Protección de datos de carácter personal (II)

[3.1] ¿Cómo estudiar este tema?

[3.2] Novedades del RGPD

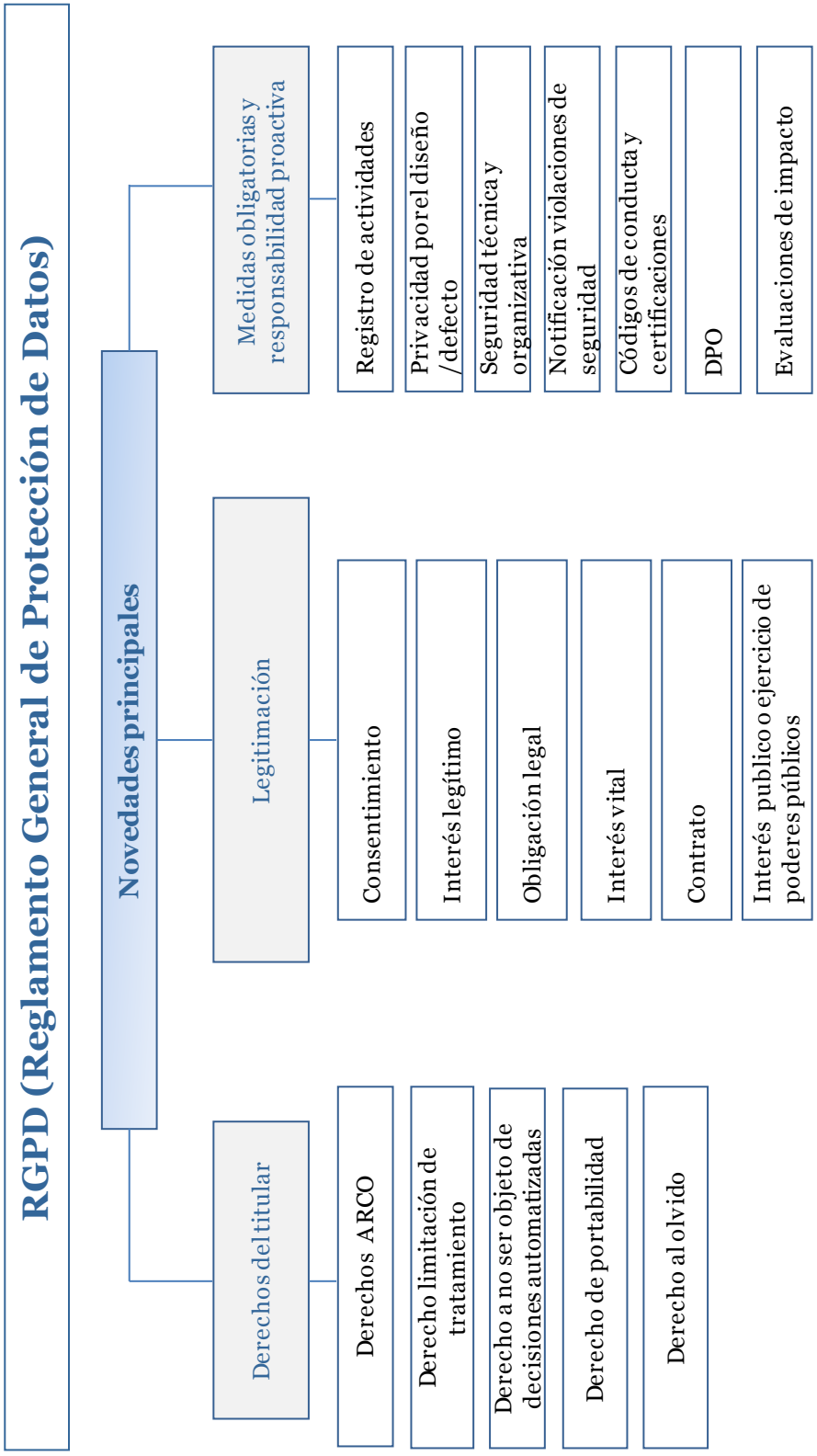
[3.3] Las medidas de cumplimiento y responsabilidad proactiva

[3.4] Las notificaciones de violaciones de seguridad

[3.5] El régimen sancionador

TEMA 3

Esquema



Ideas clave

3.1. ¿Cómo estudiar este tema?

Para estudiar este tema deberás leer y comprender las **Ideas clave** expuestas en este documento.

En este tema veremos las siguientes cuestiones:

- Analizar las **diferencias** entre las comunicaciones de datos y los supuestos del encargado del tratamiento.
- Analizar las novedades del RGPD, las obligaciones de los responsables de tratamiento y derechos de los titulares de datos personales.
- Profundizaremos sobre los diferentes tipos de legitimación del tratamiento de datos en el RGPD.
- Estudiaremos las medidas de cumplimiento según el RGPD.
- Analizaremos la privacidad desde el diseño y por el defecto y la figura del delegado de protección de datos.
- Entenderemos cuál es la obligatoriedad respecto a la notificación de las brechas de seguridad.

3.2. Novedades del RGPD

Novedades en las obligaciones del responsable

A tener en cuenta que:

- El **deber de información** en la recogida por parte del responsable.
  - Es un deber «prestacional» y el contenido esencial del derecho.
  - Es el requisito necesario para la existencia de consentimiento.
  - No puede concebirse como una mera operación formal
  - Debe ser contextual, funcional al tratamiento y si es necesario debe complementarse.

- El **poder de disposición del individuo**:
  - Es *consentir o rechazar* un tratamiento de datos sobre él mismo.

- ¡Atención! Este poder no se agota con el mero consentimiento, ya que podrá ejercitar los derechos ARCO (siempre que sepa qué tratamiento y quién es el responsable).

- El responsable del tratamiento deberá informar en relación con los siguientes aspectos (contenido mínimo):
  - Identidad y 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.
  - 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.
  - En el supuesto de que la comunicación de datos personales sea obligatoria, se deberá informar de las posibles consecuencias de no facilitar los datos.
  - Información sobre la posible existencia de decisiones automatizas, incluida la elaboración de perfiles, la lógica aplicada y las consecuencias previstas.

- Cuando los datos personales **se recaben de los interesados,** se puede facilitar la «**información por capas**», distinguiendo entre una información básica (primer nivel) y una información adicional (segundo nivel).

- Por su parte, el RGPD establece una regulación más exigente en relación con la «Información que deberá facilitarse cuando los datos personales **no se recaben del interesado».** En dicho precepto se dispone que en este caso:
  - Se deberá informársele de las «categorías de datos que se van a tratar».
  - De la «fuente de la que proceden los datos personales».
  - En su caso, sobre si proceden de «fuentes de acceso público».

Derechos de los interesados

Figura 1. Derechos de los interesados.

A. Derechos de acceso, rectificación y supresión.

- **Derecho a acceso.** Antes del RGPD se debían facilitarse todos los datos de base del afectado, pero no las copias o documentos (excepto en el caso de la historia clínica). Después, con la llegada del RGPD, se reconoce el derecho a obtener una copia de los datos personales objeto del tratamiento. Ahora, los responsables podrán atender a este derecho facilitando el acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales.

- **Derecho a rectificación.** Este derecho supone la posibilidad de que el titular de dichos datos obtenga la modificación de sus datos personales **inexactos o incompletos**, debiendo en la solicitud de rectificación indicar **qué datos** desea que se modifiquen o corrijan. A dicha solicitud, el titular de los datos deberá acompañar la documentación justificativa en la que base su pretensión. El RGPD reconoce específicamente tanto el derecho de rectificación como el de supresión de los datos de carácter personal, regulándolos como derechos independientes.

- **Derecho de supresión (al olvido)**: Este derecho tiene por objeto la eliminación de los datos personales cuando:
  - Los datos personales **ya no sean necesarios.**
  - El interesado **retire el consentimiento**.
  - El interesado **se oponga** al tratamiento.
  - Los datos personales hayan sido tratados **ilícitamente**.
  - Los datos personales deban suprimirse para el cumplimiento de una **obligación legal.**
  - Los datos personales se hayan obtenido en relación con la oferta de servicios de la **sociedad de la información**.

Las **excepciones** que se contemplan al ejercicio de este derecho son: a) para ejercer el derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos c) por razones de interés público d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

A su vez, en el RGPD, se realiza una referencia al **Derecho al olvido,** que se vincula con el propio derecho de supresión. La AEPD fue pionera al considerar que el tratamiento de datos que realizan los motores de búsqueda de Internet, tales como *Google, Bing o Yahoo*, está sometido a las normas de protección de datos de la Unión Europea, y que los ciudadanos pueden solicitar, bajo ciertas condiciones, que los enlaces a sus datos personales no aparezcan en los resultados de una búsqueda realizada por su nombre y apellidos. Esta tesis propugnada por la AEPD fue avalada en 2014 por el Tribunal de Justicia de la Unión Europea, y se popularizó con la denominación de «Derecho al olvido». No está considerado un **derecho autónomo o diferenciado** de los clásicos derechos ARCO, sino la consecuencia de la aplicación del derecho al borrado de los datos personales. En definitiva, se trata de una manifestación de los derechos de cancelación u oposición en el **entorno *online*** (según la jurisprudencia que el Tribunal de Justicia de la UE estableció en el caso Google Spain).

B. Derecho a la oposición

El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. Cuando el tratamiento de datos personales tenga por objeto la **mercadotecnia directa,** el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

C. Derecho a no ser objeto de decisiones individualizadas

Todo interesado tiene derecho a no ser objeto de una decisión basada *únicamente* en el tratamiento automatizado de su información de carácter personal, incluida la

elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Las **excepciones** a este derecho se concretan en los supuestos en que dicho tratamiento sea necesario para la celebración o ejecución de un contrato**,** esté permitido por el Derecho de la UE o de los Estados miembros -con medidas adecuadas para salvaguardar los derechos y libertades del titular de los datos-, o bien exista consentimiento explícito del titular de los datos.

D. Derecho a la portabilidad

Es una forma avanzada del derecho de acceso por el cual la copia que se proporciona al interesado debe ofrecerse en un formato **estructurado, de uso común y lectura mecánica**. El derecho a la portabilidad implica que los datos personales del interesado se transmiten **directamente** de un responsable a otro, sin necesidad de que sean transmitidos previamente al propio interesado, **siempre que ello sea técnicamente posible.**

Este derecho **solo** puede ejercerse:

- Cuando el tratamiento se efectúe por medios automatizados.
- Cuando el tratamiento se base en el consentimiento o en un contrato.
- Cuando el interesado lo solicita respecto a los datos que haya proporcionado al responsable y que le conciernan, incluidos los datos derivados de la propia actividad del interesado.

E. Derecho a la limitación del tratamiento

Supone que, a petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían. Se puede solicitar la limitación cuando: (i) El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender a la solicitud; (ii) el tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello; (iii) los datos ya no son necesarios para el tratamiento, que también determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

La existencia de estas limitaciones requiere su formulación por Ley, que **respete los derechos y libertades fundamentales.** Asimismo, se exige que se trate de una **medida necesaria y proporcionada** en una sociedad democrática para el logro de los objetivos.

Legitimación

El Reglamento europeo de protección de datos enumera las diversas bases jurídicas que **legitiman** el tratamiento de datos personales en términos de igualdad.

Figura 2. Legitimación.

A. El consentimiento.

Es una **manifestación de voluntad libre, específica, informada e inequívoca** por la que el afectado acepta el tratamiento mediante una declaración o una clara acción afirmativa. Se considera que puede existir un **acto afirmativo** claro en supuestos como una **declaración por escrito**, inclusive por medios electrónicos, o una declaración verbal. También puede considerarse un acto afirmativo:

- Marcar una casilla de un sitio web en Internet.
- Escoger parámetros técnicos para la utilización de servicios de la sociedad de la información,
- O cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales.

Por tanto, el silencio, las **casillas premarcadas** o la inacción del afectado **no constituyen un consentimiento válido.** En el caso de que el tratamiento tenga varios fines deberá prestarse para cada uno de ellos.

El Reglamento no implica necesariamente una obligación de recabar un nuevo consentimiento si el que se hubiera obtenido antes de su aplicación fuese conforme a los requisitos que establece. En ningún caso hay aplicación retroactiva, dado que las normas del Reglamento no se aplican a tratamientos anteriores al momento en que produce plenos efectos. Aunque pudimos ver el 25 de mayo de 2018 que números responsables de tratamiento mandaron emails masivos solicitando consentimiento nuevamente cuando no era necesario.

Accede a más información a través del siguiente enlace:
https://www.vozpopuli.com/economia-y-finanzas/ley-datos-correos-clientes-empresas_0_1138387045.html

B. El interés legítimo

Será necesario realizar en cada caso concreto una **ponderación** para poder determinar la prevalencia o no del interés legítimo. Ponderación que deberá tener en cuenta no solo la incidencia del tratamiento en los derechos y libertades del afectado, sino también en sus propios intereses. Se recogen algunos ejemplos de intereses legítimos, aunque sin considerarlos por sí mismos como prevalentes. Entre ellos se citan los siguientes:

- La *prevención del fraude*, siempre que se cumpla el principio de minimización.
- El *marketing directo*.
- Las transmisiones de datos en *grupos de empresas* para fines administrativos internos como puede ser la centralización de datos de clientes o empleados.
- Las transmisiones de datos para garantizar la seguridad de las redes, para impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.

La nueva LOPD recoge una previsión de gran importancia al establecer que una **LEY** pueda considerar que un tratamiento fundado en el interés legítimo del responsable o de un tercero prevalece sobre los derechos del afectado. En cuyo caso, **no sería necesario que los responsables que tratan los datos tengan que realizar una ponderación adicional.**

Finalmente, el Reglamento establece que el interés legítimo NO puede ser una base jurídica aplicable a los tratamientos realizados por las **autoridades públicas** en el ejercicio de sus funciones, al señalar que es el propio legislador el que debe establecer por **ley** la base jurídica para el tratamiento de datos por parte de las autoridades públicas.

C. Tratamientos necesarios para el cumplimiento de una obligación legal

Respecto de estas bases jurídicas el Reglamento prevé que deben ser establecidas por el derecho de la Unión o de los Estados miembro. La finalidad del tratamiento para el cumplimiento de una **obligación legal** debe quedar determinada en la norma que la establezca.

D. Tratamientos necesarios para el tratamiento para el cumplimiento del interés vital

El tratamiento de datos personales **es lícito cuando sea necesario para proteger intereses vitales** del interesado o de otra persona física. A esta base jurídica para el tratamiento tiene un carácter que podría calificarse como subsidiario, al indicar que la misma únicamente debe aplicarse cuando el tratamiento no puede basarse en otra base jurídica distinta. En este sentido cita como ejemplos el tratamiento con fines humanitarios, incluido el control de epidemias y su propagación o las situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

E. Tratamiento necesario para el cumplimiento de un interés público

La finalidad del tratamiento para el cumplimiento de una **misión de interés público o para el ejercicio de poderes debe ser necesaria para el cumplimiento o ejercicio de los mismos.** Ahora bien, el tratamiento de datos para estas finalidades deberá estar sujeto a garantías adecuadas para garantizar los derechos y libertades de los afectados conforme al Reglamento.

3.3. Las medidas de cumplimento y responsabilidad proactiva

El tratamiento solo será **lícito** si se cumple al menos **una** de las siguientes condiciones:

Figura 3. Condiciones.

Ahora, con el RGPD, los responsables y encargados (ambos) establecerán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo. El RGPD pide que se tomen en consideración más variables. El responsable **solo** debe elegir encargados que ofrezcan garantías de cumplimiento. A continuación, comentamos algunos elementos a tener en cuenta:

Relaciones entre responsable y encargado/s

El encargado del tratamiento no recurrirá a otro encargado sin la **autorización previa** por escrito, específica o general, del responsable. También informará de forma previa de cualquier cambio respecto a los mismos. En caso de subencargo de tratamiento, se mantendrán las **mismas obligaciones** de protección de datos que las estipuladas entre el responsable y el encargado, especialmente las relativas a las garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas. El contenido del contrato de encargo de tratamiento.

- Objeto, duración, naturaleza y la finalidad del tratamiento.
- Tipo de datos personales y categorías de interesados.
- Obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable.
- Condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones.
- Asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados.

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

El registro de actividades como nueva obligación

Responsables y encargados (ambos) deberán mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el RGPD y que contenga cuestiones como:

- Nombre y datos de contacto del responsable o corresponsable y del Delegado de Protección de Datos si existiese.
- Finalidades del tratamiento.
- Descripción de categorías de interesados y categorías de datos personales tratados.
- Transferencias internacionales de datos.

Están exentas las organizaciones que empleen a menos de 250 trabajadores, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales. Según la Guía del ciudadano de la AEPD, las posibilidades para organizar el registro de actividades de tratamiento son partir de los ficheros que actualmente tienen notificados los responsables en el Registro General de Protección de Datos, detallando todas las operaciones que se realizan sobre cada conjunto estructurado de datos.

Privacidad desde el diseño y por el defecto

- **Privacidad desde el diseño.** Implica que la protección de datos ha de estar presente en las **primeras fases** de concepción de un proyecto y formar parte de la lista de elementos a considerar antes de iniciar sucesivas etapas de desarrollo. Se tendrá en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los **riesgos** de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas. Estos requisitos se van a traducir en **medidas técnicas y organizativas** Un ejemplo de dichas medidas, que se establece de forma expresa en el RGPD, es que el propio tratamiento incorpore medidas para la **seudoanonimización** temprana o, **minimización de datos.**

- **Privacidad por defecto.** La idea principal estriba en que solo sean objeto de tratamiento los datos personales que sean estrictamente necesarios para cada uno de los fines de tratamiento y en los momentos en que sea estrictamente necesario. El principio de *need-to-know* o necesidad de conocer establece que en una organización las personas han de tener acceso solo a la información precisa para ejecutar sus tareas.

Análisis de riesgo

Para la adopción de medidas, el análisis de riesgo precedente se tendrá especialmente en cuenta si**:**

- El tratamiento puede generar discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.
- Afectar a derechos de afectados o privarles del control de sus datos personales.
- Tratamiento no accidental o accesorio de categorías especiales de datos o infracciones administrativas.
- Evaluación de aspectos personales de los afectados. Creación de perfiles (respecto a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos).
- Tratamiento de datos de grupos vulnerables (menores, discapacitados).
- Tratamiento masivo de datos.
- Transferencias internacionales no a países seguros.

Evaluaciones de impacto. Tratamientos de alto riesgo

¿Cuándo será necesario la evaluación de impacto? Cuando **sea probable** que un tipo de tratamiento, en particular: si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un **alto riesgo** para los **derechos y libertades** de las personas físicas, el responsable del tratamiento realizará**, antes del tratamiento**, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

La evaluación de impacto se requerirá **en particular en caso de:**

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un **tratamiento automatizado**, como la **elaboración de perfiles**, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.
- Tratamiento **a gran escala** de las **categorías especiales** de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o
- Observación sistemática a gran escala de una zona de **acceso público.**

La evaluación deberá incluir como **mínimo**:

- Una descripción sistemática de las operaciones de tratamiento previstas y de los **fines del tratamiento,** inclusive, cuando proceda, **el interés legítimo** perseguido por el responsable del tratamiento.
- Una evaluación de la **necesidad y la proporcionalidad** de las operaciones de tratamiento con respecto a su finalidad.
- **Una evaluación de los riesgos** para los derechos y libertades de los interesados.
- ***Las medidas previstas para afrontar los riesgos, incluidas*** garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

El responsable del tratamiento recabará el **asesoramiento** del **delegado de protección de datos**, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos. Las **fases mínimas** que pueden tenerse en cuenta en la elaboración de una evaluación de impacto son las siguientes (Según la guía de AEPD):

- Análisis de necesidad.
- Determinación de los flujos de datos y procesos.
- Identificación de riesgos.
- Gestión de riesgos.
- Cumplimiento normativo necesario.
- Informe final.
- Consulta previa a la autoridad de protección de datos.

- Implantación de resultados.
- Seguimiento.

Medidas de seguridad técnica y organizativa

Antes: la LOPD imponía una serie de medidas de seguridad estándar en función a la clasificación de los ficheros: bajo, medio o alto.

Ahora: el RGPD parte de otro enfoque de la seguridad ya que no ofrece un repertorio de medidas de seguridad predefinidas Las medidas se aplicarán en función del riesgo y serán proporcionales.

El responsable y el encargado del tratamiento (ambos) aplicarán **medidas técnicas y organizativas** apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

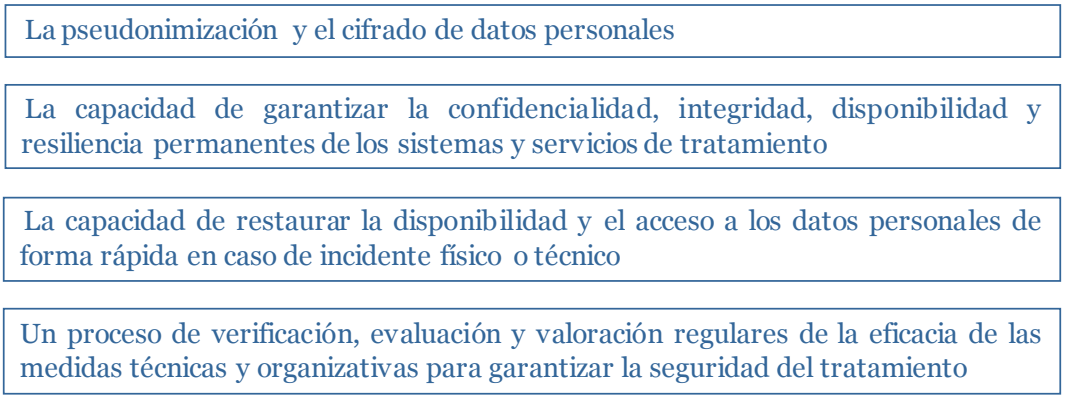


Figura 4. Medidas técnicas y organizativas.

- Según la AEPD:
  - **Medidas organizativas:**
    - Deber de información.
    - Deber de confidencialidad y secreto. Ej. Papeles sobre la mesa, pantallas abiertas, pen drives en la basura, HCE personal sanitario. El deber persiste finalizada la relación laboral.
    - Derechos titulares.
    - Violaciones de seguridad de datos personales.

  - **Medidas técnicas:**
    - Identificación de usuarios.

- Deber de salvaguarda:
- Actualización de ordenadores y dispositivos. Ojo, BYOD.
- *Malware*.
- Cortafuegos o *firewall*.
- Cifrado de datos.
- Copia de seguridad.
- Control de acceso a los datos. Cada empleado accederá a los datos que son estrictamente necesarios para su trabajo.
- Identificación y autentificación de todos los usuarios que tengan acceso a la base de datos.
- Registro de actividades del tratamiento.
- Cifrado de soportes.
- Seudonimización.
- Minimización de los datos.
- Procedimientos de copias de seguridad.
- Confección de los avisos legales en el que el consentimiento se preste según nuevo Reglamento.
- Actualización de los derechos de los interesados.

El DPO o DPD, delegado de protección de datos o *Data Privacy Officer*

El DPO es la **persona encargada informar a la entidad responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de 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 esta y la entidad responsable del tratamiento de datos. ¿Cuándo debe designarse un DPO? Debe designarse **si:**

- El tratamiento lo lleve a cabo una **autoridad u organismo público**, excepto los tribunales que actúen en ejercicio de su función judicial;
- Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una **observación habitual y sistemática de interesados a gran escala**.
- O las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de **categorías especiales de datos personale**s con

arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

¿En qué entidades debe designarse un DPO? Según la nueva LOPD:

- Debe designarse en las siguientes **entidades:**
  - Colegios profesionales y sus consejos generales.
  - Centros docentes.
  - Entidades que exploten redes y presten servicios de telecomunicaciones (LGT).
  - Prestadores SSI.
  - Entidades financieras.
  - Establecimientos financieros de crédito.
  - Empresas de servicios de inversión.
  - Aseguradoras y reaseguradoras.
  - Distribuidores y comercializadores de energía eléctrica.
  - Empresas de evaluación de solvencia patrimonial y riesgo crediticio.
  - Publicidad y prospección comercial.
  - Centros sanitarios.
  - Empresas de emisión de informes comerciales referentes a personas físicas.
  - Operadores de juego a través de canales telemáticos
  - Empresas de seguridad privada.

3.4. Las notificaciones de violaciones de seguridad

Es toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

El responsable ha de notificar la violación de la seguridad, siempre que exista **riesgo para los derechos y libertadas** de las personas físicas, riesgo que ha de ser evaluado por el responsable. En caso de que el encargado del tratamiento sufra una violación de seguridad, este debe notificar sin dilación al responsable la existencia de la misma. La notificación de la brecha a la autoridad de control se ha de **producir antes de las 72 horas,** es decir, en los tres días siguientes al conocimiento por el responsable de la existencia de la violación. El responsable debe notificar la violación de seguridad a la **autoridad competente y los interesados.**

No será necesario cuando se haya adoptado medidas de protección técnicas y organizativas apropiadas en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos. Ej. Datos cifrados. Tampoco cuando la comunicación suponga un esfuerzo desproporcionado, en estos casos, valdrá una comunicación pública.

3.5. Régimen sancionador

Antes: la antigua LOPD, concretamente en su artículo 44, regulaba tres grados de infracción**: leve, grave y muy grave.** Cada una de ellas prevé un rango de sanciones diferente que variará teniendo en cuenta la graduación anteriormente mencionada.

Ahora: el Reglamento **endurece el régimen sancionador** aplicable no solo a los responsables del tratamiento de los datos, sino a los encargados, procediendo a incrementar las cuantías de las sanciones por incumplimiento de las disposiciones normativas.

- En este sentido merece especial mención el art. 83 en sus apartados 4 y 5, que sin hacer mención específica a cuantías mínimas, prevé la posibilidad de sancionar las infracciones cometidas con respecto al tratamiento de datos de carácter personal con **multas administrativas de 10.000.000 o 20.000.000 de euros**, o en el caso de que se trate de una empresa, **de una cuantía equivalente al 2 % o al 4 % como máximo del volumen de negocio** anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Norma Aplicable	Sanciones		
	Leve	Grave	Muy grave
LOPD/RLOPD (Antes)	900 € - 40.000 €	40.001€-300.000€	300.001-600.000€
RGPD (Ahora)	No se establece un rango mínimo de cuantía	Multa administrativa de hasta 10.000.000€ o, en el caso de empresas, de cuantía equivalente al 2% como máximo del volumen de negocios total anual global del ejercicio financiero anterior, lo que resulte mayor en cuantía.	Multa administrativa de hasta 20.000.000€ o, en el caso de empresas, de cuantía equivalente al 4% como máximo del volumen del negocio anual global del ejercicio financiero anterior, lo que resulte en mayor cuantía.

Tabla 1. Sanciones.

- Debemos tener en consideración el artículo 83, apartados 1 y 2, del RGPD, que señala lo siguiente:
  - Las **multas administrativas** (poder correctivo contemplado en el artículo 58.2.i del RGPD) **serán efectivas, proporcionadas y disuasorias.**
  - Se impondrán **en función de las circunstancias** de **cada caso individual**, a título adicional o sustitutivo de las medidas contempladas en el artículo 58.2 en donde se relacionan los **poderes correctivos** que disponen las Autoridades de Control.

- **Conclusión:** la intención del legislador europeo es clara y así lo plasma en el Considerando 152 en el propio artículo 83. Las sanciones tendrán una **finalidad disuasoria**, actuando como elemento de presión, o de coacción, para que las empresas o entidades cumplan.

Lo + recomendado

No dejes de leer…

Reclamaciones de telecomunicaciones

En esta guía la Agencia Española de Protección de Datos sobre las reclamaciones de las telecomunicaciones.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
https://www.aepd.es/areas/telecomunicaciones/index.html

Guías de privacidad y seguridad en Internet

La Agencia Española de Protección de Datos realiza en esta guía sobre la privacidad y la seguridad en Internet.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
https://www.aepd.es/media/guias/guia-privacidad-y-seguridad-en-internet.pdf

Código de buenas prácticas

Esta guía publicada por la Agencia Española de Protección de Datos nos presenta un Código de buenas prácticas en protección de datos para proyectos Big Data.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

No dejes de ver…

DPO, presente y futuro de la profesión.

En la siguiente *Openclass* de UNIR se hablará del delegado de protección de datos (DPO).

Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=YKG8ehbZy38

Retos legales y técnicos en la protección de datos

En la siguiente *Openclass* de UNIR Sergio Sanfulgencio, abogado del despacho Cuatrecasas, nos hablará de la protección de datos enmarcada en el nuevo reglamento europeo.

Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=_bTUWKtzgEU

Día europeo de protección de datos: Retos del GDPR

En la siguiente *Openclass* de UNIR, con motivo de la celebración del Día Europeo de la Protección de Datos, hacemos un repaso al nuevo Reglamento General de Protección de Datos (GDPR). De la mano de Jesús Yañez avanzamos las novedades interpretativas surgidas por el Grupo de Trabajo del Artículo 29 en este tiempo y resolvemos dudas.

Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=VXCRqGQadaI

La segunda revolución cuántica y cifrado de la información

¿Qué es la computación cuántica, porqué revolucionará nuestro mundo? Antonio Acin, experto en esta temática, nos da respuestas a estas preguntas, nos advierte de sus consecuencias y también nos explica sus infinitas posibilidades.

Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?feature=share&v=9kHAKwcRhtY&app=desktop

+ Información

A fondo

Guía análisis de riesgos RGPD

En el siguiente enlace podemos ver la guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD.

Accede a la guía a través el aula virtual o desde la siguiente dirección web:
https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

Guía para las evaluaciones de impacto de protección de datos

Guía práctica para las evaluaciones de Impacto en la Protección de los datos sujetas al RGPD.

Accede a la guía a través el aula virtual o desde la siguiente dirección web:
https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

Guías para brecha de seguridad

Guía para la gestión y notificación de brechas de seguridad.

Accede a la guía a través el aula virtual o desde la siguiente dirección web:
https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf

Orientaciones y garantías en los procedimientos de anonimización de datos personales

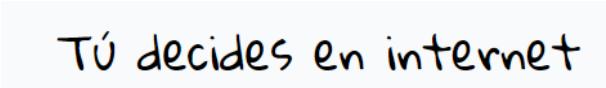
Guía de la Agencia Española de Protección de Datos sobre las orientaciones y garantías en los procedimientos de anonimización de datos personales.

Accede a la guía a través el aula virtual o desde la siguiente dirección web
https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

Enlaces relacionados

Protección de datos para menores

Página de la Agencia Española de la Protección de Datos sobre el uso de Internet. Incluye recursos y una guía para centros educativos.



Accede a la página web a través del aula virtual o desde la siguiente dirección:
http://www.tudecideseninternet.es/agpd1/

Test

1. El interés legítimo:

A. Requiere de una ponderación para poder determinar la prevalencia o no del mismo, mayor aún si se tratan de titulares menores.

B. Requiere que se señalen los propios intereses legítimos concretos del responsable.

C. Puede encontrarse en la prevención del fraude si se lleva a cabo el principio de minimización o en las transmisiones de datos en grupos de empresas a efectos administrativos internos.

D. Todas son correctas.

2. El contenido mínimo del deber de información con la llegada del nuevo Reglamento europeo:

A. Es la información de la figura del DPO, la base legal que lo justifica, el interés legítimo y el plazo.

B. Tiene que incluir además si hay transferencias internacionales, si hay decisiones automatizadas

C. Tiene que incluir la posibilidad de presentar una reclamación ante una autoridad de control o el derecho de portabilidad.

D. Todas las anteriores.

3. El derecho al olvido es el derecho:

A. Que supone la posibilidad de que el titular de dichos datos obtenga la modificación de sus datos personales inexactos o incompletos.

B. Que tiene por objeto la eliminación de los datos persona.

C. De supresión.

D. Las dos anteriores.

4. El consentimiento es:

A. Una manifestación de voluntad libre y específica al afectado.

B. Una manifestación de voluntad libre, específica, informada e inequívoca por el afectado.

C. Una manifestación de voluntad libre, específica, informada al afectado.

D. Ninguna de las anteriores.

5. Las casillas premarcadas:

A. Constituyen un consentimiento válido.

B. No constituye un consentimiento válido.

C. Depende.

D. Ninguna de las anteriores.

6. El derecho que implica que los datos se transmitan directamente de un responsable a otro sin necesidad de que sean transmitidos previamente al propio interesado es:

A. El derecho de acceso.

B. El derecho de minimización.

C. El derecho a la portabilidad.

D. El deber de información.

7. El registro de actividades está exento para empresas para empresas responsables y encargados con:

A. Menos de 200 trabajadores.

B. Menos de 250 trabajadores.

C. No hay exención.

D. Ninguna es correcta.

8. ¿Cuándo será necesario la evaluación de impacto?

A. Si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.

B. Si hay un tratamiento de gran escala de categorías especiales.

C. Si hay una evaluación como elaboración de perfiles (*profiling*).

D. Las 3 anteriores son correctas.

9. ¿Cuál de las siguientes entidades necesitan un DPO?

A. Entidades que exploten redes y presten servicios de telecomunicaciones.

B. Operadores de juego a través de canales telemáticos.

C. Colegios profesionales, hospitales y colegios.

D. Las tres anteriores son correctas.

10. ¿Cuál es el plazo máximo que existe para comunicar una brecha de seguridad?

A. Antes de las 24 horas.

B. Antes de las 72 horas.

C. No hay plazo.

D. Ninguna de las anteriores.