Las obligaciones en materia de Protección de Datos para la abogacía joven

Ponente: Javier Álvarez Hernando

6-5-2021
19:00 H.

AAj
AGRUPACIÓN DE LA ABOGACÍA JOVEN DE VALLADOLID

MARCO JURÍDICO

- Art. 18.4 CE
- La “constitucionalización” del derecho fundamental a la protección de datos:
  - –A) **Carta de Derechos Fundamentales de la Unión Europea: art. 8.1**
  - **–B) Artículo16.1 del Tratado de Funcionamiento de la UE (TFUE)**
- **Reglamento (UE) 2016/679** del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
- **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales.**
- **LOPD 15/1999.- Vigente. Arts. 23 y 24.** Referidos a los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado.

MARCO JURÍDICO

PROTECCIÓN DE DATOS COMO DERECHO AUTÓNOMO

- ✓ **Poder de disposición y control sobre los propios datos personales**
- ✓ **Facultad de decidir sobre**
  - **Qué datos se pueden recabar**
  - **Qué datos ceder a un tercero**
- ✓ **Facultad de conocer**
  - **Quién posee esos datos personales**
  - **Para qué los posee**
  - **A quién se van a ceder**
- ✓ **Facultad de oponerse a su posesión o uso**
  - **Solicitando su rectificación o supresión**
  - **Revocando el consentimiento para su uso**

- El derecho a la protección de datos se considera como un **derecho fundamental (no absoluto).**
- DF exclusivo de **personas físicas.**

Algunos conceptos y definiciones (art. 4)

¿QUÉ ES UN DATO PERSONAL?

toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona

¿CUÁNDO UNA PERSONA ES IDENTIFICABLE?

Atención a factores objetivos, (costes y tiempo necesarios para la identificación, tecnología disponible o avances tecnológicos).

¿CUÁLES SON LAS CATEGORÍAS ESPECIALES DE DATOS?

Origen étnico o racial, opiniones políticas, religión, convicciones filosóficas, afiliación sindical, datos genéticos y biométricos (dirigidos a identificar de una manera unívoca a una persona), salud, vida y orientación sexual.

Algunos conceptos y definiciones (art. 4)

¿QUÉ ES UN 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

¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO?

Persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o conjuntamente con otros determine los fines y los medios del tratamiento

¿QUIÉN ES EL ENCARGADO DEL TRATAMIENTO?

Persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento

ÁMBITO DE APLICACIÓN MATERIAL

Artículo 2 RGPD

"1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

Necesidad de superar la idea de fichero como eje de la normativa de protección de datos, que descansa en el concepto de tratamiento. La noción de fichero es meramente residual para el caso de tratamiento no automatizado:

FICHERO: ***todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica***

EXCLUSIONES

- Actividades no comprendidas en el ámbito de aplicación del Derecho de la UE (**seguridad nacional**)
- Tratamiento por los Estados miembros en materia de política exterior y de seguridad común
- Tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas
- **Tratamientos sometidos a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales, o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública por las autoridades competentes** ***(Directiva 2016/680 y Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves)***
- Tratamiento por las instituciones, órganos y organismos de la UE (Reglamento (CE) 45/2001)
- Los datos de las personas fallecidas. **No se aplica el RGPD pero los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de éstas (lo recoge la LOPDGDD)**
- Datos de personas jurídicas

Ámbito de aplicación TERRITORIAL más amplio: el RGPD se aplica a responsables y a encargados:

- establecidos en la UE si tratan datos personales.
- no establecidos en la UE si realizan tratamiento de datos que deriven de la oferta de bienes y servicios (incluso gratis) destinados a ciudadanos europeos, o bien como consecuencia de la monitorización o seguimiento de su comportamiento (perfilado). Estas organizaciones deben designar un representante en la UE e informar de ello a los ciudadanos.

En conclusión, el RGPD….

- Es aplicable a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, y en relación con el tratamiento de sus datos personales.
- No aplica a las Personas jurídicas, pero sí a las personas físicas que presten servicios en aquellas.
- Tampoco se aplica a las actividades personales o domésticas, ni a las personas fallecidas.
- Las organizaciones no establecidas en la UE que ofrecen bienes o servicios a ciudadanos EU, o que vigilan su comportamiento se encuentran dentro del ámbito de aplicación del RGPD.

PRINCIPIOS

PROTECCIÓN DE DATOS

- **Licitud, lealtad y transparencia**
- **Minimización de datos**
- **Limitación de finalidad**
- **Exactitud**
- **Limitación del plazo de conservación**
- **Integridad y confidencialidad**
- **Responsabilidad proactiva**

Principios

- **Principio de licitud, lealtad y transparencia**, es decir, los datos personales no pueden ser recogidos de forma fraudulenta, desleal o ilícita. El tratamiento será lícito si cumple con alguna de las condiciones del art. 6 del RGPD. Además el responsable debe facilitar al interesado toda la información sobre el tratamiento de forma concisa, transparente, inteligible y de fácil acceso.

Principios

•**Principio de limitación de la finalidad**. Los fines para los que se recogen los datos personales deben ser determinados, explícitos y legítimos, y no serán tratados ulteriormente de forma incompatible con esos fines. No son fines incompatibles: el archivo en interés público, la investigación científica e histórica o los estadísticos, aunque podrán aplicarles garantías específicas, como anonimizarlos o, en algunos, casos seudonimizarlos.

Principios

Principio de limitación del plazo de conservación de los datos, es decir, sólo deben ser mantenidos, de forma que se permita la identificación, durante el tiempo necesario para los fines del tratamiento. Además se ha de informar al interesado, al tiempo de recoger los datos, de este plazo de conservación o de los criterios para determinarlo.

EJEMPLO:

Se conservarán durante el tiempo estrictamente necesario para cumplir con la finalidad para la que se obtuvieron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos.

Principios (2)

- **Principio de minimización de datos**. Los datos deben ser adecuados, pertinentes y limitados a los fines para los que se recogen. En este sentido, se podrán *seudonimizar*, es decir, tratar de manera que ya no puedan atribuirse al interesado sin utilizar información adicional que estará separada y protegida.
- **Principio de exactitud de datos**. Los datos han de ser exactos, correctos y completos, suprimiéndose o rectificándose, sin dilación, los que no estén actualizados o sean inexactos. El interesado tiene derecho a solicitar la rectificación de sus datos al responsable, que tendrá 1 mes para hacerlo.

Principios (3)

- **Principio de integridad y confidencialidad**, es decir, los tratamientos han de garantizar la seguridad adecuada de los datos, aplicando medidas técnicas u organizativas (en base a un análisis de riesgos) apropiadas para:
  - la protección contra el tratamiento no autorizado o ilícito, y
  - la protección contra su pérdida, destrucción o daño accidental.

POR TANTO, LA OBLIGACION DE CONFIDENCIALIDAD DERIVA DE:

- Principio de integridad y confidencialidad (art. 5.1.f).
- Secreto profesional.
- Fuente de la obligación: Derecho de la Unión Europea o nacional, estatutaria, contractual u otra….
- Art. 5 LOPDyGDD.

El principio de responsabilidad activa o «accountability».

- ✓ Una de las grandes novedades que presenta el RGPD es el denominado principio de responsabilidad activa (en su concepción anglosajona, *accountability*), que **viene a imponer al responsable, y al encargado del tratamiento, estar en condiciones de demostrar que cumple con las previsiones normativas en materia de protección de datos de carácter personal.**

RESPONSABILIDAD PROACTIVA (ART. 24 RGPD)


Responsabilidad proactiva
Limitación plazo conservación
Integridad y confidencialidad
Exactitud
Licitud, lealtad, transparencia
Limitación de la finalidad
Minimización de datos

PRINCIPIO DE LICITUD

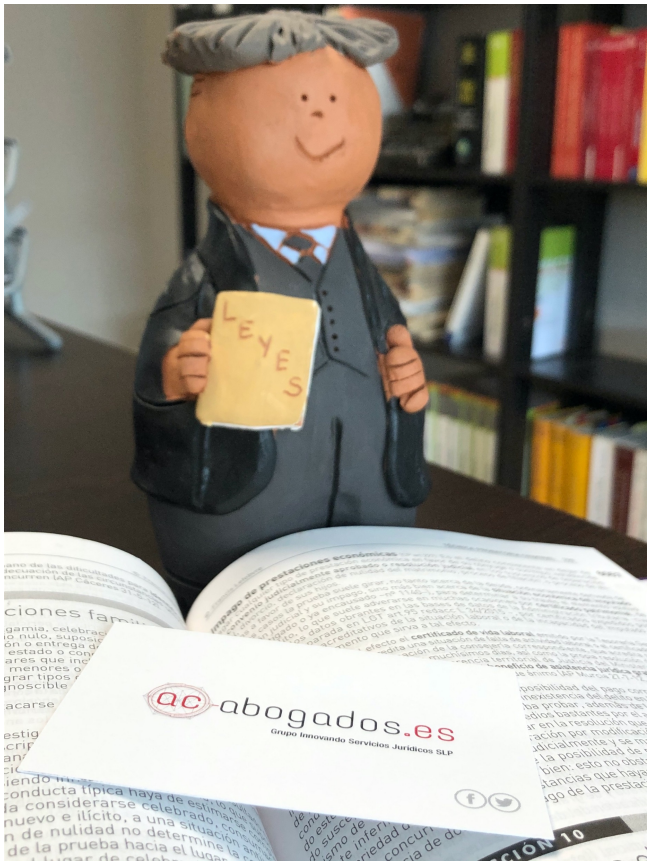
TODO tratamiento de datos personales exige una base jurídica que lo legitime, a saber (art. 6 RGPD):

- **Consentimiento** de afectado.
- Existencia de una **relación contractual**.
- Existencia de un **interés legítimo** prevalente del responsable o de terceros a los que se ceden o comunican los datos personales. **No aplicable a PRIORI la AAPP**.
- Justificado en una **necesidad vital** del interesado.
- Cuando resulte una **obligación legal** para el responsable del tratamiento.
- Exista un **interés público** o se derive del ejercicio de poderes públicos: *smart cities; servicios públicos de salud…*

✓ *En estos dos últimos casos (6.3 RGPD) esa base jurídica debe determinar la finalidad, y puede contener otras disposiciones específicas.*

Causas de legitimación del tratamiento de datos por abogados/as

La relación *abogado/cliente* tiene naturaleza de **arrendamiento de servicios**, y por lo tanto es una relación contractual (STS de 23 de mayo de 2006). El contrato de prestación de servicios se rige por el artículo 1544 del Código Civil. Teniendo esto en cuenta, debemos analizar la **legitimación en el tratamiento de datos**, por parte de los abogados/as o procuradores/as, que podría estructurarse conforme a la tabla siguiente--------



OPERACIÓN DE TRATAMIENTO DEL DESPACHO DE ABOGACIA	CAUSA DE LEGITIMACIÓN PARA EL TRATAMIENTO
Tratamiento de datos de clientes del despacho	- Artículo 6.1.b RGPD. Tratamiento sea necesario para la ejecución de un **contrato** en el que el interesado es parte. Es decir, el arrendamiento de servicios profesionales. - Artículo 6.1.f RGPD. Cuando el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan otros intereses o derechos. Este podría ser la causa de legitimación del tratamiento de datos en procedimientos de **jura de cuentas**, o la comunicación de datos de clientes "morosos" al **Registro de Impagados Judiciales** (el Considerando 47 RGPD se refiere al interés legítimo en tratamientos dirigidos a la prevención del fraude)

Tratamiento de datos de clientes asignados en turno de oficio	- **Artículo 6.1.c RGPD. Tratamiento es necesario para el cumplimiento de una obligación legal (Ley 1/1996, de 10 de enero, de Asistencia Jurídica Gratuita).**
Tratamiento de datos de la contraparte (en un procedimiento judicial o previo a su interposición)	- Artículo 6.1.c RGPD. Tratamiento es necesario para el cumplimiento de una obligación legal: artículo 24 CE. Existe una colisión de derechos fundamentales: protección de datos y derecho de defensa y tutela judicial efectiva (artículo 24 CE) debiendo prevalecer este último. Del mismo modo un despacho de abogacía trata datos (cediendo información a terceros) por exigencia legal, como, por ejemplo, por la Ley de Blanqueo de Capitales, normativa sobre Seguridad Social o exigencias frente a la Agencia Tributaria. - Artículo 6.1.f RGPD. Cuando el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan otros intereses o derechos.

Tratamiento de datos de potenciales clientes (remisión de presupuestos, un newsletter, diversas comunicaciones electrónicas, etc.)	- **Artículo 6.1.b RGPD. Tratamiento sea necesario para la ejecución de medidas precontractuales solicitadas por el interesado, como la solicitud de presupuestos previos.** - **Artículo 6.1.a RGPD. Consentimiento del interesado para uno o varios fines específicos.** - **Artículo 6.1.c RGPD. Tratamiento es necesario para el cumplimiento de una obligación legal: artículo 21 de la Ley 34/2002, en los casos de comunicaciones comerciales electrónicas.**
Videovigilancia del despacho	- Artículo 6.1.e RGPD. Existencia de interés público. El artículo 22 LOPDGDD dedicado a la videovigilancia determina que es posible llevar a cabo el tratamiento de datos de videovigilancia, con el fin de preservar la seguridad de las personas, bienes e instalaciones. La catalogación en esta causa de legitimación viene determinada por el preámbulo de la LOPDGDD.

Facturación y contabilidad	- **Artículo 6.1.b RGPD. Tratamiento sea necesario para la ejecución de un contrato en el que el interesado es parte.** - **Artículo 6.1.c RGPD. Tratamiento es necesario para el cumplimiento de una obligación legal, como normas tributarias.**
Recursos humanos o personal del despacho	- Artículo 6.1.b RGPD. Tratamiento sea necesario para la ejecución de un contrato en el que el interesado es parte. - Artículo 6.1.c RGPD. Tratamiento es necesario para el cumplimiento de una obligación legal: control horario.

CATEGORÍAS ESPECIALES DE DATOS

- ✓ No todos los datos concernientes a una persona son objeto del mismo nivel de protección, siendo considerados como **CATEGORIAS ESPECIALES o** especialmente protegidos los que se refieran a la origen étnico o racial; opiniones políticas; convicciones religiosas o filosóficas; afiliación sindical; datos genéticos y biométricos; datos de salud; vida u orientación sexual (art. 9 REPD).
- ✓ La regla general contemplada en el Reglamento es la prohibición del tratamiento de categorías especiales de datos (art. 9). No obstante, se recoge numerosas excepciones.

CATEGORÍAS ESPECIALES DE DATOS

REGLA GENERAL: QUEDA PROHIBIDO SU TRATAMIENTO

EXCEPCIONES

- **Consentimiento (LOPDPGDD precisa los datos en los que no es suficiente: ideología, afiliación, sindical, religión, orientación sexual, creencias, o étnico)**
- **Habilitación en el ámbito del derecho laboral y de seguridad o protección social (puede basarse en Convenio Colectivo)**
- **Tratamiento para la protección de intereses vitales del afectado o un tercero**
- **Datos manifiestamente públicos**
- **Tratamiento necesario por razones de Interés público esencial según la Ley UE o Nacional siempre que sea proporcional a la finalidad perseguida**
- **Defensa y reclamaciones y Tribunales**
- **Razones de interés público en el ámbito de la salud pública, así como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios**
- **Archivo y fines de investigación histórica o científica o estadísticos en los términos del propio Reglamento**

Medicina preventiva o laboral y evaluación de la capacidad laboral, diagnóstico médico o prestación sanitaria, gestión de los sistemas o servicios sanitarios. Exigencia de tratamiento llevado a cabo por profesional sujeto a deber de secreto o bajo su responsabilidad

DATOS DE INFRACCIONES Y SANCIONES

- **No están calificados como categorías especiales de datos (art. 10 RGPD y 27 LOPDPGDD)**
- **Su tratamiento exige (LOPDPGDD):**
  - **Ser órgano competente para procedimientos sancionadores y declaración de infracciones y sanciones**
  - **Limitado estrictamente a la finalidad del órgano**
- **Si no: consentimiento interesados o autorización por Ley**
- **Excepción: Abogados y procuradores cuyo objeto sea recoger la información facilitada por sus clientes.**

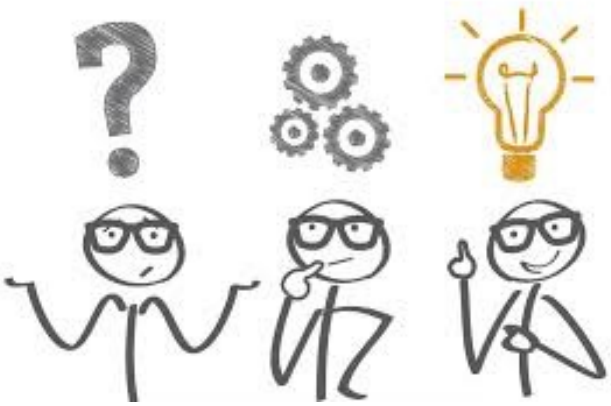
Artículo 27.LOPDGDD

Tratamiento de datos relativos a infracciones y sanciones administrativas.

1. A los efectos del artículo 86 del Reglamento (UE) 2016/679, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá:
   a) Que los responsables de dichos tratamientos sean los **órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.**
   b) Que el tratamiento se limite a los **datos estrictamente necesarios** para la finalidad perseguida por aquel.
2. Cuando **no se cumpla alguna de las condiciones previstas en el apartado anterior**, los tratamientos de datos referidos a infracciones y sanciones administrativas habrán de contar con el **consentimiento del interesado o estar autorizados por una norma con rango de ley**, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados.
3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a infracciones y sanciones administrativas solo serán posibles cuando sean llevados a cabo por **abogados y procuradores** y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO (ART 25 RGPD)

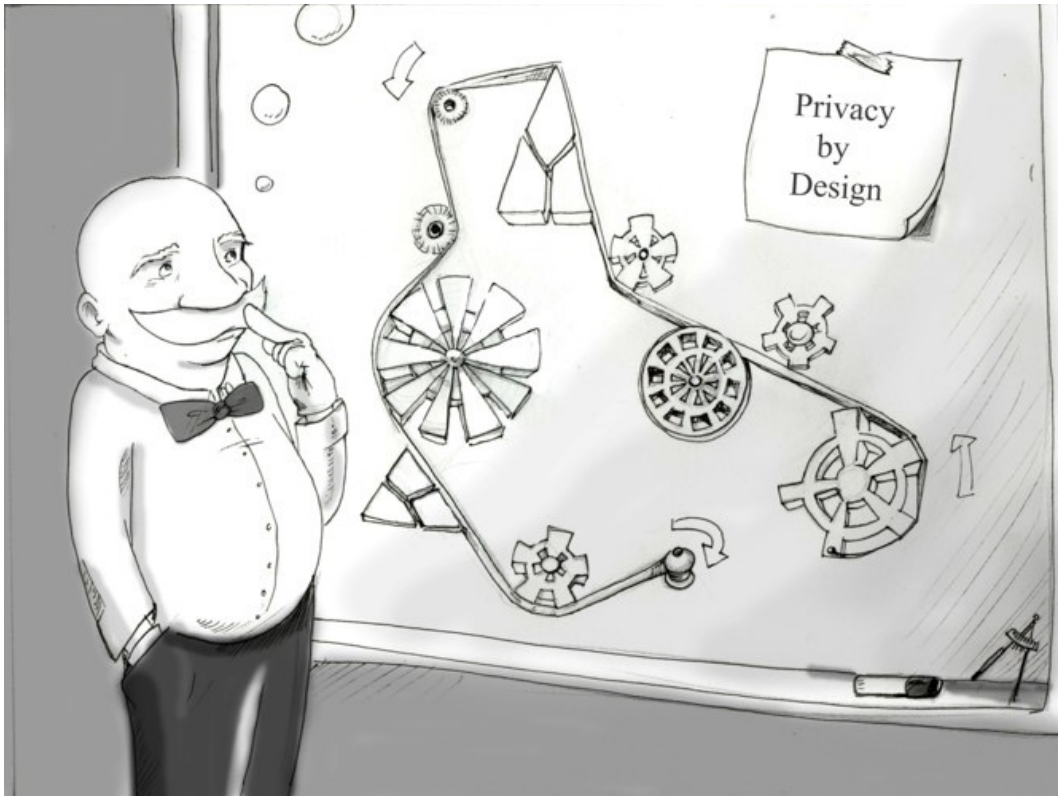
- Aplicar medidas técnicas y organizativas apropiadas para garantizar el cumplimiento de los principios de protección de datos personales y proteger los derechos de los interesados.



- Por ejemplo, **establecer controles**, basados en políticas o estándares, que tengan por objeto asegurarse de que **no se tratan más datos personales de los necesarios,** que se **conservan únicamente por el tiempo necesario** para **cumplir con el fin o fines del tratamiento** o un procedimiento de evaluación en materia de protección de datos personales a la hora de **contratar servicios electrónicos**, tales como la nube, o adquirir productos tecnológicos para el tratamiento de datos personales.

Protección de datos desde el diseño. *Privacy by Design (art. 25 y C78)*

Se impone la obligación al responsable del tratamiento de establecer medidas técnicas y organizativas adecuadas (como, por ejemplo, la seudonimización y la minimización de datos) para aplicar principios de protección de datos de forma eficaz y proteger así los derechos de los afectados.



Protección de datos desde el diseño. *Privacy by Design*

Para la fijación de estas medidas **debe tenerse en cuenta:**

— La naturaleza, ámbito, contexto y finalidad del tratamiento.

— Los riesgos de diversa probabilidad y gravedad (no sólo respecto al riesgo alto).

— Estado de la técnica.

— Coste.

El establecimiento de las necesarias garantías se debe producir **en dos momentos diferenciados:**

1. en el momento de determinar los medios para el tratamiento.
2. en el preciso momento en el que se realiza el tratamiento de datos.

Protección de datos por defecto (art. 25)

Se exige al responsable que adopte medidas técnicas y organizativas adecuadas a fin de que el tratamiento (fijado por defecto) emplee los datos personales estrictamente necesarios para cada fin específico.

Esta obligación se debe extender:

— a la cantidad de los datos recopilados.

— a la extensión del tratamiento.

— al periodo de almacenamiento.

— a la accesibilidad

— y en particular, debe evitarse la accesibilidad a un número indeterminado de datos personales sin intervención de alguien.

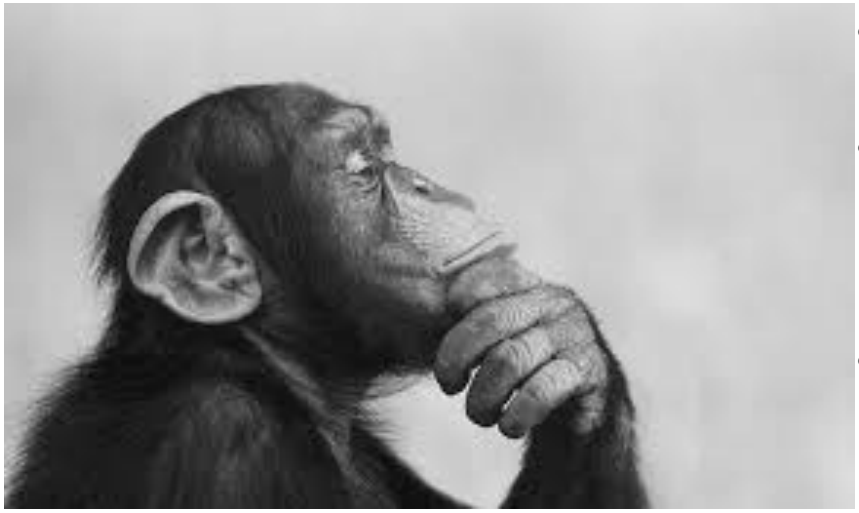
Registro de Actividades de Tratamiento

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Mantenimiento de un registro de las actividades de tratamiento de datos (art. 30 y C 82 y 37 de la LOPD):

- ✓ Obligadas empresas que empleen a más de 250 personas, y aquellas que realicen tratamientos con riesgo; **no de forma ocasional**; tratamiento con categorías especiales de datos o con datos relativos a condenas e infracciones penales.
- ✓ Responsables como encargados.
- ✓ Por escrito (formato electrónico) y a disposición de la AEPD.
- ✓ Podrá organizarse en torno a conjuntos estructurados de datos (fichero)
- ✓ Deben **hacerse público por medios electrónicos en determinados casos** (AAPP; Universidades Públicas;): 31.2. LOPD. Los sujetos enumerados en el artículo 77.1 de la LOPD harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

CONTENIDO DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO (ART. 30.1)



- a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
- b) los fines del tratamiento;
- c) una descripción de las categorías de interesados y de las categorías de datos personales;
- d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y la documentación de garantías adecuadas;
- f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
- g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

01 IDENTIFICACIÓN DEL RESPONSABLE

02 FINES DEL TRATAMIENTO

03 DESCRIPCIÓN DE CATEGORÍAS

04 CATEGORÍAS DE DESTINATARIOS

05 TRANSFERENCIAS INTERNACIONALES

06 PLAZOS PREVISTOS SUPRESIÓN DATOS

07 DESCRIPCIÓN GENERAL DE MEDIDAS DE SEGURIDAD

Derechos de los Afectados

DERECHOS

- Catálogo tradicional con tres novedades
  - Información
  - Acceso
  - Rectificación
  - Cancelación (derecho al olvido)
  - Limitación del tratamiento
  - Portabilidad
  - Oposición

- Previsiones sobre ejercicio de estos derechos
  - Lenguaje claro e inteligible
  - Obligación de "facilitar el ejercicio"
  - Plazos de respuesta → 1 mes
  - Formas de ejercicio → Posible vía electrónica
  - Gratuidad
  - Uso de iconos para proporcionar información

DERECHOS DE LOS INTERESADOS

Artículo 13 Información que deberá facilitarse cuando los datos personales se obtengan del interesado

1. Cuando se obtengan de un interesado datos personales relativos a él, **el responsable del tratamiento**, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación….

Artículo 14 Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado

1. Cuando los datos personales no se hayan obtenidos del interesado, **el responsable del tratamiento** le facilitará la siguiente información….

Artículo 15 Derecho de acceso del interesado

1. El interesado tendrá derecho a obtener **del responsable del tratamiento** confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información

Artículo 16 Derecho de rectificación

El interesado tendrá derecho a obtener sin dilación indebida **del responsable del tratamiento** la rectificación de los datos personales inexactos que le conciernan.

Artículo 17 Derecho de supresión («el derecho al olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida **del responsable del tratamiento** la supresión de los datos personales que le conciernan

DERECHOS DE LOS INTERESADOS

Artículo 18 Derecho a la limitación del tratamiento

1. El interesado tendrá derecho a obtener **del responsable del tratamiento** la limitación del tratamiento de los datos

Artículo 19 Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los **destinatarios** a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Artículo 20 Derecho a la portabilidad de los datos

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un **responsable del tratamiento**

EL DERECHO/DEBER DE INFORMACIÓN

Se incrementa la información que habrá de facilitarse cuando los datos se recaban del afectado

- **Identidad y los datos de contacto del responsable y, en su caso, de su representante**
- **Datos de contacto del delegado de protección de datos**
- **Fines y base jurídica del tratamiento**
- **Intereses legítimos del responsable o de un tercero**
- **Destinatarios o las categorías de destinatarios de los datos personales, en su caso**
- **Transferencias internacionales previstas**
- **Plazo de conservación**
- **Derechos de acceso, rectificación o supresión, limitación del tratamiento, oposición y portabilidad**
- **Posibilidad de revocación del consentimiento**
- **Derecho a presentar una reclamación ante una autoridad de control**
- **Si la comunicación de datos personales es obligatoria y las posibles consecuencias de no facilitar los datos**
- **Existencia de decisiones automatizadas, incluida la elaboración de perfiles, la lógica aplicada y las consecuencias previstas**

Código Deontológico de la Abogacía Española, aprobado en marzo de 2019, dispone, en su artículo 12.B.3 que los abogados/as deben poner "(…) especial atención en efectuar las correspondientes advertencias al cliente en lo que respecta a la normativa (…) derivada de la legislación sobre protección de datos de carácter personal".

Real Decreto 135/2021, de 2 de marzo, por el que se aprueba el Estatuto General de la Abogacía Española.

Artículo 48. *Deberes de información e identificación*

1. **DEBE** facilitar al cliente su **nombre, NIF, Colegio al que pertenece y número de colegiado, domicilio profesional** y **medio para ponerse en comunicación** con él o con su despacho, incluyendo la **vía electrónica.**
2. Cuando se trate de una **sociedad profesional o despacho colectivo**, deberá informar al cliente de su denominación, forma, datos de registro, régimen jurídico, código de identificación fiscal, dirección o sede desde la que se presten los servicios y medios de contacto, incluyendo la vía electrónica.
3. Cuando los servicios requeridos exijan la participación de diferentes profesionales de la Abogacía de una misma sociedad u organización, **el cliente tendrá derecho a conocer la identidad de todos ellos**, el Colegio al que pertenecen y, si se tratara de sociedades profesionales, si son o no socios, así como el profesional de la Abogacía **que asuma la dirección del asunto.**
4. obligación de informar a su cliente **sobre la viabilidad del asunto** que se le confía, procurará disuadirle de promover conflictos o ejercitar acciones judiciales sin fundamento y le aconsejará, en su caso, sobre las vías alternativas para la mejor satisfacción de sus intereses.
5. informará sobre los **honorarios y costes de su actuación**, mediante la presentación de la hoja de encargo o medio equivalente. También le hará saber las consecuencias que puede tener una **condena en costas y su cuantía aproximada.**
6. deberá informar a su cliente acerca del **estado del asunto** en que esté interviniendo y sobre las **incidencias** y **resoluciones** relevantes
7. En los procedimientos administrativos y judiciales, **si el cliente lo requiere**, le proporcionará **copia de los diferentes escritos que se presenten o reciban, de las resoluciones judiciales** o administrativas que le sean notificadas y de las **grabaciones** de actuaciones que se hayan producido
8. **En ningún caso** el profesional de la Abogacía podrá retener documentación del cliente, sin perjuicio de que pueda **conservar copia.**

De que debemos informar:

Identidad y datos de contacto del letrado/a o procurador/a responsable, o de la sociedad profesional que corresponda.

El meritado Código Deontológico, en su artículo 21.3, establece que "en especial, en las comunicaciones, aplicaciones, webs y servicios profesionales prestados por medios electrónicos deberá (…) identificarse con su nombre y, en su caso, el de la sociedad profesional titular del servicio, Colegio de adscripción y número de colegiación".

En su caso) Los datos de contacto del **delegado de protección de datos**, aunque, por regla general, un despacho de abogacía no debe disponer de esta figura

Los **fines del tratamiento** a que se destinan los datos personales y la base jurídica del tratamiento, es decir, el fin de tratamiento será *la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial*. Debe indicarse la **base jurídica del tratamiento.**

Debe detallarse quienes son los **destinatarios de los datos**, como, por ejemplo, otros abogados/as colaboradores, peritos, procuradores/as, etc.

Debe indicarse el **plazo durante el cual se conservarán** los datos personales.

En este caso, un abogado/a puede acogerse a plazos por mandato tributario (4 años según el artículo 111 de la Ley General Tributaria); o, por ejemplo, de prescripción general de acciones personales por mandato del artículo 1964 del Código Civil Señala el artículo 1964.2 del CC: "Las acciones personales que no tengan plazo especial prescriben a los cinco años desde que pueda exigirse el cumplimiento de la obligación. En las obligaciones continuadas de hacer o no hacer, el plazo comenzará cada vez que se incumplan."

Derechos de los interesados. Debe informarse acerca de la existencia del derecho a solicitar al abogado/a o procurador/a el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento;

En el caso de que el tratamiento esté basado en el **consentimiento del interesado** (es decir, del propio cliente) debe informarse de la existencia del derecho a retirar el mismo en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

El **derecho a presentar una reclamación** ante la Agencia Española de Protección de Datos.

Si la comunicación de datos personales es un requisito legal o contractual (como por ejemplo podría ocurrir cuando se produce una designación en turno de oficio), o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos y está informado de las posibles consecuencias de no facilitar tales datos.

Información por capas o niveles

- ✓ Por el **principio de transparencia** (arts. 12.1 REPD y 11 LOPD) la información a los interesados debe proporcionarse con un lenguaje claro y sencillo; de forma concisa, transparente, inteligible y de fácil acceso.

- ✓ **Información proporcionada por capas o niveles** (art. 11. LOPD): información básica (identidad, finalidad, ejercicio derechos, referencia si elaboración de perfiles + información adicional.

"Guía para el cumplimiento del deber de informar", publicada en 2017 AEPD.

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

Cláusula propuesta para Hoja de Encargo.

En virtud de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, le informamos que el responsable del tratamiento es Dxxxxxxxxx, letrado en ejercicio, colegiado en el Iltre. Colegio de Abogados de xxxxx, con número profesional: ___. Los datos de contacto son: Pza._____ Nº____de xxxxxx. E-mail: ejemplo@mail.com . El fin de tratamiento de los datos, que voluntariamente nos facilite, será la formulación, el ejercicio o la defensa de la reclamación judicial o extrajudicial objeto del concreto encargo profesional. Consecuencia de ello, la base jurídica del tratamiento se encuentra en el artículo 6.1.b RGPD (ejecución de un contrato o relación precontractual). Igualmente, le informamos que los destinatarios de la información serán los peritos o procuradores que usted designe en el marco del procedimiento encargado. El plazo de conservación de los datos personales será de 5 años una vez finalizada la prestación del servicio. Por otro lado, le informamos de su derecho a ejercer sus derechos de acceso, rectificación o supresión, o la limitación de su tratamiento, o a oponerse al mismo. Por otro lado, le advertimos de su derecho a retirar, en cualquier momento, el consentimiento prestado para tratar sus datos, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada. Finalmente, le recordamos, por imperativo legal, su derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, si considerara que el tratamiento de datos no es acorde a la normativa europea.

El letrado/abajo firmante, ha sido designado/a **mediante designación de turno de oficio**, para la defensa de los intereses de:

Nombre	
Apellidos	
Dirección	
Teléfono móvil	
Correo electrónico	

Cuya pretensión es (*detallar*):

Cláusula de Protecció

Cláusula de Protección de datos.

En virtud de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, le informamos que el responsable del tratamiento es D. Javier ....., letrado en ejercicio colegiado en el Iltre. Colegio de Abogados de Valladolid, con número profesional: ..... Los datos de contacto son: ..... El fin de tratamiento de los datos, que voluntariamente nos facilite, será la formulación, el ejercicio o la defensa de la reclamación judicial o extrajudicial objeto del concreto encargo profesional, ***mediante la designación en turno de oficio.*** *Consecuencia de ello, la base jurídica del tratamiento se encuentra en el artículo 9 del Reglamento Europeo y en el artículo 24 de la Constitución Española. Igualmente, le informamos que los destinatarios de la información serán los peritos o procuradores designados en turno de oficio en el marco del procedimiento encargado,* ***así como los datos esenciales del procedimiento, con el fin de justificar la asistencia realizada ante el Iltre. Colegio de Abogados de ……*** *El plazo de conservación de los datos personales, por parte del letrado será durante el tiempo estrictamente necesario para cumplir con la finalidad para la que se obtuvieron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos.*

Por otro lado, le informamos de su derecho a ejercer sus derechos de acceso, rectificación o supresión, o la limitación de su tratamiento, o a oponerse al mismo. Por otro lado, le advertimos de su derecho a retirar, en cualquier momento, el consentimiento prestado para tratar sus datos, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada. Finalmente, le recordamos, por imperativo legal, su derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, si considerara que el tratamiento de datos no es acorde a la normativa europea.

TRATAMIENTO POR ABOGADOS Y PROCURADORES DE LAS PARTES DE UN PROCESO

Datos de nuestros clientes.

- ✓ Base jurídica legitimadora: Relación contractual o precontractual o consentimiento para tratar los datos. No se basa en el interés legítimo prevalente.
- ✓ Pero si deberíamos informarles de lo previsto en el Arts. 13 y 14 RGPD: **PRINCIPIO DE INFORMACIÓN**. ¿Cómo? En las hojas de encargo, facturas, hojas específicas (verbalmente….problemas de prueba). INFORMACION POR CAPAS (info básica + info adicional)
- ✓ Ejercicio de derechos de acceso, cancelación, rectificación u oposición, SUPRESION; PORTABILIDAD

TRATAMIENTO POR ABOGADOS Y PROCURADORES DE LAS PARTES DE UN PROCESO (2)

Datos de la contraparte:

JURISPRUDENCIA Y AEPD CRITERIO UNANIME:

Colisión de dos Derechos Fundamentales: 1) Tutela Judicial Efectiva (24.2 CE) y 2) A la Protección de Datos.

T.C.: NO HAY D.F. ABSOLUTOS: PREVALENCIA DEL 24.2. ya que si los abogados y procuradores solicitan su consentimiento a los afectados de contrario o les comunican determinada información que se pudiera disponer procedentes de los clientes, podrían perjudicar claramente a su derecho a obtener la tutela judicial efectiva. Información a la contraparte: **art. 14.5.b RGPD no se exige cuando imposibilite u obstaculice gravemente el logro del tratamiento.**

Ejercicio de derechos de acceso, olvido…..: DENEGACIÓN. **¡¡OBLIGATORIO CONTESTAR!!**


ANTES DE CONTINUAR, ¿ACEPTA NUESTRA POLÍTICA DE PRIVACIDAD Y SECRETO DE CONFESIÓN?
Aceptar
Salir
@ElChisteDeMel
MEL

REGLAS GENERALES DE EJERCICIO DE DERECHOS

Art. 12, junto con disposiciones relativas a transparencia.

1. Mandato de facilitar el ejercicio (art. 12.2)

- ➢ Principio *"pro ejercicio"* preside toda la regulación
  - ✓ Amplio margen de configuración del responsable

2. La identificación del interesado (art. 12.2 y 6)

Dos supuestos:

a) La **identidad** del solicitante está **acreditada** pero **no se pueden determinar los datos** que le conciernen

Relacionado con **art. 11**: El responsable no está obligado a mantener, obtener o tratar información adicional para identificar al interesado a efectos de cumplir con el Reglamento

- Si puede demostrar que no está en condiciones de determinar cuáles son los datos del solicitante, le informa y **decaen los derechos** (art. 11.2)
- Excepción: el interesado aporta información adicional que permita determinar los datos que le corresponden (art. 11.2)

✓ Si, a pesar de las informaciones aportadas, no se pueden determinar los datos que corresponden al solicitante, se puede **denegar la solicitud** (art. 12.2)

- ➢ **Carga de la prueba** corresponde al responsable: *"salvo que pueda demostrar"*

b) Hay **dudas sobre la identidad** del solicitante

- ✓ Se puede solicitar que facilite información adicional necesaria para confirmar la solicitud

¿Copia DNI?

Petición sistemática es cuestionable. Sólo si del contexto se derivan dudas razonables sobre la identidad

REGLAS GENERALES DE EJERCICIO DE DERECHOS

3. Obligación de contestar con celeridad (art. 12.3 y 4)

Obligación de contestar todas las solicitudes, respuesta positiva (12.3) o negativa (12.4)

Respuesta negativa:

- **Motivada** (informar de las "razones")
- **Informar** de las posibilidades de presentar **reclamación** ante la autoridad de control y de ejercer **acciones** judiciales

Celeridad: "sin dilación", plazo máximo de un mes

Prorrogable por otros dos meses (complejidad y volumen), informando e indicando motivos

- Prórroga sólo si la respuesta es positiva: se debe tomar la decisión en 1 mes

4. Forma

- Regla general 12.1: "*forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo*"
  Si se presenta por medios electrónicos, respuesta igual si es posible, salvo que interesado solicite otro modo

5. Gratuidad

12.5: "*serán a título gratuíto*"

Sólo si las solicitudes son "*manifiestamente infundadas o excesivas*", alternativa:

a) Cobrar un **canon razonable** (costes administrativos)

b) Negarse a "*actuar*"

- El responsable soporta la **carga de la prueba**: ("demostrar el carácter manifiestamente infundado o excesivo")

DERECHO DE ACCESO. Alcance

- Confirmación de la existencia de tratamiento
- Acceso a los datos y a la información vinculada a los mismos
  - Fines
  - Categorías de datos
  - Categorías (al menos) de destinatarios
  - Plazo de conservación o criterios de fijación
  - Información de derechos de rectificación y supresión
  - Posibilidad de reclamación a la autoridad de control
  - Información disponible sobre el origen de los datos
  - Existencia de decisiones automatizadas o perfilado
  - Garantías adecuadas implantadas en caso de transferencia

Modo de acceso: copia de los datos

- Gratuidad de la primera copia y canon orientado a costes en las ulteriores
- Uso de medios electrónicos si el derecho se ejercitó por ellos

Restricción: perjuicio de derechos de terceros

Aclaraciones (considerando 63)

- Posibilidad de satisfacer el acceso mediante acceso remoto seguro
- Posibilidad de que el responsable pueda pedir aclaración al interesado

DERECHO DE ACCESO (2)

Art. 15: **derecho general de acceso** a la información personal

- Complemento de las obligaciones de información activa arts. 13 y 14
- Derecho capital, posición central en el haz de derechos comprendidos en el derecho fundamental

❖ **Contenido y límites**

➢ Confiere **dos tipos de facultades** para ejercer otras tantas pretensiones:

a) Derecho de **acceso a los datos** y a las **"metainformaciones"** vinculadas a los tratamientos

Incondicionado, sin requisitos previos ni supuestos habilitantes.

b) El derecho a obtener una **copia** de los datos personales

❖ **Alcance y obligaciones del responsable**

➢ **Obligación de contestar**

- Si trata datos, el contenido de la respuesta ha de ser más amplio:

1. **Qué datos** está tratando: información exhaustiva sobre todos los datos que estén siendo tratados, sin excepción.

Actualizada al **momento** de atender el derecho

- No hay que informar sobre datos tratados con anterioridad pero que ya no se tratan

DERECHO DE ACCESO (3)

2. Metainformaciones

La mayoría son informaciones que se han debido proporcionar (arts. 13 y 14)

- Derecho/obligación autónomo: haber proporcionado la información no deja sin objeto el derecho de acceso ni exime de la obligación de proporcionarlas
- Actualizadas al momento de atender el derecho

a) Los **fines** del tratamiento (no se exige base jurídica del tratamiento)

b) Las **categorías** de datos

c) **Destinatarios** o categorías de destinatarios

En caso de **colisión** entre el derecho de acceso y el interés de mantener en secreto el destinatario, con carácter general prevalece el derecho de acceso. Se puede establecer normas específicas para atender intereses legítimos en el marco del art. 23

- Impone una obligación de **registrar** qué datos se han comunicado a terceros y a quienes.

d) **Plazo** de conservación o criterios para determinarlo (= art. 13.2)

e) Informar sobre los **derechos** de rectificación, supresión, limitación y oposición (= art. 13, pero no incluye portabilidad)

f) Derecho a presentar una **reclamación** (= art. 13)

g) Información sobre **origen**, cuando no se hayan obtenido del interesado, (= art. 14.2.f)

- Impone obligación de **registrar** y conservar la información sobre el origen

h) La existencia de **decisiones automatizadas**, incluida la elaboración de perfiles (arts. 13.2 f y 14.2.g)

- **Transferencias internacionales**, informar sobre garantías (similar arts. 13 y 14)

DERECHO DE ACCESO (4)

❖ **Forma y procedimiento**

➢ Se rige por art. 12

- **Solicitud no requiere forma**, no se exigen contenidos específicos, pero debe permitir encontrar la información que es objeto de la solicitud. (Cons. 63: caso de gran cantidad de información el responsable puede solicitar que especifique la información o actividades de tratamiento a que se refiere la petición)
- **Contestación**: ha de cumplir su **finalidad**, permitir pleno ejercicio de los derechos

❖ **Derecho a obtener una copia**

- **Novedad**. Enriquece y amplia el derecho de acceso.
- En la mayoría de los casos, cubre derecho general de acceso, pero no lo sustituye plenamente.

Contenido.

- Los datos en el estado en que se encuentren. No hay derecho a elaboración.
- Copia **completa**, pero sólo los datos que conciernen al solicitante. Pueden (deben) suprimirse o eliminarse el resto de las informaciones de los soportes

Límites.

15.4: "*no afectarán negativamente a los derechos y libertades de otras personas*".

✓ Incluye al **responsable**. Cons. 63 ej.: los secretos comerciales, propiedad intelectual., esp. software

➢ **Sólo** afectan a la información **sensible**. No justifican negativa absoluta: **copia parcial**

✓ Susceptible de **limitaciones** derivadas de regulaciones amparadas en art. 23, basadas en la protección de intereses públicos.

Gratuidad.

- 1ª copia, se puede pedir canon razonable por ulteriores

DERECHO DE RECTIFICACIÓN (ART 16 RGPD)

Art. 16: confiere potestad de obtener del responsable la **rectificación de los datos inexactos** (complementa el principio de exactitud del art. 5)

- Doble contenido: derecho a **que se rectifiquen** los datos inexactos y derecho a **que se completen** los incompletos

❖ **Rectificar:**

"Datos inexactos": los que no se corresponden con la realidad

- Criterio objetivo, alude a cuestiones fácticas, no valorativas.
- Tanto si eran inexactos en el momento de la recolección como si lo devienen con posterioridad.
- Independiente de la culpabilidad del responsable y del origen de la inexactitud.

"Sin dilación indebida"

El tiempo estrictamente indispensable para comprobar la exactitud y proceder a la corrección

❖ **Completar:**

Valoración de la integridad, en atención a los fines del tratamiento.

❖ **Límites y excepciones:**

- Susceptible de limitaciones con arreglo a lo previsto en el art. 23: *vid.* legislaciones sectoriales
  - Art. 89.2: en relación con los tratamientos con fines de investigación científica o histórica o estadísticos si imposibilitan u obstaculizan gravemente el logro de estos fines, en la medida que las excepciones sean necesarias para ello.
  - Art. 85 habilita a los estados para establecer excepciones para conciliar el derecho a la protección de datos con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos, de expresión académica, artística o literaria

- Obligación de **informar a los destinatarios** (art. 19)

DERECHO A LA SUPRESIÓN "OLVIDO"

Art. 17 RGPD: básicamente clásico derecho de supresión o cancelación, + obligación de cancelación.

"Derecho al olvido", queda sólo apartado 2

❖ **Derecho y obligación**

Art. 17 no sólo reconoce un derecho subjetivo sino que **impone una obligación** al responsable: "*el cual estará obligado…*"

Requerida por los principios del art. 5. No es necesario esperar a una solicitud.

Pueden darse situaciones problemáticas: colisión obligación con otros derechos, esp., limitación

❖ **Supuestos:**

a) Dejan de ser necesarios

¿Cuándo dejan de ser necesarios **en una administración**? Dificultad de concreción: se pueda excluir que los datos tengan relevancia para las actividades administrativas en interés público o en cumplimiento de una función pública.

- Aconsejable **protocolo de supresión con plazos** para determinados tipos de datos. **Revisión periódica** de la necesidad
- Plazo de conservación/supresión ha de figurar en el **RAT**

Excepción: cuando se den los requisitos para tratar los datos con una finalidad distinta

- Vid., 6.4 y 5.1 en relación con 89

➢ Ha de **conciliarse** con el **derecho de limitación** del art. 18: antes de suprimir, se deberá informar al interesado y ofrecerle la oportunidad de hacer valer el derecho del art. 18.

DERECHO A LA SUPRESIÓN "OLVIDO"

b) Retirada del consentimiento

Si no hay otra base, tratamiento ilícito: **obligación** de supresión, sin necesidad de solicitud

Escasa aplicación en administraciones públicas

c) Oposición al tratamiento

✓ Comprende el supuesto general del art. 21.1 y el específico del 21.2 (mercadotecnia directa)

- 22. 1, admite **excepciones**: que "*se acrediten motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado o, que sea necesario para la formulación, el ejercicio o la defensa de reclamaciones*".
- En 21.2, **no** hay excepciones

d) Ilicitud de los tratamientos

Tenor: "*hayan sido tratados ilícitamente*" incorrecto. Debe darse en el momento **presente**.

Observar el derecho a la limitación del art. 18: **informar** a los interesados antes de suprimir.

e) Cumplimiento de una obligación legal de supresión

f) Datos de menores obtenidos en relación con oferta de SSI

❖ **Contenido de la obligación y del derecho**

- El RGPD no contiene definición "supresión". Hay que entender: hacerlos **inutilizables**
- Diferentes procedimientos. Relevante el **resultado**: imposibilidad de utilizar la información como información personal

➢ Obligación de **comunicar** la supresión a cada uno de los **destinatarios** art. 19

➢ Obligación de **bloqueo** (art. 32 del Proyecto)

DERECHO A LA SUPRESIÓN "OLVIDO"

- **Informar a otros responsables en caso de publicación (art. 17.2)**

- Con. 66: sirve al **objetivo** de conseguir una mayor efectividad del derecho al olvido en Internet: enlaces, copias o réplicas.
- **Requiere solicitud** expresa del interesado
- **Alcance**: "medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales" en función de "la tecnología disponible y el coste de su aplicación".
  - Publicación en la web en el lugar en el que se hizo pública la información
  - Meta-tags: borrar información en cahés de los buscadores
  - Técnicas de Digital Rights Management (DRM)
- Art. 70.1.d) prevé que CEPD emitirá directrices, recomendaciones y buenas prácticas
- Relación con obligación art. 19: no sólo a los destinatarios directos.

- **Excepciones (art. 17.3)**

Cuando el tratamiento sea necesario:

a) Para ejercer el derecho a la **libertad de expresión e información**
  - No sólo profesionales de la información, tb no profesionales
  - No tiene carácter absoluto, requiere ponderación

b) Para el **cumplimiento de una obligación legal**, **misión en interés público** o en **ejercicio de poderes públicos**.

c) Por razones de **interés público** en el ámbito de la **salud pública**

d) Con fines de **archivo** en interés público, investigación científica o histórica o fines estadísticos, art. 89

e) Para la formulación, ejercicio o defensa de **reclamaciones**

Artículo 32. LOPDGDD . *Bloqueo de los datos.*

1. El responsable del tratamiento estará obligado a bloquear los datos **cuando proceda a su rectificación o supresión.**
2. El bloqueo de los datos consiste en la **identificación y reserva de los mismos**, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, **excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes**, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Transcurrido ese plazo deberá procederse a la destrucción de los datos.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.
4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un **copiado seguro de la información de modo que conste evidencia digital**, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.
5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, dentro del ámbito de sus respectivas competencias, **podrán fijar excepciones a la obligación de bloqueo** establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

DERECHO DE LIMITACIÓN DEL TRATAMIENTO (ART. 18)

- Los datos **no se suprimen** pero **no pueden ser objeto de tratamiento**, salvo excepciones

- **Supuestos:**

a) Impugnación de la exactitud de los datos

Con el objeto de que sean rectificados (16) suprimidos (17)

No se exige ningún requisito adicional

b) Tratamiento sea ilícito pero el interesado se opone a la supresión y solicita la limitación

No se requiere alegar motivos

c) El interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones

Necesidad real y efectiva, no mera posibilidad abstracta: probabilidad de conflicto o litigio

d) Oposición al tratamiento

La oposición no prospera si prevalecen los motivos legítimos del responsable, hasta que se clarifique, si lo solicita el interesado, el responsable está obligado a limitar el tratamiento

- **Atención del derecho:**

- Conforme art. 4.3 se ha de **proceder al marcado** de los datos conservados con el fin de limitar su tratamiento
- ✓ Además, se deben establecer las **medidas adecuadas** para que los datos marcados **no sean tratados para fines distintos de los previstos en 18.2**. V.gr.:
  - Tratamientos no automatizados: retirarlos y guardarlos en otro lugar con acceso restringido
  - Tratamientos automatizados: restricción de acceso por software salvo para fines 19.2. Con registro o documentación de acceso y tratamientos
  - Cons. 67 menciona otros ejemplos de limitación

DERECHO DE LIMITACIÓN DEL TRATAMIENTO (ART. 18)

- **Tratamientos admitidos (art. 18.2)**

  a) **Conservación**: siempre como consecuencia lógica

  b) Con **consentimiento**: el interesado puede, al ejercer el derecho o con posterioridad consentir explícitamente determinados tratamientos

  c) Formulación, ejercicio o defensa de **reclamaciones**

  d) Protección de los **derechos de otra persona física o jurídica**

  Enunciado muy genérico. Requiere una interpretación estricta para no vaciar de contenido el derecho a la limitación. En todo caso, habrá de ser una necesidad actual

  e) **Razones de interés público importante** de la Unión o de un Estado

  Similar a la previsión del art. 23.1 para restricciones de los derechos

- **Levantamiento de la limitación (art. 18.3)**

  El responsable está obligado a informar antes del levantamiento de la limitación

- **Rechazo de la pretensión**
  - Se ha de motivar
  - Se ha de informar sobre reclamación ante APD y tribunales
  - La Agencia puede ordenar la limitación (art. 58.2.g)

- **Obligación de comunicar** a los destinatarios la limitación (art. 19)

DERECHO DE PORTABILIDAD (ART. 20)

- Finalidad: simplificar el cambio de proveedor y la gestión de los datos.
- Principalmente concebido para prestadores de servicios en red, pero tb aplicable a otros ámbitos

Muy limitada aplicación en el ámbito de las administraciones públicas

❖ **Requisitos:**

a) Comprende sólo los datos que el interesado hay facilitado

No abarca los datos resultantes de tratamientos por el responsable

No es necesario que los haya facilitado activamente, también en caso de los recogidos, v.gr. monitorización

b) El tratamiento ha de estar basado en el consentimiento o en un contrato

c) El tratamiento ha de efectuarse por medios automatizados

d) No se aplica a los tratamientos que sean necesarios para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos

- ✓ Quedan fuera los tratamientos realizados por entidades públicas cuando tienen como finalidad el cumplimiento de funciones públicas
- ✓ También quedan fuera los tratamientos realizados por entidades privadas cuando ejerzan funciones públicas conferidas.

DERECHO DE OPOSICIÓN (ART. 21)

- El artículo 21 regula **tres tipos** distintos de derecho de oposición:

1. Tratamientos basados en la necesidad para el ejercicio de funciones públicas o en un interés legítimo prevalente (art. 6.1, letras e y f)

- Sirve para tomar en consideración situaciones especiales o intereses especiales de los afectados.
- Se han de hacer valer **motivos** que se derivan de la **situación particular** del interesado.
- Son aplicables situaciones jurídicas, económicas, religiosas, sociales, familiares, etc.

- **Momento**: se puede presentar "en cualquier momento", tb una vez iniciados los tratamientos
- **Alcance**: puede oponerse a todos los tratamientos o sólo a algunos (v.gr. comunicaciones), referirse a todos los datos o sólo a algunos.
- **Efectos**: El responsable debe **dejar de tratar los datos, salvo** que tenga motivos que lo justifiquen.

  En concreto el art. 21, prevé **2 motivos** que justifican que se continúe el tratamiento:

  - **Motivos legítimos imperiosos** que prevalezcan sobre los intereses, derechos y libertades del interesado. El responsable tiene la **carga** de la **argumentación** y **prueba**: "*salvo que acredite*"
  - Se traten para la formulación, ejercicio o defensa de **reclamaciones**.

- En caso de que proceda la oposición plena, el responsable está **obligado a suprimir** los datos conforme art. 17

DERECHO DE OPOSICIÓN (2) (ART. 21)

2. Tratamientos con objeto de mercadotecnia directa

En este caso el criterio es la **finalidad** de los tratamientos, no la base jurídica

✓ Comprende **toda comunicación directa** por carta, prospectos, llamadas telefónicas, e-mail, sms...

¿Comercial? No hay ningún sustento en RGPD para entender que sólo comunicaciones comerciales. Publicidad con fines políticos o religiosos quedaría comprendida

- Incluye tanto las ofertas del responsable como de terceros.
- A diferencia de lo que ocurre con el supuesto general del apartado 1, **no es necesaria motivación**.

❑ **Efectos:**

➢ Determina la obligación de **poner fin al tratamiento para esos fines** (21.3)

- Efectos **automáticos**, sin necesidad de examen ni requisitos adicionales.
- El responsable no tiene la posibilidad de alegar motivos para continuar el tratamiento.
- Si continúa, tratamiento **ilícito**.

3. Tratamientos con fines de investigación o estadísticos (21.6)

- Son **tratamientos privilegiados** en múltiples aspectos
- El derecho de oposición otorga al interesado cierta **compensación**

❑ **Motivación:** ha de hacer valer motivos relacionados con su situación particular =21.1

❑ **Efectos:** Debe **poner fin** a los tratamientos **salvo**:

✓ Que sea **necesario para el cumplimiento de una misión realizada por razones de interés público**

Que no esa posible cumplir la misión sin el tratamiento de datos personales. Vgr. con datos anonimizados

El responsable debe **realizar ponderación** entre derecho fundamental e interés público.

DERECHO A NO SER OBJETO DE DECISIONES AUTOMATIZADAS (ART. 22)

- El art. 22 no regula la admisibilidad de los tratamientos automatizados sino la utilización de determinados resultados de los tratamientos

- **Alcance:**
  - La prohibición **no afecta a todas** las decisiones automatizadas sino a las ***"basadas únicamente en tratamientos automatizados"***
  - La prohibición afecta lógicamente sólo a las decisiones automatizadas **que implican valoraciones de aspectos de la personalidad**, no cuando se utilizan otros aspectos

- **Las decisiones vedadas**

  Art. 22 no prohíbe cualquier decisión basada únicamente en tratamiento automatizados sino sólo las que a) **produzcan efectos jurídicos en el interesado** o, b) **le afecten significativamente de modo similar**.

- **Las excepciones**

  Art. 22 prevé 3 excepciones que relativizan la prohibición:

  a) Sea necesaria para la celebración o la ejecución de un **contrato**
  b) Esté **autorizada** por el **Derecho** de la Unión o de los Estados
  c) Se base en el **consentimiento** explícito del interesado

- **Las categorías especiales de datos**

  22.4. Excepción de las excepciones: no se aplican a las **categorías especiales de datos** reguladas en art. 9

  A su vez, prevé **dos excepciones** a la prohibición general:

  9.2.a) el interesado dio su **consentimiento explicito**

  9.2.g) sea necesario por razones de **interés público esencial**

Acción de reclamación de indemnización daños y perjuicios derivados de una infracción en materia de protección de datos. Art. 82 y C146 RGPD

El RGPD reconoce el derecho a una indemnización efectiva y solidaria, a toda persona que haya sufrido daños y perjuicios («materiales o inmateriales») como consecuencia de una infracción del Reglamento (art. 82.1 y Cons. 146 RGPD).

En España existen **otras acciones indemnizatorias** que pudiera ejercitar el interesado, además de la que contempla el art. 82 RGPD; como la prevista en el art. 9.3 de la *Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*; y la responsabilidad extracontractual, por culpa, del artículo 1902 del *Código Civil*, que resultarían compatibles, a priori, con la regulada en el art. 82 RGPD.

ENCARGADOS DEL TRATAMIENTO

Encargados del tratamiento: obligación de diligencia debida en su elección.

- ✓ El RGPD exige (art. 28.1) que las relaciones responsable/encargado del tratamiento **se regulen en un contrato, o en un acto jurídico** (esta es la novedad).
- ✓ Se regula, de una forma minuciosa, el contenido mínimo de los contratos de encargo con acceso a datos por cuenta de terceros.
- ✓ Con el RGPD, se introduce un **principio de responsabilidad activa, en la elección y supervisión de los encargados,** los cuales deben ofrecer garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas, conforme establece el RGPD. En este sentido Art 28 PLOPD), VALORAR SI PROCEDE realización de una evaluación de impacto y la consulta previa. El propio precepto menciona una serie de **riesgos concretos** que pueden aconsejar la adopción de medidas técnicas y organizativas adecuadas.

RESPONSABLE/ENCARGADO DEL TRATAMIENTO

- **Previsión de que el responsable "realice auditorías y contribuya a ellas, incluidas las inspecciones dirigidas por el responsable o por otro auditor autorizado por dicho responsable"**
- **Fin de la prestación implica borrado o devolución de datos, sin incluir transferencia a otro encargado**
- **Obligación de informar al responsable "si, en su opinión, una instrucción infringe el presente Reglamento o las disposiciones nacionales o de la Unión en materia de protección de datos"**
- **Posibilidad de "contratos modelo"**

OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO

- **Asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados: acceso, oposición, rectificación, cancelación, limitación, portabilidad, decisiones automatizadas**

- **Ayudará al responsable a garantizar el cumplimiento de las obligaciones sobre seguridad del tratamiento, brechas de seguridad, evaluaciones de impacto y consulta a la AEPD**

- **Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.**

TRATAMIENTOS BAJO LA AUTORIDAD DEL RESPONSABLE (ART. 29)

El encargado y cualquier persona que actúe bajo la autoridad del responsable y encargado y tenga acceso a datos personales

Instrucciones del responsable

Salvo que exista una obligación exigible en virtud del Derecho de la Unión Europea o nacional

Delegado de Proteccion de Datos

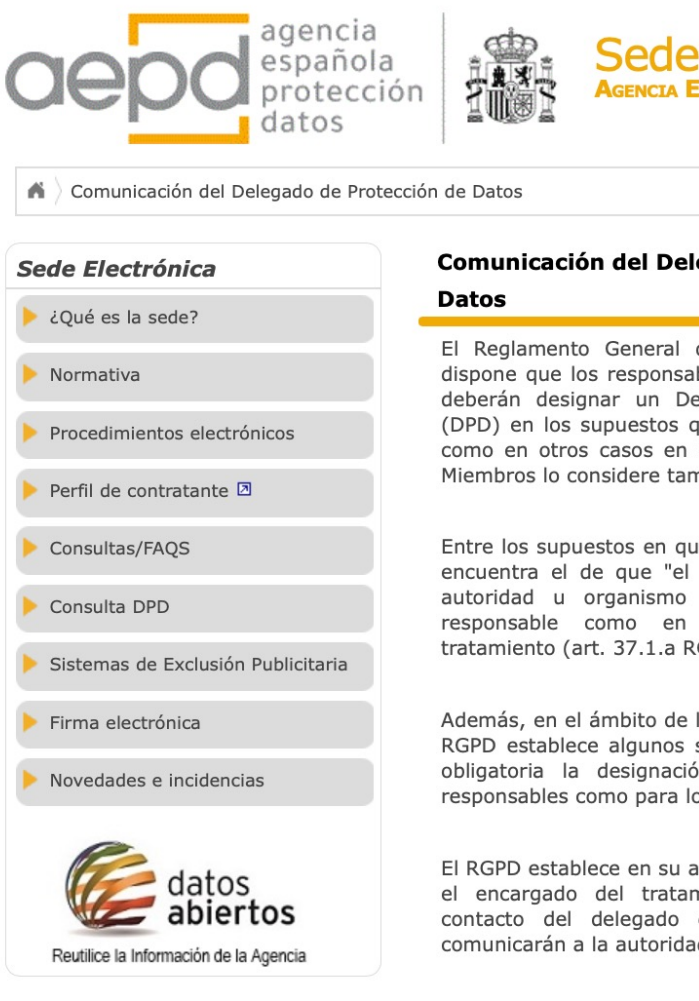
Delegado de protección de datos

- ✓ Persona encargada informar a la entidad responsable o al encargado sobre sus obligaciones legales en protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la autoridad de control y actuar como punto de contacto entre ésta y la entidad responsable.
- ✓ Uno de los ejes fundamentales del *ppio. res. activa* (art. 39).
- ✓ Funciones:
  - ✓ **información y asesoramiento normativo** (Evaluaciones Impacto, registro actividades, empleados..).
  - ✓ **supervisión de cumplimiento normativo**. Auditoria (informe anual, formación…)
  - ✓ **cooperación y enlace con la autoridad de control**.
  - ✓ **atención a los interesados.**

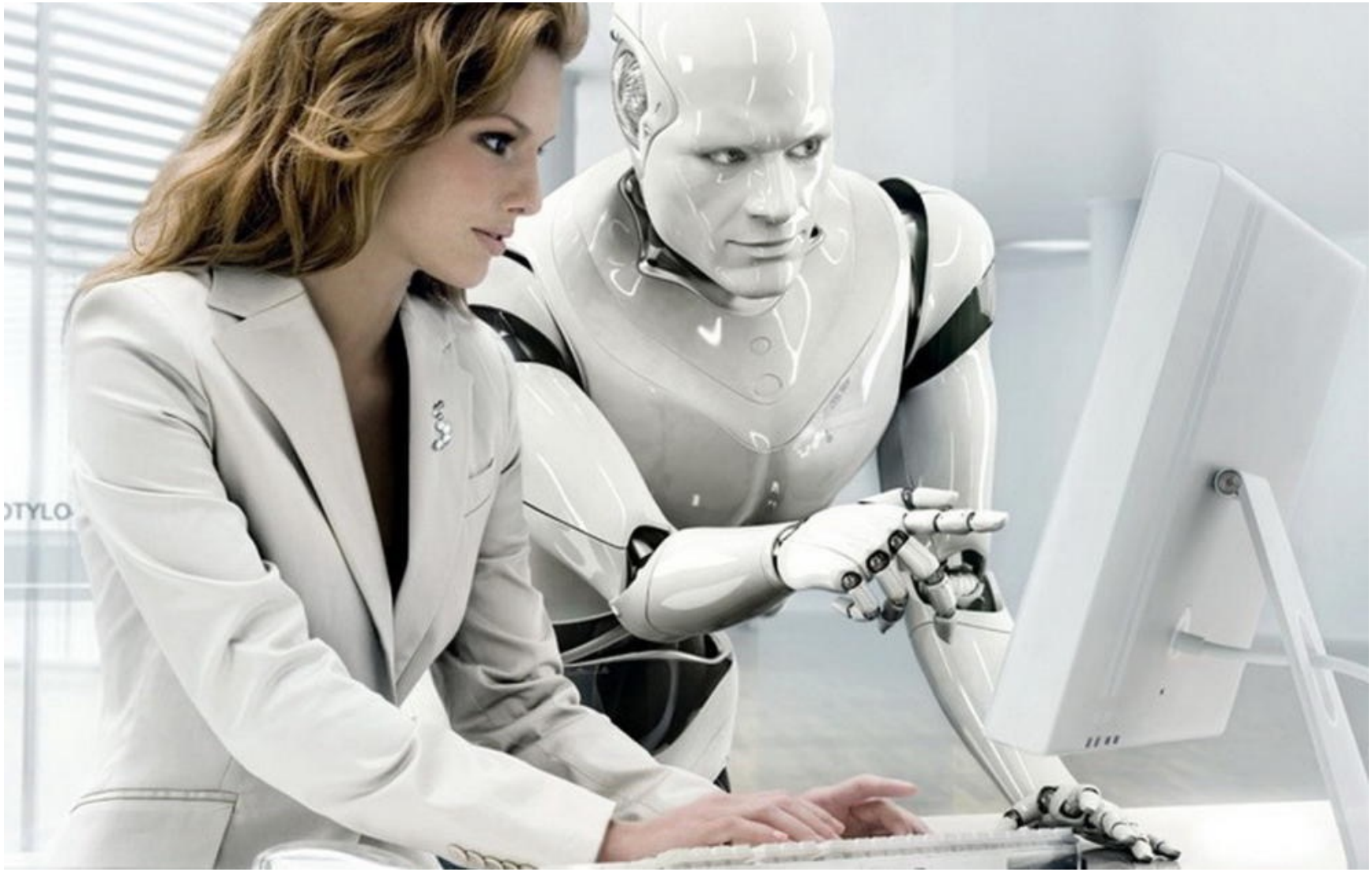
Delegado de protección de datos

Cuando es OBLIGATORIO un DPD (art. 37 RGPD y 34 LOPD):

- *RGDP:* ***Entidades públicas****; Privadas que tratan datos especiales a gran escala, en su actividad principal*
- El art. 34 LOPDGDD recoge un listado de entidades que DEBEN contar con un DPO.
  - Colegios profesionales.
  - Centros docentes.
  - Empresas de seguridad privada…
  - Etc.



¿UN DESPACHO DE ABOGADOS TIENE QUE TENER UN DPO?



DPO y abogacía

Los despachos de abogacía cuando lleven a cabo tratamientos de datos relativos a condenas e infracciones penales (incluidos los relativos a medidas cautelares y de seguridad conexas) considerados "a gran escala", deberán designar DPO.

Cuando nos referimos al ejercicio individual, ese letrado/a no requiere nombrar un DPO.

Artículo 37. LOPD *Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.*

1. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado **podrá, con carácter previo a la presentación de una reclamación** contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.

En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

2. Cuando el afectado **presente una reclamación** ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, **aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.**

Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

Delegado de protección de datos

Fuente: Miguel Recio, 2018.

Delegado de protección de datos

- ✓ Obligación de **comunicación en 10 días a la AEPD** que lo publicara en su sede electrónica. (art. 34.3 y 4 LOPD).
- ✓ La figura del DPD (art 37.5): debe ser designado atendiendo a sus cualidades profesionales y, en particular, se refiere expresamente el Reglamento a sus **conocimientos especializados del Derecho y la práctica en materia de protección de datos** y a su capacidad para desempeñar las funciones asignadas.
- ✓ Art. 35 LOPD*: "sea una persona física o jurídica, podrá demostrarse entre otros medios a través de **mecanismos de certificación**".*
- ✓ En el **Esquema de la AEPD de certificación de delegados de protección de datos** se recogen las competencias requeridas: **MODELO DE CERTIFICACION**: dos esquemas de certificación (siguiendo los criterios de la norma internacional ISO/IEC 17024:2012) de la siguiente forma:
  1. esquema que acredite aquellas entidades para que, a su vez, puedan actuar como certificadoras de DPO. Corresponderá a **ENAC** acreditar a las mencionadas entidades.
  2. esquema para certificar a DPOs, es decir, los requisitos necesarios para que se pueda obtener esta certificación.

ENAC
Entidad Nacional de Acreditación

Sede Electrónica

- ¿Qué es la sede?
- Normativa
- Procedimientos electrónicos
- Perfil de contratante
- Consultas/FAQS
- Firma electrónica
- Novedades e incidencias

datos abiertos
Reutilice la Información de la Agencia

Comunicación del Delegado de Protección de Datos

El Reglamento General de Protección de Datos (RGPD) dispone que los responsables y encargados de tratamiento deberán designar un Delegado de Protección de Datos (DPD) en los supuestos que el propio RGPD establece, así como en otros casos en que la legislación de los Estados Miembros lo considere también obligatorio.

Entre los supuestos en que habrá de designarse un DPD se encuentra el de que "el tratamiento lo lleve a cabo una autoridad u organismo público", tanto en calidad de responsable como en funciones de encargado de tratamiento (art. 37.1.a RGPD).

Además, en el ámbito de las entidades del sector privado el RGPD establece algunos supuestos en los que es también obligatoria la designación de los DPD tanto para los responsables como para los encargados del tratamiento.

El RGPD establece en su artículo 37.7 que "El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control".

El RGPD fue publicado en mayo de 2016 y entró en vigor en ese mismo mes. Sin embargo, será aplicable sólo a partir del 25 de mayo de 2018. La designación de los DPD en el ámbito público y en el privado que resulten obligados deberá haberse producido con antelación a esa fecha.

Además, las empresas que, aunque no resultan obligadas por las previsiones del RGPD, consideran necesario implantar esta figura en el seno de sus corporaciones pueden utilizar este formulario con el fin de proceder a su comunicación.

Solicitar

Con Certificado

Medidas de seguridad

El art. 24.1 del RGPD impone la obligación de adoptar **medidas técnicas y organizativas adecuadas a la naturaleza, el ámbito, el contexto y los fines** del tratamiento, así **como los riesgos** de diversa índole y gravedad (**destrucción, perdida o alteración accidental, y el acceso o cesión no autorizadas**).

Realización de análisis y gestión de riesgos en los despachos

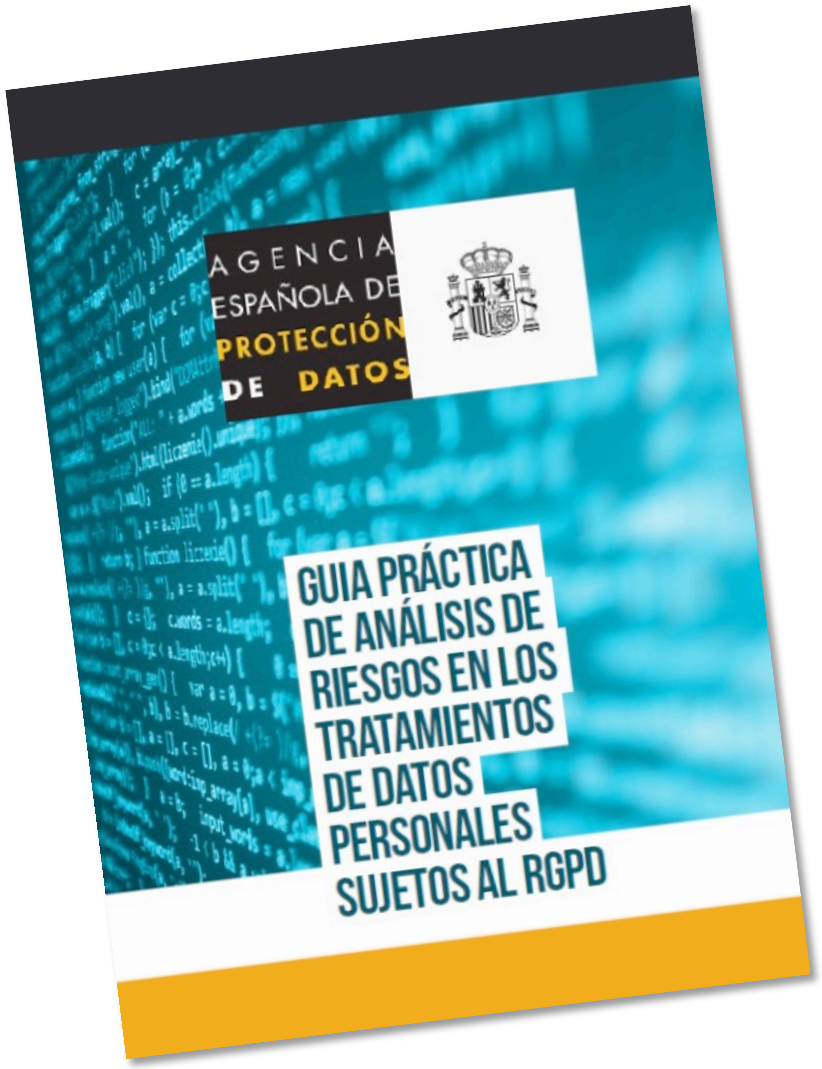
El RGPD impone la obligación de todo responsable del tratamiento de adoptar medidas técnicas y organizativas adecuadas a la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa índole y gravedad para los derechos de las personas.

Se exige, por tanto, que los abogados/as o procuradores/as o sus despachos evalúen los riesgos inherentes al tratamiento que realicen y aplicar las medidas adecuadas para mitigarlos (artículos 24.1; 32.1; Considerando 83 RGPD).

La aplicación de las medidas de seguridad previstas por el RGPD debe adaptarse a las características de los despachos de abogacía.

Los riesgos en un despacho pueden afectar:

- A la integridad de los datos (modificación o alteración).
- A la disponibilidad de los datos (pérdida o borrado, accidental o no).
- A la confidencialidad de los datos (accesos no autorizados).
- Al ejercicio de los derechos de los clientes interesados, como, por ejemplo, la ausencia de procedimientos de respuesta…..etc.



*"**Gestión de riesgos** es el conjunto de actividades y tareas que permiten controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como, las medidas para su reducción o mitigación."*

Fuente:
http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/AnalisisDeRiesgosRGPD.pdf

Informes y Guías de Interés

Guía para gestionar una fuga de información en un despacho de abogados. Se publica en colaboración con el Instituto Nacional de Ciberseguridad (INCIBE) y la Agencia Española de Protección de Datos. Está accesible en la dirección http://www.abogacia.es/2012/10/24/guias-tic-gestionar-una-fuga-de-informacion/ (acceso 20/03/2020).

Guía de gestión de riesgos. En esta Guía se presenta de forma práctica como abordar dicha gestión en el ámbito de las tecnologías de la información. Abogacía Española e Instituto Nacional de Ciberseguridad (INCIBE). Está accesible en la dirección http://www.abogacia.es/2012/03/14/guias-tic-gestion-de-riesgos/ (acceso 20/03/2020).

Buenas prácticas informáticas para la abogacía. Se publica en colaboración con el Instituto Nacional de Ciberseguridad (INCIBE) y la AEPD. Disponible en https://www.abogacia.es/wp-content/uploads/2018/09/Buenas-practicas-informaticas-para-la-Abogacia.pdf (acceso 20/03/2020).

"Informe de la AEPD sobre la utilización del *Cloud Computing* por los despachos de abogados y el derecho a la protección de datos de carácter personal» de junio de 2012. Disponible en https://www.abogacia.es/wp-content/uploads/2012/07/informe_CLOUDCOMPUTING.pdf (acceso 20/03/2020).

Evaluaciones de impacto sobre la protección de datos (EIPD) Arts. 35 y 36 REPD. Considerando 84.

- ✓ La realización de evaluaciones de impacto es, básicamente, un **ejercicio de análisis de los RIESGOS** que un determinado sistema de información, producto o servicio puede entrañar para el derecho a la protección de datos y, como consecuencia de ese análisis, la gestión de dichos riesgos mediante **la adopción de las MEDIDAS necesarias para eliminar o mitiga**r en lo posible aquellos que se hayan identificado.

Supuestos tasados en los que se exige una Evaluación de impacto

1. que pudieran generar discriminación.

2.conllevar una usurpación de identidad.

3.generar fraude.

4 pérdida de confidencialidad de datos sujetos al secreto profesional, como por ejemplo abogados o médicos.

5.reversión no autorizada de la seudonimización.

6.cualquier perjuicio económico, moral o social significativo para los afectados.

7. privar a los afectados de sus derechos o pudiera impedirles el ejercicio del control sobre sus datos personales.

8.tratamiento no meramente incidental o accesorio de las categorías especiales de datos (de los arts. 9 y 10 RGPD) o de los datos relacionados con infracciones administrativas.

9.evaluación de aspectos personales de los afectados con la finalidad de perfilado en: el ámbito de rendimiento laboral, situación y solvencia económica, salud, preferencias personales, comportamiento y geolocalización.

10 tratamiento de datos de personas de especial vulnerabilidad, en particular, menores de edad y discapacitados.

11.tratamientos masivos de datos personales.

12. cuando hay transferencias internacionales de datos (TID) habituales sin que se hubiese declarado un nivel adecuado de protección.

13..cualesquiera otros que pudieran tener relevancia para el responsable o encargado del tratamiento.

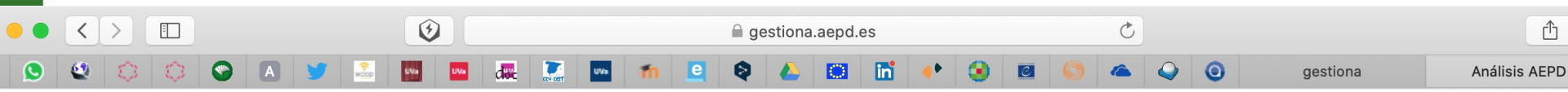
14.aquellos previstos en códigos de conducta.

15 aquellos estándares definidos por esquemas de certificación.

El artículo 35 RGPD, cuando trata los supuestos en los que se exige la realización de una EIPD, se refiere, entre otros, a la realización de tratamientos a gran escala de las categorías especiales de datos (contemplados en el artículo 9, apartado 1 RGPD), o de los **datos personales relativos a condenas e infracciones penales** (a que se refiere el artículo 10 RGPD).

Sin embargo, los abogados/as y procuradores/as **que ejerzan su actividad de forma individual no tendrán, a priori, obligación de realizar una evaluación de impacto**, a la vista de la "*Lista orientativa de la AEPD sobre tipos de tratamientos que no requieren una EIPD*", según el artículo 35.5 RGPD y Considerando 91 RGPD.

En definitiva, **un despacho de abogacía penalista (no así aquellos que trabajen otras disciplinas) conformado por más de un letrado/a o procurador/a está obligado a realizar, no sólo un informe de riesgos, sino una evaluación de impacto en protección de datos**, a diferencia de lo que se exige, a un letrado o procurador que desarrolla su actividad de forma individual.



GESTIONA EIPD

La Evaluación de Impacto en la Protección de Datos Personales (EIPD) es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos. El análisis de riesgos para un determinado tratamiento permite identificar los riesgos que se ciernen sobre los datos de los interesados y establecer una respuesta adoptando las salvaguardas necesarias para reducirlos hasta un nivel de riesgo aceptable.

La EIPD es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.

El resultado de la EIPD se debe tener en cuenta, necesariamente, a la hora de tomar las decisiones relacionadas con el cumplimiento de lo previsto en el RGPD y la toma de decisión de la viabilidad o no de llevar a cabo el tratamiento de los datos.

Una EIPD no se requiere siempre, en cada actividad de tratamiento, se debe valorar la necesidad de llevar a cabo la misma. Es fundamental realizar el siguiente análisis previo para determinar de forma preliminar el nivel de riesgo al que puede estar expuesto el tratamiento y tomar la decisión adecuada en base a ello.

Herramienta FACILITA

Cargar análisis previos

Iniciar nueva EIPD

Iniciar análisis de riesgos

Consulta previa a la AEPD en las Evaluaciones de impacto

- ✓ El responsable **debe consultar a la AEPD o autoridad de control**, previamente a comenzar el tratamiento de datos cuando una evaluación de impacto muestre que el **tratamiento entrañaría un alto riesgo** si el responsable no toma medidas para mitigarlo (art. 36.1).
- ✓ La autoridad de control deberá, en un plazo de **8 semanas** desde la solicitud de la consulta, asesorar por escrito al responsable

*"(84) El **resultado** de la evaluación debe tenerse en cuenta cuando se decidan las **medidas adecuadas** que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un **alto riesgo** que el responsable no puede mitigar con medidas adecuadas en términos de **tecnología disponible y costes de aplicación**, debe **consultarse a la autoridad de control antes del tratamiento**."*

Sede Electrónica

- ¿Qué es la sede?
- Normativa
- Procedimientos electrónicos
- Perfil de contratante
- Consultas/FAQS
- Firma electrónica
- Novedades e incidencias

datos abiertos
Reutilice la Información de la Agencia

Consulta previa al inicio de tratamientos de riesgo alto (art. 36 RGPD)

Este trámite electrónico **está dirigido exclusivamente a responsables del tratamiento** (en adelante, responsables) cuya Evaluación de Impacto relativa a la Protección de Datos (en lo siguiente, EIPD) muestre que el tratamiento sigue teniendo un **alto riesgo para los derechos y libertades de los interesados** aún tras aplicar las garantías, medidas de seguridad y mecanismos de protección razonables en cuanto a técnica disponible y costes de aplicación.

No es un trámite dirigido a ciudadanos ni a responsables que no requieran completar una EIPD. Tampoco va dirigido a responsables que hayan conseguido mitigar el riesgo tras la aplicación de las medidas oportunas. Para estos casos, la AEPD pone a su disposición medios de consulta y petición de información a través del canal del ciudadano y el del responsable, respectivamente.

El procedimiento de Consulta Previa, regulado en el artículo 36 del *Reglamento General de Protección de Datos*, obliga al responsable a **consultar a la autoridad de control** (Agencia Española de Protección de Datos) **antes de proceder al tratamiento** cuando una evaluación de impacto relativa a la

Servicios

- Canales de acceso
- Quejas y sugerencias
- Fecha hora y calendario de días hábiles
- Estado de la tramitación
- Guía de navegación
- Medios electrónicos
- Verificar la integridad del documento con CSV
- Certificado y sello electrónico de la sede
- Notificación por Comparecencia en Sede

Enlaces de Interés

- B.O.E.
- Administracion.gob.es
- CERES
- DNI Electrónico
- Ventanilla Única de la Directiva

Medidas de seguridad de mínimos.

- ✓ El REPD, en su artículo 32, referido a la "seguridad del tratamiento" determina una serie de medidas que deben implementarse como **MINIMO**. Teniendo en cuenta el **estado de la técnica, los costes, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad** variables , el responsable y el encargado deben aplicar medidas para garantizar un **nivel de seguridad adecuado al riesgo,** que incluya, entre otros:

  - ✓ La **seudonimización**: separación de los datos identificativos con barreras técnicas u organizativas que impidan su identificación posterior.
  - ✓ El **cifrado** de datos personales.
  - ✓ La capacidad de garantizar la **confidencialidad, integridad, disponibilidad y resiliencia** (capacidad de un sistema de soportar y recuperarse ante desastres y perturbaciones.) permanentes de los sistemas y servicios de tratamiento.
  - ✓ La **capacidad de restaurar** la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
  - ✓ Un proceso de **verificación, evaluación y valoración regulares** de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Motivaciones de los atacantes:

El FBI ha acuñado el acrónimo MICE para resumir las distintas motivaciones de los atacantes:

-Money (DINERO)

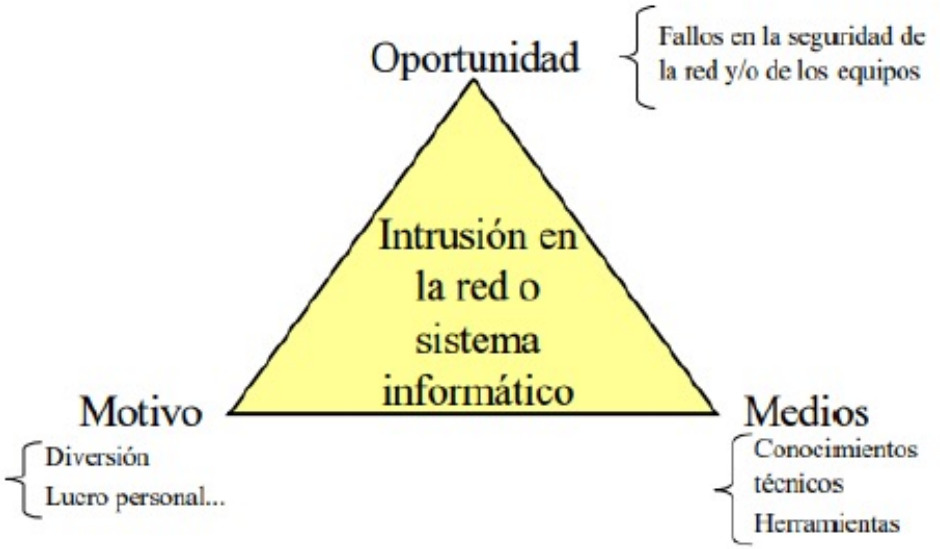
-Ideology (IDEOLOGÍA)

-Compromisey (COMPROMISO)

-Ego (EGO)

Triángulo de la Intrusión:

Para poder llevar a cabo un ataque informático los intrusos deben disponer de los medios técnicos, los conocimientos y las herramientas adecuadas, deben contar con una determinada motivación o finalidad, y se tiene que dar además una determinada oportunidad que facilite el desarrollo del ataque.



Las 5 leyes de la Ciberseguridad (Nick Espinoza, 2018)

1. **Si existe una vulnerabilidad, será explotada.**
2. **Todo es vulnerable de alguna manera, incluso con pensamiento lateral.**
3. **El ser humano es el activo más vulnerable, porque confía.**
4. **Con cada innovación llegan nuevas vulnerabilidades.**
5. **En caso de duda, aplíquese la Ley 1.**

https://www.ted.com/talks/nick_espinosa_the_five_laws_of_cybersecurity?language=es

Incidencias seguridad en despachos de abogados

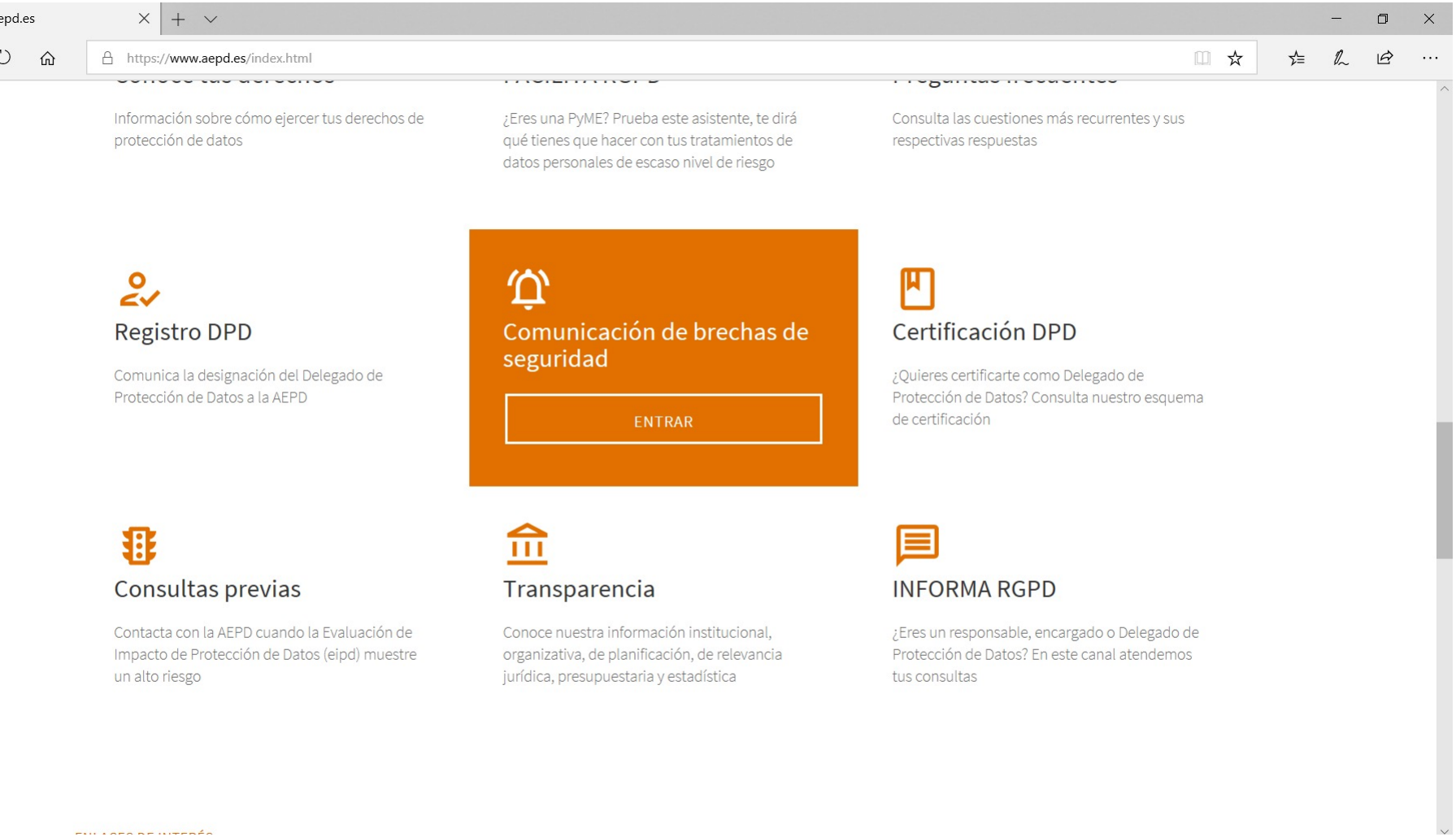
- ✓ Según datos del Instituto de Ciberseguridad de España (INCIBE), gestionó más de 130.000 incidentes de ciberseguridad durante el año 2020.
- ✓ https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2020_incibe.pdf
- ✓ En despachos de abogados:
  - **ransomware**, programas informáticos que infectan y bloquean los archivos y sistemas, exigiendo el pago de un rescate a cambio de liberarlos.
  - **páginas web de despachos con programas maliciosos inyectados**, otras **víctimas de una alteración** de su apariencia original, y **webs de bufetes con alojamiento de phishing**,

Notificación de violaciones o quiebras de la seguridad de los datos a la AEPD (art. 33 RGPD).

- ✓ Si se detecta una violación de la seguridad de los datos, se impone la **OBLIGACION a notificarla**, sin dilación indebida, **a la autoridad de control**, a **más tardar 72 horas después** de que haya tenido constancia de ella.

- ✓ Esta obligación **no se impone** en el caso de que "sea **improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas**". Es, decir, el responsable debe **analizar subjetivamente** el supuesto concreto y determinar ese improbable riesgo.

- ✓ En cualquier caso, el responsable **debe documentar cualquier violación** de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas (art. 33.5).

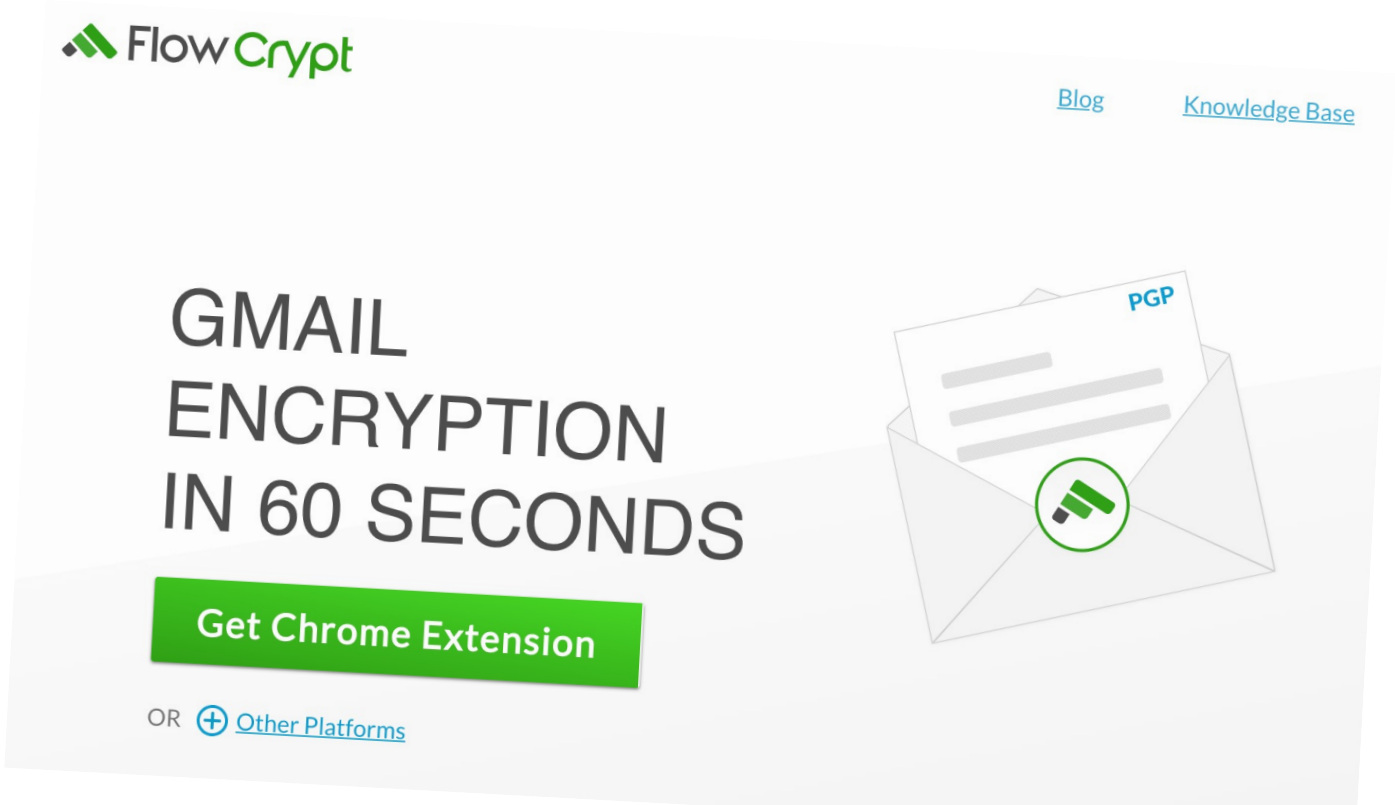

epd.es
https://www.aepd.es/index.html
Información sobre cómo ejercer tus derechos de protección de datos
¿Eres una PyME? Prueba este asistente, te dirá qué tienes que hacer con tus tratamientos de datos personales de escaso nivel de riesgo
Consulta las cuestiones más recurrentes y sus respectivas respuestas
Registro DPD
Comunica la designación del Delegado de Protección de Datos a la AEPD
Comunicación de brechas de seguridad
ENTRAR
Certificación DPD
¿Quieres certificarte como Delegado de Protección de Datos? Consulta nuestro esquema de certificación
Consultas previas
Contacta con la AEPD cuando la Evaluación de Impacto de Protección de Datos (eipd) muestre un alto riesgo
Transparencia
Conoce nuestra información institucional, organizativa, de planificación, de relevancia jurídica, presupuestaria y estadística
INFORMA RGPD
¿Eres un responsable, encargado o Delegado de Protección de Datos? En este canal atendemos tus consultas

ENCRIPTACION

https://www.acerodocs.com/es/ cifrar archivos 50/60 euros año

AxCrypt o DiskCryptor.

FLOWCRYPT: encriptar mensajes desde gmail



Servicio AntiBotnet (INCIBE)

https://www.osi.es/es/servicio-antibotnet

Resumen del diagnóstico

Su nivel de seguridad es adecuado pero mejorable. Ya es consciente de que sus empleados son uno de los elementos en los que más tiene que invertir en Ciberseguridad y tiene algunas medidas pero aún le falta hacer un esfuerzo para organizar y controlar mejor algunos aspectos.

- El **Kit de concienciación** puede ser muy útil para fortalecer este eslabón de la cadena.
- Aún le queda camino que recorrer para establecer unas políticas adecuadas, le recomendamos intente establecer un **Plan Director de Seguridad**.
- Si la web es una parte esencial para su negocio puede seguir los consejos de la sección **Protege tu web**.
- En caso de que los dispositivos móviles sean imprescindibles para su actividad revise el apartado de **Protección en movilidad y conexiones inalámbricas**.

Ahora que ya conoces el nivel de riesgo de tu empresa, ¿quieres conocer el estado de seguridad de tu datos? Puedes hacerlo con la herramienta EVALÚA de la Agencia Española del Protección de Datos.

El resultado de la encuesta concluye que el riesgo en su empresa es:

45.4%

Este porcentaje está considerado como

RIESGO MEDIO

Niveles de riesgo

Personas	54.3%	Riesgo MEDIO	¿Quieres reducirlo?
Procesos	41.6%	Riesgo MEDIO	¿Quieres reducirlo?
Tecnología	40.3%	Riesgo MEDIO	¿Quieres reducirlo?

Comparte esta herramienta en las redes sociales

Permite que tus contactos y amigos evalúen los riesgos de seguridad de su negocio en tan solo cinco minutos.

Volver a la página principal

Presentación

Introducción

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en adelante LOPD-, establece un conjunto de principios, derechos y deberes que requieren adaptar las organizaciones para su cumplimiento. Empresas, asociaciones, autónomos, o administraciones, tratan datos personales para su gestión ordinaria y ello les obliga a plantearse muchas preguntas:

- ¿Qué son datos personales?
- ¿Qué es un fichero?
- ¿Qué es un tratamiento?
- En caso de tratar datos, ¿hay algún dato exento de la LOPD?
- ¿Cuáles son mis obligaciones?

Esta herramienta ofrece respuesta a éstos y a muchos otros interrogantes mediante un procedimiento de diagnóstico basado en un autotest basado en preguntas con respuesta múltiple. Basta con realizar el mismo para que al final, la Agencia Española de Protección de Datos, le facilite un informe con indicaciones y recursos que le orienten, en su caso, para cumplir con lo dispuesto en la LOPD.

El informe que emitirá el programa depende de sus respuestas por ello no olvide seguir las siguientes instrucciones:

1. Lea atentamente la información previa, le ayudará a comprender los principales conceptos y a identificar los elementos que debe conocer de su organización antes de iniciar el autotest.
2. Cada pregunta incluye un pequeño enlace a una "ayuda", si no comprende la pregunta pínchelo y léalo atentamente.
3. El test le ocupará aproximadamente entre 30 y 45 minutos. Si Ud. desea abandonarlo se le proporcionará un código que le permite reanudarlo en cualquier momento guardando la información.
4. El test es completamente anónimo, la Agencia Española de Protección de Datos no identifica a quienes lo realizan y su formalización no genera responsabilidad alguna.
5. El resultado del test es meramente orientativo. Es una herramienta de ayuda cuyos resultados dependen de las respuestas facilitadas. Por lo tanto, su realización no exime del cumplimiento de la LOPD ni podrá exhibirse con la finalidad de justificar o eximir la responsabilidad ante una eventual infracción.

Conceptos Previos

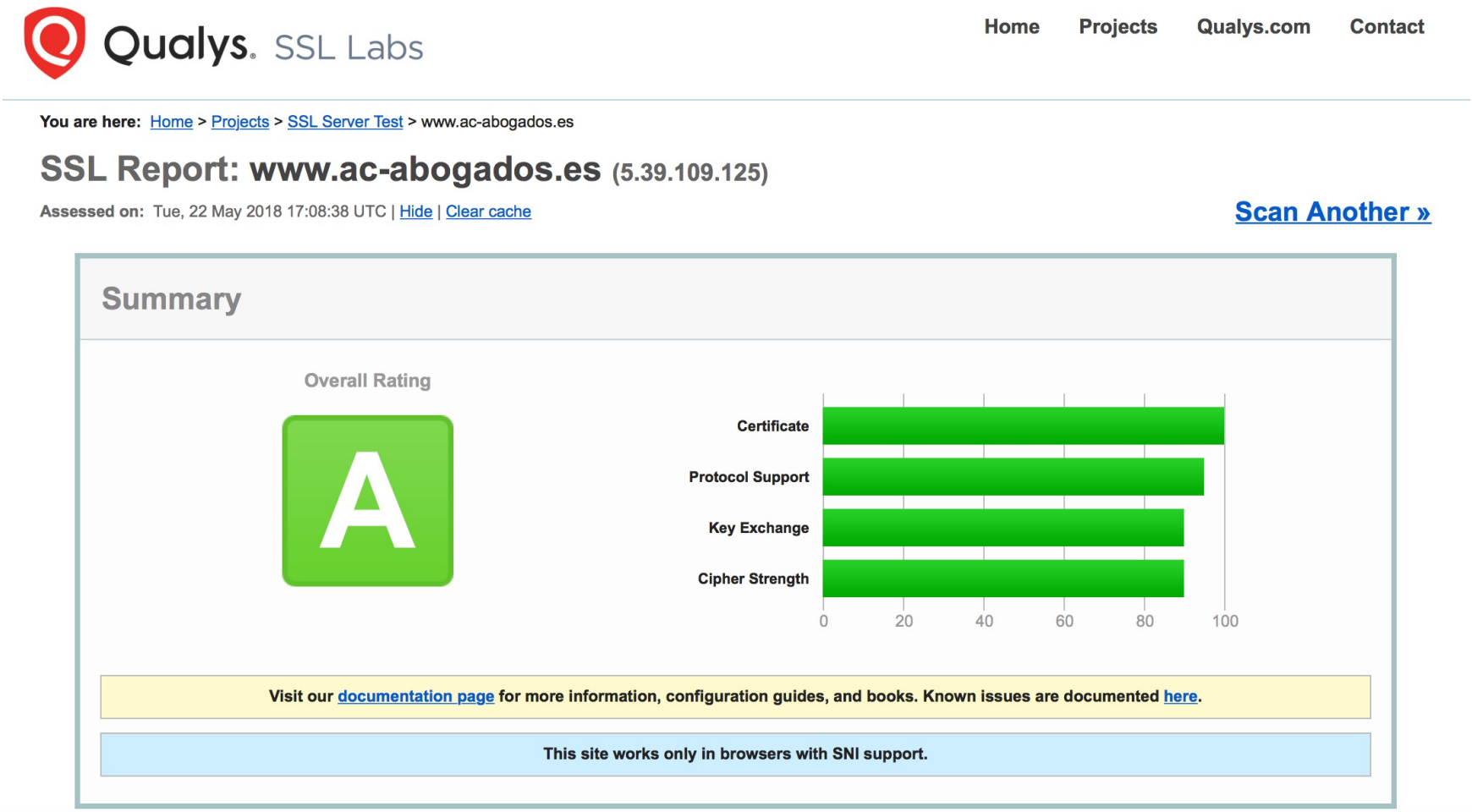
Realice esta suma

35 + 16 =

IniciarEncuesta ContinuarEncuesta

https://www.ssllabs.com/ssltest/index.html

Averigua el nivel de seguridad SSL de la página web (HTTPs)



Guías Abogacía Española

https://www.abogacia.es/tag/guias-tic/?seccion=actualidad

Buenas prácticas informáticas para la abogacía

Hoy en día las empresas, y también los despachos de abogados, basa
sistemas de información, apoyando su gestión con los nuevos soport
la mayoría de despachos no disponen de un departamento de inform

Decálogo de buenas prácticas en ciberseguridad para la Abogacía

El buen funcionamiento e, incluso, la supervivencia de los despacho
depende en gran medida de su adaptación al medio online. Hoy en
algunos inmersos en procesos de digitalización, pero todos inmersos en un entorno

Guía de Ciberseguridad y reputación online para despachos de abogados

Los despachos de abogados son cada vez más conscientes de la imp
comunicación a través de medios digitales, incluidas las redes socia
online del despacho se convierte, así, en una medida de la opinión que los demás …

GUIAS TIC: Gestión de riesgos

La gestión de riesgos está presente en distintos ámbitos de la sociedad y la
supuesto, en el ejercicio de la Abogacía. En esta Guía TIC Abogacía Español
de forma práctica como abordar dicha gestión en … [+]

Glosario de terminología TIC

¿Sabes qué significan las siglas ADSL? ¿De qu
¿Qué es un motor de búsqueda? ¿A qué corre
muchas cuestiones responde este 'Glosario d

GUÍAS TIC: Gestionar una fuga de información

Una fuga de información es una las mayores amenazas a las que se
de abogados. No hay que olvidar que la abogacía es una profesión
confianza que los clientes depositan en estos … [+]

Notificación de violaciones o quiebras de la seguridad de los datos a los afectados.

- ✓ Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable **lo deberá comunicar al interesado sin dilación indebida** con un "lenguaje claro y sencillo", como mínimo (art. 34 y C86).:
  - La naturaleza de la violación de la seguridad de los datos.
  - Nombre y datos de contacto del DPO de la organización.
  - Una descripción de las posibles consecuencias de la violación de seguridad.
  - Una descripción de las medidas adoptadas para corregir la violación o, a menos, mitigar sus efectos.
- ✓ **Esta comunicación NO es necesaria si se cumplen ALGUNA de las condiciones siguientes**
  - el responsable haya adoptado medidas de protección apropiadas sobre los datos afectados, en particular aquellas que hagan ininteligibles los datos personales para personas no autorizadas, como el cifrado;
  - el responsable haya tomado **medidas ulteriores que garanticen que ya no exista la probabilidad** de que se concretice el alto riesgo
  - suponga un **esfuerzo desproporcionado.** En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

OBLIGACIONES PARA LOS ABOGADOS

1. Existencia y mantenimiento de un **registro de las actividades de tratamiento de datos** (artículo 30 RGPD).
2. **Informacion / hojas de encargo /página web**.
3. El despacho de abogados debe hacer un **análisis de riesgos** (art. 32.1 RGPD) y determinar las **medidas de seguridad adecuadas**, pero (salvo penalistas o y ejercicio colectivo) **NO** una **evaluación de impacto** (art. 35 RGPD).
    - Análisis de riesgos desde una doble vertiente: 1) medidas de seguridad técnicas y organizativas 2) riesgos para los derechos de las personas.
    - Medidas de seguridad adecuadas entre otros (art.32.1) seudonimización; cifrado; capacidad de garantizar confidencialidad, integridad, disponibilidad, resiliencia, restaurar la disponibilidad y acceso a los datos; procesos de verificación, evaluación y valoración regulares.
    - **Notificación de «quiebras de seguridad»** (concepto: art. 4.12), en 72 horas tanto a la autoridad de control, como a los interesados (arts 33 y 34 RGPD). No imposición de sanciones por la AEPD salvo gravedad.
4. **Medidas de Protección de datos desde el diseño** (artículo 25.1 RGPD) **y por defecto** (artículo 25.2 RGPD).
5. **No** se requiere la existencia de un **delegado de protección de datos** (artículos 37 a 39 del RGPD) **(DE MODO GENERAL).**
6. Adhesión (según el artículo 24.3 RGPD) a **códigos de conducta** (artículo 40 RGPD) o **mecanismos de certificación** (artículos 25.3 y 42 RGPD).

MUCHAS GRACIAS

Javier Alvarez Hernando. Abogado.
@_JavierAlvarez