Reglamento General de Protección de Datos

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 actual Directiva 95/46/CE de protección de datos
- Sustituye en aquello que lo contradiga a la LOPD y al RLOPD

Será aplicable 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

INTRODUCCIÓN

Objeto del RGPD

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.

ÁMBITO DE APLICACIÓN

Ámbito de aplicación general

- **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

ÁMBITO DE APLICACIÓN

Nuevos ámbitos 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

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).

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

D A T O S D E C A R Á C T E R P E R S O N A L

“ 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*** **“**

DATOS DE CARÁCTER PERSONAL

Persona física 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; o

«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 …

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)

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.)

  → dirigidos a identificar de manera unívoca a una persona física

CATEGORÍAS ESPECIALES DE DATOS

Regla general:

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)

T R ATA M I E N T O S D E D AT O S

RESPONSABLE Y ENCARGADO

- **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 ;

- **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;

- **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 ;

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.

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.

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 lícito 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.

P R I N C I P I O D E R E S P O N S A B I L I D A D P R O A C T I V A

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

L I C I T U D D E L T R ATA M I E N T O

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 legitimo** siempre que, sobre dichos intereses, no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales

A G E N C I A E S PA Ñ O L A D E P R O T E C C I Ó N D E D AT O S

Con el RGPD se mantienen, como es el caso de la AEPD, 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.

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.

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)

El consentimiento debe darse para todas las actividades de tratamiento y para todos los fines

DERECHO DE INFORMACIÓN

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

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

- la procedencia de los datos
- las categorías de datos

DERECHOS

TÍTULO III. LOPD
Derechos de las personas

- Derecho de acceso
- Derecho de rectificación
- Derecho de cancelación
- Derecho de oposición

CAPÍTULO III. RGPD
Derechos del interesado

- Derecho de acceso
- Derecho de rectificación
- Derecho de supresión ("derecho al olvido")
- Derecho a la limitación del tratamiento
- Derecho a la portabilidad de los datos
- Derecho de oposición

DATOS DE CONTACTO

Anteproyecto de LOPD

Un responsable del tratamiento podrá alegar que tiene un **interés legítimo** para tratar los **datos de contacto** de las personas físicas que presten servicios en una empresa:

- Si únicamente trata los datos imprescindibles para localizar profesionalmente a dicho contacto
- Si trata estos datos con la única finalidad de mantener relaciones con dicha empresa

Igualmente, un responsable del tratamiento podrá alegar que tiene un interés legítimo para tratar los datos de **empresarios individuales** , siempre que no se traten dichos datos para entablar una relación con los mismos como personas físicas.

C O N T R AT O S C O N E N C A R G A D O S

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

MEDIDAS DE SEGURIDAD

Enfoque de aproximación al riesgo

¿Qué posibles escenarios de riesgo (PER) pueden llegar a afectar a los derechos y libertades de los individuos?

- Den lugar a discriminación, usurpación de la identidad, pérdidas financieras, daño para la reputación, pérdida de confidencialidad …
- Afecten a los derechos y libertades de los individuos
- Datos sensibles, condenas e infracciones penales, datos de personas vulnerables (niños)
- Elaborar perfiles con el fin de crear o utilizar perfiles personales sobre rendimiento laboral, economía, salud, intereses personales …
- Gran cantidad de datos personales y afecten a un gran número de personas

MEDIDAS DE SEGURIDAD

Enfoque de aproximación al riesgo

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

- Seudonimización y cifrado de datos
- Aquellas que garanticen confidencialidad, integridad, disponibilidad y resiliencia 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 la seguridad del tratamiento y el cumplimiento del RGPD (listas de verificación, evaluación de riesgos, auditorías …)
- Auditorías regulares de la eficacia de estas medidas
- Otras medidas: nombrar a un DPO, certificados, registro de actividades de tratamiento …

SEUDONIMIZACIÓN Y ANONIMIZACIÓN

Es el tratamiento de datos de carácter personal, de manera que ya no puedan atribuirse a un interesado sin utilizar información adicional. Es decir, a una técnica que **reduciría el vínculo existente entre los datos de carácter personal y la persona a la que identifican** .

Sólo nos encontraremos ante un dato **anonimizado** cuando en ningún caso sea posible la vinculación del dato con la persona a la que hubiese identificado. Es decir, cuando sea **imposible** volver a identificar a la persona a través de ese dato.

C I F R A D O D E D AT O S

Al igual que la seudonimización, el cifrado de los datos (o de las comunicaciones) **reduce el riesgo** en el tratamiento de datos personales.

No se establece en qué supuestos es obligatorio, pero sí se considera una buena práctica establecerla desde el inicio (privacidad desde el diseño) para garantizar un tratamiento de datos más seguro. Principalmente, cuando existe un riesgo para los derechos y libertades de los individuos.

¿Qué debe tenerse en cuenta para decidir implantar ciertas medidas de seguridad como el cifrado o la seudonimización?

- el estado de la técnica
- los costes de aplicación
- la naturaleza, el alcance, el contexto y los fines del tratamiento,
- los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas

E V A L U A C I O N E S D E I M PA C T O

Supuestos obligatorios

- **Listas de la AEPD** (aún sin publicar)
  - Supuestos en los que **no es** obligatorio realizar una EIPD
  - Supuestos en los que **es** obligatorio realizar una EIPD

- **RGPD** : siempre que sea probable que un tratamiento entrañe un alto riesgo para los derechos y libertades de individuos, es decir, que puedan vulnerar gravemente los derechos y libertades de los individuos.

  - evaluación sistemática exhaustiva de aspectos personales (evaluación de perfiles)
  - tratamiento datos sensibles a gran escala
  - condenas e infracciones penales
  - **observación sistemática de zonas de acceso público a gran escala**

BRECHAS DE SEGURIDAD

Una **brecha de seguridad** es *"toda violación de la seguridad 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 autorizado a dichos datos"*

Principales causas de los incidentes de seguridad:

- Hackers
- Proveedores negligentes
- Publicación accidental
- Empleado desleal
- Ordenador perdido o robado
- USB perdido o robado

NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

Notificación de una violación de la seguridad a la AEPD

En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la AEPD **sin dilación indebida** y, de ser posible, a más tardar **72 horas** después de que haya tenido constancia de ella, salvo que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y libertados de los individuos.

Notificación de una violación de la seguridad a los interesados

En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la **AEPD sin dilación indebida** , cuando la misma entrañe un **alto riesgo** para los derechos y libertades de los interesados.

NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

Contenido de la notificación

- Descripción de la **naturaleza** de la violación de la seguridad de los datos personales, incluido, cuando sea posible, las categorías y el número aproximado de interesados **afectados** , así como también las categorías y el número aproximado de **registros** de datos personales afectados.
- El nombre y los datos de contacto del **DPO** (si lo hubiere) o de otro punto de contacto en la empresa del que se pudiere obtener información.
- Descripción de las **consecuencias** de la violación de la seguridad de los datos personales.
- Descripción de las **medidas** adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, así como también las medidas que se adopten para mitigar los posibles efectos negativos.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Formulario estandarizado de la AEPD: notificación de quiebras de seguridad para los operadores/proveedores de servicios de comunicaciones electrónicas

D E L E G A D O D E P R O T E C C I Ó N D E D A T O S

El Delegado de Protección de Datos (DPD) o, en inglés, “Data Protection Officer ” (DPO), es una nueva figura en la protección de datos personales.

Debe ser un especialista en derecho de protección de datos.

Es obligatorio para el responsable y el encargado de tratamiento designar a un DPO en los siguientes **supuestos** :

- **Tratamiento llevado a cabo por una autoridad u organismo públicos**
- **Que la actividad principal del responsable o encargado conlleve:**
  - **El tratamiento a gran escala de datos sensibles**
  - **El tratamiento de datos relativos a condenas e infracciones penales**
  - **Observación habitual y sistemática de interesados a gran escala**

DELEGADO DE PROTECCIÓN DE DATOS

Funciones

- 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 en las EIPD
- Supervisar que se implantan las medidas acordadas en las EIPD
- Cooperar con la autoridad de control
- Actuar como punto de contacto con la autoridad de control

Fases de las auditorías de Protección de Datos

1

Revisión de la documentación de la empresa

Se debe comprobar que todos los contratos y acuerdos de confidencialidad estén firmados, y que se cuenta con el consentimiento expreso de los interesados.

2

Planificación previa de la auditoría

Durante la auditoría de Protección de Datos será necesario entrevistar al personal, por lo que se deben planificar estas entrevistas.

3

Análisis y documentación

Se debe analizar y verificar si se están cumpliendo todos los requisitos obligatorios en materia de Protección de Datos dentro de la empresa.

4

Creación y entrega del informe

Se debe elaborar un informe final en el que se detallarán aspectos a mejorar, posibles deficiencias y propuestas de mejora.

AUDITORIA RGPD

- **ÁREA DE TRABAJO:** Gestión de la privacidad
- **DESCRIPCIÓN:** Todos aquellos aspectos “burocráticos” dentro de la estructura, que están relacionados con el cumplimiento del RGPD.
- **CONTROLES:**
- Existencia de una política de privacidad adecuada
- Existencia de roles y responsables de diversos aspectos relacionados con la privacidad
- Existencia de normas internas sobre privacidad y seguridad
- Si es necesario, nombramiento y comunicación a la AEPD del DPD
- Auditorías LOPD/RGPD anteriores
- Si corresponde, normas corporativas vinculantes

- **ÁREA DE TRABAJO:** Legalidad de los tratamientos
- **DESCRIPCIÓN:** Aspectos relacionados con la base jurídica que soporta el tratamiento.
- **CONTROLES:**
- Comprobación de las bases jurídicas del tratamiento
- Comprobación de la existencia de los consentimientos necesarios
- Cláusulas informativas en contratos, entornos online y comunicaciones
- Si corresponde, comprobación de consultas a Listas Robinson

- **ÁREA DE TRABAJO:** Gestión de derechos
- **DESCRIPCIÓN:** Todos aquellos aspectos y procedimientos definidos para la gestión de los derechos de los usuarios.
- **CONTROLES:**
- Información sobre los diferentes derechos a los usuarios en los diversos entornos, online y offline
- Procedimientos de derecho
- Pruebas y controles del ejercicio de derechos
- Existencia o no de un canal centralizado de ejercicio de derechos
- Verificación de personas responsables

- **ÁREA DE TRABAJO:** Registro de Actividades de Tratamiento (RAT)
- **DESCRIPCIÓN:** Existencia y justificación del RAT
- **CONTROLES:**
- Existencia del RAT
- Inclusión, si corresponde, de nuevos tratamientos de datos
- Actualización, si corresponde, de los tratamientos de datos existentes
- Verificación de las bases jurídicas
- Revisión de las finalidades de cada uno de los RAT
- Entornos, procedimientos y aplicaciones que soportan cada RAT
- Comprobación de los plazos de conservación de los tratamientos

- **ÁREA DE TRABAJO:** Encargados de tratamiento
- **DESCRIPCIÓN:** Procesos relacionados con la gestión de los encargados de tratamiento con acceso a datos
- **CONTROLES:**
- Revisión y actualización del listado de encargados de tratamiento
- Revisión del procedimiento de idoneidad como encargado de tratamiento
- Revisión y actualización, si corresponde, de los contratos de encargo de tratamiento

- **ÁREA DE TRABAJO:** Corresponsabilidad en el tratamiento
- **DESCRIPCIÓN:** Procesos destinados a validar la corresponsabilidad de un tratamiento de datos
- **CONTROLES:**
- Revisión de los acuerdos de corresponsabilidad
- Revisión de los trabajos coordinados entre los responsables
- Información destinada al usuario sobre el acuerdo suscrito

- **ÁREA DE TRABAJO:** Transferencias internacionales de datos
- **DESCRIPCIÓN:** Revisión de los procesos de transmisión de información a terceros países fuera de la UE.
- **CONTROLES:**
- Revisión y actualización de destinos para la transferencia de datos
- Revisión de las garantías existentes en cada país destino
- Si existen, revisión de consultas a la AEPD

- **ÁREA DE TRABAJO:** Cumplimiento
- **DESCRIPCIÓN:** Medidas destinadas a garantizar el cumplimiento normativo dentro de la estructura.
- **CONTROLES:**
- Formación y acreditación de dicha formación al personal
- Documentos y/o planes de concienciación al personal
- Existencia de planes de revisión de cumplimiento periódicos
- Controles y KPI’s destinados a verificar el cumplimiento

- **ÁREA DE TRABAJO:** Delegado de Protección de Datos
- **DESCRIPCIÓN:** Procedimientos relacionados con la gestión de la figura dentro de la empresa.
- **CONTROLES:**
- Justificación de la existencia de la figura del DPD
- Nombramiento y comunicación a la AEPD
- Análisis y definición de las funciones

- **ÁREA DE TRABAJO:** Privacidad por defecto y desde el diseño
- **DESCRIPCIÓN:** Procesos de verificación de las políticas de privacidad por defecto y desde el diseño
- **CONTROLES:**
- Procedimientos y políticas de minimización de datos
- Procedimientos y políticas de conservación de datos
- Justificaciones para la implantación o no de la privacidad por defecto o desde el diseño

- **ÁREA DE TRABAJO:** Medidas de seguridad
- **DESCRIPCIÓN:** Medidas y procedimientos implantados para asegurar la información y el cumplimento normativo.
- **CONTROLES:**
- Existencia de una relación de medidas de seguridad
- Roles y perfiles implicados en su aplicación
- Existencia de Evaluaciones de Impacto o Análisis de Riesgos, cuando corresponda

- **ÁREA DE TRABAJO:** Notificación de brechas de seguridad
- **DESCRIPCIÓN:** Verificación de la existencia de procedimientos para la comunicación de brechas de seguridad y violaciones de datos ante la AEPD.
- **CONTROLES:**
- Procedimiento de verificación y comunicación de brechas
- Revisión de las comunicaciones de brechas existentes, si corresponde
- Procedimientos para restauración del estado de los datos tras el incidente

- **ÁREA DE TRABAJO:** Evaluación de impacto y análisis de riesgos
- **DESCRIPCIÓN:** Existencia y justificación del RAT
- **CONTROLES:**
- Existencia de evaluaciones de impacto y análisis de riesgo, según corresponda
- Existencia de comunicaciones a la AEPD, sobre la necesidad de una evaluación de impacto
- Metodologías utilizadas
- Evaluación de las medidas implantadas tras la evaluación de impacto o el análisis de riesgos