Guía de Privacidad desde el Diseño

v. octubre 2019

v. octubre 2019

INDICE

I. LA PRIVACIDAD DESDE EL DISEÑO

CONCEPTO DE PRIVACIDAD DESDE EL DISEÑO

La idea de 'protección de datos desde el diseño' existe desde hace más de 20 años y se ha trabajado intensamente en ella bajo la terminología de 'privacidad desde el diseño' (*Privacy by Design*, PbD). Este concepto fue desarrollado por la Comisionada de Protección de Datos de Ontario, Ann Cavoukian, en la década de los 90; presentado en la 31ª Conferencia Internacional de Comisionados de Protección de Datos y Privacidad del año 2009 bajo el título *"Privacy by Design: The Definitive Workshop"* [1][2] y aceptado internacionalmente en la 32ª Conferencia Internacional de Comisionados de Protección de Datos y Privacidad, celebrada en Jerusalén en el año 2010, con la aprobación de la "Resolución sobre la Privacidad por Diseño" [3].

En esta resolución se reconocía la importancia de incorporar los principios de privacidad dentro de los procesos de diseño, operación y gestión de los sistemas de la organización para alcanzar un marco de protección integral en lo que a protección de datos se refiere. Además, se animaba a la adopción de los Principios Fundacionales de la Privacidad desde el Diseño definidos por Ann Cavoukian y se invitaba a las Autoridades de Protección de Datos a trabajar activamente e impulsar la incorporación de la privacidad desde el diseño en las políticas y la legislación en materia de protección de datos de sus respectivos Estados.

Principios Fundacionales de la Privacidad desde el Diseño
1. Proactivo, no reactivo; Preventivo, no correctivo
2. La privacidad como configuración predeterminada
3. Privacidad incorporada en la fase de diseño
4. Funcionalidad total: pensamiento "todos ganan"
5. Aseguramiento de la privacidad en todo el ciclo de vida.
6. Visibilidad y transparencia
7. Enfoque centrado en el sujeto de los datos

Tabla 1 – Principios de la "Privacidad desde el diseño"

El Reglamento (UE) 2016/679, General de Protección de Datos [4](en adelante, RGPD), en su artículo 25 [5] y bajo el epígrafe 'Protección de datos desde el diseño y por defecto', incorpora a la normativa de protección de datos la práctica de considerar los requisitos de privacidad desde las primeras etapas del diseño de productos y servicios. Por lo tanto,

1 Peter Hustinx, European Data Protection Supervisor. *Privacy by Design: Delivering the Promises,* Madrid 2009 https://edps.europa.eu/sites/edp/files/publication/09-11-02_madrid_privacybydesign_en.pdf

2 Ann Cavoukian, Identity in the Information Society, Ago 2010, Volume 3, Issue 2, pp 247-251. *Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D* https://link.springer.com/content/pdf/10.1007%2Fs12394-010-0062-y.pdf

3 Resolución de Privacidad desde el Diseño. 32ª Conferencia Internacional de Comisionados de Privacidad y Protección de Datos. Jerusalén (Israel) 27-29/10/2010 https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf

4 Reglamento (UE) 679/2016, General de Protección de Datos https://www.boe.es/doue/2016/119/L00001-00088.pdf

5 Artículo 25. "Protección de datos desde el diseño y por defecto" - Reglamento (UE) 2016/679, General de Protección de Datos https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e3126-1-1

le confiere la categoría de requisito legal al principio de integrar las garantías para la protección de los derechos y libertados de los ciudadanos con relación a sus datos personales desde las primeras etapas del desarrollo de sistemas y productos. Entendido pues como la necesidad de considerar la privacidad y los principios de protección de datos desde la concepción de cualquier tipo de tratamiento y a los efectos de redacción de este documento, los términos 'protección de datos desde el diseño' y 'privacidad desde el diseño' pueden ser considerados equivalentes [6] [7] [8].

Figura 1 – Privacidad desde el diseño como suma integral
del enfoque al riesgo y la responsabilidad proactiva

La privacidad desde el diseño (en adelante, PbD) implica utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva [9] para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso). Por ciclo de vida del objeto se entiende todas las etapas por las que atraviesa este, desde su concepción hasta su retirada, pasando por las fases de desarrollo, puesta en producción, operación, mantenimiento y retirada. Más aun, implica que se tengan en cuenta, no sólo la aplicación de medidas de protección de la privacidad en las etapas tempranas del

6 European Data Protection Supervisor (EDPS). *Opinion 5/2018 Preliminary Opinion on Privacy by design,* May 2018 https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf "'*Privacy by Design' or 'Data Protection by Design'? For the purpose of this Opinion, we use the term "privacy by design" to designate the broad concept of technological measures for ensuring privacy as it has developed in the international debate over the last few decades. In contrast, we use the terms "data protectionby design" and "data protection by default" to designate the specific legal obligations established by Article 25 of the GDPR."*

7 European Union Agency for Cybersecurity (ENISA). *Privacy and Data Protection by Design – from policy to engineering*, Dic 2014 https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport *"The term "Privacy by Design", or its variation "Data Protection by Design", has been coined as a development method for privacy-friendly systems and services, thereby going beyond mere technical solutions and addressing organisational procedures and business models as well".*

8 Information Commissioner's Office (ICO). *Data protection by design and default*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ *"This concept is not new. Previously known as 'privacy by design', it has always been part of data protection law. The key change with the GDPR is that it is now a legal requirement."*

9 La nueva normativa europea supone un cambio de paradigma en la forma de garantizar los derechos y libertades de los interesados en lo que al tratamiento de sus datos personales se refiere y se apoya en el enfoque de riesgo, como planteamiento dinámico y de mejora continua para entender los riesgos a la privacidad y determinar las medidas técnicas y organizativas a implantar, y en la responsabilidad proactiva, entendida como un autoanálisis crítico, continuo y rastreable del responsable del tratamiento en el cumplimiento de las obligaciones que le exige la normativa.

proyecto, sino que además se contemplen también todos los procesos y prácticas de negocio involucrados en el tratamiento de datos asociado, logrando así una verdadera gobernanza de la gestión de los datos personales por parte de las organizaciones.

El objetivo último es que la protección de datos esté presente desde las primeras fases de desarrollo y no sea una capa añadida a un producto o sistema. La privacidad debe formar parte integral de la naturaleza de dicho producto o servicio.

PRINCIPIOS FUNDACIONALES DE LA PRIVACIDAD DESDE EL DISEÑO

La PbD se fundamenta en la construcción de la privacidad como el modo de operación predeterminado dentro del modelo de negocio de las organizaciones y que se extiende a los sistemas de tecnologías de la información que soportan el tratamiento de los datos, los procesos y las prácticas de negocio relacionadas y el diseño físico y lógico de los canales de comunicación utilizados. Este aseguramiento de la privacidad puede lograrse mediante la puesta en práctica de los siete Principios Fundacionales definidos por Ann Cavoukian [10] [11]:

1. *Proactivo, no reactivo; preventivo, no correctivo.*

La PbD implica anticiparse a los eventos que afecten a la privacidad antes de que sucedan.

Cualquier sistema, proceso o infraestructura que vaya a utilizar datos personales debe ser concebida y diseñada desde cero identificando, a priori, los posibles riesgos a los derechos y libertades de los interesados y minimizarlos para que no lleguen a concretarse en daños. Una política de PbD se caracteriza por la adopción de medidas proactivas que se anticipan a las amenazas, identificando las debilidades de los sistemas para neutralizar o minimizar los riesgos en lugar de aplicar medidas correctivas para resolver los incidentes de seguridad una vez sucedidos. Es decir, la PbD huye de la "política de subsanar" y se adelanta a la materialización del evento de riesgo.

Esto implica:

- Un claro compromiso por parte de la organización y que debe ser impulsado desde los escalones más altos de la Dirección.
- El desarrollo de una cultura de compromiso y mejora continua por parte de todos los trabajadores, ya que de nada sirve una política si esta no se traduce en acciones concretas que se realimenten de sus resultados.
- Definición y asignación de responsabilidades concretas, de modo que cada miembro de la organización sepa claramente cuáles son sus funciones en materia de privacidad.
- Desarrollar métodos sistemáticos en base a indicadores para la detección temprana de procesos y prácticas que estén ofreciendo resultados deficientes en la garantía de la privacidad.

10 Ann Cavoukian, Ph.D. Information & Privacy Commissioner Ontario, Canada. *Privacy by Design: The 7 Foundational Principles,* Ene 2011 https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

11 Ann Cavoukian, Ph.D. Information & Privacy Commissioner Ontario, Canada. *Operationalizing Privacy by Design. A guide to implementing strong privacy practices,* Dic 2012 http://www.ontla.on.ca/library/repository/mon/26012/320221.pdf

2. *La privacidad como configuración predeterminada*

La PbD persigue proporcionar al usuario el máximo nivel de privacidad dado el estado del arte y, en particular, que los datos personales estén automáticamente protegidos en cualquier sistema, aplicación, producto o servicio.

La configuración por defecto deberá quedar establecida desde el diseño a aquel nivel que resulte lo más respetuoso posible en términos de privacidad. En el caso de que el sujeto no tome ninguna acción de configuración, su privacidad debe estar garantizada y mantenerse intacta, pues está integrada en el sistema y configurada por defecto.

Este principio, llevado a términos prácticos, se fundamenta en la minimización de datos a lo largo de todas las etapas del tratamiento: recogida, uso, conservación y difusión.

Para ello se debe:

- Fijar criterios de recogida limitados a la finalidad que persigue el tratamiento.
- Limitar el uso de los datos personales a la(s) finalidades para la(s) que fueron recogidos y asegurarse de que existe una base legitimadora del tratamiento.
- Restringir los accesos a los datos personales a las partes implicadas en los tratamientos atendiendo al principio de "*need to know*" y según la función que realicen mediante la creación de perfiles de acceso diferenciados.
- Definir plazos estrictos de conservación y establecer mecanismos operativos que garanticen su cumplimiento.
- Crear barreras tecnológicas y procedimentales que impidan la vinculación de no autorizada de fuentes de datos independientes.

3. *Privacidad incorporada en la fase de diseño*

La privacidad debe formar parte integral e indisoluble de los sistemas, aplicaciones, productos y servicios, así como de las prácticas de negocio y procesos de la organización. No es una capa adicional o módulo que se añade a algo preexistente , sino que debe estar integrada en el conjunto de requisitos no funcionales desde el mismo momento en el que se concibe y diseña.

Para garantizar que la privacidad se tiene en cuenta desde las primeras etapas del diseño se debe:

- Considerar como un requisito necesario en el ciclo de vida de sistemas y servicios, así como en el diseño de los procesos de la organización.
- Ejecutar un análisis de los riesgos para los derechos y libertades de las personas y, en su caso, evaluaciones de impacto relativas a la protección de datos, como parte integral del diseño de cualquier nueva iniciativa de tratamiento.
- Documentar todas las decisiones que se adopten en el seno de la organización con un enfoque "*privacy design thinking*"

4. *Funcionalidad total: pensamiento "todos ganan"*

Tradicionalmente se ha entendido que se gana privacidad a costa de perder otras funcionalidades, presentando dicotomías como privacidad vs usabilidad, privacidad vs funcionalidad, privacidad vs beneficio empresarial, incluso privacidad vs seguridad.

Esta aproximación es artificial [12] y el objetivo ha de ser buscar el balance óptimo en una búsqueda tipo "gana-gana", con una mentalidad abierta a nuevas soluciones para conseguir sistemas plenamente funcionales, eficaces y eficientes también a nivel de privacidad.

Para ello, desde las primeras etapas de concepción de los productos y servicio, la organización debe:

- Asumir que pueden coexistir intereses diferentes y legítimos: los de la entidad y los de los usuarios a los que presta servicio; y que es necesario identificarlos, evaluarlos y balancearlos apropiadamente.
- Establecer canales de comunicación para colaborar y consultar a las partes interesadas con el objeto de comprender y hacer converger múltiples intereses, que aparentemente y en una primera aproximación, pueden parecer divergentes.
- Si la solución propuesta plantea amenazas a la privacidad, buscar nuevas soluciones y alternativas para alcanzar las distintas funcionalidades e intereses perseguidos, pero siempre sin perder de vista que deben gestionarse adecuadamente los riesgos para la privacidad del usuario.

5. Aseguramiento de la privacidad en todo el ciclo de vida

La privacidad nace en el diseño, antes de que el sistema esté en funcionamiento y debe garantizarse a lo largo de todo el ciclo de vida completo de los datos.

La seguridad de la información impone confidencialidad, integridad, disponibilidad y resiliencia de los sistemas que los cobija. La privacidad garantiza además la desvinculación *(unlinkability)*, la transparencia y la capacidad de intervención y control en el tratamiento por parte del sujeto del dato *(intervenability)*.

Para integrar la privacidad a lo largo de todas las etapas del tratamiento de datos, se deben analizar detenidamente las distintas operaciones implicadas (recogida, registro, clasificación, conservación, consulta, difusión, limitación, supresión, …) e implementar, en cada una de ellas, las medidas más adecuadas para proteger la información y entre las que cabe considerar:

- La seudonimización temprana o técnicas de anonimización como la k-anonimidad [13].
- Clasificación y organización de los datos y operaciones de tratamiento en base a perfiles de acceso.
- El cifrado por defecto de modo que el estado "natural" de los datos en caso de pérdida o robo sea "ilegible".
- La destrucción segura y garantizada de la información al final de su ciclo de vida.

12 Este tipo de aproximaciones ya se plantearon cuando se introdujeron conceptos en las organizaciones como el de ciberseguridad o el de calidad.

13 Agencia Española de Protección de Datos (AEPD) – Unidad de Evaluación y Estudios Tecnológicos. *La K-anonimidad como medida de la privacidad,* Jun 2019 https://www.aepd.es/media/notas-tecnicas/nota-tecnica-kanonimidad.pdf *"La **K**-anonimidad es una propiedad de los datos anonimizados que permite cuantificar hasta qué punto se preserva la anonimidad de los sujetos presentes en un conjunto de datos en el que se han eliminado los identificadores. Dicho de otro modo, es una medida del riesgo de que agentes externos puedan obtener información de carácter personal a partir de datos anonimizados."*

6. *Visibilidad y transparencia*

Una de las claves para poder garantizar la privacidad es poder demostrarla, verificando que el tratamiento es acorde a la información dada.

La transparencia en el tratamiento de datos se asienta como pilar para demostrar la diligencia y la responsabilidad proactiva ante la Autoridad de Control y como medida de confianza ante los sujetos cuyos datos son tratados. Tal y como establece el considerando 39 del RGPD [14], para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados.

Fomentar la trasparencia y la visibilidad pasa por adoptar una serie de medidas como:

- Hacer públicas las políticas de privacidad y protección de datos que rigen el funcionamiento de la organización.
- Desarrollar y publicar cláusulas de información concisas, claras e inteligibles, que sean fácilmente accesibles y que permitan a los interesados comprender el alcance del tratamiento de sus datos, los riesgos a los que pueden verse expuestos, así como el modo de hacer valer sus derechos en materia de protección de datos.
- Aun no siendo obligatorio para todos los responsables, hacer pública, o al menos fácilmente accesible para los interesados, la lista de los tratamientos realizados en la organización.
- Difundir la identidad y contacto de la persona responsable en la organización de los asuntos en materia de privacidad.
- Establecer mecanismos de comunicación, compensación y reclamación accesibles, sencillos y efectivos dirigidos a los titulares de los datos.

7. *Respeto por la privacidad de los usuarios: mantener un enfoque centrado en el usuario*

Sin obviar los intereses legítimos que persigue la organización con el tratamiento de datos que realiza, el fin último debe ser garantizar los derechos y libertades de los usuarios cuyos datos son objeto de tratamiento, por lo que cualquier medida adoptada debe ir encaminada a garantizar su privacidad. Ello supone diseñar procesos, aplicaciones, productos y servicios “con el usuario en mente”, anticipándose a sus necesidades.

El usuario debe tener un papel activo en la gestión de sus propios datos y en el control de la gestión que otros hagan con ellos. Su inacción no debe suponer un menoscabo a la privacidad, retomando uno de los principios ya mencionados y que propugna una configuración de privacidad por defecto que ofrezca el máximo nivel de protección.

Un diseño de procesos, aplicaciones, productos y servicios que estén focalizados en garantizar la privacidad de los sujetos de datos pasa por:

- Implementar configuraciones de privacidad por defecto “robustas” y en las que se informe a los usuarios de las consecuencias a su privacidad que supone la modificación de los parámetros prestablecidos.

14 Reglamento (UE) 679/2016, General de Protección de Datos https://www.boe.es/doue/2016/119/L00001-00088.pdf

- Facilitar información completa y adecuada que conduzca a un consentimiento informado, libre, específico e inequívoco que deberá ser explícito en aquellos casos en que se requiera.
- Proporcionar a los interesados acceso a sus datos y a la información detallada de las finalidades del tratamiento y de las comunicaciones realizadas.
- Implementar mecanismos eficientes y efectivos que permitan a los interesados el ejercicio de sus derechos en materia de protección de datos.

Figura 2 – Principios Fundacionales de la Privacidad desde el Diseño

SUJETOS OBLIGADOS A LA PROTECCIÓN DE DATOS DESDE EL DISEÑO

El RGPD establece la 'protección de datos desde el diseño' como requisito legal de cumplimiento. El artículo 83 [15] considera sancionable [16] no atender esta obligación, al igual que su correcta aplicación constituye uno de los criterios para baremar la gravedad de una infracción.

Tal y como establece el artículo 25 del RGPD [17], la obligación de implementar la protección de datos desde el diseño es aplicable a todos los responsables del tratamiento con independencia de su tamaño, el tipo de datos tratados o la naturaleza del tratamiento. En concreto, se les exige que se apliquen las medidas técnicas y organizativas apropiadas *"tanto en el momento de determinar los medios de tratamiento como en el propio tratamiento"*.

Si bien el cumplimiento de esta obligación aplica específicamente al responsable del tratamiento, a la luz del considerando 78 [18] y lo establecido en el artículo 28 del RGPD [19], la protección de datos desde el diseño se proyecta sobre otros actores participantes en el tratamiento de datos personales como son los proveedores y prestadores de servicios, desarrolladores de productos y aplicaciones o fabricantes de dispositivos. A

15 Artículo 83. "Condiciones generales para la imposición de multas administrativas" - Reglamento (UE) 2016/679, General de Protección de Datos https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e6301-1-1

16 La Autoridad Rumana de Protección de Datos anunció el 4 de julio de 2019 que había multado a la entidad UNICREDIT BANK S.A. por incumplimiento del artículo 25.1 del RGPD https://www.dataprotection.ro/index.jsp?page=Comunicat_Amenda_Unicredit&lang=en

17 Artículo 25. "Protección de datos desde el diseño y por defecto" - Reglamento (UE) 2016/679, General de Protección de Datos https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e3126-1-1

18 Reglamento (UE) 679/2016, General de Protección de Datos https://www.boe.es/doue/2016/119/L00001-00088.pdf

19 Artículo 28. "Encargado del tratamiento" - Reglamento (UE) 2016/679, General de Protección de Datos https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e3210-1-1

estos, el responsable ha de alentar a *"que tengan en cuenta el derecho a la protección de datos cuando desarrollen y diseñen estos productos, servicios y aplicaciones"* y, cuando necesite encargar a un tercero el tratamiento de los datos, debe seleccionar a aquel "*encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.*".

En resumen, es el responsable del tratamiento, en aplicación de su deber de diligencia, quién debe ceñirse a la selección de productos y de encargados capaces de garantizar el cumplimiento de los requisitos del RGPD, y en particular, la obligación de garantizar la protección de datos desde el diseño y por defecto.

Esta exigencia es también aplicable a los corresponsables del tratamiento en función de sus responsabilidades respectivas asumidas conjuntamente en la determinación de medios y fines del tratamiento.

Figura 3 – Privacidad desde el diseño como base de la cultura de privacidad de la organización

(La figura ha sido diseñada usando imágenes de Freepik.com)

II. REQUISITOS DE PRIVACIDAD DEL SISTEMA

Comprender cómo un tratamiento de los datos personales puede llegar a afectar a la privacidad de los individuos es la clave para diseñar y desarrollar sistemas confiables desde un punto de vista de protección de datos.

El RGPD consagra en su artículo 5 [20] los principios básicos que han de tenerse en cuenta a la hora de realizar los tratamientos, de modo que estos seis principios (licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad) unidos al de responsabilidad proactiva (o *accountability*) se convierten en el núcleo de la norma y en

20 Artículo 5. "Principios relativos al tratamiento" - Reglamento (UE) 2016/679, General de Protección de Datos https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e1873-1-1

el objetivo que todo sistema, aplicación, servicio o proceso debe garantizar en su diseño, además de los requisitos o requerimientos funcionales a satisfacer propios del sistema.

OBJETIVOS DE PRIVACIDAD Y SEGURIDAD

Tradicionalmente, el diseño de sistemas seguros y confiables se ha centrado en analizar los riesgos y dar respuesta a las amenazas que afectan a los objetivos de la seguridad que están más orientados a la privacidad:

- confidencialidad, evitando los accesos no autorizados a los sistemas,
- integridad, protegiéndolos de modificaciones no autorizadas de la información y
- disponibilidad, garantizando que los datos y los sistemas están disponibles cuando es necesario.

Sin embargo, aunque el acceso y la modificación no autorizada de los datos personales puede llegar a ser un aspecto crítico que amenace la privacidad de los individuos, existen otros factores de riesgo que pueden aparecer durante un procesamiento autorizado de los datos [21] y que deben ser identificados durante la evaluación de riesgos para los derechos y libertades de los sujetos de los datos.

La pérdida de autonomía en la toma de decisiones, la recogida excesiva de datos, la re-identificación, la discriminación y/o estigmatización de las personas, el sesgo en las decisiones automatizadas, la falta de comprensión de los usuarios del alcance y los riesgos de un tratamiento o un perfilado no legitimado, invasivo o incorrecto son ejemplos de riesgos a la privacidad con una clara afectación en los derechos y libertades de las personas que no pueden ser gestionados utilizando un modelo tradicional de riesgos enfocado a la protección exclusiva de los objetivos de seguridad.

Teniendo en cuenta el escenario descrito y los posibles riesgos a la privacidad asociados con el funcionamiento planificado y autorizado de los sistemas que recopilan, usan y divulgan datos personales, es preciso ampliar el marco de análisis para que este cubra tanto los riesgos derivados de su tratamiento no autorizado como aquellos que pueden surgir de un procesamiento planeado y permitido de la información.

Para dar cobertura a estos posibles riesgos han de incluirse en el esquema de análisis tres nuevos objetivos de protección [22][23], específicos de la privacidad, y cuya garantía se convierte en salvaguarda de los principios de tratamiento establecidos por el RGPD:

- **Desvinculación (Unlinkability):** persigue que el procesamiento de la información se realice de modo que los datos personales de un dominio de tratamiento no puedan vincularse con los datos personales de otro dominio diferente o que el establecimiento de dicha vinculación suponga un esfuerzo desproporcionado. Este objetivo de privacidad minimiza el riesgo de un uso no autorizado de los datos personales y la creación de perfiles mediante la interconexión de información perteneciente a diferentes conjuntos de datos,

21 Sean Brooks, Michael Garcia, Naomi Lefkovitz, Susanne Lightman, Ellen Nadeau - National Institute of Standards and Technology (NIST). *NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems*, Ene 2017 https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

22 Harald Zwingelberg, Marit Hansen. 7th PrimeLife International Summer (PRIMELIFE), Sep 2011, Trento, Italy. pp.245-260. *Privacy Protection Goals and Their Implications for eID Systems*. https://hal.inria.fr/hal-01517607/document

23 Marit Hansen. 7th PrimeLife International Summer (PRIMELIFE), Sep 2011, Trento, Italy. pp.14-31. *Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals* https://hal.inria.fr/hal-01517612/document

estableciendo garantías sobre los principios de limitación de la finalidad, la minimización de datos y la limitación del plazo de conservación.

- **Transparencia (Transparency):** busca clarificar el tratamiento de los datos de modo que la recogida, el procesamiento y el uso de la información pueda ser comprendido y reproducido por cualquiera de las partes implicadas y en cualquier momento del tratamiento. Este objetivo de la privacidad pretende que el contexto del tratamiento quede perfectamente delimitado y que la información sobre las finalidades y las condiciones legales, técnicas y organizativas aplicables esté disponible antes, durante y después del tratamiento a todas las partes implicadas, tanto para el responsable como para el sujeto cuyos datos son tratados, minimizando así los riesgos que pueden afectar a los principios de lealtad y transparencia.
- **Control (Intervenability):** garantiza la posibilidad de que las partes involucradas en el tratamiento de los datos personales y, principalmente, los sujetos cuyos datos son tratados, pueden intervenir en el tratamiento cuando sea necesario para aplicar medidas correctivas al procesamiento de la información. Este objetivo está íntimamente relacionado con la definición e implementación de procedimientos para el ejercicio de derechos en materia de protección de datos, la presentación de reclamaciones o la revocación de los consentimientos prestados por parte de los interesados, así como mecanismos para garantizar, por parte del responsable, la evaluación del cumplimiento y la efectividad de las obligaciones que le son fijadas por la normativa, lo que contribuye a respetar los principios de exactitud y responsabilidad proactiva marcados por el RGPD.

Estos tres nuevos objetivos de protección, junto con los objetivos de seguridad existentes, establecen un marco global de protección en el tratamiento de los datos personales y determinan, como resultado de la realización de una evaluación de los riesgos sobre su afectación, otro tipo de atributos o requisitos no funcionales que debe satisfacer el sistema y que se convierten en las entradas de los procesos de diseño de la privacidad.

OBJETIVOS DE PROTECCIÓN DE LA PRIVACIDAD		
DESVINCULACIÓN	**TRANSPARENCIA**	**CONTROL**
Minimización de datos Limitación del plazo de conservación Integridad y confidencialidad	Licitud, lealtad y transparencia Limitación de la finalidad	Limitación de la finalidad Exactitud Integridad y confidencialidad Responsabilidad proactiva

Tabla 2 – Garantía de los principios del tratamiento del RGPD a través de los objetivos de privacidad

Vistos de forma global y conjunta, los seis objetivos de protección son complementarios entre sí [24] y en ocasiones se solapan, por lo que, para cada evaluación de impacto sobre la protección de datos (EIPD) [25] [26] que se realice sobre los tratamientos de datos a acometer, habrá que valorar la posible preponderancia de un objetivo sobre otro y buscar un equilibrio en las medidas y salvaguardas adoptadas para su garantía.

III. PRIVACY ENGINEERING: LA INGENIERÍA DE LA PRIVACIDAD

La **privacy engineering** [27] o ingeniería de la privacidad [28] es un proceso sistemático y dirigido por el enfoque al riesgo cuyo objetivo es traducir en términos prácticos y operativos los principios de la privacidad desde el diseño (PbD) dentro del ciclo de vida de los sistemas de información encargados del tratamiento de datos personales:

- especificando las propiedades y funcionalidades de privacidad que debe cumplir el sistema de una manera que sea posible su diseño e implementación (*definición de los requisitos de privacidad*)
- diseñando la arquitectura e implementando los elementos del sistema que den cobertura a los requisitos de privacidad definidos (*diseño e implementación de la privacidad*)
- confirmando que los requisitos de privacidad definidos han sido correctamente implementados y satisfacen las expectativas y necesidades de las partes interesadas (*verificación y validación de la privacidad*)

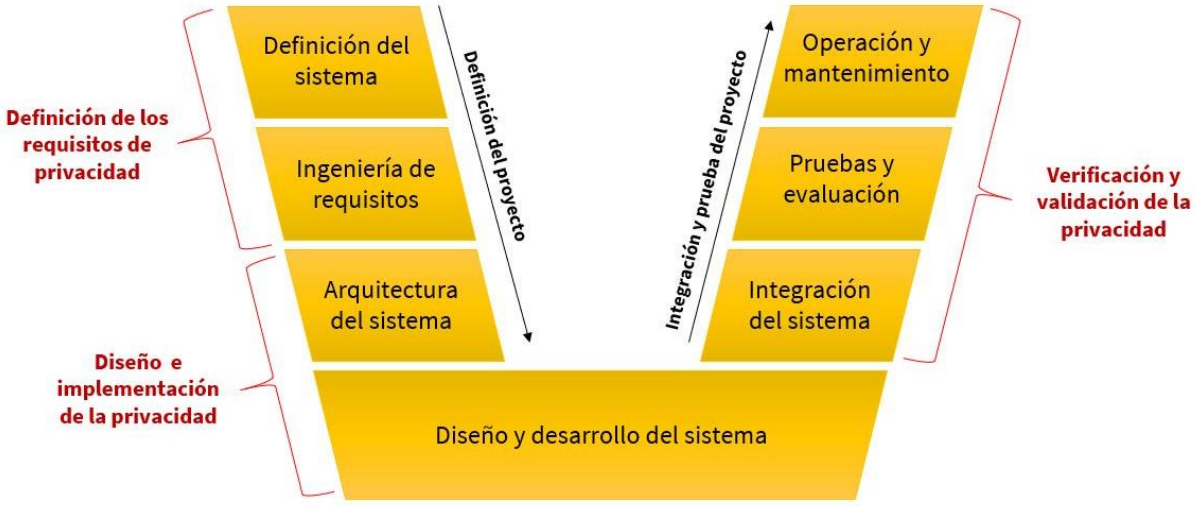

Figura 4 – Ingeniería de la privacidad [28]

24 Marit Hansen, Meiko Jensen, Martin Rost.. International Workshop on Privacy Engineering. *Protection Goals for Privacy Engineering*, May 2015 https://www.ieee-security.org/TC/SPW2015/IWPE/2.pdf

25 Agencia Española de Protección de Datos (AEPD). *Guía para la Evaluación de Impacto en la Protección de Datos personales,* Oct 2018 https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

26 Agencia Española de Protección de Datos (AEPD). *Modelo de Informe de Evaluación de Impacto en la Protección de Datos (EIPD) para las Administraciones Públicas* https://www.aepd.es/reglamento/cumplimiento/evaluaciones-de-impacto.html

27 En este apartado tratamos la ingeniería de la privacidad como un proceso dentro del diseño y desarrollo del objeto. La ingeniería de la privacidad también se puede entender como una disciplina tal y como se describe en: : https://www.aepd.es/blog/2019-09-11-ingenieria-privacidad.html

28 Massachusetts Institute of Technology Research & Engineering (MITRE) – Privacy Community of Practice (CoP). *Privacy Engineering Framework*, Jul 2014 https://www.mitre.org/sites/default/files/publications/14-2545-presentation-privacy-engineering-framework-july2014.pdf

El objetivo es que la privacidad quede integrada como parte del diseño del sistema, de modo que los requisitos de privacidad sean definidos en términos de propiedades y funcionalidades plenamente implementables y cualquier riesgo sobre la privacidad que se haya identificado sea adecuadamente gestionado por el sistema de manera proactiva.

Para ello, debe seguirse una aproximación sistemática y metodológica, trasladando el *qué* de las fases de concepción y análisis (los requisitos de privacidad identificados) al *cómo* de las fases de diseño e implementación (estrategias y soluciones concretas) trabajando, de forma secuencial, en diferentes niveles de abstracción.

En el nivel más alto, en las fases iniciales de concepción del objeto y del análisis de sus requisitos, hay que trabajar con **estrategias de privacidad** [29], enfoques genéricos a alto nivel dirigidos a identificar aquellas tácticas a seguir durante las diferentes etapas del procesamiento de los datos encaminadas a garantizar los objetivos de privacidad y el cumplimiento de los principios de tratamiento. Las estrategias proporcionan un modelo accesible a través del cual los ingenieros que diseñan el objeto pueden concretar los requisitos de privacidad identificados durante las fases de análisis y requerimiento. Las estrategias de privacidad sirven de puente entre los principios de tratamiento impuestos por la norma y la implementación de la privacidad en soluciones concretas. Como se verá más adelante, están centradas en dar respuesta a las acciones que puedan suponer una amenaza a la privacidad en las actividades de tratamiento y su uso no es excluyente. Muy al contrario, lo deseable es aplicarlas todas o el máximo posible de ellas de cara a conseguir que el objeto desarrollado sea lo más *privacy-friendly* posible.

Las estrategias de privacidad se materializan, a más bajo nivel, en **patrones de diseño de la privacidad** [29] soluciones reutilizables empleadas en la fase de diseño que son aplicables para resolver problemas comunes y repetibles de privacidad que se presentan de forma reiterada en el desarrollo de productos y sistemas. El objetivo de los patrones es crear catálogos de soluciones reutilizables en el diseño de la privacidad de los sistemas y estandarizar el proceso de diseño.

La asociación entre patrones y estrategias no es biunívoca, de modo que un mismo patrón puede implementar y dar respuesta a más de una estrategia de privacidad, proporcionando solución a diferentes problemas que se presentan a lo largo de las actividades de tratamiento de los datos.

Por último, en el más bajo nivel, en la fase de desarrollo, se encuentran las tecnologías de privacidad mejorada o **PETS (Privacy Enhancing Technologies)** que se utilizan para implementar los patrones de diseño de la privacidad con una tecnología concreta [29]. La Comisión, en su Comunicación al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET) las define *como "un sistema coherente de medidas de TIC que protege el derecho a la intimidad suprimiendo o reduciendo los datos personales o evitando el tratamiento innecesario o indeseado de datos personales, sin menoscabo de la funcionalidad del sistema de información."*[30]. Al igual que ocurría con los patrones y las estrategias de diseño de la privacidad, una misma solución PET puede implementar varias soluciones de patrones de diseño.

29 Jaap-Henk Hoepman. Institute for Computing and Information Sciences (ICIS) – Radboud University Nijmegen, The Netherlands. *Privacy Design Strategies,* Oct 2012 https://www.cs.ru.nl/~jhh/publications/pdp.pdf

30 COM(2007)228 COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52007DC0228&from=EN

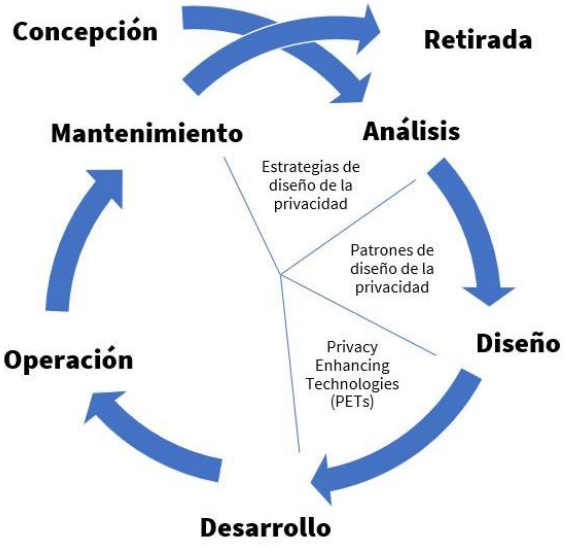

Figura 5 – Estrategias, patrones y técnicas (PET) de privacidad dentro del ciclo de vida del sistema [31]

IV. ESTRATEGIAS DE DISEÑO DE LA PRIVACIDAD

El estado del arte identifica ocho estrategias de diseño de la privacidad [31][32] que se conocen como 'minimizar', 'ocultar', 'separar', 'abstraer', 'informar', 'controlar', 'cumplir' y 'demostrar'.

A su vez, estas ocho estrategias pueden clasificarse en dos categorías [31]: las estrategias orientadas al tratamiento de los datos y las estrategias orientadas a los procesos. Las primeras, que incluyen las estrategias de 'minimizar', 'ocultar', 'separar' y 'abstraer', son de carácter más técnico y se centran en un tratamiento *privacy-friendly* de los datos recogidos. Las segundas, que incluyen las estrategias de 'informar', 'controlar', 'cumplir' y 'demostrar', tienen un carácter más organizativo y están orientadas a la definición de procesos que implementen una gestión responsable de los datos personales.

OBJETIVO DE PROTECCIÓN DE LA PRIVACIDAD	ESTRATEGIAS DE DISEÑO DE LA PRIVACIDAD ORIENTADAS A DATOS	ESTRATEGIAS DE DISEÑO DE LA PRIVACIDAD ORIENTADAS A PROCESOS
DESVINCULACIÓN	MINIMIZAR, ABSTRAER, SEPARAR, OCULTAR	
CONTROL		CONTROLAR, CUMPLIR, DEMOSTRAR
TRANSPARENCIA		INFORMAR

Tabla 3 – Asociación entre los objetivos de privacidad y las estrategias de diseño de la privacidad

31 Jaap-Henk Hoepman. *Privacy Design Strategies (The Little Blue Book)*, Mar 2019 https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf

32 Michael Colesky, Jaap-Henk Hoepman – Digital Security. Radboud University Nijmegen, The Netherlands, Christiaan Hillen – Valori Security. Nieuwegein, The Netherlands. *A Critical Analysis of Privacy Design Strategies*, May 2016 https://www.researchgate.net/publication/305870977_A_Critical_Analysis_of_Privacy_Design_Strategies

Aunque, dependiendo del contexto, determinadas estrategias pueden ser más aplicables que otras en el marco de desarrollo de un sistema, estas ocho estrategias, consideradas desde las etapas iniciales de su concepción y análisis y aplicadas conjuntamente, permiten incorporar salvaguardas y medidas de protección en las operaciones y procedimientos de tratamiento de los datos personales consiguiendo que los resultados finales tengan en cuenta los requisitos de privacidad que garantizan los derechos y libertades de los sujetos de datos.

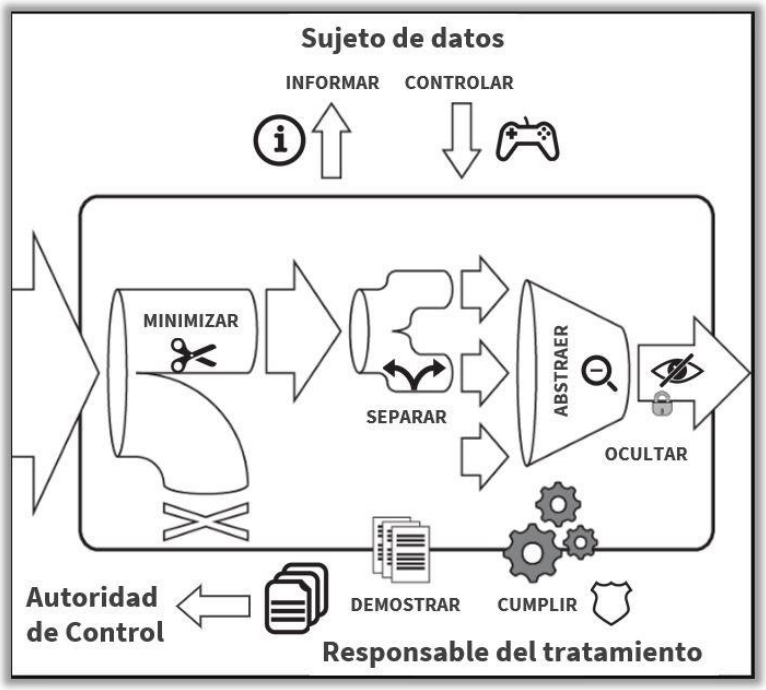

Figura 6 – Estrategias de diseño de la privacidad.

(Imagen tomada del documento Privacy Design Strategies (The Little Blue Book) [31])

Minimizar

El objetivo que persigue esta estrategia es recoger y tratar la mínima cantidad de datos posible, de modo que, evitando el procesamiento de datos que no sean necesarios para las finalidades perseguidas en el tratamiento, se limitan los posibles impactos en la privacidad. Esto puede lograrse recogiendo datos de menos sujetos (reducir el tamaño de la población de estudio) o menos datos de los sujetos (reducir el volumen de información recopilada) para lo cual pueden utilizarse las siguientes tácticas:

- **Seleccionar:** elegir únicamente la muestra de individuos relevante y los atributos necesarios siguiendo una actitud conservadora al establecer el criterio de selección y realizar el tratamiento únicamente sobre los datos que respondan a dicho criterio (lista blanca).
- **Excluir:** es el enfoque inverso al anterior, y consiste en excluir de antemano los sujetos y atributos que resulten irrelevantes para el tratamiento realizado (lista negra). En este caso se debe adoptar una actitud abierta, intentando excluir el máximo posible de registros a menos que pueda justificarse que son absolutamente necesarios para la finalidad perseguida.
- **Podar**: eliminar parcialmente los datos personales tan pronto dejen de ser necesarios lo cual supone determinar de antemano cuál es el periodo de conservación para cada uno de los datos recogidos y establecer mecanismos

automáticos de borrado cuando se cumpla dicho plazo. En el caso de que los datos formen parte de un registro en el que figure más información que sea necesario conservar, el valor de los campos no necesarios puede modificarse a un valor por defecto prefijado.

- **Eliminar**: suprimir por completo los datos personales tan pronto dejen de ser relevantes asegurándose que no es posible su recuperación ni siquiera de las copias de seguridad realizadas.

También es necesario tener en cuenta que sólo se deben comunicarse y compartirse los datos estrictamente necesarios y que, en el caso de tratamientos que infieran nueva información personal, también deben seleccionarse para su exclusión aquellos datos que se generen y no sean necesarios para la finalidad perseguida.

Ocultar

Esta estrategia se centra en limitar la exposición de los datos, estableciendo las medidas necesarias para garantizar la protección de los objetivos de confidencialidad y desvinculación. Para dar respuesta a esta estrategia son útiles las siguientes tácticas:

- **Restringir:** gestionar de forma restrictiva el acceso a los datos personales limitándolo mediante una política de control de acceso que implemente el principio de *"need to know"* tanto en espacio (detalle y tipo de datos accedidos) como en tiempo (etapas del tratamiento).
- **Ofuscar:** hacer que los datos personales sean ininteligibles para aquellos que no estén autorizados a su consulta utilizando técnicas de cifrado y hashing, tanto en operaciones de almacenamiento como de transmisión de la información.
- **Disociar:** eliminar la vinculación entre conjuntos de datos que se han de mantener independientes, así como los atributos identificativos de los registros de datos para evitar correlaciones entre ellos, con especial atención a los metadatos.
- **Agregar:** Agrupar la información relativa a varios sujetos utilizando técnicas de generalización y supresión[33] para evitar así correlaciones.

Separar

El objetivo que persigue esta estrategia es evitar, o al menos minimizar, el riesgo de que, durante el procesamiento, en una misma entidad, de diferentes datos personales pertenecientes a un mismo individuo y utilizados en tratamientos independientes, se pueda llegar a realizar un perfilado completo del sujeto. Para ello, es necesario mantener contextos de tratamiento independientes que dificulten la correlación de grupos de datos que deberían estar desligados. Las siguientes tácticas contribuyen a implementar la estrategia de separación:

- **Aislar:** recoger y almacenar los datos personales en diferentes bases de datos o aplicaciones que sean independientes desde el punto de vista lógico o incluso que se ejecuten sobre sistemas físicos distintos, adoptando medidas adicionales para garantizar esa desvinculación como el borrado programado de tablas de indexación entre bases de datos.

33 Agencia Española de Protección de Datos (AEPD) – Unidad de Evaluación y Estudios Tecnológicos. *La K-anonimidad como medida de la privacidad,* Jun 2019 https://www.aepd.es/media/notas-tecnicas/nota-tecnica-kanonimidad.pdf

- **Distribuir:** diseminar la recogida y el tratamiento de los diferentes subconjuntos de datos personales correspondientes a diferentes tipos de tratamiento sobre unidades de tramitación y gestión que, dentro de la organización, sean físicamente independientes y utilicen sistema y aplicaciones distintos intentando implementar arquitecturas descentralizadas y distribuidas con procesamiento local de la información siempre que sea posible en lugar de soluciones centralizadas con accesos unificados y que dependan de una misma unidad de control.

Abstraer

La idea que subyace bajo el uso de esta estrategia es limitar al máximo el detalle de los datos personales que son tratados. A diferencia de la estrategia 'minimizar' que realiza una selección previa de los datos recogidos, esta estrategia se centra en el grado de detalle con el que los datos son tratados y en su agregación mediante el empleo de tres tácticas:

- **Sumarizar:** generaliza los valores de los atributos utilizando intervalos o rangos de valores, en lugar de utilizar el valor concreto del campo.
- **Agrupar:** agrega la información de un grupo de registros en categorías en lugar de utilizar la información detallada de cada uno de los sujetos que pertenecen al grupo trabajando con los valores medios o generales.
- **Perturbar:** utilizar valores aproximados o modificar el dato real mediante el empleo de algún tipo de ruido aleatorio en lugar de trabajar con el valor exacto del dato personal.

En cada tratamiento es necesario estudiar cómo afecta el grado de detalle de los datos de entrada al resultado de este, y cuál es la precisión necesaria para que el tratamiento sea efectivo. En particular, el tiempo trascurrido desde la recogida de los datos puede afectar a la relevancia de estos, por lo que conviene revisar periódicamente la información almacenada y aplicar este tipo de estrategias [34].

Informar

Esta estrategia es la implementación del objetivo y el principio de trasparencia establecido por el Reglamento y persigue que los interesados estén plenamente informados del procesamiento de sus datos en tiempo y forma. Siempre que se realice un tratamiento, los sujetos cuyos datos son tratados deberían conocer qué información es la que se procesa, con qué propósito y a qué terceras partes es comunicada además del resto de información que se establece en los artículos 13 [35] y 14 [36] del RGPD. La trasparencia respecto a esta información se convierte en un requisito básico de privacidad pues permite a los interesados tomar decisiones informadas sobre los tratamientos realizados y prestar, en su caso, un consentimiento libre, específico,

34 No hay que perder de vista que incluso un tratamiento agregado de los registros presenta cierto riesgo para la privacidad cuando es posible determinar la pertenencia de un sujeto a un determinado grupo o perfil (por ejemplo, en el caso de personal con determinada enfermedad o que presenten un perfil de riesgo concreto).

35 Artículo 13. "Información que deberá facilitarse cuando los datos personales se obtengan del interesado" - Reglamento (UE) 2016/679, General de Protección de Datos https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e2317-1-1

36 Artículo 14. "Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado" - Reglamento (UE) 2016/679, General de Protección de Datos https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e2418-1-1

informado e inequívoco. Cualquier modificación que se produzca en el tratamiento con respecto a la información previamente facilitada debería ser comunicada, incluyendo las posibles brechas de seguridad que puedan afectar de manera significativa a los derechos y libertades de los sujetos de datos. Esta estrategia se apoya en la existencia de cláusulas de privacidad que faciliten el global de esta información a los interesados junto con el uso de las siguientes tácticas:

- **Facilitar:** suministrar a los interesados toda la información exigida por el RGPD en relación con qué datos personales son tratados, cómo se procesan y por qué mediante la identificación del motivo y finalidad. Se debe proporcionar detalles en relación con los plazos de conservación de los datos, así como de las comunicaciones de estos que se realicen a terceras partes. Junto a toda esta información, que debe ser fácilmente accesible y proporcionarse de forma continuada en el tiempo para fomentar una auténtica trasparencia, debe indicarse también con quién y cómo pueden ponerse en contacto los sujetos de datos para plantear cuestiones relativas a su privacidad, así como los derechos que les asisten en materia de protección de datos personales
- **Explicar:** facilitar la información relativa a los tratamientos de forma concisa, transparente, inteligible y de fácil acceso utilizando un lenguaje claro y sencillo. Para evitar políticas de información densas, complejas y farragosas conviene adoptar una aproximación por capas o niveles en la que se presente una información básica, en un primer nivel y de forma resumida, en el mismo momento y medio en el que se recojan los datos y remitir a información adicional y detallada disponible en un segundo nivel [37].
- **Notificar:** comunicar el tratamiento a los interesados, cuando los datos no se recaben directamente de ellos, en momento en que estos hayan sido obtenidos y a más tardar en el plazo de un mes, o si van a utilizarse para comunicarse con ellos, en la primera comunicación. También se les debe comunicar si está previsto transferir los datos a terceras partes. Igualmente deben implementarse mecanismos para notificar a los interesados las violaciones de seguridad que hayan ocurrido y que puedan suponer un alto riesgo para sus derechos y libertades, utilizando un lenguaje claro y sencillo en el que se describa la naturaleza de la violación.

Habida cuenta de que los procedimientos de recogida de información pueden ser muy variados, los modos de informar deben adaptarse a las circunstancias de cada uno de los medios empleados incluyéndose, adicionalmente, la posibilidad de utilizar iconos estandarizados que ofrezcan una visión conjunta del tratamiento previsto.

Controlar

Esta estrategia está íntimamente ligada a la estrategia de informar y persigue el objetivo de proporcionar a los interesados control en relación a la recogida, tratamiento, usos y comunicaciones realizadas sobre sus datos personales mediante la implementación de mecanismos que permitan el ejercicio de los derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación al tratamiento así como la prestación y retirada del consentimiento o la modificación de las opciones de privacidad

37 Agencia Española de Protección de Datos, Autoridad Catalana de Protección de Datos, Agencia Vasca de Protección de Datos. *Guía para el cumplimiento del deber de informar*, Ene 2017 https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

en aplicaciones y servicios. La implementación de estos mecanismos que se apoya en el empleo de las siguientes tácticas:

- **Consentir:** recoger el consentimiento de los sujetos de datos, en aquellos casos en los que no haya otra base de legitimación, y que debe ser prestado de manera inequívoca, mediante manifestación o una clara acción afirmativa, debiendo ser explícito en determinadas situaciones como el tratamiento de datos sensibles, la adopción de ciertas decisiones automatizadas o las transferencias internacionales. Además, el interesado debe poder retirar su consentimiento en cualquier momento, mediante mecanismos y procedimientos que garanticen que es tan fácil retirarlo como prestarlo.
- **Alertar:** hacer al usuario consciente del momento en el que se está realizando una recogida de datos personales aun cuando ya haya sido informado de manera genérica de la base legal que justifica el tratamiento o incluso este haya prestado su consentimiento.
- **Elegir:** proporcionar la funcionalidad granulada [38] de aplicaciones y servicios, en particular la funcionalidad básica, sin que esta esté supeditada al consentimiento del tratamiento de datos personales que no sean necesarios para su ejecución.
- **Actualizar:** implementar mecanismos que faciliten a los usuarios o incluso les permita realizar directamente, en aquellos casos que sea posible, la revisión, actualización y rectificación de los datos que se hayan facilitado para un tratamiento concreto de manera que sean exactos y se ajusten a la realidad.
- **Retirar:** proporcionar mecanismos para que los usuarios puedan suprimir o solicitar el borrado de los datos personales que hayan facilitado a un responsable en el marco de un tratamiento.

El avance tecnológico, a la vez que permite una recogida continua de información, permite que los datos pueden ser fácilmente administrados por los propios interesados mediante la implementación de plataformas de privacidad que les permite acceder a los mismos, actualizarlos, cancelarlos y modificar las opciones de privacidad configuradas. Estas funcionalidades deben ser tenidas en cuenta desde el diseño de la aplicación.

Cumplir

Esta estrategia asegura que los tratamientos de datos personales son compatibles y respetan los requisitos y obligaciones legales impuestos por la normativa. Para ello, es preciso definir un marco de privacidad y una estructura de gobernanza que incluya una política de protección de datos apoyada desde la alta dirección, así como los roles y responsabilidades que velen por su cumplimiento. La cultura de la privacidad debe formar parte esencial de la organización y hacer partícipes a todos los miembros de esta, para lo que las siguientes tácticas pueden servir de catalizador:

- **Definir:** especificar una política de protección de datos que sea el reflejo interno de las cláusulas de privacidad comunicadas a los interesados. Deben crearse las estructuras y asignarse los recursos necesarios para dar soporte a esta política y que garanticen que las actividades de tratamiento llevadas a cabo por la organización respetan y son conformes a la normativa en materia de protección de datos. También debe elaborarse y llevarse a cabo un plan de

38 Las funcionalidades que requieran una legitimación basada en el consentimiento han de poderse seleccionarse de forma independiente tanto del propósito principal del objeto como entre ellas.

formación y concienciación para todos los miembros de esta que busque garantizar una actitud comprometida y responsable como parte de la responsabilidad proactiva.

- **Mantener:** dar soporte a la política definida mediante el establecimiento de procedimientos y la implantación de las medidas técnicas y organizativas necesarias. Debe revisarse la existencia de mecanismos y procedimientos efectivos para garantizar el ejercicio de derechos, la gestión y notificación de incidentes de seguridad, la adecuación de los posibles encargos de tratamiento a los requisitos legales y la acreditación del cumplimiento de las obligaciones impuestas por la normativa.
- **Defender:** asegurar el cumplimiento, eficacia y eficiencia de la política de privacidad y de los procedimientos, medidas y controles implantados para verificar que responden en todo momento a la realizad de las actividades de tratamiento y al día a día de la organización.

La figura del Delegado de Protección de Datos juega un papel fundamental en la implementación de esta estrategia, al asesorar al responsable y supervisar el cumplimiento de la normativa de protección de datos dentro de la organización. También resulta efectivo la implementación de modelos de gestión de la privacidad como el propuesto por la reciente norma ISO/IEC 27701:2019 [39] que especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de información de la privacidad (PIMS, *Privacy Information Management System*).

Demostrar

El objetivo de esta estrategia va un paso más allá de la anterior y pretende que, de acuerdo con el artículo 24 del RGPD [40], el responsable del tratamiento pueda demostrar, tanto a los interesados como a las autoridades de supervisión, el cumplimiento de la política de protección de datos que esté aplicando, así como del resto de requisitos y obligaciones legales impuestos por el Reglamento. Desde el punto de vista práctico, es la implementación del *accountability* o responsabilidad proactiva que exige el Reglamento, basada en un autoanálisis crítico, continuo y rastreable de todas las decisiones tomadas en el marco de los tratamientos y garantía de una auténtica gobernanza de los datos personales en el seno de la organización. Las siguientes tácticas permiten llevar a cabo esta estrategia a fin de garantizar y poder demostrar que los tratamientos son conformes al Reglamento:

- **Registrar:** documentar todas y cada una de las decisiones tomadas en el tiempo aun cuando hayan resultado contradictorias, identificando quién las tomó, cuándo y la justificación para hacerlo.
- **Auditar:** revisar de forma sistemática, independiente y documentada el grado de cumplimiento de la política de protección de datos.
- **Informar:** documentar los resultados de las auditorías realizadas y cualquier incidente que se produzca en las operaciones de tratamiento de datos personales y ponerlo a disposición de la autoridad de control cuando sea necesario. En el caso de nuevos tratamientos y si el resultado de la evaluación

39 Comité Técnico ISO/IEC JTC 1 /SC 27. *ISO/IEC 27701:2019 Security techniques – Extension to ISP/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines,* Agosto 2019 https://www.iso.org/standard/71670.html

40 Artículo 24. "Responsabilidad del responsable del tratamiento" - Reglamento (UE) 2016/679, General de Protección de Datos https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e3106-1-1

de impacto relativa a la protección de datos arroja que el tratamiento entrañaría un alto riesgo para los derechos y libertades de los interesados si el responsable no toma medidas para mitigarlos, realizar la consulta previa a la que se refiere el artículo 36 [41] del RGPD.

La realización de un análisis de riesgos y, en su caso, de la evaluación de impacto de protección de datos junto con la documentación de las decisiones adoptadas en base a los resultados obtenidos son un buen punto de partida para, además de fijar los requisitos de privacidad que deban implementarse en aplicaciones y sistemas como parte de la privacidad desde el diseño, documentar por completo cómo se realizan los tratamientos de datos personales y dar cumplimiento al principio de responsabilidad proactiva. Otros recursos para demostrar el cumplimiento de las obligaciones por parte del responsable es la adhesión a códigos de conducta y mecanismos de certificación como instrumentos opcionales para implementar la estrategia de demostrar.

ESTRATEGIA DE DISEÑO DE LA PRIVACIDAD		DESCRIPCIÓN Y TÁCTICAS	CONTROLES Y PATRONES DE DISEÑO
Estrategias orientadas a datos	Minimizar	Limitar al máximo posible el tratamiento de datos personales. TÁCTICAS: **seleccionar**, **excluir**, **podar** y **eliminar**	Anonimización Seudonimización Bloqueo de correlación en sistemas de gestión de identidad federada
	Ocultar	Evitar que los datos personales se hagan públicos o sean conocidos TÁCTICAS: **restringir**, **ofuscar**, **disociar** y **agregar**)	Cifrado Redes de mezcla Atributos basados en credenciales
	Separar	Mantener separados los conjuntos de datos personales. TÁCTICAS: **aislar** y **distribuir**	Listas negras anónimas Cifrado homomórfico Separación física y lógica
	Abstraer	Limitar al máximo el nivel de detalle utilizado en los tratamientos de datos personales. TÁCTICAS: **sumarizar**, **agrupar** y **perturbar**	Agregación en el tiempo K-anonimidad Ofuscación de medidas mediante agregación de ruido Granularidad dinámica de ubicación Privacidad diferencial

41 Artículo 36. "Consulta previa" - Reglamento (UE) 2016/679, General de Protección de Datos https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e3713-1-1

ESTRATEGIA DE DISEÑO DE LA PRIVACIDAD		DESCRIPCIÓN Y TÁCTICAS	CONTROLES Y PATRONES DE DISEÑO
Estrategias orientadas a procesos	Informar	Mantener informados a los sujetos de datos de la naturaleza y condiciones del tratamiento. TÁCTICAS: **facilitar**, **explicar** y **notificar**	Notificación de brechas de privacidad Visualización dinámica de la política de privacidad Iconos de privacidad Alertas de tratamiento
	Controlar	Proporcionar a los sujetos de datos un control efectivo sobre sus datos personales. TÁCTICAS: **consentir**, **alertar**, **elegir**, **actualizar**, **retirar**	Paneles de preferencias de privacidad Transmisión activa de presencia Selección de credenciales Consentimiento informado
	Cumplir	Respetar e impulsar el cumplimiento de las obligaciones impuestas en la normativa vigente y en la propia política de protección de datos. TÁCTICAS: **definir**, **mantener**, **defender**	Evaluación de impacto de privacidad en soluciones de gestión de identidad federada Control de acceso Gestión de obligaciones Políticas adheridas
	Demostrar	Poder demostrar que los tratamientos se realizan de una forma respetuosa con la privacidad. TÁCTICAS: **registrar**, **auditar** e **informar**.	Auditoría Registro

Tabla 4 – Estrategias de diseño de la privacidad junto con las tácticas y patrones para implementarlas

V. PATRONES DE DISEÑO DE LA PRIVACIDAD

Una vez establecidos los objetivos y estrategias de privacidad que debe incorporar el producto, sistema, aplicación o servicio como parte de su definición es necesario integrarlos en su diseño. Para ello se hace uso de los patrones de diseño de la privacidad como soluciones reutilizables utilizadas para resolver problemas comunes y repetibles de privacidad que se presentan de forma reiterada en un contexto concreto durante el desarrollo de productos y sistemas.

Típicamente, la descripción de un patrón de diseño contiene, como mínimo, su nombre, propósito, descripción del contexto de aplicación, objetivos, estructura, implementación (relación con otros patrones), consecuencias de su aplicación y usos conocidos.

Ofuscación de medidas mediante agregación de ruido

Resumen.- Agregar ruido a las mediciones tomadas como parte de la operación de un servicio.

Problema.- La prestación de un servicio puede requerir que se tomen medidas repetitivas y detalladas vinculadas a un sujeto de datos, por ejemplo, para realizar la facturación adecuada del mismo o adaptar el suministro del servicio a la demanda. Sin embargo, estas mediciones pueden revelar más información (por ejemplo, hábitos personales, etc.) cuando se repiten con el tiempo.

Contexto.- Un prestador de servicios obtiene mediciones continuas de determinados valores vinculados al usuario abonado al servicio.

Objetivos.- Obtener mediciones fiables de los atributos del servicio para cumplir con sus requisitos operativos, pero sin inferir información personal adicional obtenida a partir de la agregación de varias mediciones provenientes del mismo usuario.

Ejemplo.- Una compañía eléctrica opera una red de contadores inteligentes que proporcionan medidas del consumo de energía instantáneo de cada usuario. La compañía utiliza esa información para adaptar la distribución de energía de forma dinámica de acuerdo con la demanda y facturar a cada cliente, periódicamente, de acuerdo con su consumo agregado durante el período de facturación. Sin embargo, esta información también puede explotarse para inferir información confidencial del usuario (por ejemplo, a qué hora se va y vuelve a casa, tipo de electrodomésticos que utiliza, etc.)

Solución.- Se agrega un valor de ruido al valor verdadero de la medida antes de que se transmita al proveedor de servicios, para ofuscarlo. El ruido se rige por una distribución previamente conocida, de modo que se puede calcular la estimación del resultado de agregar varias mediciones, mientras que un atacante u otra tercera parte no autorizada no podría inferir el valor real de ninguna medición individual. Tenga en cuenta que el ruido no necesita ser ni aditivo ni gaussiano. De hecho, estos pueden no ser útiles para la ofuscación orientada a la privacidad. El ruido de escala y el ruido aditivo laplaciano han demostrado ser más útiles para la preservación de la privacidad.

Restricciones y Consecuencias.- El patrón se aplica a cualquier escenario en el que se esté monitorizando el uso de un recurso a lo largo del tiempo (por ejemplo, red inteligente, computación en la nube). El dispositivo que proporciona la medida debe ser confiable a fin de garantizar que cumpla con el patrón de ruido establecido.

Parte de la información se pierde debido al ruido agregado. Esta pérdida de información permite evitar que la información sea explotada para otros fines. Esto es, en parte, una de las consecuencia previstas y perseguidas (por ejemplo, evitar descubrir hábitos de usuario) pero también puede impedir otros usos legítimos.

Para que la información sea útil después de la adición de ruido, el número de puntos de datos sobre los que se agregan las mediciones (es decir, el tamaño de la base de usuarios) debe ser alto. De lo contrario, el intervalo de confianza sería demasiado amplio o la privacidad diferencial no podría lograrse de manera efectiva.

Usos conocidos.-

Bohli, J.-M.; Sorge, C.; Ugus, O., "A Privacy Model for Smart Metering," Communications Workshops (ICC), 2010 IEEE International Conference on , vol., no., pp.1,5, 23-27 May 2010

Xuebin Ren; Xinyu Yang; Jie Lin; Qingyu Yang; Wei Yu, "On Scaling Perturbation Based Privacy-Preserving Schemes in Smart Metering Systems," Computer Communications and Networks (ICCCN), 2013 22nd International Conference on , vol., no., pp.1,7, July 30 2013-Aug. 2 2013

Mivule, K. (2013) Utilizing noise addition for data privacy, an overview. arXiv preprint arXiv:1309.3958.

Categorías.- Abstraer, Ocultar, Minimizar

Patrones relacionados.- Gateway de agregación; Complemento de aseguramiento de la privacidad

Nivel de preparación tecnológica.- TRL-4: tecnología validada en laboratorio

Figura 7 – Ejemplo de patrón de diseño de la privacidad

Como ya se indicó anteriormente, un mismo patrón de diseño puede servir para implementar más de una estrategia de privacidad de las ya enumeradas por lo que no se trata de soluciones cerradas y excluyentes, debiendo verse el diseño de las estrategias de privacidad como un enfoque conjunto e integral. Por ejemplo, el patrón de diseño '*Ofuscación de medidas mediante agregación de ruido*' mostrado en la figura 7 y cuyo objetivo es añadir ruido a las medidas reales tomadas durante la operación de un servicio para que no se pueda inferir información adicional, permite implementar a la vez las estrategias de abstraer, ocultar y minimizar.

CATÁLOGOS DE PATRONES DE DISEÑO

Existen diferentes repositorios o catálogos de patrones diseño de la privacidad donde es posible consultar una definición exhaustiva de los mismos, su finalidad y modo de empleo. Así, en el marco del proyecto PRIPARE (*Preparing Industry to Privacy by design by supporting its Application in Research*), [42] financiado por la Unión Europea, se ha desarrollado un catálogo que incluye 26 patrones de diseño de privacidad [43].

Otra iniciativa similar es el resultado de un proyecto [44][45] desarrollado en la Universidad de Economía y Negocios de Viena y que crea un repositorio de soluciones interactivo [46] que clasifica 40 patrones de diseño de la privacidad en atención a los 11 principios de protección definidos en el marco establecido por la ISO/IEC 29100:2011 [47].

También existe una iniciativa de colaboración entre varios centros y universidades que mantiene un catálogo de patrones [48] con el objetivo de operacionalizar los requisitos legales en soluciones concretas, estandarizar el lenguaje de la privacidad, documentar y recopilar soluciones comunes a problemas concretos y ayudar a los diseñadores de sistemas y aplicaciones a identificar los problemas de privacidad y darles respuesta.

En el Anexo 1 se recogen, en forma de tabla y enlazados a su ficha, una selección de 54 patrones de diseño de privacidad publicados en los sitios web desarrollados como consecuencia de las iniciativas enumeradas, indicando para cada uno de ellos un breve resumen de la finalidad que persiguen y la estrategia, o estrategias, de diseño de privacidad a las que intentan dar respuesta.

VI. PRIVACY ENHANCING TECHNOLOGIES (PETS)

Definidas las estrategias y diseñados los patrones de privacidad del producto, sistema aplicación o servicio que se va a desarrollar resta su implementación en la fase de desarrollo haciendo uso de una solución tecnológica concreta.

Las Privacy Enhancing Technologies o PETs son un conjunto organizado y coherente de soluciones TIC que reducen los riesgos que afectan a la privacidad, implementando las estrategias y patrones definidos anteriormente.

Debido al cambiante contexto tecnológico, la eficacia, en términos de protección de la privacidad, varía de una PET a otra y en el tiempo, siendo complicado proporcionar

42 ATOS, Inria, Gradiant, Trilateral y UPM. *Privacy and Security by Design Methology Handbook* , Dic 2015 http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf

43 Online - *privacypatterns.eu - collecting patterns for better privacy* https://privacypatterns.eu/

44 Olha Drozd, Sabrina Kirrane, Sarah Spiekermann – Vienna University of Econimics and Business. *Towards an Interactive Privacy Pattern Catalog*. 12th Symposium on Usable Privacy and Security (SOUPS 2016), Jun 2016, Denver CO. https://www.researchgate.net/publication/305811615_Towards_an_Interactive_Privacy_Pattern_Catalog

45 Olha Drozd – Vienna University of Econimics and Business. *Privacy Pattern Catalog: A Tool for Integrating Privacy Principles of ISO/IEC 29100 into Software Development Process*., Julio 2016, https://www.researchgate.net/publication/304995300_Privacy_Pattern_Catalogue_A_Tool_for_Integrating_Privacy_Principles_of_ISOIEC_29100_into_the_Software_Development_Process

46 Online – *privacypatterns* http://privacypatterns.wu.ac.at:8080/catalog/

47 Comité Técnico ISO/IEC JTC 1 /SC 27. *ISO/IEC 29100:2011 Information Technology - Security techniques – Privacy Framework,* Dic 2011 https://www.iso.org/standard/45123.html

48 Online – *Privacy patterns* https://privacypatterns.org/

una clasificación y tipología actualizada [49]. Una PET puede ser tanto una herramienta independiente que el usuario final compra e instala en un ordenador personal como una compleja arquitectura de sistemas de información.

CLASIFICACIÓN DE LAS PETS

Existen múltiples clasificaciones de las PETs, la mayor parte de ellas basadas en sus características técnicas [50]. Otra posible clasificación de estas herramientas, que es la se ofrece en esta guía, es en base a la finalidad que persiguen [51]. Por lo tanto, se clasificarán según estén dirigidas a proteger la privacidad o a gestionarla, manteniendo así un enfoque coherente con la clasificación de las estrategias vistas. El primer grupo reúne herramientas y tecnologías que protegen la privacidad de manera activa y durante el tratamiento de los datos personales (por. ejemplo, ocultado datos personales o eliminando la necesidad de identificación). El segundo grupo abarca herramientas y tecnologías que dan soporte a la administración de los procedimientos relacionados con la gestión de la privacidad pero que no operan, como tal, sobre los datos.

CATEGORÍA	SUBCATEGORÍA	DESCRIPCIÓN
Protección de la privacidad	Herramientas para seudonimizar	Permiten efectuar transacciones sin solicitar información personal
	Productos y servicios para anonimizar	Proporcionan el acceso a servicios sin requerir la identificación del sujeto de datos
	Herramientas de cifrado	Protegen los documentos y transacciones de ser visualizados por terceras partes
	Filtros y bloqueadores	Evitan emails y contenido web no deseado
	Supresores de seguimiento	Eliminan las trazas electrónicas de la actividad digital del usuario
Gestión de la privacidad	Herramientas de información	Crean y verifican las políticas de privacidad
	Herramientas administrativas	Gestionan la identidad y los permisos del usuario

Tabla 5 – Una de las posibles clasificaciones de las PETs (*META Group Report*)

CATÁLOGOS DE PETS

Como ocurría con los patrones de diseño, no existe un único repositorio unificado de herramientas y tecnologías PET, aunque existen distintas iniciativas.

---

49 COM(2007)228 COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52007DC0228&from=EN

50 Lothar Fritsch, Norwegian Computing Center Report, No 1013. *State of the art of Privacy-enhancing Technology (PET),* Nov 2007 https://www.nr.no/publarchive?query=4589

51 Ministerio de Ciencia, Tecnología e Innovación de Dinamarca. *Privacy Enhancing Technologies – META Group Report v1.1,* Mar 2005 https://danskprivacynet.files.wordpress.com/2008/07/rapportvedrprivacyenhancingtechlologies.pdf

La División de Análisis Tecnológico de la Oficina del Comisionado de Privacidad de Canadá ha desarrollado una visión general de las mismas atendiendo a la funcionalidad que proporcionan y presentando algunos ejemplos concretos de soluciones [52].

El Centro para Internet y la Sociedad (CIS) de la Facultad de Derecho de Standford (California) tiene publicada, mediante un sistema wiki de contribución pública, una base de datos de herramientas y tecnologías PETs gratuitas para que los usuarios mejoren el control sobre sus datos personales [53].

A nivel europeo, el Supervisor Europeo de Protección de Datos (EDPS), ha desarrollado la red IPEN, Red de Ingeniería de Privacidad en Internet *(Internet Privacy Engineering Network)*[54] con el objeto de dar soporte a los desarrolladores en el empleo de patrones de diseño y otros bloques reutilizables orientados a proteger y mejorar la privacidad de manera eficiente y efectiva.

En 2015, ENISA realizó el estudio *"Online privacy tools for the general public"*[55] que analizaba herramientas PET para la protección online de la privacidad y en el que se recogían una relación de portales web que promueven el uso de este tipo de tecnologías. Aunque las herramientas sugeridas en los portales que se muestran en la tabla 5 son, en general, aplicaciones software enfocadas a usuarios finales para mejorar la protección de sus datos personales, su análisis y estudio también resulta de utilidad para los responsables del tratamiento como fuente de ejemplos de requisitos de privacidad que deben ser incorporados a los servicios, productos y aplicaciones que desarrollen. Si este tipo de soluciones (cifrado para comunicaciones seguras, anonimizadores, bloqueadores de seguimiento, etc) vienen integradas de serie en los sistemas se evitará que el usuario final esté desprotegido o que, en el mejor de los casos, tenga que añadir la capa de privacidad no implementada en una instalación posterior de herramientas de terceros.

A partir de este estudio inicial, ENISA ha publicado varios informes [56][57][58][59] sobre la evolución de herramientas PET y el desarrollo de una metodología para comparar su nivel de madurez, trabajando en el desarrollo de una plataforma que le dé soporte y un repositorio centralizado desde el que obtener información de la solución que mejor se ajuste a los objetivos de privacidad perseguidos [60].

---

52 The Technology Analysis Division of the Office of the Privacy Commissioner. *Privacy Enhancing Technologies – A review of Tools and Techniques*, 2017 https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/

53 The Center for Internet and Society Stanford Univeristy. *Ciberlaw PET wiki*, https://cyberlaw.stanford.edu/wiki/index.php/PET

54 https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en

55 European Union Agency for Cybersecurity (ENISA). *Online privacy tools for the general public*, Dic 2015 https://www.enisa.europa.eu/publications/privacy-tools-for-the-general-public/at_download/fullReport

56 European Union Agency for Cybersecurity (ENISA). *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies*, Mar 2016 https://www.enisa.europa.eu/publications/pets/at_download/fullReport

57 European Union Agency for Cybersecurity (ENISA). *PETs control matrix – A systematic approach for assessing online and mobile privacy tools*, Dic 2016 https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools/at_download/fullReport

58 European Union Agency for Cybersecurity (ENISA). *Privacy Enhancing Technologies: Evolution and State of the Art*, Mar 2017 https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art/at_download/fullReport

59 European Union Agency for Cybersecurity (ENISA). *A tool on Privacy Enhancing Technologies (PETs) knowledge management and maturity assessment*, Mar 2018 https://www.enisa.europa.eu/publications/pets-maturity-tool/at_download/fullReport

60 UNIPI Workshop on Privacy Enhancing Technologies. Evgenia Nikolouzou - ENISA Data Security and Standardization Unit. *PETs Repository Community Building and Evaluation*, Nov 2018 https://www.enisa.europa.eu/events/personal-data-security/pets-maturity

PORTAL	ORGANIZACIÓN	URL	DESCRIPCIÓN
Secure Messaging Scorecard	Electronic Frontier Foundation (EFF)	https://www.eff.org/deeplinks/2018/03/secure-messaging-more-secure-mess	Una presentación y evaluación de aplicaciones y herramientas de mensajería segura utilizando una lista de criterios predefinidos
PRISM Break	Nylira (Peng Zhong)	https://prism-break.org/en/	Una selección de herramientas contra la vigilancia y seguimiento masivo, como herramientas de cifrado, anonimizadores, etc.
Security in-a-box	Tactical Technology Collective and Front Line Defenders	https://securityinabox.org/en/	Portal de seguridad de uso general, que incluye herramientas para la protección de la privacidad, como herramientas de cifrado.
EPIC Online Guide to Practical Privacy Tools	Electronic Privacy Information Center (EPIC)	https://www.epic.org/privacy/tools.html	Ofrece listas de herramientas de privacidad clasificadas en diferentes áreas (complementos de navegador web, anonimizadores, etc.).
The Ultimate Privacy Guide	BestVPN (4Choice Ltd)	https://proprivacy.com/guides/the-ultimate-privacy-guide	Portal de seguridad de uso general que ofrece clasificaciones para VPN comerciales. La guía de privacidad proporciona una lista de herramientas clasificadas por áreas.
Free Software Directory	Free Software Foundation (FSF)	https://directory.fsf.org/wiki/Main_Page	Portal de uso general dirigido a software libre con área específica de seguridad y privacidad,

PORTAL	ORGANIZACIÓN	URL	DESCRIPCIÓN
			enfocado principalmente en cifrado.
Privacytools .io	Privacytools.io	https://www.privacytools.io	Ofrece listas de herramientas para preservar la privacidad, como VPNs, complementos del navegador, etc.
Me & My Shadow	Tactical Technology Collective	https://myshadow.org	Un portal enfocado principalmente en rastros digitales y rastreo en línea. Ofrece recomendaciones sobre varias herramientas relevantes.
Gizmo's Freeware	Gizmo's Freeware	http://www.techsupportalert.com/content/free-windows-desktop-software-security-list-privacy.htm	Portal de herramientas freeware de uso general, que ofrece también una lista de herramientas de privacidad abiertas.
Best Privacy Tools	Best Privacy Tools	http://bestprivacytools.com/	Ofrece una lista de herramientas de privacidad, especialmente aplicaciones de chat, VPN, navegación segura, etc.
Internet Privacy Tools	Internet Privacy Tools	http://privacytools.freeservers.com	Ofrece una lista de herramientas de privacidad, especialmente filtros de correo electrónico, encriptación del navegador, etc.

PORTAL	ORGANIZACIÓN	URL	DESCRIPCIÓN
Reset The Net **Privacy Pack**	Fight for the Future and Center for Rights	https://pack.resetthenet.org	Ofrece una lista de herramientas de privacidad gratuitas y consejos relevantes (por ejemplo, comunicación segura, navegación anónima, etc.).

Tabla 6 – Portales web que fomentan el uso de herramientas online de privacidad dirigidas al público en general según el estudio de ENISA *Online privacy tools for the general public*

VII. CONCLUSIONES

En un contexto en el que cada día organizaciones y empresas desarrollan servicios basados en un uso intensivo de los datos personales cuyo impacto en la privacidad se ve potenciado por el uso de tecnologías disruptivas, se hace necesario adoptar medidas técnicas y organizativas eficaces y eficientes que contribuyan a garantizar el respeto a los derechos y libertades de las personas en lo que a su tratamiento de datos personales se refiere.

Asegurar la privacidad y establecer un marco de gobernanza que garantice la protección de los datos personales no representa un obstáculo para la innovación. Muy al contrario, ofrece ventajas y oportunidades para los distintos participantes:

- para las organizaciones supone mejorar la eficiencia, optimizar sus procesos, establecer una estrategia de reducción de costes y obtener una ventaja competitiva
- para el mercado supone desarrollar modelos económicos sostenibles a largo plazo
- para la sociedad en su conjunto supone poder acceder a las ventajas de los avances tecnológicos sin comprometer la libertad e independencia de los individuos.

En definitiva, asegurar la privacidad es innovación en sí misma e introduce una nueva disciplina tecnológica: la ingeniería de la privacidad.

La implementación eficaz y eficiente de los principios de privacidad exige que estos formen parte integral de la naturaleza de los productos y servicios, y para ello han de ser tenidos en cuenta desde la fase inicial de concepción, diseño y desarrollo de los mismos como una parte más del conjunto de especificaciones, funcionales y no funcionales. Esta aproximación se conoce con el nombre de Privacidad desde el Diseño.

La Privacidad desde el Diseño implica utilizar un enfoque metodológico orientado a la gestión del riesgo y de responsabilidad proactiva que permita fijar los requisitos de privacidad mediante prácticas, procedimientos y herramientas. Para ello:

- A partir del análisis de riesgo se establecerán tanto los objetivos específicos de protección de datos (desvinculación, transparencia y control) como los objetivos de seguridad desde la perspectiva de la privacidad (confidencialidad,

disponibilidad e integridad), que garanticen los principios básicos establecidos en el artículo 5 [61] del RGPD.

- A continuación, se estudiarán las estrategias de privacidad en las que se concretan los requisitos de cada objetivo de privacidad, tanto las orientadas a los datos como a los procesos. Estas estrategias son: 'minimizar', 'ocultar', 'separar', 'abstraer', 'informar', 'controlar', 'cumplir' y 'demostrar'; y para cada una de ellas se identificarán las tácticas de protección que las implementen de forma efectiva.
- Una vez en la fase de diseño, se integrarán las tácticas seleccionadas mediante soluciones ya conocidas, es decir, los patrones de diseño de la privacidad, que abordan problemas comunes y repetibles, accediendo a los catálogos disponibles, de los que una selección se presenta en este documento.
- Finalmente, en la fase de desarrollo, se realizará la implementación concreta de dichos patrones. Esta implementación se realizará por el equipo de desarrollo bien programando en código la funcionalidad necesaria o, si es posible, haciendo uso de soluciones TIC ya existentes, es decir, utilizando Privacy Enhancing Technologies.

En cualquier caso, la protección de datos desde el diseño es una obligación del responsable, y es este quien debe velar por garantizarla sea cual sea la forma de desarrollo, adquisición o subcontratación del sistema, producto o servicio, no pudiendo delegar completamente en terceros (fabricantes y encargados) la responsabilidad de aplicación de este principio.

En cumplimiento de su deber de diligencia deberá participar activamente en las tareas de ingeniería de la privacidad definiendo los requisitos que tienen que ser contemplados, haciendo un seguimiento continuo de su correcta implantación y verificando su plena operatividad antes de la puesta en producción del sistema, de modo que la privacidad de los individuos cuyos datos son objeto de tratamiento quede garantizada.

61 Artículo 5. "Principios relativos al tratamiento" - Reglamento (UE) 2016/679, General de Protección de Datos https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e1873-1-1

VIII. ANEXO 1: SELECCIÓN DE PATRONES DE DISEÑO DE LA PRIVACIDAD

NOMBRE DEL PATRÓN DE DISEÑO	OBJETIVO Y FINALIDAD	ESTRATEGIA(S) A LA(S) QUE DA SOPORTE
Ofuscación de medidas mediante agregación de ruido	Modifica las medidas detalladas de uso o cualquier otro atributo de un servicio mediante la adición de valores de ruido que enmascaren los datos reales con el objetivo de evitar deducir patrones y comportamientos por parte de un tercero no autorizado que intercepte la comunicación.	Abstraer Ocultar Minimizar
Agregación en el tiempo	Consiste en recopilar datos correspondientes a diferentes momentos temporales y procesar información de manera agregada para proteger la privacidad.	Abstraer
Privacidad diferencial	Mediante este patrón se modifica el resultado de las consultas añadiéndoles nuevos datos (ruido) extraídos aleatoriamente de una distribución generada a partir de los datos originales de modo que la estadísticamente dicha modificación tiene un efecto insignificante en los resultados del algoritmo que analiza los datos y sin embargo permite preservar la privacidad de los individuos.	Abstraer
Complemento de aseguramiento de la privacidad	En muchas ocasiones la prestación de un servicio requiere la toma de medidas detalladas y repetitivas que, evaluadas en el tiempo, pueden revelar un comportamiento y poner en riesgo la privacidad del interesado. Este complemento, agrega, de manera confiable, los valores detallados de los registros en el lado del usuario proporcionando la finalidad perseguida, pero ocultando los valores desagregados detallados.	Abstraer
Granularidad de ubicación dinámica	En el caso de servicios basados en la geolocalización (LBS) permite que la información de ubicación del usuario	Abstraer Minimizar

NOMBRE DEL PATRÓN DE DISEÑO	OBJETIVO Y FINALIDAD	ESTRATEGIA(S) A LA(S) QUE DA SOPORTE
	logre el k-anonimato reduciendo la precisión, pero manteniendo un equilibrio con la utilidad de la información necesaria para la prestación del servicio.	
Gateway de agregación	Implementa el cifrado homomórfico, cifrando, agregando y descifrando posteriormente la información tratada. Operando sobre la información cifrada, es posible realizar tratamientos de medidas tomadas en distintos momentos temporales sobre un usuario, pero sin extrapolar un patrón de comportamiento. Trabaja con datos agregados sin tener acceso a la información individual.	Abstraer Ocultar Separar
Transmisión activa de presencia	Permite al usuario decidir cuándo quiere compartir información de una manera activa, en particular, información asociada a su ubicación. Los ajustes de difusión de información no deben aplicarse de forma holística por defecto y en caso de duda debe solicitarse confirmación.	Control
Consentimiento informado	Para determinados tratamientos el responsable necesita recabar el consentimiento informado del usuario. La implementación de este patrón garantiza mostrar un aviso claro, conciso y comprensible antes de recoger los datos e iniciar el tratamiento de que, al usar el servicio, el usuario está consintiendo en el tratamiento de los datos necesario y conoce las posibles consecuencias. Los detalles completos deberían ser fácilmente accesibles de modo que el usuario tenga la oportunidad de elegir utilizar o no el servicio.	Control

NOMBRE DEL PATRÓN DE DISEÑO	OBJETIVO Y FINALIDAD	ESTRATEGIA(S) A LA(S) QUE DA SOPORTE
Enlaces privados	En entornos en los que el responsable proporciona a los usuarios un servicio de almacenamiento de contenido, potencialmente pueden existir datos personales. Si el usuario desea compartir parte de este contenido, pero de forma limitada, implementar este patrón permite enviar un enlace privado a los interesados concediendo acceso a la información, pero sin necesidad de hacerlo totalmente público.	Control
Políticas adheridas	Son políticas de privacidad leídas e interpretadas de forma automática y que acompañan a los datos comunicados a terceras partes para definir sus posibilidades de uso, limitaciones y las preferencias del usuario, mejorando así el control que este tiene sobre sus datos personales	Control
Elección desagregada de funcionalidades	Con frecuencia, los responsables recopilan más datos de los estrictamente necesarios con el objetivo de proporcionar funcionalidades adicionales con respecto a la finalidad principal del tratamiento. Este patrón permite a los usuarios elegir, de forma desagregada, las funcionalidades del sistema que desean utilizar y proporcionar únicamente los datos requeridos para su consecución.	Control
Control de acceso selectivo	Utilizado en foros, redes sociales y servicios web de publicación de contenido, proporciona a los usuarios un mecanismo para definir la visibilidad de sus publicaciones y el contenido que comparten mediante la definición de reglas de acceso y la configuración de las opciones de privacidad.	Control

NOMBRE DEL PATRÓN DE DISEÑO	OBJETIVO Y FINALIDAD	ESTRATEGIA(S) A LA(S) QUE DA SOPORTE
Opción de divulgación selectiva	Muchos productos y servicios requieren la recopilación de una cantidad prefijada de datos, en ocasiones excesiva, con antelación a que el usuario pueda comenzar a hacer uso de este. Sin embargo, hay personas que prefieren elegir libremente qué tipo de información comparten. Este patrón recomienda que los servicios admitan una opción de divulgación selectiva, adaptando la funcionalidad que se presta al nivel de exposición de datos que el usuario se siente cómodo de compartir.	Control
Plataforma de configuración de las preferencias de privacidad	Este patrón permite a los usuarios monitorizar y fácilmente configurar los permisos concedidos y sus preferencias en cuanto a privacidad al ofrecer un punto centralizado donde se puede acceder, previa autenticación, a las opciones configurables que determinan el tratamiento.	Control Informar
Control de acceso	Establece mecanismos de control de acceso a la información en base al principio de “need to know” para que esta sea procesada legítimamente y por las partes autorizadas.	Cumplir
Evaluación de impacto de la privacidad en soluciones de gestión de identidades federadas	Las soluciones de gestión de la identidad permiten desacoplar las funciones relacionadas con la autenticación, la autorización y la gestión de los atributos del usuario por un lado y la prestación de los servicios a los que acceden esos usuarios por otro, constituyendo un sistema federado que involucra flujos de datos complejos y la transmisión de la identidad del usuario entre las distintas partes. Estos flujos implican riesgos y amenazas con respecto a la privacidad que deben ser analizados mediante una evaluación de impacto de protección de datos.	Cumplir

NOMBRE DEL PATRÓN DE DISEÑO	OBJETIVO Y FINALIDAD	ESTRATEGIA(S) A LA(S) QUE DA SOPORTE
Gestión de obligaciones	El patrón permite que las obligaciones relacionadas con el intercambio, almacenamiento y procesamiento de datos se transfieran y administren entre múltiples partes que intervienen en el tratamiento. De este modo es posible gestionar la política de privacidad definida y las preferencias de usuario, controlando el ejercicio de los derechos o la retirada de consentimientos cuando los datos han sido comunicados o son compartidos por varios responsables/encargados.	Cumplir
Auditorías	Realizar auditorías periódicas para examinar la efectividad de los mecanismos de cumplimiento.	Demostrar
Registro	La aplicación de este patrón permite demostrar al responsable en cumplimiento del principio de *accountability* que los requisitos normativos en materia de protección de datos están debidamente implantados.	Demostrar
Términos y condiciones abreviados	Persigue que los usuarios puedan comprender mejor los términos y condiciones presentados en la política de privacidad (riesgos, derechos, cesiones, …) si estos se presentan de una forma concisa y abreviada que sea comprensible para el interesado.	Informar
Alerta de tratamiento	Proporcionar un aviso discreto, pero claramente perceptible cuando un sensor esté recopilando datos personales o se esté realizando el seguimiento de un individuo de modo que los usuarios puedan obtener más información en tiempo real, si lo requieren, sobre el uso de los datos y así poder revocar los permisos. Una alternativa a este patrón es el denominado Aviso asincrónico	Informar

NOMBRE DEL PATRÓN DE DISEÑO	OBJETIVO Y FINALIDAD	ESTRATEGIA(S) A LA(S) QUE DA SOPORTE
Feedback de privacidad	Con el objetivo de asegurar que el interesado entiende el alcance del tratamiento se le envía una notificación para confirmar que comprende qué datos son recogidos, a quién se le van a comunicar, cómo van a utilizarse y qué riesgos para su privacidad implica y así pueda ajustar sus preferencias de privacidad antes de utilizar la aplicación o servicio.	Informar
Iconos de privacidad	Muchas veces, las políticas de privacidad son enrevesadas y difíciles de entender. El uso de iconos, preferiblemente estandarizados, permite transmitir la información más rápidamente y apoyar la comprensión del texto, convirtiéndose en una herramienta útil para aumentar la trasparencia y el nivel de información que ofrece la política de privacidad.	Informar
Sensibilización	Hacer conscientes a los usuarios sobre las potenciales consecuencias de compartir sus datos, informándoles de cuán visibles son y qué riesgos pueden derivarse de esa exposición. Esto les permite reconsiderar sus configuraciones de privacidad y tomar medidas si lo desean.	Informar
Notificación de brechas de privacidad	Este patrón asegura que no de que, en el caso en que se produzca un acceso y procesamiento no autorizado de datos personales, sea detectado y se informe a la autoridad supervisora y, en su caso, a los usuarios afectados, sin demoras indebidas.	Informar
Visualización dinámica de la política de privacidad	No todos los entornos son adecuados para mostrar una política de privacidad extensa y, sin embargo, los interesados necesitan poder consultar información detalladas respecto a algún punto concreto. Este patrón proporciona información adicional de la política de	Informar

NOMBRE DEL PATRÓN DE DISEÑO	OBJETIVO Y FINALIDAD	ESTRATEGIA(S) A LA(S) QUE DA SOPORTE
	privacidad de manera contextual (haciendo un clic o pasando el ratón por un enlace) ajustada al contexto o dispositivo desde el que se consulta.	
Gestión y notificación de actividades inusuales en las cuentas de usuario	Muchos servicios web se basan en sistemas de autenticación débiles basados en usuario y contraseña. Conviene establecer mecanismos para identificar actividades anómalas en la cuenta de usuario, alertar a los titulares y utilizar autenticación multifactor para proteger los sistemas de accesos indebidos.	Informar
Advertencia sobre el grado de divulgación	Para evitar que los usuarios intercambien o publiquen información de carácter personal de forma inconsciente o por error durante el uso de aplicaciones o servicios pueden utilizarse alertas contextuales de privacidad que ofrezcan información en relación con el nivel de divulgación de los datos antes de que esa información sea definitivamente publicada o transmitida.	Informar
Contraseñas seguras	El método habitual de autenticación para acceder a un servicio es en forma de usuario y contraseña. Debido a la debilidad de este método de autenticación el responsable debe utilizar este patrón para asistir al usuario en la elección de una contraseña robusta y mantenerles informados de la importancia de su protección y custodia.	Informar
Diseño de capas de políticas de privacidad	Las políticas de privacidad tienden a ser largas, complejas y difíciles de entender lo que lleva a que el usuario no las lea y en consecuencia no esté adecuadamente informado del tratamiento. Este patrón sugiere que el responsable organice la política de privacidad en niveles anidados de detalle y extraiga los aspectos más relevantes a un primer	Informar

NOMBRE DEL PATRÓN DE DISEÑO	OBJETIVO Y FINALIDAD	ESTRATEGIA(S) A LA(S) QUE DA SOPORTE
	nivel para, desde cada uno de ellos, proporcionar acceso a los sucesivos niveles de detalle donde los usuarios puedan encontrar de una forma fácil y cómoda la información relevante para ellos.	
Minimización de la asimetría de información	La asimetría de información se define como la situación en la que una de las partes involucrada en una transacción tiene más o mejor información sobre esta que la otra. Para que exista una relación de confianza entre el responsable y el sujeto de datos, este debe conocer y entender la naturaleza del tratamiento. El uso de este patrón se traduce en minimizar la cantidad y tipo de datos obtenidos del usuario para que sólo se procesen los datos personales requeridos para el propósito perseguido y establecer políticas claras y concisas fácilmente comprensibles por el usuario, reduciendo así el desequilibrio responsable – sujeto de datos.	Informar
Registro de datos personales	Aun cuando en muchos casos no constituye una obligación legal para el responsable, la publicación del inventario de tratamientos fomenta la transparencia y haciéndolos fácilmente accesibles por el usuario permite que estos estén informados con todo detalle de las características del tratamiento: qué datos se recogen, por quién, para qué finalidad, a quiénes se comunican, por cuánto tiempo se conservan, … Puede valorarse incluso la posibilidad de dar acceso en bruto al registro de los datos que son objeto de tratamiento a distinto nivel de detalle.	Informar

NOMBRE DEL PATRÓN DE DISEÑO	OBJETIVO Y FINALIDAD	ESTRATEGIA(S) A LA(S) QUE DA SOPORTE
Panel de concienciación en privacidad	Existen servicios y aplicaciones que tienen un impacto en la privacidad del usuario de maneras que no resultan evidentes para el usuario en un primer momento. Es posible que los usuarios, si no son plenamente conscientes de las consecuencias y actúan desinformados, tomen decisiones incorrectas en relación con cómo utilizan los servicios pudiendo incluso llegar a pensar que las acciones que realizan son anónimas y no les identifican. Este patrón permite enviar a los usuarios recordatorios sobre quién puede ver el contenido que divulgan, qué se hace con él y cómo podría llegar a identificárseles.	Informar
Codificación de privacidad mediante colores	Utilizado en entornos web en lo que se publican datos personales, como las redes sociales, permite a los usuarios apreciar rápidamente y a simple vista mediante la codificación por medio de colores cuáles son los parámetros de privacidad que se aplican al contenido compartido.	Informar
Etiquetas de privacidad	Debido al esfuerzo requerido, los usuarios a menudo no consultan las diversas políticas de privacidad de los servicios que utilizan lo que conduce a desinformación sobre las posibles consecuencias de su consentimiento y opciones de privacidad configuradas. Definir los aspectos básicos del tratamiento de forma tabular y haciendo uso de etiquetas ayuda a comprender más fácilmente la naturaleza y características del tratamiento.	Informar
Espejos de privacidad	Los usuarios, con frecuencia, desconocen el nivel al que un sistema procesa sus datos personales. Debido a esto, unas veces se acepta el uso indefinido y sin control de los datos y otras, por el	Informar

NOMBRE DEL PATRÓN DE DISEÑO	OBJETIVO Y FINALIDAD	ESTRATEGIA(S) A LA(S) QUE DA SOPORTE
	contrario, se limita más de lo necesario resultando en una pérdida de funcionalidad. Este patrón implementa un sistema una reflexión a alto nivel sobre qué datos personales conoce el sistema, qué acceso se le da a otros y qué tipo de datos personales se pueden deducir proporcionando así una interfaz que permite a los usuarios considerar su privacidad en contexto y tomar decisiones informadas ajustadas a sus necesidades.	
Proxy de privacidad	Las políticas de privacidad publicadas en servicios web son, en muchas ocasiones, difíciles de leer y entender por los interesados. Este patrón, aplicable a soluciones web, implementa un proxy de privacidad capaz de analizar e interpretar las políticas y traducirlas a un formato más fácil de leer.	Informar
Selección de credenciales	En procesos que requieren autenticación, proporcionar información exacta a los usuarios de los datos personales y los metadatos que el responsable obtendrá una vez finalizada la transacción y habilitar un mecanismo que permita seleccionar entre diferentes opciones, permitiendo identificarse de manera granular, proporcionando más o menos información según su elección.	Informar Controlar
Anonimización	Desvincular los atributos sensibles de los identificadores correspondientes para que los sujetos de datos no puedan ser identificados.	Minimizar
Seleccionar antes de recoger	Su implementación limita la recogida de datos personales a los necesarios para los propósitos especificados y para los que existe una base jurídica, evitando así una recopilación indiscriminada de datos	Minimizar

NOMBRE DEL PATRÓN DE DISEÑO	OBJETIVO Y FINALIDAD	ESTRATEGIA(S) A LA(S) QUE DA SOPORTE
	y potencialmente, un desvío de finalidad del tratamiento.	
Eliminación de metadatos	Deben ocultarse los metadatos que se generan durante determinados tratamientos (datos exif en las fotografías, cabeceras en el email o en otro tipo de comunicaciones, sellos de tiempo en los ficheros, …) que no son necesarios para la finalidad perseguida y que, si se hacen públicos, pueden representar una amenaza para la privacidad.	Minimizar
Credenciales basadas en atributos	Permiten autenticar de manera flexible y selectiva el cumplimiento de diferentes propiedades o atributos sobre una entidad o sujeto, pero sin revelar su identidad o información adicional sobre ella (propiedad de conocimiento cero)	Minimizar Ocultar
Protección frente al seguimiento	Este patrón evita el seguimiento de las personas que visitan un sitio web a través del empleo de cookies, mediante la implementación de mecanismos entre el navegador y el servidor web que se encarguen de eliminarlas de forma regular (por ejemplo, en cada inicio del sistema operativo) o deshabilitándolas de manera permanente.	Minimizar Ocultar
Redes de mezcla	Las redes de mezcla son protocolos de enrutamiento que crean comunicaciones difíciles de rastrear usando una cadena de servidores proxy que reciben mensajes de múltiples emisores, los reordenan y los reenvían en orden aleatorio al próximo destino (posiblemente otro nodo de mezcla). De esta manera se rompe el enlace entre la fuente de la petición y el destino, haciendo más difícil la tarea de alguien que pretende escuchar las comunicaciones de extremo a extremo.	Ocultar

NOMBRE DEL PATRÓN DE DISEÑO	OBJETIVO Y FINALIDAD	ESTRATEGIA(S) A LA(S) QUE DA SOPORTE
	Este patrón proporciona desvinculación en las comunicaciones extremo a extremo dificultando establecer correlaciones y el rastreo de las comunicaciones.	
Encaminamiento de cebolla	Este patrón es un caso particular del patrón de Redes de mezcla y proporciona desvinculación entre el emisor y el receptor de una comunicación encapsulando los datos en diferentes capas de cifrado y limitando así el conocimiento por parte de los nodos intermedios de la ruta de la comunicación logrando así un enrutado anónimo.	Ocultar
Seudonimización	Este patrón permite realizar el tratamiento de datos personales de manera que no puedan atribuirse a un sujeto de datos específico sin el uso de información adicional, siempre que dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas para garantizar la no atribución	Ocultar
Identidad seudónima	Es posible interaccionar de forma anónima en determinados servicios, como los foros, mediante el uso de seudónimos que oculten la identidad real del interesado en sus participaciones, de modo que el resto de los usuarios no puedan vincularlas con la identidad real del sujeto.	Ocultar
Mensajería seudónima	Se trata de un servicio de mensajería en línea mejorados en el que un tercero de confianza se encarga de intercambiar los identificadores de las partes involucradas en la comunicación por seudónimos manteniendo así la anonimidad entre los extremos.	Ocultar

NOMBRE DEL PATRÓN DE DISEÑO	OBJETIVO Y FINALIDAD	ESTRATEGIA(S) A LA(S) QUE DA SOPORTE
Enmascaramiento	Este patrón oculta las acciones realizadas por un usuario al agregar otras interacciones falsas que no se pueden distinguirse de las reales. Se utiliza para proteger la privacidad en servicios de localización notificando diferentes ubicaciones para ocultar la localización real, en comunicaciones anónimas mediante el envío de mensajes falsos a destinatarios falsos para proteger el perfil, o en servicios de búsqueda web para ocultar las preferencias reales.	Ocultar
Conjunto anónimo	Agrega múltiples ocurrencias de registros relativos a interesados en un único conjunto de datos, de modo que no se pueda identificar una ocurrencia concreta dentro del conjunto, evitando así acciones como realizar seguimiento de la localización de un sujeto, analizar el comportamiento u otras operaciones que pueden poner en riesgo la privacidad	Ocultar Abstraer
Cifrado con claves administradas por el usuario	Protege la confidencialidad de la información personal codificando el contenido de los mensajes transmitidos por la red o almacenados usando un servicio proporcionado por terceros no confiables mediante el uso de algoritmos de cifrado y utilizando claves administradas por el usuario, de modo que sólo aquellos que dispongan de la clave de descifrado pueden recuperar el contenido	Ocultar Controlar
Bloqueo de correlación en sistemas de gestión de identidad federada	En sistemas de gestión de identidad federada el uso de este patrón evita la correlación de las solicitudes entre el usuario final y el proveedor de los servicios que pueden llegar a hacer los otros actores participantes en el sistema mediante el uso de un orquestador de las peticiones que corre en el entorno cliente.	Ocultar Cumplir

NOMBRE DEL PATRÓN DE DISEÑO	OBJETIVO Y FINALIDAD	ESTRATEGIA(S) A LA(S) QUE DA SOPORTE
Custodia de datos por el usuario	Es habitual desarrollar arquitecturas de tipo centralizado en las que el tratamiento de los datos personales se realiza en un único sistema o entidad en el que el usuario se ve obligado a confiar e incluso compartir datos sensibles. Este patrón evita un tratamiento centralizado de los datos personales al trasladar parte de este a entornos de confianza del usuario (por ejemplo, sus propios dispositivos), permitiéndoles así controlar los datos exactos que son compartidos con los proveedores de servicios.	Separar
Listas negras anónimas	Mantener el control sobre los usuarios que hacen un uso incorrecto del servicio y prohibirles el acceso creando listas negras, pero sin conocer su identidad.	Separar Ocultar

IX. ANEXO 2: EXTRACTOS NORMATIVOS

A continuación, para comodidad del lector, se trascriben aquellos artículos y considerandos del Reglamento (UE) 2016/679 General de Protección de Datos que han sido referenciados a lo largo de esta guía y que guardan relación con el concepto de privacidad desde el diseño y por defecto.

CONSIDERANDO 39

"Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento."

CONSIDERANDO 78

"La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la

debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos."

ARTÍCULO 5 PRINCIPIOS RELATIVOS AL TRATAMIENTO

"1. Los datos personales serán:

a)tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c)adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d)exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e)mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f)tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)."

ARTÍCULO 13 INFORMACIÓN QUE DEBERÁ FACILITARSE CUANDO LOS DATOS PERSONALES SE OBTENGAN DEL INTERESADO

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

a)la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b)los datos de contacto del delegado de protección de datos, en su caso;

c)los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d)cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e)los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f)en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a)el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b)la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c)cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d)el derecho a presentar una reclamación ante una autoridad de control;

e)si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f)la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información."

ARTÍCULO 14 INFORMACIÓN QUE DEBERÁ FACILITARSE CUANDO LOS DATOS PERSONALES NO SE HAYAN OBTENIDO DEL INTERESADO

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

a)la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b)los datos de contacto del delegado de protección de datos, en su caso;

c)los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

d)las categorías de datos personales de que se trate;

e)los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f)en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

a)el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;

b)cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;

c)la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

d)cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;

e)el derecho a presentar una reclamación ante una autoridad de control;

f)la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

g)la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:

a)dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;

b)si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o

c)si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a)el interesado ya disponga de la información;

b)la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;

c)la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o

d)cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria."

ARTÍCULO 24 RESPONSABILIDAD DEL RESPONSABLE DEL TRATAMIENTO

"1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento."

ARTÍCULO 25 PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

"1. Teniendo 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, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la

extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo."

ARTÍCULO 28 ENCARGADO DEL TRATAMIENTO

"1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

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

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.

7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.

9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento."

ARTÍCULO 32 SEGURIDAD DEL TRATAMIENTO

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y

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

a)la seudonimización y el cifrado de datos personales;

b)la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c)la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d)un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros."

ARTÍCULO 36 CONSULTA PREVIA

"1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

a)en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;

b)los fines y medios del tratamiento previsto;

c)las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;

d)en su caso, los datos de contacto del delegado de protección de datos;

e)la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y

f)cualquier otra información que solicite la autoridad de control.

4. Los Estados miembros garantizarán que se consulte a la autoridad de control durante la elaboración de toda propuesta de medida legislativa que haya de adoptar un Parlamento nacional, o de una medida reglamentaria basada en dicha medida legislativa, que se refiera al tratamiento.

5. No obstante lo dispuesto en el apartado 1, el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública."

ARTÍCULO 83 CONDICIONES GENERALES PARA LA IMPOSICIÓN DE MULTAS ADMINISTRATIVAS

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4.

5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

6. El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

8. El ejercicio por una autoridad de control de sus poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

9. Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. Los Estados miembros de que se trate notificarán a la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable."