apdcat
Autoritat Catalana de Protecció de Dades

La privacidad desde el diseño y la privacidad por defecto

Guía para desarrolladores

Febrero 2023

Colección Guías. N.º 7

Generalitat de Catalunya

Índice

1. Introducción

El concepto de la privacidad desde el diseño, desarrollado ya desde finales de los años 90 en gran medida gracias a la actividad del Comisionado de Protección de Datos de Andalucía, hace referencia a la necesidad de tener en cuenta el impacto en términos de privacidad de los productos o servicios, especialmente los tecnológicos, ya desde la fase de su diseño.

Estrechamente ligado con este concepto aparece también el de la privacidad por defecto, que requiere aplicar las medidas técnicas y organizativas adecuadas para garantizar que, sin que el usuario tenga que hacer ningún tipo de acción (por defecto), únicamente se tratan los datos personales indispensables para cada una de las finalidades específicas del tratamiento.

Con la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas con respecto al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante RGPD), tanto la protección de datos desde el diseño, como la protección de datos por defecto pasan de ser una recomendación o una buena práctica a ser una obligación.

En concreto, el artículo 25 del RGPD exige:

> 1. Que, ya desde el momento en que se diseñe un servicio o una aplicación, se implementen las medidas técnicas y organizativas adecuadas, como la seudonimización, la minimización de datos y otras garantías para aplicar de manera efectiva los principios de la protección de datos personales, para garantizar el cumplimiento del RGPD y los derechos y las libertades de las personas interesadas (**protección de datos desde el diseño**).
>
> 2. Que se apliquen las medidas técnicas y organizativas adecuadas para garantizar que, por defecto, los datos personales que se traten y el alcance del tratamiento que se haga sean sólo los necesarios para cada una de las finalidades específicas del tratamiento (**protección de datos por defecto**).
>
> Esta obligación se aplica a:
>
> - La cantidad de datos que se recogen.
> - El alcance del tratamiento.
> - El plazo de conservación.
> - La accesibilidad de los datos, de manera que, por defecto, los datos no sean accesibles a un público indeterminado sin la intervención de la persona afectada.

Detectar estas necesidades y darles solución ya desde el mismo momento del diseño de las herramientas tecnológicas permite ahorrar tiempo, recursos, perjuicios a las personas afectadas y los evidentes costes reputacionales, que se pueden derivar de la incorporación tardía de estos requerimientos.

Por otra parte, al ser una obligación, incumplirla puede constituir una infracción de conformidad con el RGPD, que puede conllevar una sanción de hasta 10 000 000 de euros o de un 2 % del volumen

de negocio total anual global del ejercicio anterior si el resultado de este cálculo resulta superior a los 10 000 000 de euros.

En cualquier caso, más allá de esta obligación, la protección de datos constituye cada vez más un factor cualitativo valorado por las empresas y las instituciones que adquieren un determinado producto o servicio y también por las personas usuarias.

En definitiva, la protección de datos es una ventaja competitiva y esta guía pretende ser un medio útil para poder sacarle provecho.

Desde la Autoridad Catalana de Protección de Datos (MILI) consideramos estratégicamente prioritario que los diferentes actores del ecosistema digital lo perciban así. Por ello, esta guía se elabora para facilitar a los desarrolladores, así como a los responsables del tratamiento que les encargan el desarrollo de aplicaciones, la identificación de los diferentes elementos relevantes para la protección de los datos personales, y las medidas que se pueden adoptar para afrontarlos, ya desde el momento del diseño.

2. Los roles vinculados a la protección de datos desde el diseño y por defecto

La protección de datos desde el diseño y por defecto, tal y como prevé el RGPD, tiene como destinatario directo al responsable del tratamiento, que es quien tiene la obligación de aplicar y velar porque se apliquen las medidas técnicas y organizativas que correspondan.

Para identificar quién es el responsable del tratamiento hay que tener en cuenta la definición del apartado 7 del artículo 4 del RGPD, que define al responsable como quien determina las finalidades del tratamiento de datos y los medios que se emplearán.

En todo caso, el propio RGPD prevé la posibilidad de que el responsable delegue el tratamiento de los datos en un tercero o, simplemente, le permita acceder a los datos para prestar un servicio por cuenta del responsable. Es lo que se llama "encargado del tratamiento". Esta figura puede abarcar tanto a las entidades prestadoras del servicio en sí mismo (como a un concesionario de un servicio público), como a los que colaboran con el responsable para prestarlo (por ejemplo, un servicio de alojamiento (*hosting*) o una empresa que haga el desarrollo o el mantenimiento de una aplicación o plataforma que comporte acceder o tratar datos personales). En cualquier caso, si el desarrollador necesita acceder a datos personales por cuenta del responsable del tratamiento, aunque sólo sea en la fase de desarrollo, hay que formalizar un contrato con el contenido que prevé la normativa de protección de datos.[1]

Cabe destacar que el responsable debe elegir un encargado del tratamiento que ofrezca suficientes garantías en cuanto a la aplicación de medidas técnicas y organizativas apropiadas. Así, un elemento a tener en cuenta a la hora de hacer esta elección es que el encargado disponga de sellos o certificaciones o de procedimientos y protocolos de actuación que incorporen la protección de datos desde el diseño y por defecto.

[1] Véase el artículo 28 del RGPD.

Especialmente, hay que tener en cuenta que los datos personales sólo pueden transferirse fuera del espacio económico europeo si el país de destino tiene una decisión de adecuación dictada por la Comisión Europea,[2] o se tienen garantías adecuadas de acuerdo con alguno de los mecanismos previstos en el artículo 46 del RGPD.

En cualquier caso, las medidas que el responsable debe cumplir en virtud de los artículos 25 y 32 del RGPD también las debe imponer al encargado del tratamiento y, asimismo, debe exigirlas a los productos y servicios que adquieran o que encarguen.

En otros términos, los nuevos productos y servicios desarrollados, ya sean internos (del propio responsable o encargado del tratamiento) o externos, deben cumplir con la protección de datos desde el diseño y por defecto. De lo contrario, el responsable del tratamiento no podrá cumplir sus obligaciones.

Por otra parte, no se puede descartar que los desarrolladores que tengan la consideración de encargados del tratamiento subcontraten alguna actuación a terceros (alojamiento, utilización de herramientas facilitadas por terceros, etc.) que comporte que deban acceder a datos personales. Estos terceros reciben la consideración de subencargados. En este caso, el desarrollador que tenga la consideración de encargado del tratamiento debe escoger un subencargado que ofrezca garantías adecuadas y debe disponer de la autorización del responsable. Al subencargado le son aplicables las mismas obligaciones y garantías que al encargado del tratamiento.

A título de resumen, en el desarrollo de una solución tecnológica encargada a un tercero que, a su vez, encarga a otro tercero el alojamiento durante esta fase, los principales roles se recogen en la tabla que figura a continuación:

Roles	**Responsable**	**Encargado**	**Subencargado**
Función	Determina las finalidades y los medios del tratamiento de datos personales	Presta un servicio al responsable que implica acceder a datos personales	Presta un servicio al encargado que implica acceder a datos personales
Ejemplo	Entidad que inicia una solución tecnológica que implica tratar datos personales	Desarrolladores	Servicio de alojamiento (hosting)

Cabe remarcar que, para que la protección de datos desde el diseño y por defecto sea efectiva, debe garantizarse especialmente que los desarrolladores han tenido en cuenta el contexto en el que se acabará aplicando su desarrollo. Para configurar el producto con todas las

[2] La lista de países con una decisión de adecuación puede consultarse en este enlace.

garantías adecuadas, es indispensable conocer las circunstancias en las que se ejecutará la aplicación.

Este conocimiento y la implementación de las garantías correspondientes constituye una clara ventaja competitiva, ya que el responsable del tratamiento debe priorizar las soluciones más adecuadas para garantizar los derechos de las personas usuarias.

3. La aplicación efectiva de la protección de datos desde el diseño y por defecto

La normativa que regula la protección de datos desde el diseño y por defecto no determina qué medidas técnicas y organizativas concretas hay que implementar. La determinación de las medidas necesarias debe ser el resultado de un análisis previo realizado por el responsable del tratamiento y, por extensión, por los desarrolladores de las soluciones tecnológicas que debe emplear el responsable del tratamiento.

Hay que aplicar las medidas que sean necesarias y proporcionales. En cualquier caso, en el momento del diseño hay que tener en cuenta:

- La naturaleza, el ámbito, el contexto y las finalidades del tratamiento.
- Los riesgos que comporta el tratamiento para los derechos y las libertades de las personas.
- El estado de la técnica.
- El coste de la aplicación.

En principio, la definición de la naturaleza, el ámbito, el contexto y las finalidades del tratamiento corresponde al responsable del tratamiento. La elección de una determinada solución tecnológica debe tener en cuenta estos elementos, pero también los riesgos inherentes a cada tecnología disponible. Por ello, la colaboración de los desarrolladores se convierte en esencial ya en esta fase.

Una vez conocidos estos aspectos, hay que valorar los riesgos que comporta el tratamiento para los derechos y libertades de las personas. Si se prevé que pueden ser altos, hay que hacer una evaluación de impacto de protección de datos (AIPD).[3] En esta valoración ya es relevante que participe el desarrollador, dado que probablemente es quien está en una posición mejor para evaluar las tecnologías que se pueden emplear y que pueden implicar un riesgo elevado para los derechos y libertades de las personas que haga necesaria la AIPD.[4] También, para contribuir a definir qué medidas se pueden implementar para reducir este riesgo, teniendo en cuenta el estado de la técnica y el coste de aplicación. En resumen, la evaluación de impacto sobre la protección de datos es un proceso sistemático que, aparte de requerir una descripción sistemática del tratamiento previsto y de su necesidad y proporcionalidad, requiere (i) evaluar los riesgos derivados del tratamiento y (ii) determinar las medidas para mitigar estos riesgos.[5]

[3] El artículo 35 del RGPD contiene una lista de supuestos no exhaustiva. También es de utilidad la relación contenida en el artículo 28.2 de la LO 3/2018 y la lista publicada por la ACPD.

[4] La ACPD dispone de materiales e incluso de una aplicación para poder hacer esta evaluación de impacto de protección de datos.

[5] Si los riesgos no pueden mitigarse suficientemente, antes de iniciar el tratamiento hay que consultar la autoridad de control.

Igualmente, en los casos en que no sea exigible hacer una AIPD, es necesario que se valoren las opciones técnicas disponibles teniendo en cuenta el estado actual de la técnica, así como el coste de implementarlas.

Con esta finalidad, serán de utilidad las tecnologías que mejoran la protección de la privacidad (*privacy enhancing technologies* o *PET*), que permiten minimizar los riesgos sin perder la funcionalidad de la aplicación o el sistema de información. En el apartado 4 de esta guía se recogen algunas medidas que se consideran clave para la protección de los datos personales y que forman parte de este conjunto más general conocido como PET.

En definitiva, el diseño de soluciones tecnológicas debe tener en cuenta los riesgos derivados del tratamiento para determinar las medidas técnicas a aplicar.

La protección de datos en el diseño y la protección de datos por defecto deben proyectarse en las diferentes fases del tratamiento de los datos:

- Diseño.
- Desarrollo y pruebas.
- Recogida de los datos.
- Uso de los datos.
- Comunicación o divulgación de los datos.
- Mantenimiento y conservación de los datos.

A continuación, se identifican sin ánimo de exhaustividad algunos de los aspectos cuya valoración se considera clave en relación con cada una de estas fases y que, desde el mismo momento del diseño, deben hacer posible el cumplimiento de los principios de protección de datos personales.

Con el fin de facilitar la revisión sistemática de los elementos que se sugiere valorar en relación con las diferentes fases que conforman el tratamiento de datos personales, se ha confeccionado un listado específico (*checklist*) que figura como anexo de esta guía. A modo de resumen, esta lista recoge los principales aspectos a tener en cuenta, que se comentan más detalladamente en los apartados 3 y 4 de esta guía y permitirá evaluar el grado de incorporación de la protección de datos en el diseño de las soluciones.

3.1 Fase de diseño

En la fase de diseño de las soluciones tecnológicas se definen los diferentes componentes en que se estructurará el software y sus interacciones, con el objetivo de cumplir una serie de requerimientos funcionales y no funcionales. La protección de datos desde el diseño y por defecto introduce la protección de datos entre estos requerimientos.

La complejidad inherente al desarrollo de software hace que el uso de una metodología de desarrollo sea esencial para gestionar los proyectos y conseguir que sean exitosos.

Si bien la protección de datos desde el diseño y por defecto no implica el uso de nuevas metodologías de diseño, sí que requiere ajustar las tareas o los análisis que se llevan a cabo. En este sentido, se habla de diferentes estrategias de diseño:[6]

- **Minimizar**: limitar al mínimo posible el tratamiento de datos personales. Tratar los mínimos datos personales, limitar el impacto que el sistema pueda tener sobre las personas.

- **Esconder**: esconder los datos personales ante quien no es necesario que los conozca, lo que dificulta que se les pueda dar un mal uso. Hay múltiples maneras de esconderlos, y su utilidad depende de la situación concreta: criptografía, control de acceso, etc.

- **Separar:** tratar los datos de manera distribuida y en compartimentos lo más separados posible. Separar los datos en diferentes compartimentos estancos evita que se pueda acceder fácilmente a los perfiles completos de las personas.

- **Agregar:** tratar los datos de la manera más agregada posible, siempre que permita alcanzar la finalidad perseguida. La agregación de datos en grupos de personas, si son lo suficientemente grandes y diversos, hace que los datos no se puedan asociar a una persona concreta.

- **Informar:** informar adecuadamente a las personas sobre el tratamiento de sus datos personales.

- **Controlar:** las personas deben poder decidir sobre el tratamiento de sus datos.

- **Hacer cumplir:** debe haber una política de privacidad, compatible con los requerimientos legales, y se deben poner los medios para que se cumpla.

- **Demostrar:** hay que ser capaz de evidenciar que el tratamiento de datos personales se llevar a cabo de manera "amigable" en términos de privacidad.

A nivel más práctico están los patrones de privacidad, que dan soluciones de diseño a problemas comunes en protección de datos.[7] Es decir, son una forma ya validada de aplicar las estrategias de diseño a problemas concretos.

Durante el diseño de una solución, hay que incluir como elementos esenciales la determinación de los flujos de la información personal que se tratará (de dónde se recogen los datos, cómo se recogen, quién debe tener acceso a ellos y para qué, etc.) y las medidas de seguridad exigibles en cada supuesto concreto.

Estas medidas dependerán del resultado del análisis de riesgos a realizar en todos los casos. En los apartados siguientes de esta guía se analizan muchas de estas medidas, agrupadas de acuerdo con la fase del tratamiento en qué tienen más relevancia. Pero es en el momento del desarrollo de la aplicación cuando hay que tenerlas en cuenta para incorporarlas en el diseño.

[6] Privacy Design Strategies (The Little Blue Book), JAAP-HENK HOEPMAN (2022)
[7] Patrones de privacidad.

3.2 Fase de desarrollo y de pruebas

La mayoría de las veces, el desarrollo de software y las pruebas exigen el uso de datos. Cuando estos datos son personales, la normativa de protección de datos es de plena aplicación.

Aspectos para tener en cuenta con respecto a la utilización de datos durante las fases de diseño y de pruebas

- Si en la fase de desarrollo y de pruebas hay que tener acceso a datos personales, el equipo o la empresa de desarrollo y los que contrate el desarrollador serán encargados del tratamiento (véase el apartado 2 de esta guía sobre "Los roles vinculados a la protección de datos desde el diseño y por defecto").

- Para garantizar la confidencialidad y la integridad de la información es necesario separar adecuadamente el entorno de producción y el de desarrollo y pruebas, y garantizar que el entorno de pruebas es seguro (si es posible, aislado de conexiones externas hasta el momento en que resulte imprescindible).

- Si se pueden hacer desarrollos y pruebas sin necesidad de emplear datos reales, hay que optar por esta posibilidad. En general, es posible utilizar datos sintéticos (véase el apartado 4 de esta guía).

  Si no se puede, hay que utilizar los datos mínimos. Con el término *minimizar* no nos referimos sólo a la cantidad, sino también a la calidad (presencia de identificadores y pseudoidentificadores, nivel de detalle, etc.).

  En el caso de que convenga emplear datos reales, si es posible utilizarlos anonimizados o pseudonimizados se recomienda decantarse por alguna de estas opciones. Si es necesario utilizar datos, se pueden reutilizar datos de los que ya disponía el responsable o recogerlos de nuevo. En este último caso, hay que tener en cuenta las recomendaciones que se hacen en el apartado 3.3 de esta guía.

- Hay que prestar especial atención a la ubicación del servidor donde se alojará la información recogida. Esta circunstancia puede llegar a comprometer la confidencialidad de la información, dado que no todos los países aplican las mismas garantías. Además, emplear un servidor de fuera del espacio económico europeo implica que se produzca una transferencia internacional de datos que para que sea válida debe cumplir determinados requisitos (capítulo V del RGPD).

- Se deben implementar mecanismos de control de acceso para evitar que usuarios no autorizados accedan a los datos. Hay que crear un usuario para cada persona que tenga que acceder, y limitar el acceso a los datos necesarios para desarrollar sus funciones.

- Las copias de seguridad de la infraestructura de desarrollo y prueba son esenciales para el éxito del proyecto, pero hay que tener en cuenta que si estas copias contienen datos personales hay que controlar el acceso.

- Cuando se empleen redes wifi, debe utilizarse el protocolo que proporcione el grado de seguridad más alto.[8]

- Los paquetes de software y librerías que se utilicen en el desarrollo deben estar actualizados. La falta de actualización puede dar lugar a vulnerabilidades en el software desarrollado.

- La entidad desarrolladora debe formar a su personal en materia de protección de datos y debe establecer los compromisos de confidencialidad adecuados.

Otros aspectos a tener en cuenta en la fase de diseño

- Utilizar alguna metodología para garantizar la calidad del código fuente. Bien sea manual, mediante revisiones del código hechas por diferentes personas, o automática con herramientas de análisis estático o dinámico. Un código de mala calidad puede dar lugar a vulnerabilidades, que pueden poner en riesgo los datos personales.

- Seguir las recomendaciones de las guías de programación segura.

En la fase de puesta en marcha de la solución tecnológica, y también en el momento de la incorporación a la organización de nuevas personas usuarias, resulta esencial una formación del personal que deba utilizarla, adecuada a los diversos perfiles. Ello implica prever sesiones formativas para conocer el funcionamiento de la solución, los riesgos derivados de su uso, las medidas organizativas y técnicas que hay que adoptar para minimizarlos y, también, disponer de manuales de uso exhaustivos.

[8] En este sentido, hay que tener presente que se han detectado vulnerabilidades importantes de los protocolos WEP, WPA y WPA2. En el momento de elaborar esta guía, el protocolo más reciente es el WPA3. También hay que tener en cuenta que algunos rúters más antiguos podrían no soportarlo.

3.3 Recogida de los datos

3.3.1 Minimización de los datos

Sólo se deben recoger los datos adecuados y necesarios para alcanzar la finalidad perseguida.

De entrada, esto implica que hay que plantearse si la finalidad se puede alcanzar sin emplear datos personales. Ello simplificaría las obligaciones del responsable, dado que la normativa de protección de datos personales no sería de aplicación.

Si es necesario utilizar datos personales, únicamente se pueden recoger los mínimos necesarios para alcanzar la finalidad concreta establecida por el responsable del tratamiento y de la que se ha informado a las personas afectadas. Todavía hay que ser mucho más restrictivo cuando se recogen categorías especiales de datos (datos que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, datos genéticos, datos biométricos destinados a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida o la orientación sexuales), de manera que, siempre que se pueda, hay que evitar recoger este tipo de datos.

Los datos que se recogen pueden ser muy variados. Pueden comprender, entre otros, los siguientes:

- Datos identificativos, de contacto, laborales, de formación, socioeconómicos, sobre aficiones, estilos de vida, etc., aparte de las categorías especiales de datos ya mencionadas.
- Registros de actividad, que se utilizan en todo tipo de servicios (servidores web, servidores de correo, en una tienda en línea, etc.).
- Datos de geolocalización.
- Datos procedentes de dispositivos conectados (*wearables*), como, pulsaciones, presión arterial, nivel de oxígeno en la sangre, etc.) que se recogen automáticamente.
- Transacciones (pagos con móvil, con tarjeta, etc.).
- Datos identificativos asociados a dispositivos o protocolos de comunicación (dirección IP, dirección MAC, número de teléfono, IMEI, ICC SIM, etc.).
- Metadatos asociados a ficheros.

Dado que la mayoría de los productos o servicios digitales recaban datos constantemente, la verificación de la necesidad de obtener datos personales debe hacerse permanentemente. Sin embargo, el primer acceso (caracterizado a menudo por la configuración de un formulario o la necesidad de dar acceso a un perfil previamente configurado) es un momento especialmente sensible en este sentido.

La verificación de la necesidad de los datos personales debe comprender "todos" los que se obtengan, independientemente del canal mediante el cual se obtienen. En este sentido, hay que prestar especial atención a los datos obtenidos por múltiples fuentes −más allá de los formularios−, entre ellos la recogida de datos sobre la actividad de los usuarios o las galletas

(*cookies*), ya sean propias o de terceros, que, además, pueden responder a finalidades diversas (patrones de comportamiento, datos demográficos). de los usuarios, etc.).

La recogida se puede producir de manera directa o indirecta. Así, por ejemplo, cuando un desarrollador utiliza determinadas librerías de terceros, esto puede conllevar el tratamiento de información personal, incluso a veces de manera inadvertida. Por ejemplo, al incluir una librería JavaScript en un web, estamos dando acceso a esta librería a la información personal contenida en el web. Todavía es más preocupante que las librerías de terceros utilizadas en el desarrollo de aplicaciones móviles tengan los mismos permisos que la aplicación desarrollada. Esto implicaría, por ejemplo, que si la aplicación puede acceder a la geolocalización o al micrófono, también podrían hacerlo las librerías externas utilizadas.

Por otra parte, cuando una aplicación solicita permisos para acceder y recoger información irrelevante para la finalidad que persigue, no se está cumpliendo adecuadamente el principio de minimización de datos. Por ejemplo, si se recoge información sobre la geolocalización, cuando el servicio que se ofrece es exactamente el mismo independientemente de la ubicación.

También es importante tener en cuenta que algún método de recogida puede implicar, incluso, una transferencia internacional de datos fuera del espacio económico europeo, lo que requiere disponer de las garantías adecuadas de acuerdo con el RGPD. A título de ejemplo, puede suceder que un servicio de obtención de datos estadísticos de los visitantes de un web remita automáticamente la información a servidores ubicados fuera del espacio económico europeo, de manera que habrá que analizar si en el país de destino de los datos hay garantías equivalentes a las que habría dentro del ámbito europeo.[9]

Aspectos relevantes

- Hay que plantearse si se puede alcanzar igualmente la finalidad perseguida sin recoger datos personales, o bien recogiendo menos de los inicialmente previstos. Es decir, si hay alguna alternativa que permita conseguir la finalidad con menos datos. Una posibilidad podría ser generar datos artificiales, que simplemente repliquen los comportamientos de los datos reales, y trabajar exclusivamente con estos datos, llamados *sintéticos*. También se podría optar por modificar los datos de manera que no puedan asociarse a una persona (seudonimización, anonimización), reducir la cantidad de datos recogidos o el nivel de detalle, restringir al máximo el acceso a los datos en las partes del sistema que los necesitan, etc.

- Conviene evitar tratar datos de categoría especial si no es estrictamente necesario. Por ejemplo, en lugar de configurar el acceso a un determinado servicio digital con datos biométricos, se

[9] En concreto, en relación con el uso de la solución "Google Analytics", la Autoridad de Protección de Datos Francesa –CNIL– en febrero de 2022 ordenó a un sitio web dejar de hacer uso de este servicio e hizo públicas unas informaciones generales en relación a la utilización de Google Analytics. Ya a principios de año, se pronunció en esta misma línea la Autoridad de Protección de Datos Austríaca.

puede hacer mediante una contraseña y, eventualmente, implementar un doble factor de autenticación.[10]

- Hay que ser especialmente cuidadosos a la hora de diseñar los formularios y, en particular, a la hora de definir los campos obligatorios. Hay que distinguir claramente la información que se debe proporcionar obligatoriamente de la que es opcional.
- La aplicación debe solicitar sólo los permisos para acceder y recoger información relevante para la finalidad que persigue.
- Hay que evitar almacenar por defecto datos técnicos que no sean estrictamente necesarios, como la dirección MAC, la dirección IP, el nombre del dispositivo o el ID de publicidad.
- Hay que evitar obtener informaciones conexas innecesarias (como metadatos, datos vinculados a la actividad, etc.).
- Hay que valorar la posibilidad de que determinada información se pueda tratar en el mismo dispositivo de la persona usuaria. Un ejemplo claro de esta manera de proceder es el sistema de rastreo descentralizado para contactos de riesgo, durante la pandemia de COVID-19.
- Hay que valorar la posibilidad de **anonimizar o seudonomizar** los datos, cuando no sea indispensable conocer la identidad de la persona usuaria que está vinculada a ellos.
- Hay que ser cuidadoso con el uso de componentes de software externos, ya que podrían tener acceso a datos personales incluso sin que este acceso esté documentado. Conviene revisar las condiciones de uso de estos componentes e, incluso, monitorizar qué acceso efectúan a datos personales.

3.3.2 Licitud de la recogida y el tratamiento de datos

Para poder recoger y tratar información personal, es necesario que concurra una base jurídica de las previstas en el artículo 6 del RGPD.

Además, si se trata de datos de categoría especial (que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical; datos genéticos; datos biométricos destinados a identificar de manera unívoca a una persona física; datos relativos a la salud o a la vida o la orientación sexuales), es necesario que concurra alguna de las excepciones previstas en el artículo 9.2 del RGPD.

[10] Hay que recordar en este sentido que un doble factor de autenticación implica la combinación de dos medios de verificación consistentes en: una información conocida por el usuario −por ejemplo, contraseña−, algo que tiene −por ejemplo, su teléfono móvil− y algo que se es −por ejemplo, algún dato biométrico−.

El consentimiento de la persona afectada es una de las bases jurídicas previstas en el artículo 6 del RGPD y, a menudo, se puede utilizar como base jurídica para recoger datos a través de aplicaciones o servicios web que las personas usuarias pueden instalarse, o a las que pueden acceder de manera voluntaria y libre. El consentimiento debe ser inequívoco, específico, informado y libre, de manera que la decisión de no prestarlo no puede tener otras consecuencias más allá de las estrictamente vinculadas a la imposibilidad de que se trate aquella información.

Aspectos para tener en cuenta con respecto a la gestión del consentimiento en el diseño de soluciones tecnológicas

- El consentimiento debe consistir en una declaración o acción afirmativa clara y ha de requerir una acción de la persona usuaria**.** Puede consistir, por ejemplo, en una casilla que debe rellenar, la firma electrónica o una acción que permita entender inequívocamente que se consiente (por ejemplo, si se accede a un enlace después de haber sido informado de manera clara). No puede ser una opción marcada previamente.

- Cuando el consentimiento se otorga para tratar categorías especiales de datos, o para recibir comunicaciones comerciales, es necesario que sea explícito. En este caso, no basta poder deducir el consentimiento de la actividad de la persona usuaria (por ejemplo, continuar navegando o acceder a determinados apartados), sino que es necesaria una declaración expresa.

- El consentimiento debe ser específico. Cuando se solicita para diversas finalidades, la persona usuaria debe poder escoger separadamente respecto de cada una (consentimiento granular), por ejemplo con casillas o botones de opción.

- Antes de solicitar el consentimiento, hay que informar a las personas afectadas sobre los aspectos a los que se refiere el apartado "Transparencia y lealtad para la persona usuaria" de esta guía.

- El consentimiento debe ser libre. No basta configurar consentimientos diferentes para diferentes usos, si se establece de manera que para poder seleccionar una determinada opción hay que otorgar también el consentimiento en otro ámbito, o se condiciona el ofrecimiento del servicio a consentir para otra finalidad que no debe ir necesariamente ligada.

- Hay que conservar los *logs* o medios para acreditar la prestación del consentimiento durante todo el tratamiento de los datos, y hasta que no haya transcurrido el plazo de prescripción de las eventuales infracciones derivadas del tratamiento (las infracciones muy graves no prescriben hasta los tres años a partir de que se hayan producido).

- El consentimiento debe poder revocarse en cualquier momento. Hay que prever mecanismos de revocación, separadamente para cada una de las finalidades previstas, que sean accesibles de manera similar a la obtención del consentimiento.

- Hay que establecer mecanismos seguros para identificar a las personas que prestan el consentimiento y lo revocan.

- El consentimiento otorgado por menores de edad únicamente es válido si son mayores de 14 años.[11] En este caso, aunque tengan una eficacia limitada, podría ser útil instaurar galletas de sesión que contengan la edad inicialmente introducida por el menor de tal manera que cuando un menor de 14 años haya introducido, por ejemplo, su fecha de nacimiento y constate que no puede acceder al servicio, no le resulte especialmente sencillo cambiar la edad.

3.3.3 Transparencia y lealtad para la persona usuaria

Para cumplir los principios de transparencia y lealtad es necesario garantizar que el usuario pueda conocer toda la información necesaria sobre cómo se tratan sus datos, para que pueda tomar las decisiones que le corresponden o ejercer sus derechos, y que el tratamiento se adecue a las expectativas que la persona afectada se ha podido generar a partir de esta información.

Corresponde al responsable del tratamiento determinar el contenido de las cláusulas informativas. No obstante, en el momento de diseñar la aplicación conviene tener en cuenta determinados aspectos sobre la manera cómo se facilita esta información.

Además, los principios de transparencia y lealtad también implican la obligación de abstenerse de incurrir en prácticas conocidas como patrones oscuros (*dark patterns*) o diseños engañosos. Estos patrones son interfaces e implantaciones de experiencias que inducen a los usuarios a tomar decisiones no intencionadas, no deseadas y potencialmente perjudiciales en relación con el tratamiento de sus datos personales.[12]

El Comité Europeo de Protección de Datos recoge varias categorías de patrones oscuros:

- **Sobrecargar** (*overloading*): ofrecer un exceso de peticiones, informaciones u opciones, para conseguir que el usuario comparta más datos o involuntariamente permita que se traten sus datos personales en contra de su verdadera voluntad. Los siguientes tres patrones oscuros forman parte de esta categoría: **indicaciones**

[11] Salvo que la normativa aplicable al sector de qué se trate de otra edad mínima.
[12] EDPB Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them. Version 1.0. Adopted on 14th March 2022.
Al respecto, véanse también las aportaciones de Harry Brignull en https://www.deceptive.design/, donde se describen diversas tipologías de diseños engañosos.

continuas (c*ontinuous prompting*), **laberinto de privacidad** (*privacy maze*), **demasiadas** opciones (*Too Many Options*).

- **Despistar** (*Skipping*): diseñar la interfaz de experiencia de usuario de manera que los usuarios se olviden o no reflexionen sobre los aspectos vinculados a la protección de datos. Los siguientes dos patrones oscuros forman parte de esta categoría: **acogida engañosa** (*deceptive snugness*) y **mira hacia allí** (*look over there*).

- **Manipular** (*Stirring*): la capacidad de elección de los usuarios se ve afectada, porque se incide sobre sus emociones o estímulos visuales. Los siguientes dos patrones oscuros forman parte de esta categoría: **conducción emocional** (*emotional steering*) y **ocultos a simple vista** (*hidden in plain sight*).

- **Obstaculizar** (*hindering*): obstaculizar o bloquear a los usuarios en el proceso de obtención de información o gestión de sus datos, de manera que esta tarea se convierta en especialmente dificultosa o imposible de alcanzar. Los siguientes tres patrones oscuros forman parte de esta categoría: **callejón sin salida** (*dead end*), **más largo de lo necesario** (*longer than necessary*) e **información engañosa** (*misleading information*).

- **Diseñar de manera inconsistente** (*fickle*): diseñar la interfaz de manera que sea inconsistente y poco clara. Como consecuencia, para el usuario es complicado navegar entre las diferentes herramientas de control de la protección de datos y entender la finalidad del tratamiento. Los siguientes dos patrones oscuros forman parte de esta categoría: **ausencia de jerarquía** (*lacking hierarchy*) y **descontextualización** (*decontextualising*).

- **Ocultar** (*left in the dark*): implica que la interfaz se diseña para ocultar información o instrumentos de control de la protección de datos, o bien para dejar al usuario sin saber cómo se tratan sus datos y cómo puede controlarlos a través del ejercicio de sus derechos. Los siguientes tres patrones oscuros forman parte de esta categoría: **discontinuidad de lenguaje** (*language discontinuity*), **información contradictoria** (*conflicting information*) y **redacción o terminología ambigua** (*ambiguous wording or information*).

Aspectos relevantes

- La información debe facilitarse antes de recoger los datos y, en su caso, antes de dar el consentimiento.

- Cuando los datos no se obtienen de la persona interesada, también hay que informarla. Hay que hacerlo en el plazo de un mes desde que se obtienen o, si se prevé emplearlos en una comunicación, como máximo en el

momento de la primera comunicación a la persona interesada o a un tercero.

- Es necesario que la información sea completa, simple, comprensible, visualmente clara y adaptada, si procede, a las personas con dificultades funcionales.[13]

- En el caso de servicios dirigidos a menores, la información debe facilitarse en un lenguaje adaptado a los conocimientos de este colectivo.

- Cuando los datos se recogen de la persona interesada, hay que informarle sobre los aspectos previstos en los apartados 1 y 2 del artículo 13 del RGPD. Si quien facilita los datos es una tercera persona, hay que dar la información prevista en los apartados 1 y 2 del artículo 14 del RGPD.

- La información se puede facilitar por capas. Así, de entrada se informa sobre la finalidad del tratamiento, la identidad del responsable y la posibilidad de ejercer los derechos de la autodeterminación informativa (derecho de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad) y cualquier otra información que se considera indispensable y, además, se ofrece a la persona usuaria la posibilidad de consultar el resto de la información, si quiere conocer más detalles sobre las implicaciones del servicio.

- La información que se proporciona debe ser fidedigna. Cualquier modificación debe comunicarse a la persona usuaria claramente y con celeridad para que pueda tomar las decisiones oportunas.

- Hay que prever que se efectúen copias de los sitios web y las aplicaciones, para poder verificar los mecanismos y el contenido de las cláusulas informativas existentes en cada momento aplicando un sello de tiempo verificable (*timestamp*).

- Es necesario abstenerse de implementar patrones oscuros.

3.4 Uso de los datos

Los datos personales que se recogen no se pueden utilizar para cualquier finalidad. La finalidad debe ser determinada (no puede ser confusa o demasiado genérica), explícita (debe estar recogida en la información facilitada a la persona afectada y al Registro de actividades del tratamiento que debe llevar el responsable del tratamiento) y legítima (véase el apartado "Licitud de la recogida y el tratamiento de datos" de esta guía).

[13] Hay que tener en cuenta la normativa sobre accesibilidad: Directiva 2016/2102 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público; Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público. También puede ser de interés: Accessibility requirements for ICT products and services i Web Content Accessibility Guidelines.

El uso efectivo que se haga debe corresponder siempre a la finalidad respecto de la cual se informó a la persona afectada al recoger los datos. Sólo se pueden utilizar para otros fines si se tiene el consentimiento de la persona afectada, si una ley lo autoriza o si se trata de una actividad que se pueda considerar compatible, de acuerdo con los criterios que establece el RGPD.[14]

Aspectos relevantes

- Conviene instaurar mecanismos técnicos de autocontrol que garanticen que el uso de la información queda en todo momento circunscrito a la finalidad declarada. Hay que disponer de un sistema adecuado de clasificación de la información, que garantice que el uso que se hace queda delimitado al uso legítimo que puede hacerse.
- Hay que instaurar mecanismos adecuados de protección para evitar el uso indebido por parte de agentes externos a la organización –por ejemplo, encargados del tratamiento− o internos (hay que tener presente que a menudo el riesgo más significativo proviene del personal de la propia organización). Sobre esta cuestión nos remitimos al apartado sobre Confidencialidad de esta guía.
- Se recomienda diseñar las soluciones tecnológicas de manera que se facilite el ejercicio de los derechos de las personas afectadas (derecho de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad), si es posible a través de la misma aplicación, y que también faciliten que el responsable los pueda hacer efectivos fácilmente.

3.5 Comunicación o divulgación de los datos

Hay que asegurar que sólo se producen comunicaciones de datos a terceras personas cuando hay una base jurídica para hacerlo y se han adoptado las medidas de seguridad adecuadas.

Aspectos relevantes

- Cuando la utilización de una aplicación o de una solución tecnológica se basa en el consentimiento de la persona afectada, es necesario establecer mecanismos para que, por defecto, los datos no sean accesibles a un número indeterminado de personas sin la intervención de la persona afectada.

[14] Artículos 5.1.*b* i 6.4 del RGPD.

- Cuando a través de la solución tecnológica se publica información, conviene prever mecanismos que posibiliten su despublicación automatizada, una vez transcurra el plazo de publicación establecido.

- Se recomienda que las comunicaciones se hagan con **cifrado de extremo a extremo**. Esto permite que los datos únicamente puedan ser descifrados en el dispositivo del receptor de las comunicaciones −mediante su clave privada− y no, por ejemplo, por los proveedores del servicio de comunicaciones.

En servicios web, hay que utilizar el **protocolo HTTPS** y configurar el servidor de manera que no sea posible acceder a él a través de otros protocolos. Este protocolo de comunicación, basado en el uso de certificados por parte del servidor, es particularmente interesante ya que no sólo garantiza la confidencialidad y la integridad (cifrado), sino también la autenticidad del prestador de servicios. Esto se puede complementar con el protocolo HSTS, que instruye el navegador para utilizar sólo HTTPS; así se evita el riesgo de ataques MitM, especialmente si se hace una precarga de la cabecera HSTS.

- Hay que analizar si el destinatario de los datos necesita acceder a ellos en claro. Si no es así (como un encargado del tratamiento que solo tiene que alojar la información), hay que cifrar los datos de manera que no pueda acceder.

- Si el destinatario necesita acceder para hacer operaciones de cálculo, hay que evaluar la posibilidad de que tenga acceso sólo a datos con cifrado homomórfico. Hay situaciones en que esto es particularmente interesante, como cuando se quiere utilizar la nube para almacenar datos y hacer cálculos.

En la misma línea, hay que tener en cuenta que hay una gran cantidad de protocolos criptográficos que permiten hacer una variedad de tareas revelando la información mínima. Por ejemplo, esquemas de compartición de secretos, pruebas de conocimiento cero, etc.

- Conviene explorar la posibilidad de emplear técnicas que permitan hacer cálculos de forma distribuida, de manera que cada agente que interviene en la computación mantenga sus datos (*secure multiparty computation SMPC)*. En una línea similar, cuando se desarrollan modelos con inteligencia artificial conviene adoptar mecanismos de aprendizaje federado, de manera que las personas que tienen los datos (individuos, entidades, etc.) pueden entrenar el modelo de forma distribuida, sin que tengan que ceder los datos a una entidad que centraliza el entrenamiento.

3.6 Mantenimiento y conservación de los datos

En este apartado, nos referiremos tanto a las medidas que hay que adoptar para garantizar la confidencialidad, la integridad y la disponibilidad de la información como a la limitación del plazo de conservación.

3.6.1 Confidencialidad, integridad y disponibilidad de la información

Hay que garantizar la seguridad de la información. Esencialmente, esto implica que la información personal no puede ser accesible a personas no autorizadas (**confidencialidad**), no se puede alterar (**integridad**) y debe estar disponible cuando se necesite (**disponibilidad**).

Estas tres características pueden protegerse con diferentes medidas, que hay que determinar de acuerdo con la probabilidad y la gravedad de los riesgos existentes.

La confidencialidad, la integridad y la disponibilidad son diferentes dimensiones de seguridad que, aunque estando vinculadas, pueden requerir algunas medidas diferentes. Por ello, a continuación se presentan diferentes medidas agrupadas en relación con las diversas dimensiones de seguridad, si bien hay que tener en cuenta que algunas medidas pueden responder a la vez a más de una de estas dimensiones. Por ejemplo, cuando se evita el acceso indebido a la información (confidencialidad), se está contribuyendo también a proteger su integridad o disponibilidad (por ejemplo, dificultando su secuestro). En definitiva, si bien se opta por esta estructura separada a efectos expositivos, hay que tener presente que la seguridad es un concepto integral.

Confidencialidad e integridad

Para garantizar la confidencialidad y la integridad, es imprescindible establecer controles de acceso a la información.

Aspectos relevantes

- Se establecerá una **política de permisos** que otorgue únicamente los permisos operativos indispensables. Hay que definir roles de manera que cada persona usuaria sólo disponga de los permisos imprescindibles para ejercer sus funciones (principio de la necesidad de conocer). Incluso si se trata de un alto directivo de la organización responsable del tratamiento, no debería tener permisos ilimitados si su labor ordinaria no lo requiere, sin perjuicio de que se le puedan otorgar puntualmente si en algún momento es necesario.

- Para identificar a las personas usuarias se pueden pedir **certificados** electrónicos, que ofrecen un alto grado de robustez. No obstante, cuando la exigencia de este medio no sea proporcionada o adecuada por otros motivos, hay que aplicar otros mecanismos de identificación, como los de clave concertada.[15]

[15] En el caso de las administraciones públicas, el artículo 9 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas regula los medios de identificación electrónica de los ciudadanos.

- Si es posible y proporcionado en términos de seguridad versus usabilidad, conviene establecer un sistema basado en **múltiples factores de autenticación**. Los sistemas basados en un único factor (como contraseña) a veces se pueden vulnerar fácilmente (por ejemplo, por una mala custodia, la poca robustez o el espionaje de reojo o *shoulder surfing*). En este sentido, se recomienda aplicar sistemas de doble factor que deben combinar aspectos diferentes, entre (i) algo que sé (contraseña), (ii) algo que tengo (testimonio o teléfono móvil) o (iii) algo que soy (aspectos biométricos).

Sobre la posibilidad de emplear datos biométricos, hay que advertir que son datos de categoría especial, de manera que sólo se pueden emplear si concurre alguna de las excepciones que prevé el RGPD y cuando hacer uso de ellos sea proporcionado. Por lo tanto, se recomienda que no se opte por esta posibilidad, salvo que sea estrictamente necesario.[16]

- **Gestión de las claves de acceso**: el otorgamiento de claves de acceso a las personas que deben acceder a la información, ya sean las usuarias últimas del servicio o las encargadas de gestionar la aplicación, debe tener en cuenta diversos aspectos que afectan tanto a las características de la clave como al procedimiento de creación, gestión y recuperación.

- **Credenciales seguras:** la exigencia de contraseñas robustas protege de ataques de *password guessing*[17] o de diccionario y fuerza bruta[18]: por ello, conviene que sea la misma aplicación la que exija un número mínimo de caracteres, mayúsculas, minúsculas y caracteres especiales.

Dada la importancia de emplear una clave bastante robusta, cuando el usuario la configura es recomendable que el sistema no sólo le indique el nivel de robusteza de la clave que está proponiendo, sino que impida establecerla si no cumple determinados requisitos de solidez.

Conviene no utilizar contraseñas establecidas por defecto en bienes o servicios.

Para afrontar estos eventuales ataques, también se pueden implantar otras medidas, por ejemplo:

1. Bloqueo del usuario, en caso de múltiples intentos fallidos de acceso: se bloquea el perfil o la IP, una vez ha habido un determinado número de intentos fallidos dentro de un periodo de tiempo previamente definido.

[16] Véase el artículo 9.2 del RGPD.

[17] *Password guessing*: puede ser protagonizado por alguien que conoce a la víctima potencial y, por lo tanto, puede intuir la palabra de paso, o bien por profesionales que, mediante técnicas de Open Source Intelligence –OSINT–, también pueden conocer datos como la fecha de nacimiento, la identidad de los hijos, etc., que a menudo se utilizan para crear contraseñas.

[18] Ataques "de diccionario" o de fuerza bruta consistentes en múltiples intentos consecutivos.

2. Introducción de un CAPTCHA en el proceso de validación.

- El **proceso de generación y,** si procede, **de comunicación** de la contraseña debe garantizar que únicamente la persona usuaria conoce las claves.
- La solución tecnológica debe configurarse de manera que el responsable deba almacenar las **credenciales de acceso de los usuarios** mediante una huella electrónica (*hash*) de la contraseña.
- Conviene establecer un mecanismo que fuerce su **renovación periódica**.
- Hay que configurar la aplicación o web para que **la sesión de los usuarios se cierre de manera automática, transcurrido un determinado periodo de tiempo** de inactividad. También para que **se invaliden las galletas que se guardan en la sesión,** de manera que para acceder de nuevo haya que volver a identificarse.
- Hay que disponer de un **registro de accesos y de actividad** que permita analizar detallada y retrospectivamente cualquier circunstancia que pueda afectar a la información. Disponer de un registro de accesos tiene múltiples beneficios, ya que en sí mismo es un elemento disuasorio, puede contribuir a detectar actuaciones anómalas o sospechosas y, si se ha producido alguna actuación indebida, permite recoger evidencias sobre qué ha sucedido efectivamente. Las evidencias pueden servir para adoptar las medidas correctoras internas o externas (incluida la notificación de una violación de seguridad, para que los usuarios puedan protegerse adecuadamente), así como para exigir las responsabilidades oportunas.

Más allá del control de accesos, también es oportuno considerar otros aspectos que contribuyen decisivamente a preservar la confidencialidad y la integridad y que guardan relación sobre "cómo" se almacena la información.

Aspectos relevantes

- Hay que asegurar que la información se mantiene **cifrada** siempre que sea posible.
- Hay que emplear firma electrónica cuando sea posible, como garantía de la autoría, la fecha y hora y la integridad del documento.
- Hay que velar que los procesos de anonimización y seudonimización que se empleen no han perdido efectividad.

Adicionalmente, también es conveniente realizar pruebas de penetración que permitan identificar posibles vulnerabilidades, así como incluir algún sistema de monitorización de incidentes que permita detectar rápidamente cualquier anomalía.

Aspectos relevantes

- Hay que **prever pruebas periódicas** que comprueben posibles vulnerabilidades en la protección de la confidencialidad de la información ante ataques externos. Principalmente, hay tres tipologías de auditorías de seguridad externas: (i) caja negra – cuando el auditor intenta acceder sin ningún conocimiento previo del sistema o aplicación – (ii) caja blanca – cuando el auditor parte de un conocimiento completo del sistema o servicio a analizar - y (iii) caja gris – cuando se facilita algún tipo de información al auditor que debe intentar el ataque-. En general, es recomendable hacer pruebas de caja negra, ya que se simula un escenario lo máximo realista posible de alguien externo que no tiene conocimientos previos del sistema que se está verificando. No obstante, puntualmente puede ser interesante proporcionar a la persona auditora algunas informaciones que le permitan simular ataques a partir de diferentes niveles de privilegio de usuario.

- Puede resultar especialmente **oportuno auditar el propio código,** para detectar posibles riesgos de seguridad.[19]

- Hay que instaurar mecanismos adecuados para **identificar comportamientos anómalos o fugas de datos,** si es posible de manera automatizada, que hagan posible una reacción rápida y adecuada. Por ejemplo, mediante medidas que controlen el tráfico de la información y que permitan detectar cualquier comportamiento anómalo y alertar a los responsables del dispositivo o servicio.

Finalmente, hay que señalar que es importante adoptar cualquier otra medida de seguridad **adecuada a los riesgosos existentes.**[20]

[19] Únicamente a corte de ejemplo, hay productos que permiten automatizar este tipo de auditorías. En concreto, se trataría de verificar, por ejemplo, que el acceso a las bases de datos se ha diseñado teniendo en cuenta que no se pueda acceder indebidamente mediante ataques de XXSS (validando los campos de *input* antes de que se ejecuten en la misma base de datos).

[20] En el caso del sector público, en el Estado español hay que tener en cuenta el Esquema Nacional de Seguridad (ENS), aprobado por el Real Decreto 311/2022, de 3 de mayo. Sin embargo, hay que tener presente que el ENS indica expresamente −en virtud de su art. 3– que prevalecen les medidas derivadas de un análisis de riesgo relativo específicamente ejecutado teniendo en cuenta la protección de los datos personales.

Disponibilidad

Aspectos relevantes

- Hay que establecer mecanismos automatizados para obtener **copias de seguridad** periódicamente y en diferente ubicación. Aunque conocer determinadas circunstancias que en un tratamiento concreto pueden afectar a la disponibilidad (cortes eléctricos, falta de conectividad, incendios, inundaciones, obsolescencia de determinadas partes del sistema de información preexistente, etc.) puede sobrepasar el ámbito que corresponde a los desarrolladores, es necesario que tengan un conocimiento exhaustivo sobre tales circunstancias a la hora de establecer el sistema de obtención de copias y el sistema de recuperación en una aplicación. El mecanismo (copias periódicas, servidor espejo, etc.) y la frecuencia de las copias dependerá de la probabilidad y la gravedad derivadas de una pérdida de disponibilidad. A menudo, se hace referencia a la regla 3-2-1: disponer de tres copias de seguridad, al menos en dos soportes diferentes y una de las copias fuera del entorno de trabajo (aislada).

- Para que este planteamiento sea efectivo, es necesario configurar **accesos diferentes a las copias de seguridad**. En caso contrario, si las credenciales de un administrador del sistema se ven comprometidas, el atacante podría acceder tanto a la información viva como a la correspondiente a las diferentes copias y, en consecuencia, podría corromperlo todo a la vez.

- Hay que prever pruebas periódicas del procedimiento de recuperación, para garantizar la disponibilidad de la información y la continuidad de los servicios.

- Dado que la disponibilidad también depende de elementos como (i) hardware, (ii) suministros como la electricidad y (iii) de conectividad, es recomendable valorar la posibilidad de redundar estos aspectos críticos.

3.6.2 Limitación del plazo de conservación

Los datos solo deben conservarse durante el tiempo necesario para alcanzar la finalidad perseguida.

Transcurrido este tiempo, deben suprimirse.

La supresión no equivale a la eliminación, sino que da lugar al bloqueo[21] durante el plazo en que sea necesario, y conservar los datos para atender eventuales

[21] El bloqueo consiste en la identificación y la reserva de los datos, con medidas técnicas y organizativas para impedir su tratamiento, incluida la visualización, salvo la puesta a disposición de los datos a los jueces y tribunales, al ministerio fiscal o a las administraciones públicas competentes. En particular, a las autoridades de protección de datos, para exigir posibles responsabilidades derivadas del tratamiento mientras no hayan prescrito (art. 32 LOPDGDD).

responsabilidades. Una vez finalizado el periodo de bloqueo, los datos deben destruirse o, en su caso, anonimizarse.

Los datos que se quieran conservar con fines estadísticos o similares no deben mantenerse −de manera que permitan identificar a las personas afectadas− más tiempo del estrictamente necesario para cumplir la finalidad del tratamiento.

Medidas

- Antes de iniciar la recogida de los datos, hay que determinar el plazo de conservación (incluido el periodo de bloqueo) e informar a las personas afectadas.[22]
- Hay que establecer mecanismos automatizados de supresión de los datos innecesarios.
- Conviene establecer mecanismos que permitan bloquear los datos suprimidos o rectificados, mientras sean necesarios para atender las eventuales responsabilidades, y faciliten su destrucción una vez finalice el periodo de bloqueo.
- Si se quieren conservar los datos con fines estadísticos más allá del periodo de conservación establecido, hay que aplicar medidas adecuadas como la anonimización de la información.
- Hay que aplicar métodos que aseguren una eliminación efectiva de la información que no se tenga que conservar. En particular, hay que borrar los ficheros y las unidades de forma segura (sobrescribiendo la información repetidas veces) o, incluso, en el caso de dispositivos que no se tengan que utilizar (discos duros, memorias USB, etc.), con la destrucción física, especialmente cuando salgan del control de la organización.
- Conviene minimizar el tiempo que se guarda la información de navegación en el equipo del usuario. Es preferible utilizar galletas de sesión que galletas persistentes y, si se utilizan, fijar una fecha de caducidad. Asimismo, hay que evitar el uso de mecanismos de almacenamiento que busquen evitar guardar datos sin que el usuario tenga ningún control. Por ejemplo, las *zombie cookies*, que utilizan varias técnicas para regenerarse cuando el usuario las borra.

[22] En el ámbito de las administraciones públicas catalanas hay que tener en cuenta los plazos de conservación establecidos en las tablas de evaluación documental.

4. Medidas clave para proteger los datos personales

En esta guía se han referido diferentes medidas que contribuyen a mejorar la protección de la información personal, en alguna o en varias fases del tratamiento.

Sin perjuicio de ello, en este apartado se hace referencia a tres medidas que, por su relevancia, están previstas de manera específica en el reglamento europeo de protección de datos. Se trata del cifrado, la anonimización y la seudonimización.

Dado que estas medidas implican un beneficio claro para la protección de los datos personales, forman parte del conjunto más amplio que en el ámbito de la protección de datos se conoce como PET (*privacy enhancing technologies*) o tecnologías que mejoran la privacidad.

4.1 Cifrado

El cifrado es un proceso que transforma una información (texto en claro), de manera que no sea comprensible (texto cifrado). El cifrado se hace de acuerdo con una clave de cifrado y sólo quien tiene la clave de descifrado puede revertir el proceso y acceder a la información. En cualquier caso, los datos personales cifrados continúan siendo datos personales sometidos a la normativa de protección de datos personales.

Los sistemas de cifrado se acostumbran a clasificar de acuerdo con el método empleado para cifrar y descifrar la información:

- **Criptosistemas simétricos o de clave privada**: se emplea la misma clave para cifrar y para descifrar.

- **Criptosistemas asimétricos o de clave pública**: se utilizan claves diferentes para cifrar y para descifrar. En este supuesto, el usuario tiene dos claves (pública y privada). Cuando se quiere enviar un mensaje o comunicación a otro usuario, el mensaje se cifra con la clave pública del receptor, de manera que sólo él (que es el único que tiene su clave privada) lo podrá descifrar.

La gran ventaja de los sistemas de clave pública es que las partes que se quieren comunicar una información de forma secreta no deben compartir en ningún momento su clave privada. Por otro lado, este sistema sí que exige un mecanismo para que las diferentes partes compartan su clave pública de forma segura. Esto se hace con certificados digitales, en que una entidad reconocida da fe de la validez de una clave; es lo que se conoce como infraestructura de clave pública (PKI).

Dado el alto coste computacional de los criptosistemas de clave pública (derivados de la complejidad de las operaciones matemáticas que requieren) también existe la posibilidad de los criptosistemas híbridos, en los que el texto en claro se cifra con un algoritmo de clave privada, mediante una clave generada aleatoriamente. A su vez, esta clave se cifra con un algoritmo de clave pública y se adjunta al mensaje. El destinatario descifrará la clave utilizando su clave privada y, así, podrá descifrar el texto.

El cifrado constituye una actuación especialmente recomendable para proteger los datos personales, tanto desde el punto de vista de la confidencialidad como de la integridad. Y ello hasta el punto de que la normativa de protección de datos considera que no es necesario notificar una violación de seguridad de los datos a la autoridad de control, ni comunicarla a las personas afectadas, si se han adoptado medidas que hagan ininteligibles los datos por cualquier persona que no esté autorizada, como el cifrado.

Sin perjuicio de lo que resulte del análisis de riesgos, es especialmente recomendable cifrar la información cuando se trata una gran cantidad de información o datos especialmente sensibles, ya sean de categoría especial u otros datos (como datos económicos). En cualquier caso, como cualquier medida de protección debe ser proporcional a los riesgos existentes, de manera que aplicar esta medida debería conllevar unos beneficios superiores a los costes de implementarla.

Si los datos cifrados deben someterse a operaciones o cálculos, puede ser de especial utilidad el cifrado homomórfico, que permite llevar a cabo determinadas operaciones algebraicas sobre datos cifrados. Esto puede ser útil, por ejemplo, cuando se guardan datos sensibles en la nube y se quiere operar sobre ellos.

Es importante tener en cuenta que los procesos de cifrado comportan siempre un cierto riesgo de descifrado. Estos riesgos pueden ser computacionales (los algoritmos de cifrado se convierten progresivamente en obsoletos) o asociados a la gestión y conservación de las claves empleadas para cifrar y descifrar la información. En este sentido, se recomienda revisar a lo largo del tiempo la robustez del algoritmo[23] y, también, que las claves se generen y se custodien de forma segura.

Existen otros mecanismos criptográficos que permiten obtener diferentes funcionalidades y que, por tanto, también hay que valorar a la hora de desarrollar una aplicación, como la firma electrónica, las funciones de huella electrónica (*hash*), los esquemas de compartición de secretos, etc.

4.2 Anonimización

Se trata de un proceso que tiene como objetivo impedir que se puedan identificar personas físicas dentro de un conjunto de datos, sin esfuerzos desproporcionados, ya sea directa o indirectamente; por tanto, es un proceso irreversible. Como los datos dejan de ser atribuibles a personas físicas, pierden la consideración de datos personales. En consecuencia, los riesgos para las personas afectadas disminuyen y la normativa de protección de datos personales deja de ser de aplicación.

[23] Por ejemplo, el CNN (Centro Criptológico Nacional) publica recurrentemente información y guías que pueden ser útiles. Así, en mayo de 2022 se ha publicado la Guía de seguridad CCN-STIC 807 "Criptología de empleo en el Esquema Nacional de Seguridad".

Antes de iniciar cualquier tratamiento, es recomendable analizar si se puede llevar a cabo sin emplear datos personales o utilizando datos anonimizados. Si es así, hay que optar por esta posibilidad.

Hay que tener presente que el proceso de anonimización en sí mismo es un tratamiento de datos personales. Por lo tanto, durante esta fase hay que tener en cuenta la normativa de protección de datos personales.

Asimismo, en el proceso de anonimización hay que establecer una separación funcional, de manera que las personas que intervienen no coincidan con las que están vinculadas al tratamiento de los datos una vez ya han sido anonimizados.

Las técnicas de anonimización alteran los datos para proteger la privacidad. Esto tiene, inevitablemente, un efecto sobre la utilidad de los datos.

4.2.1 Técnicas de anonimización

Las técnicas de anonimización se clasifican en dos grandes categorías, de acuerdo con el procedimiento empleado: enmascaramiento y generación de datos sintéticos.

Técnicas de enmascaramiento

Las técnicas de enmascaramiento parten de los datos originales y los modifican. Se mantiene una relación entre los registros de datos originales y los registros de datos enmascarados. Esta relación obliga a que el riesgo de reidentificación deba tenerse muy en cuenta.

El abanico de técnicas de enmascaramiento es muy amplio.[24] Según cómo afecta a la veracidad de los datos, estas técnicas se clasifican en perturbacionales y no perturbacionales. Las perturbacionales alteran su veracidad. Por ejemplo, son técnicas de enmascaramiento perturbacional:

- **Añadir ruido**. Se añade un cierto nivel de ruido aleatorio a los datos originales para que los valores no sean exactos. El riesgo asociado a estos datos dependerá del nivel de ruido añadido. Cuanto mayor sea, más incertidumbre tendremos sobre los datos originales y, por lo tanto, el riesgo será menor.

- **Microagregación**. Consiste en agrupar los registros en grupos, con una cardinalidad mínima fijada, y reemplazar cada uno de los grupos por un nuevo registro que sea representativo del grupo. De esta manera, los registros de los datos anonimizados ya no se corresponden a una persona concreta, sino que hacen referencia a un grupo de personas. Cuanto mayor sean los grupos, menor será el riesgo.

[24] Para más información: A Network of Excellence in the European Statistical System in the field of Statistical Disclosure Control.

- **Intercambio de rango**. Se trata de reemplazar el valor de un atributo de un registro por el valor de otro registro que está dentro de un rango del valor inicial. A diferencia de la adición de ruido, en el intercambio de rango se preserva la distribución de datos en cada atributo.

Cada técnica de enmascaramiento tiene alguna propiedad que la puede hacer más adecuada que otra, en una situación concreta. Ahora bien, hay que tener siempre presente que estas técnicas alteran la veracidad de los datos. Desde el punto de vista de la privacidad esto es positivo porque, aunque se reidentifique un registro, habría incertidumbre sobre la veracidad de los datos que contiene. Por otro lado, esta pérdida de veracidad de los datos hace que estas técnicas no se puedan utilizar en determinadas situaciones.

Para mantener la veracidad de los datos pueden emplearse técnicas de enmascaramiento no perturbacional, que reducen la granularidad de la información de manera que no se pueda reidentificar un registro. Por ejemplo, son técnicas de enmascaramiento no perturbacional las siguientes:

- **Supresión**. Consiste en eliminar determinados datos, de manera que la persona afectada ya no sea identificable. La supresión es muy común con las variables identificativas; las variables identificativas, en general, no aportan mucho valor estadístico y, por lo tanto, suprimirlas no acostumbra a ser problemático. Por otro lado, la reidentificación también puede producirse por la combinación de diferentes atributos que, por sí solos, no son identificadores (estas combinaciones de atributos se conocen como *cuasi-identificadores*). Para evitar la reidentificación, es necesario suprimir los cuasi-identificadores que pueden permitir identificar personas concretas.

- **Generalización** (o recodificación global). Consiste en reemplazar la información en una variable o atributo de manera que el nuevo valor corresponda a una categoría más amplia. Por ejemplo, se puede reemplazar la edad con rangos de edad.

Generación de datos sintéticos

Con la aplicación de generación de datos sintéticos se obtienen datos nuevos a partir de un modelo de los datos originales. No hay una relación directa entre los originales y los sintéticas.

La idea es que el modelo debe preservar las propiedades estadísticas de los datos que interesa analizar. Hay que tener en cuenta que los datos sintéticos sólo recogen determinadas propiedades. Por lo tanto, el uso de este tipo de datos puede limitar la tipología de los análisis que pueden hacerse.

El hecho de que los datos sintéticos no reproduzcan los datos originales aisladamente considerados hace que se considere una técnica segura contra el riesgo de reidentificación. Ahora bien, este hecho, así como el riesgo de revelación, depende del modelo que se ha utilizado. Un modelo demasiado preciso puede conllevar unos riesgos elevados. Si el modelo consiste únicamente en algunas propiedades estadísticas de los datos originales que queremos preservar, el riesgo de reidentificación puede estar controlado. Ahora bien, la utilización de modelos muy complejos puede dar lugar a un sobreajuste; es decir, que el modelo no sea una representación de las propiedades estadísticas de los datos originales, sino que representa datos concretos. En este caso, el riesgo de reidentificación puede ser alto.

Por lo tanto, determinar las propiedades de los datos que interesa tratar es crítico. Por ejemplo, en la fase de desarrollo y pruebas, puede ser que baste preservar la validez sintáctica y semántica de los datos (es decir, que tengan los tipos adecuados y que no haya combinaciones sin sentido). Unos datos generados de esta manera evitan cualquier riesgo.

4.2.2 Riesgos en la anonimización

Los procesos de anonimización no garantizan de manera absoluta que sea imposible averiguar información personal a partir de los datos anonimizados. Una vez aplicadas las técnicas descritas anteriormente, hay que evaluar cuál es el nivel de riesgo y ajustar la anonimización.[25]

Muchas técnicas de anonimización se basan en suposiciones sobre la información disponible para un eventual atacante. Cuanto más información tenga, más fácil será, por ejemplo, que pueda reidentificar un registro. Puede ser muy difícil determinar cuál es la información disponible externamente y, además, esta información puede cambiar con el paso del tiempo, por lo que es necesario evaluar los riesgos existentes en cada momento.

En los procesos de anonimización que se acaban de describir, hay modelos de privacidad que buscan dar unas garantías de privacidad ya en el momento de hacer la anonimización. De esta manera, primero se fija el riesgo y, después, se aplica una técnica de anonimización para alcanzarlo.

Entre los modelos de privacidad más conocidos están el k-anonimato (y sus modelos relacionados, como l-diversidad y t-proximidad) y la privacidad diferencial.

K-anonimato

El k-anonimato trata con el riesgo de reidentificación haciendo que cada registro pueda asociarse a un conjunto de k personas. El k-anonimato asume que las reidentificaciones se producen a través de un conjunto de atributos (los cuasi-identificadores) y exige que cada combinación de estos cuasi-identificadores que aparezca en los datos anonimizados se repita, como mínimo, k veces.

Las formas más habituales de obtener k-anonimato son las siguientes:

- **Generalización y supresión**. Se reduce la granularidad de la información en los cuasi-identificadores, de manera que cada combinación de valores presente en los datos anonimizados se repita k veces.

[25] En relación con la efectividad de la anonimización, se puede consultar el capítulo 2 "How do we ensure anonymisation is effective" de la guía sobre anonimización, seudonimización y tecnologías de ampliación de la privacidad anonimización, seudonimización y tecnologías de ampliación de la privacidad (PET en sus siglas en inglés) que está confeccionando la *Information Commissioner's Office*.

- **Microagregación**. Se aplica microagregación sobre los cuasi-identificadores con grupos de tamaño k.

El k-anonimato puede acabar permitiendo la identificación de personas concretas, cuando la variabilidad de un atributo en un grupo de registros k-anónimo es pequeña. Para evitar este problema, se han desarrollado otros modelos de privacidad, como la l-diversidad y la t-proximidad, que exigen una variabilidad mínima.

Privacidad diferencial

La privacidad diferencial es un modelo de privacidad para las consultas a bases de datos. Es decir, no se genera una nueva base de datos anonimizada que puede analizarse, sino que las consultas se hacen sobre la base de datos original y se altera el valor de la respuesta para proteger la privacidad.

La privacidad diferencial es reconocida porque proporciona fuertes garantías de protección de la privacidad que, además, son independientes de la información disponible externamente. Ahora bien, la aplicación estricta de la privacidad diferencial presenta muchas limitaciones por el gran impacto que tiene sobre la utilidad de los datos. Por ejemplo, la privacidad diferencial se utiliza en el censo de los EE. UU., pero para mantener la utilidad de los datos, hay que aplicar unos parámetros tan extremos que se pierden todas las garantías.[26]

4.3 Seudonimización

La seudonimización es un proceso mediante el cual deja de ser posible identificar a la persona física a quien corresponden los datos si no se recurre a información adicional que debe estar almacenada por separado y sujeta a medidas técnicas y organizativas para evitar la reidentificación de las personas interesadas.[27] Es decir, sólo quien ha hecho la seudonimización puede acabar relacionando la información con personas identificadas o identificables. En cambio, las terceras personas no pueden establecer esta relación.

A diferencia de la anonimización, la seudonimización es un proceso reversible. Los datos personales seudonimizados siguen siendo datos personales y, por tanto, les es de aplicación la normativa de protección de datos.

Algunas de las técnicas para hacer efectiva la seudonimización son las siguientes:

- Uso de seudónimos: sólo quien tenga la correspondencia entre el seudónimo y la identidad real debe poder atribuir la información a la persona individual.
- Uso de códigos aleatorios que no sean previsibles para terceras personas.
- El cifrado habitualmente también se considera una técnica de seudonimización, dado que el proceso es reversible mediante el uso de una clave.

[26] Diferential Privacy for census data explained.

[27] Por este motivo los datos resultantes de la seudonimización siguen considerándose datos personales y, por tanto, permanecen sujetos a las obligaciones del RGPD. Sin embargo, la normativa europea fomenta el uso de seudónimos en el tratamiento de datos personales. Además, el RGPD considera que la seudonimización permite reducir los riesgos para las personas interesadas y contribuir al cumplimiento de la normativa.

Como en el caso de la anonimización, para que la seudonimización despliegue toda su eficacia conviene establecer una separación funcional, de manera que las personas que intervienen en el proceso de seudonimización no coinciden con las que están vinculadas al proceso del tratamiento de los datos una vez ya han sido pseudonimizados. Tambié hay que tener presente que los procesos de seudonimización no garantizan al 100 % que terceras personas no puedan acabar reidentificando a las personas afectadas, por lo que hay que analizar este riesgo y revisarlo periódicamente.

Hay que hacer referencia también a la posibilidad en determinados contextos (por ejemplo, redes sociales, metaverso, etc.) de recurrir a la utilización de identidades digitales diferenciadas de la identidad real. El uso de alias o avatares, aunque no son propiamente una técnica de seudonimización, puede ser especialmente útil para preservar un cierto grado de privacidad, dado que no deja de ser una capa de protección entre la identidad real del usuario y sus actuaciones en el ecosistema digital con estas otras identidades. Sin embargo, este mecanismo no constituye una garantía de anonimización, ni siquiera de seudonimización, dado que según el contexto y la información asociada se puede acabar identificando a la persona afectada. Por lo tanto, son datos personales.

5. Normativa de protección de datos

Normativa general

Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas con respecto al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPGDD).

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (LOPDSPJP).

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

Otras normas

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE) (arts. 21, 22, 38.3 *c*, *d* e *i*, 38.4 *d, g* y *h*, 43.1.

6. Bibliografía

Privacidad desde el diseño y por defecto

Privacy by Design. The 7 Foundational Principles. Ann Cavoukian. Ph.D. Information and Privacy Commissioner, Ontario, Canadá.

Privacy Design Strategies (The Little Blue Book), JAAP-HENK HOEPMAN (2022).

Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices. (2012) Ann Cavoukian, Ph.D.

Directrices 4/2019 relativas al artículo 25. Protección de datos desde el diseño y por defecto. (versión 2.0, 2020). Comité Europeo de Protección de Datos.

Data protection by design and by default. Information Commissioner's Office (ICO).

Guía RGPD CNIL del equipo de desarrollo. Commission Nationale d'Informatique et des Libertés (CNIL).

Directrices Desarrollo de software con protección de datos por diseño y por defecto, (2017). Autoridad de protección de datos de Noruega.
Guía de privacidad desde el diseño. Agència Española de Protección de Datos (AEPD).

Guía de protección de datos por defecto. Agència Española de Protección de Datos (AEPD).

Protección de datos desde el diseño y protección de datos por defecto. Garante per la Protezioni dei Dati Personali (GPDP).

Informe *"Ingeniería de protección de datos. De la teoria a la práctica"* (2022). ENISA.

Informe Privacidad y protección de datos desde el diseño: desde la política hasta la ingeniería (2014). ENISA.

Otros recursos

Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, (2013). Grupo de Trabajo del artículo 29, sobre protección de datos.

Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them (v. 1.0). Comité Europeo de Protección de Datos.

Deceptive design. Harry Brignull.

PETs Maturity Assessment Repository (2019). ENISA.

Protecting privacy in practice. (2019) . The Royal Society.

Privacy patterns. Privacy Patterns.org.

Web Security Testing Guide. Open Web A*pplication Security Project (OWASP).*

Cross Site Scripting Prevention Cheat Sheet. Open Web Application Security Project (OWASP).

Dictamen 5/2014, sobre técnicas de anonimización. Grupo de Trabajo del artículo 29.

Data Pseudonymisation: Advanced Techniques and Use Cases (2021). ENISA.

Anonymisation, pseudonymisation and privacy enhancing technologies guidance. (2021). Information Commissioner's Office (ICO).

Orientaciones y garantías en los procedimientos de anonimización de datos personales. Agència Espanyola de Protección de Dades (AEPD).

Introducción al Hash como técnica de seudonimización de datos personales. Agència Española de Protección de Datos (AEPD).

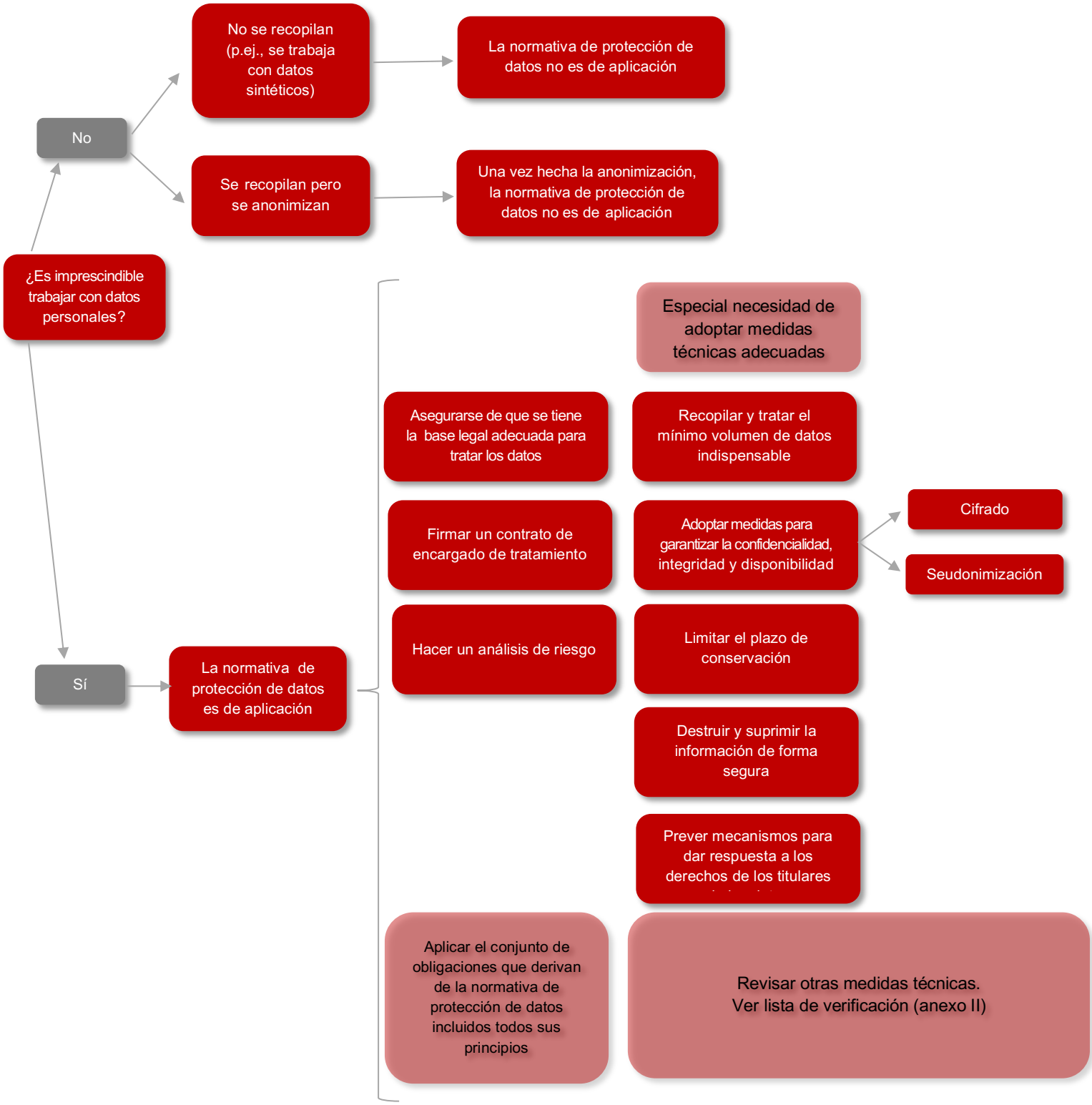
10 malentendidos relacionados con la anonimización. Agència Española de Protección de Dades (AEPD).

Cifrado y Privacidad III: Cifrado Homomórfico (2020). Agència Española de Protección de Datos (AEPD).

Guía práctica Evaluación de impacto relativa a la protección de datos (2019). Autoridad Catalana de Protección de Datos (MILI).

Guidance on AI and data protection. Information Commissioner's Office (ICO)

Anexo I. Análisis previo



Anexo II. Checklist

Fase de diseño

☐ Introducir estrategias de diseño para garantizar la protección de los datos
☐ Aplicar patrones de privacidad

Fase de desarrollo y de pruebas

☐ Firmar un contrato de encargo del tratamiento si el desarrollador o un tercero contratado por éste deben acceder a datos personales.
☐ Separar adecuadamente los entornos de producción y el de desarrollo y pruebas.
☐ Valorar la posibilidad de trabajar con datos ficticios, en entornos de pruebas.
☐ Minimizar la cantidad de datos recogidos ya en la fase de pruebas.
☐ Valorar la posibilidad de anonimizar o seudonimizar los datos recogidos en la fase de pruebas o utilizar datos sintéticos.
☐ Garantizar que la ubicación donde se aloja o se trata la información es en un país que ofrezca garantías adecuadas.
☐ Utilizar el protocolo wifi que proporcione un mayor grado de seguridad.
☐ Revisar la calidad del código utilizado y seguir las recomendaciones de las guías de programación segura.
☐ Hacer un análisis de riesgos para determinar las medidas de seguridad.
☐ Prever la formación del personal para garantizar, en todo momento, la minimización de riesgos.

Recogida de los datos

☐ Recoger sólo los datos imprescindibles. Esto afecta a lo siguiente:
- Datos recogidos mediante formularios.
- Datos técnicos que se recopilen (IP, MAC, geolocalización, etc.).
- Código insertado que pueda transferir informaciones.
- Otras vías de recogida de datos.

☐ Valorar la posibilidad de anonimizar o seudonimizar los datos personales recogidos.
☐ Minimizar especialmente la recogida de categorías especiales de datos.
☐ Distinguir claramente la información que debe proporcionarse obligatoriamente de la que es opcional.
☐ Pedir sólo los permisos para acceder y recoger información que sean relevantes para la finalidad que persigue.
☐ Valorar la posibilidad de que el tratamiento se haga directamente en los dispositivos de los usuarios.
☐ Informar adecuadamente a las personas afectadas sobre cómo se tratarán sus datos.
☐ Hacer copias de las cláusulas informativas existentes en cada momento, aplicando un sello de tiempo verificable (*timestamp*).
☐ Abstenerse de implementar patrones oscuros (*dark patterns*).
☐Verificar que se cumplen los requisitos para que el consentimiento, si es necesario, sea válido:
- Las casillas no pueden estar remarcadas.
- El consentimiento debe ser diferente para cada finalidad.
- No puede haber vinculación o acondicionamiento entre consentimientos.

- Establecer mecanismos que permitan verificar la identidad de quien presta el consentimiento.
- Verificar la identidad y la edad de la persona que otorga el consentimiento.
- El consentimiento debe poder revocarse con mecanismos de complejidad equivalente a los utilizados para otorgarlo.

☐ Conservar evidencias del consentimiento obtenido.

Uso de los datos

☐ Implementar mecanismos que permitan clasificar adecuadamente la información, de acuerdo con los fines y tratamientos a que deben someterse.
☐ Incorporar medidas que faciliten el ejercicio y la atención de los derechos.

Comunicación o divulgación de los datos

☐ Cuando la difusión se basa en el consentimiento de la persona afectada, hay que establecer mecanismos para que, por defecto, los datos no sean accesibles a terceras personas.
☐ Establecer controles sobre quién accede a la información.
☐ Prever la despublicación automatizada una vez se cumplan los plazos de uso de la información.
☐ Incluir el cifrado de extremo a extremo en las comunicaciones y, en su caso, la posibilidad de emplear conexiones VPN.
☐ Utilizar protocolos https para servicios vía web.
☐ Analizar la posibilidad de comunicar los datos cifrados.
☐ En la fase de desarrollo y aprendizaje de modelos de inteligencia artificial aplicar sistemas de aprendizaje federado.

Mantenimiento y conservación de los datos

Confidencialidad e integridad

☐ Establecer una política de permisos adecuada.
☐ Explorar la opción de requerir como mecanismos de identificación y autenticación los siguientes:

- El uso de certificados electrónicos
- Sistemas basados en múltiples factores de autenticación
- Sistemas de clave concertada

☐ Garantizar la seguridad y el proceso de gestión y custodia de las claves de acceso:

- Garantizar la robusteza de las credenciales.
- Implantar mecanismos técnicos de prevención de ataques de diccionario o de fuerza bruta.
- Establecer un procedimiento seguro de gestión y recuperación de las contraseñas.
- Garantizar que sólo el usuario puede conocer sus credenciales.
- Cifrar las claves.
- Obligar a renovar periódicamente las contraseñas.

☐ Configurar un *time-out* de sesión y que se borre la memoria cau.
☐ Instaurar un registro de accesos y de actividad.
☐ Mantener la información cifrada (si procede, con cifrado homomórfico) siempre que sea posible.
☐ Utilizar firma electrónica, si es posible.
☐ Asegurar que los procesos de anonimización o seudonimización empleados no han perdido efectividad.
☐ Hacer pruebas que comprueben vulnerabilidades a ataques y programarlas de manera periódica.
☐ Auditar periódicamente el código.
☐ Establecer mecanismos de detección automática de intrusiones y fugas de información.
☐ Adoptar cualquier otra medida de seguridad adecuada a los riesgos existentes.

Disponibilidad

☐ Configurar la ejecución de copias de seguridad.
☐ Establecer permisos diferenciados para acceder a las diferentes copias (*back-ups*).
☐ Prever pruebas de recuperación de la información a partir de copias.
☐ Valorar redundar el hardware, suministro eléctrico y redes de conectividad.

Limitación del plazo de conservación

☐ Definir el periodo de conservación de la información e informar a las personas afectadas.
☐ Implementar mecanismos automatizados para facilitar el cumplimiento de los plazos de supresión y bloqueo establecidos.
☐ Aplicar medidas como la anonimización si los datos se quieren conservar con fines estadísticos más allá del periodo de conservación establecido.
☐ Destruir los soportes de manera efectiva cuando se trate de elementos de hardware que dejan de utilizarse.
☐ Verificar que no se utilizan galletas persistentes o, alternativamente, fijar fecha de caducidad para este tipo de galleta.