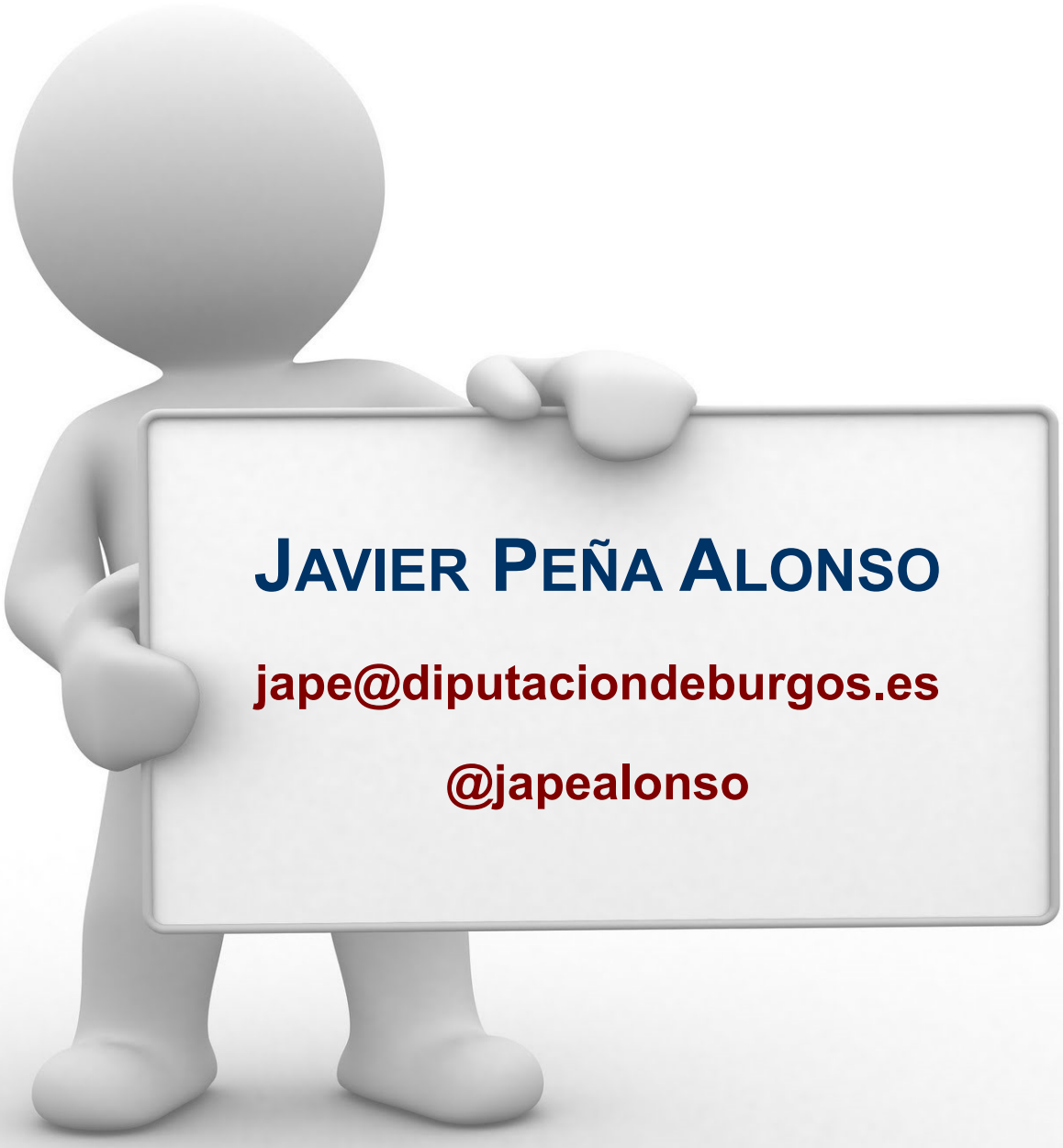
- Que deberán **definirse los plazos de conservación** de los datos personales de los propietarios afectados.
- Que deberán establecerse procedimientos para determinar que se han cumplido los plazos máximos de conservación de los datos personales de los copropietarios.

Deber de secreto.

- Que se deberá informar adecuadamente a todas las personas que tratan datos de carácter personal de la **obligación de guardar secreto** sobre los datos que conozcan en el ejercicio de sus funciones, de sus obligaciones y de las consecuencias de no cumplirlas.
- Que se **deberá dejar constancia de dicha información**.

Obligaciones en materia de seguridad.

- Que deberá elaborarse el correspondiente **documento de seguridad.**
- Que deberá llevarse a cabo, a través del documento de seguridad, la clasificación e **identificación del nivel de seguridad** en relación con cada uno de los ficheros o tratamientos de datos personales.
- Que deberá **formar e informar de sus obligaciones al personal que maneje datos de carácter personal,** definiendo claramente sus funciones, su deber de secreto, y sus posibilidades y limitaciones de acceso a los datos personales.
- Que deberá **controlar los accesos a la información de carácter personal**, gestionar adecuadamente los soportes de información, y garantizar la identificación y autenticación de los usuarios del sistema de información.
- Que debe existir un procedimiento para gestionar **las autorizaciones para la salida de dispositivos portátiles** que contienen datos personales fuera de los locales u oficina del responsable.



JAVIER PEÑA ALONSO

jape@diputaciondeburgos.es

@japealonso