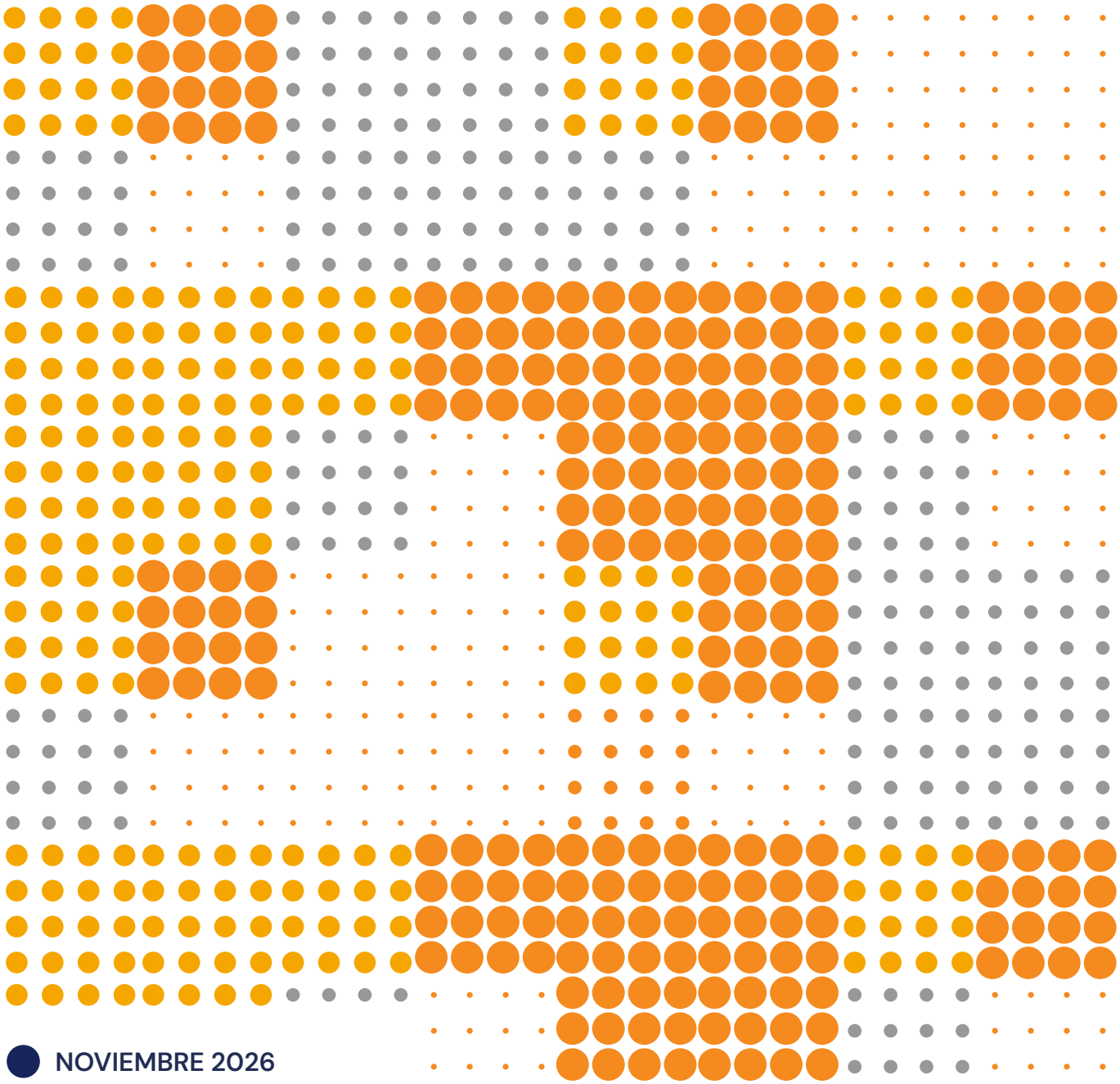
agencia española protección datos

HELLENIC DATA PROTECTION AUTHORITY

ENTORNOS DE TRATAMIENTO SEGURO DESDE LA PERSPECTIVA DE LA PROTECCIÓN DE DATOS



NOVIEMBRE 2026

Este documento ha sido elaborado en colaboración por las autoridades de protección de datos de España y Grecia.

Autores principales:

- En nombre de la Agencia Española de Protección de Datos (AEPD): la División de Innovación Tecnológica, representada por Luis de Salvador Carrasco y Teresa Martínez Sánchez.
- En nombre de la Autoridad Helénica de Protección de Datos (HDPA): el Departamento de Investigación y Estudios, representado por Konstantinos Limniotis y Eleni Maragou.

Revisores:

El documento se ha beneficiado de las valiosas contribuciones de los siguientes expertos durante su revisión:

- Fabio Ricciato (Eurostat, Comisión Europea).
- Carlos Alonso Peña y Guillermo Pérez de Arenaza Pozo (Dirección General del Dato, Ministerio para la Transformación Digital y de la Función Pública, España).
- Giuseppe D'Acquisto (Autoridad Italiana de Protección de Datos "*Garante per la protezione dei dati personali*", Italia).
- Paul Comerford (Autoridad Británica de Protección de Datos "*Information Commissioner's Office*", Reino Unido).

ÍNDICE

LISTA DE ACRÓNIMOS 5

RESUMEN EJECUTIVO 6

I. INTRODUCCIÓN 7

II. ¿QUÉ ES UN ENTORNO DE TRATAMIENTO SEGURO? 9

A. DEFINICIÓN Y REFERENCIA LEGAL 9

1. DGA 9

2. EEDS 11

3. OTRAS NORMATIVAS 12

B. ETS Y CUMPLIMIENTO DE PROTECCIÓN DE DATOS 13

1. DEFINICIÓN DE ROLES EN LOS ETS 14

2. TÉRMINOS CONTRACTUALES Y ASIGNACIÓN DE RESPONSABILIDADES 14

3. TERCEROS Y LA IMPLEMENTACIÓN DEL ETS 15

4. TRANSFERENCIAS INTERNACIONALES 18

5. FACILITAR EL EJERCICIO DE LOS DERECHOS DE LOS INTERESADOS 18

6. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO 19

7. GESTIÓN DE RIESGOS DE PROTECCIÓN DE DATOS 23

III. CONSIDERACIONES Y MEDIDAS DE IMPLEMENTACIÓN 27

A. MEDIDAS QUE SE DEBEN APLICAR 27

1. GOVERNANZA Y RESPONSABILIDAD PROACTIVA 27

2. GESTIÓN DE DATOS 28

3. GESTIÓN DE IDENTIDAD Y CONTROL DE ACCESOS 29

4. SEGURIDAD FÍSICA 29

5. SEGURIDAD DE REDES Y COMUNICACIONES 29

6. SEGURIDAD DE SISTEMAS Y APLICACIONES 30

7. AUDITORÍA, REGISTRO Y SEGUIMIENTO 30
8. RESPUESTA A INCIDENTES, RECUPERACIÓN Y RESILIENCIA 31
9. GESTIÓN DE TERCEROS 31
10. CULTURA ORGANIZATIVA Y FORMACIÓN 31
B. INGENIERÍA DE PROTECCIÓN DE DATOS PARA IMPLEMENTAR UN ETS 32
1. ETS vs TEEs 32
2. CIFRADO HOMOMÓRFICO 33
3. COMPUTACIÓN MULTI PARTE SEGURA 34
4. CIFRADO POLIMÓRFICO Y SEUDONIMIZACIÓN 34
5. SEUDONIMIZACIÓN CIEGA 35
6. PRIVACIDAD DIFERENCIAL 36
7. APRENDIZAJE FEDERADO 36
C. MAPEO DE AMENAZAS Y MEDIDAS 37
IV. UN CASO PRÁCTICO 38
A. DESCRIPCIÓN DEL ESCENARIO 38
B. ANÁLISIS DE RIESGOS DE PROTECCIÓN DE DATOS (*RELACIONADO CON LA VINCULACIÓN*) 38
C. ENFOQUE DE INGENIERÍA DE PROTECCIÓN DE DATOS 39
D. LA TÉCNICA DE INGENIERÍA DE PROTECCIÓN DE DATOS EN DETALLE 40
1. FASE 1: ACUERDO Y CONFIGURACIÓN 40
2. FASE 2: GESTIÓN DE CLAVES CRIPTOGRÁFICAS 40
3. FASE 3: ENVIAR LOS DATOS CIFRADOS AL OADS 40
4. FASE 4: COMPUTACIÓN SEGURA VÍA OADS 41
5. FASE 5: COMPARTIR RESULTADOS 41
6. FASE 6: ANÁLISIS E INFORMES 41
V. REFLEXIONES FINALES 43
VI. REFERENCIAS 45

LISTA DE ACRÓNIMOS

DA	Reglamento de Datos (por sus siglas en inglés "*Data Act*")
DGA	Reglamento de Gobernanza Digital (por sus siglas en inglés "*Data Governance Act*")
DLP	Prevención de Pérdida de Datos (por sus siglas en inglés "*Data Loss Prevention*")
DPD	Delegado de Protección de Datos
EDPB	Comité Europeo de Protección de Datos (por sus siglas en inglés "*European Data Protection Board*").
EEDS	Reglamento del Espacio Europeo de Datos de Salud
EIPD	Evaluación del Impacto en la Protección de Datos
ENISA	Agencia de la Unión Europea para la Ciberseguridad
ETS	Entorno de Tratamiento Seguro
FAIR	Localizables, accesibles, interoperables y reutilizables (por sus siglas en inglés "*Findable, Accessible, Interoperable and Reusable*")
FL	Aprendizaje Federado (por sus siglas en inglés "*Federated Learning*")
HE	Cifrado homomórfico (por sus siglas en inglés "*Homomorphic Encryption*")
IA	Inteligencia artificial
MFA	Autenticación multifactor (por sus siglas en inglés "*Multi-factor Authentication*")
NIST	Instituto Nacional de Estándares y Tecnología (por sus siglas en inglés "*National Institute of Standards and Technology*")
OADS	Organismo de Acceso a Datos de Salud
PoLP	Principio del menor privilegio (por sus siglas en inglés "*Principle of least privilege*")
RGPD	Reglamento General de Protección de Datos
TEE	Entorno de Ejecución Confiable (por sus siglas en inglés "*Trusted Execution Environment*")
VDI	Infraestructura de escritorio virtual (por sus siglas en inglés "*Virtual Desktop Infrastructure*")

RESUMEN EJECUTIVO

Los Entornos de Tratamiento Seguro (ETS) permiten un acceso controlado a los datos en condiciones diseñadas para salvaguardar los derechos y libertades de los individuos y proteger los intereses legítimos de los titulares de datos, sin depender exclusivamente de las salvaguardas legales, organizativas o técnicas implementadas por los usuarios de datos. Esta garantía reforzada es esencial para fomentar la confianza en la economía basada en los datos y fortalecer la confianza entre individuos y empresas en el uso seguro y responsable de los datos. En particular, los ETS apoyan el cambio desde la tradicional compartición de datos hacia el acceso controlado a los datos, permitiendo el tratamiento autorizado sin necesariamente transferir los datos subyacentes a los usuarios de datos. El Reglamento de Gobernanza de Datos (DGA) y el Reglamento Europeo de Espacio de Datos de Salud (EEDS) establecen un marco legal con el objetivo de facilitar el acceso a datos protegidos o sensibles, a la vez que asegurando los derechos fundamentales y otros intereses legítimos.

Este documento examina los ETS desde una perspectiva de protección de datos, centrándose en sus dimensiones legales, organizativas y técnicas. Su objetivo es proporcionar una orientación de alto nivel sobre las consideraciones y salvaguardas relevantes para su diseño, implementación y funcionamiento, especialmente dentro de los marcos de la DGA y el EEDS.

Con este fin, el documento subraya que el diseño e implementación de los ETS requieren un enfoque integral que combine salvaguardas legales, organizativas y técnicas, yendo más allá de las medidas convencionales de ciberseguridad. Su implementación debe garantizar el cumplimiento del Reglamento General de Protección de Datos (RGPD), incluyendo la protección de datos desde el diseño y por defecto, la responsabilidad proactiva, la minimización de datos y el ejercicio efectivo de los derechos de los interesados. Se pone especial énfasis en la necesidad de que la entidad encargada de proporcionar el ETS mantenga un control genuino y efectivo sobre las operaciones de tratamiento, incluyendo cuando la infraestructura o los servicios son proporcionados por terceros. Las garantías contractuales por sí solas pueden ser insuficientes si no están respaldadas por medidas técnicas adecuadas, supervisión efectiva y capacidad real de auditoría.

El documento también subraya la importancia de un enfoque integral e integrado de gestión de riesgos que vaya más allá de los riesgos convencionales de ciberseguridad y protección de datos personales. Los ETS deben abordar, en un enfoque específico de su contexto, una amplia gama de riesgos interconectados, incluidos aquellos relacionados con otros derechos fundamentales, dependencias de terceros y soberanía digital. Además, los desarrollos tecnológicos, geopolíticos y legales en evolución pueden introducir amenazas adicionales que deben considerarse. Dado que los riesgos que surgen en un área también pueden afectar a la protección de datos personales, su evaluación no debe realizarse de forma aislada, sino dentro de un marco unificado de gestión de riesgos. Con esta situación dada, las Evaluaciones de Impacto en Protección de Datos (EIPD) desempeñan un papel central en la identificación y evaluación de riesgos para los derechos y libertades de las personas, al tiempo que contribuyen a la selección de las salvaguardas adecuadas.

Más allá de las medidas convencionales de seguridad, el documento explora cómo técnicas avanzadas de ingeniería de privacidad, incluyendo cifrado homomórfico, computación segura multi parte, seudonimización ciega y aprendizaje federado, pueden fortalecer las salvaguardas de privacidad. Estas técnicas pueden permitir cálculos autorizados limitando el acceso a datos personales subyacentes, aunque su idoneidad y limitaciones deben evaluarse en cada contexto específico. Se incluye un caso de uso ilustrativo en investigación sanitaria que explica cómo el cifrado homomórfico puede soportar análisis estadísticos entre múltiples fuentes de datos sin requerir la divulgación de datos originales al proveedor de ETS o a los investigadores.

Este documento proporciona orientación inicial para los responsables de tratamiento para la gestión del ETS y los tratamientos autorizados en él, así como para los Delegados de Protección de Datos

(DPDs), asesores de protección de datos y terceras partes implicadas en el diseño, despliegue y operación de dichos entornos. Su propósito es facilitar la implementación efectiva de los ETS, guiados por principios de protección de datos y adecuadamente integradas en su diseño. Este enfoque se complementa con una estrategia integral para identificar y gestionar la amplia gama de riesgos asociados a su diseño, despliegue y operación.

I. INTRODUCCIÓN

El Reglamento de Gobernanza de Datos[1] (en adelante DGA por sus siglas en inglés) y el Reglamento Europeo de Espacio de Datos de Salud[2] (en adelante EEDS) tienen como objetivo establecer una visión europea común para el desarrollo de un ecosistema de datos abierto, federado y fiable. Esta visión se basa en el principio de soberanía de los datos, asegurando que los titulares de los datos[3] e interesados[4] mantengan un control efectivo sobre cómo se acceden y utilizan los datos[5]. Para lograr este objetivo, ambas regulaciones promueven la creación de infraestructuras interoperables respaldadas por políticas, normas y estándares de gobernanza que definen colectivamente un marco de confianza para todas las partes interesadas. Este marco se implementa mediante una combinación de medidas organizativas, legales y técnicas diseñadas para permitir la reutilización de los datos, protegiendo al mismo tiempo los derechos fundamentales, los intereses económicos y los objetivos de política pública y, de forma específica y explícita, los derechos y libertades de los interesados respecto al tratamiento de sus datos personales.

Además de las preocupaciones sobre la protección de datos personales, la reutilización de datos conlleva una amplia gama de riesgos que también deben tenerse en cuenta. Estos riesgos pueden afectar a los secretos comerciales y estadísticos, los derechos de propiedad intelectual e industrial, los intereses de seguridad nacional, las políticas públicas y las obligaciones de confidencialidad de los titulares de los datos.

Tanto la DGA como el EEDS identifican situaciones en las que las salvaguardas organizativas, legales o técnicas que los usuarios de datos[6] pueden proporcionar son insuficientes para garantizar la protección de los intereses de los titulares de datos y para alcanzar los objetivos perseguidos por estas normativas al conceder acceso a los datos, entre los cuales está la confianza a todas las partes interesadas. Independientemente de la naturaleza del usuario de datos (ya sea una entidad privada, un organismo público o un investigador individual), ciertas circunstancias requieren la implementación de salvaguardas más estrictas para regular el acceso y la reutilización de datos. Estas garantías reforzadas son esenciales para fomentar la confianza en la economía basada en datos y fortalecer la confianza entre individuos y empresas en el uso seguro y responsable de los

[1] Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos) (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32022R0868)

[2] Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847 (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=OJ:L_202500327)

[3] Artículo 2.8) de la DGA: "«titular de datos», toda persona jurídica, incluidos los organismos del sector público y organizaciones internacionales, o persona física que no sea el interesado con respecto a los datos específicos en cuestión, que, de conformidad con el Derecho de la Unión o nacional aplicable, tenga derecho a conceder acceso a determinados datos personales o no personales o a compartirlos;"

[4] Artículo 4.1) del RGPD: "(...) una persona física identificada o identificable («el interesado»);"

[5] Esta visión se expuso por primera vez en "Una Estrategia Europea de Datos" [febrero de 2020] (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0066) y continúa en la "Estrategia para una Unión de Datos. Desbloqueando datos para la IA" [noviembre de 2025] (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52025DC0835).

[6] Artículo 2.9) de la DGA: "«usuario de datos», toda persona física o jurídica que tenga acceso legítimo a determinados datos personales o no personales y el derecho, incluido el que le otorga el Reglamento (UE) 2016/679 en el caso de los datos personales, a usarlos con fines comerciales o no comerciales;"

datos. Basándose en la experiencia práctica adquirida a través de varias iniciativas europeas tanto en los ámbitos estadístico como sanitario, proporcionando ejemplos indicativos en la práctica[7], surge la infraestructura de Entorno de Tratamiento Seguro (en adelante "ETS") como solución.

El objetivo del ETS es garantizar el cumplimiento legal y la soberanía digital para la entidad que lo proporciona sin necesidad de depender de las garantías ofrecidas por el usuario de datos. Un ETS no es una solución o producto tecnológico único, sino un conjunto integral de medidas organizativas, legales y técnicas que en conjunto crean un entorno controlado para el tratamiento de datos, permitiendo, al mismo tiempo, el análisis y reutilización de datos (especialmente sensibles o específicamente protegidos). El ETS es una de las formas de implementar el modelo basado en el "acceso a datos", tal como lo establece la DGA, donde los datos permanecen bajo el control del titular de los datos y el usuario de datos tiene la capacidad de realizar operaciones de tratamiento autorizadas dentro de límites predefinidos.

La DGA establece que, en ciertos casos, los datos solo pueden usarse y reutilizarse en un ETS proporcionado o controlado por el organismo del sector público[8]. Pero es en el contexto del EEDS donde los ETS adquieren una importancia especial. El objetivo del EEDS es mejorar el acceso y control de las personas físicas sobre sus datos electrónicos de salud en el contexto sanitario (usos primarios), así como lograr otros fines que impliquen el uso de datos electrónicos de salud en otros sectores que beneficiarían a la sociedad (usos secundarios). El EEDS establece que el acceso a los datos electrónicos de salud para fines secundarios debe realizarse a través de los ETS[9] como "*una garantía esencial para proteger los derechos y las libertades de las personas físicas en relación con el tratamiento de sus datos de salud electrónicos para uso secundario*". Esto refleja la alta sensibilidad de los datos de salud, la posterior necesidad de un nivel de protección reforzado y la correspondiente necesidad de salvaguardas técnicas y organizativas sólidas que vayan más allá de los mecanismos tradicionales de control de acceso.

El EEDS aclara además la relación entre las ETS y el Reglamento General de Protección de Datos[10] (en adelante RGPD). Su considerando (77) especifica que el tratamiento de datos personales dentro de un ETS debe cumplir plenamente con el RGPD. Por tanto, los ETS no son una alternativa al cumplimiento del RGPD, sino un medio para poner en práctica los principios de protección de datos en escenarios complejos y a gran escala de tratamientos de datos. Es importante destacar que los ETS no son mutuamente excluyentes con otras técnicas que mejoran la privacidad o preservan la seguridad. Por el contrario, pueden usarse en combinación con medidas complementarias como anonimización, pseudonimización, privacidad diferencial, tratamientos federados, computación segura multipartita, cifrado homomórfico y otras tecnologías avanzadas, dependiendo del perfil de riesgo y del uso previsto de los datos.

El alcance de esta guía es proporcionar un análisis de alto nivel de los requisitos organizativos, legales y técnicos que los entornos de tratamiento seguro deben cumplir para gestionar eficazmente los riesgos para la protección de datos personales. No evalúa implementaciones específicas ni prescribe enfoques técnicos u organizativos detallados para el diseño y despliegue de dichos entornos. Como documento guía inicial, está destinado simplemente a apoyar la comprensión del concepto y, por

[7] Ejemplos destacados incluyen el "KIOSK" de Eurostat (entorno de investigación de confianza del sistema estadístico europeo), los Centros de Datos Seguros INE de España, el CASD de Francia (Centre d'Accès Sécurisé aux Données), el Centro de Datos de Salud francés (HDH), el BELab de España, el BPLIM de Portugal, Findata de Finlandia y los Entornos de Investigación de Confianza (Trusted Research Environments) del NHS del Reino Unido.

[8] Artículo 5.3.b) y Considerando (7) de la DGA.

[9] Artículo 73 y Considerando (77) del EHDS.

[10] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679)

tanto, no debe interpretarse como una declaración exhaustiva de requisitos. Aunque un ETS es un tipo de infraestructura que puede implementarse en diferentes contextos, este texto se centra en los ETS en actividades de tratamiento dentro del ámbito de la DGA y el EEDS.

II. ¿QUÉ ES UN ENTORNO DE TRATAMIENTO SEGURO?

Este apartado examina el alcance de la definición de ETS en diversos marcos legales europeos y analiza una serie de consideraciones relevantes sobre la protección de datos dentro de estos entornos.

A. Definición y referencia legal

1. DGA

La DGA proporciona la definición formal a nivel de la UE de un Entorno de Tratamiento Seguro (ETS). El artículo 2.20) describe un ETS como un "*entorno físico o virtual y los medios organizativos para garantizar el cumplimiento del Derecho de la Unión, como, por ejemplo, el Reglamento (UE) 2016/679, en particular, por lo que respecta a los derechos de los interesados, los derechos de propiedad intelectual y la confidencialidad comercial y estadística, la integridad y la accesibilidad, así como para garantizar el cumplimiento del Derecho nacional aplicable y permitir que la entidad encargada de proporcionar el entorno de tratamiento seguro determine y supervise todas las acciones de tratamiento, incluida la presentación, el almacenamiento, la descarga y la exportación de datos, así como el cálculo de datos derivados mediante algoritmos computacionales*".

Según la definición de la DGA, un ETS es una infraestructura que garantiza el cumplimiento legal para la entidad que lo proporciona **sin necesidad de depender de las garantías ofrecidas por los usuarios de datos**, ya sean estos últimos una entidad privada, un organismo público o un investigador individual. Al permitir dicho control y supervisión sobre las operaciones de tratamiento, el ETS también puede entenderse como un apoyo a la soberanía digital para la entidad que la proporciona. En términos prácticos, un ETS es más que una forma de implementar los "principios de datos FAIR"[11] y la ciberseguridad, es una infraestructura controlada, ya sea una instalación física segura o una plataforma virtual, diseñada para garantizar que los datos sensibles se traten bajo estrictas salvaguardas técnicas y organizativas[12]. Un elemento clave de la definición es la capacidad del proveedor de ETS para mantener una supervisión efectiva de cada operación realizada dentro del entorno, desde el acceso y visualización de datos hasta la transformación y la generación de resultados. Así, los ETS funcionan no solo como sistemas informáticos seguros, sino como marcos integrales de cumplimiento.

Los ETS permiten la implementación del modelo de acceso a datos en lugar de un modelo tradicional de compartición de datos, reflejando una distinción conceptual clave que sustenta la DGA y la EEDS.

---

[11] Hacer que los datos sean localizables, accesibles, interoperables y reutilizables (*Findable, Accessible, Interoperable and Reusable*). https://force11.org/info/the-fair-data-principles/

[12] La correcta implementación de los ETS es esencial para cumplir los requisitos establecidos para alcanzar los objetivos técnicos de soberanía establecidos en la "Comunicación de la Comisión al Parlamento Europeo, el Consejo, el Comité Económico y Social Europeo y el Comité de las Regiones sobre la Soberanía Tecnológica Europea, acompañada de una Estrategia de Código Abierto de la UE" (COM(2026) 503 final) (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52026DC0503), y en particular lo siguiente:
"II) garantizar la oferta de tecnologías digitales que apuntalen la competitividad de Europa, entre otras cosas diversificando las cadenas de suministro y reduciendo las dependencias específicas de un único proveedor o un número limitado de proveedores no pertenecientes a la UE, también a través de asociaciones comerciales y de inversión de confianza;
III) obtener y mantener el control sobre las infraestructuras de datos y los datos críticos, desarrollando al mismo tiempo la capacidad para aprovecharlos eficazmente;"

Según el artículo 2.10) de la DGA, "compartir datos" se refiere a la provisión de datos por parte de un interesado o de un titular de datos a un usuario de datos para uso conjunto o individual, basado en acuerdos voluntarios u obligaciones legales, y puede implicar la transmisión de datos directamente o a través de un intermediario. El intercambio tradicional de datos implica inherentemente que las copias de los datos se transfieren o se ponen a disposición del usuario, quien puede procesarlas en sus propios sistemas, sujetas a restricciones contractuales o legales. En cambio, el artículo 2.13) de la DGA define "acceso" como el uso de datos conforme a requisitos técnicos, legales u organizativos específicos, sin implicar necesariamente la transmisión o descarga de los datos. En un modelo basado en el acceso, los datos permanecen bajo el control del titular de los datos, y al usuario se le concede la capacidad de realizar operaciones de tratamiento autorizadas dentro de límites predefinidos.

Los ETS desempeñan un papel fundamental en facilitar el acceso, en lugar del intercambio tradicional de datos, especialmente para conjuntos de datos protegidos o sensibles. Históricamente, una vez que los datos se transfieren fuera de los sistemas del titular original, supervisar o limitar su uso posterior se vuelve difícil. Los ETS pretenden alterar fundamentalmente este paradigma pasando de "mover los datos" a "llevar al usuario a los datos". Todo el tratamiento se realiza en un entorno estrictamente controlado donde el acceso está restringido, las acciones del usuario se registran y monitorizan, y técnicamente se impiden salidas no autorizadas.

Como se establece en el considerando (7) de la DGA, "*en muchos casos, la aplicación de dichas técnicas [la anonimización, la privacidad diferencial, la generalización, la supresión y la aleatorización, el uso de datos sintéticos o de métodos similares, y otros métodos punteros de protección de la privacidad que pueden contribuir a un tratamiento de datos más respetuoso de la privacidad], evaluaciones de impacto y otras salvaguardias implica que los datos pueden usarse y reutilizarse solo en un entorno de tratamiento seguro creado o supervisado por el organismo del sector público*"; por lo tanto, la DGA posiciona a los ETS como el principal mecanismo para permitir la reutilización de datos protegidos del sector público, incluidos datos personales, secretos comerciales y estadísticas confidenciales[13], así como ciertos tipos de datos no personales que pueden identificarse como altamente sensibles (por ejemplo, en el ámbito sanitario, transporte, energía, medio ambiente y finanzas)[14].

Según el artículo 5.3) de la DGA, los organismos del sector público están obligados a preservar la naturaleza protegida de los datos durante su reutilización, previendo tres enfoques distintos. El primero implica el pretratamiento de datos (por ejemplo, anonimizar datos personales o aplicar métodos de control de divulgación como agregación o modificación). Sin embargo, cuando estas medidas resultan insuficientes o poco prácticas, la DGA enfatiza soluciones basadas en ETS para los dos enfoques restantes. Más concretamente, el artículo 5.3) establece que los organismos del sector público pueden establecer los siguientes requisitos: *"a) (...), b) que el acceso y reutilización a distancia de los datos se lleven a cabo en un entorno de tratamiento seguro facilitado o controlado por el organismo del sector público; c) que el acceso y reutilización de los datos se lleven a cabo en los locales físicos en los que se encuentre el entorno de tratamiento seguro de conformidad con unas normas de seguridad estrictas, siempre que no pueda habilitarse el acceso a distancia sin que ello ponga en peligro los derechos e intereses de terceros"*. Por lo tanto, en ambos escenarios basados en ETS, el entorno actúa como una salvaguarda técnica y organizativa, asegurando que los datos sensibles (ya sean personales, comerciales o estadísticos) puedan ser tratados y reutilizados sin salir nunca de un espacio supervisado y controlado.

El acceso a dichos datos solo puede concederse dentro de una ETS controlada por el organismo del sector público[15], asegurando que la información siempre permanezca en un espacio monitorizado y protegido. En esencia, la DGA enmarca las ETS como un conjunto de instrumentos legales,

[13] Considerando (7) de la DGA.

[14] Considerando (24) de la DGA.

[15] Considerando (15) de la DGA.

organizativos y técnicos que implementan la soberanía de los datos y concilian el acceso a los datos con protecciones sólidas para secretos comerciales, propiedad intelectual y confidencialidad comercial y estadística, al tiempo que se salvaguardan los objetivos legítimos de política pública de la Unión identificados, como la protección de la salud pública, la seguridad, el medio ambiente, la moralidad pública, la protección del consumidor, la privacidad y la protección de datos personales. (AEPD, Espacios de Datos, soberanía y protección de datos desde el diseño, 2023)

Haciendo de nuevo uso del considerando (7) de la DGA donde se establece que *"en muchos casos, la aplicación de dichas técnicas, evaluaciones de impacto y otras salvaguardias implica que los datos pueden usarse y reutilizarse solo en un entorno de tratamiento seguro creado o supervisado por el organismo del sector público"* se abre, por tanto, la posibilidad de que un ETS sea implementado por un tercero bajo el control y supervisión del organismo del sector público. Sin embargo, la implicación de dicho tercero no determina por sí sola su papel bajo el RGPD, ni necesariamente significa que este tercero pueda desempeñar el rol de encargado de tratamiento. En tales casos, las garantías, salvaguardas y control sobre las operaciones de tratamiento por parte del tercero requeridas por la entidad cargada de proporcionar el ETS deberían ser más robustas y extensas que las requeridas a un usuario de datos.

Más concretamente, la noción de "supervisión" (en la versión inglesa de la norma se refiere como "*control*") no debe entenderse únicamente en términos legales (control *de iure*), es decir, como la autoridad legal para determinar cómo pueden utilizarse el ETS y los datos que se ponen a disposición en ella. Dicha autoridad debe ir acompañada en la práctica de un control efectivo (control *de facto*), respaldado por medidas técnicas y organizativas apropiadas que permitan a la entidad responsable del ETS determinar, restringir, supervisar y, cuando sea necesario, impedir las operaciones de tratamiento. Por tanto, debe prestarse especial atención cuando un proveedor externo tiene la capacidad técnica de acceder o tratar datos de forma independiente de la entidad responsable de la ETS, especialmente cuando esté sujeto a las leyes de un país fuera del Espacio Económico Europeo.

Este enfoque pretende fortalecer la confianza entre los titulares de datos[16] y los usuarios de datos[17], al tiempo que garantiza la protección de los derechos de los interesados[18]. En otras palabras, los requisitos legales deben ser respaldados y ejecutados eficazmente mediante medidas técnicas adecuadas: lo que está legalmente prohibido también debería, en la medida de lo posible, ser prevenido técnicamente. Por tanto, los controles técnicos deben complementar y dar efecto a los controles legales. Las autoridades públicas, las instituciones sanitarias y las empresas privadas tienen que estar seguros de que los datos solo se utilizan para la finalidad autorizada, mientras que los investigadores pueden acceder a conjuntos de datos que de otro modo permanecerían inaccesibles.

2. EEDS

Del mismo modo, el EEDS se basa directamente en el concepto de ETS de la DGA. El EEDS desarrolla y especifica ciertos aspectos de la DGA para el contexto particular de los datos de salud y su uso secundario.

[16] El artículo 2.8) de la DGA para la definición de titulares de datos.

[17] El artículo 2.9) de la DGA para la definición de usuarios de datos.

[18] El considerando (5) de la DGA establece que "Un marco de gobernanza a nivel de la Unión debe tener como objetivo generar confianza entre individuos y empresas en relación con el acceso, control, compartir, usar y reutilizar datos, en particular estableciendo mecanismos adecuados para que los sujetos de datos conozcan y ejerzan significativamente sus derechos, así como en lo relativo a la reutilización de ciertos tipos de datos en poder de los organismos del sector público, la prestación de servicios por parte de proveedores de servicios de intermediación de datos a los sujetos, titulares y usuarios de datos, así como la recopilación y el tratamiento de datos puestos a disposición para fines altruistas por personas físicas y jurídicas"

El uso secundario de los datos de salud está establecido en el Capítulo IV del EEDS y se explica en el considerando (61): *"El uso secundario de los datos de salud en el marco del EEDS debe permitir que las entidades públicas, privadas y sin ánimo de lucro, así como los investigadores individuales, tengan acceso a los datos de salud para la investigación, la innovación, la formulación de políticas, las actividades educativas, la seguridad de los pacientes, las actividades de regulación o la medicina personalizada, en consonancia con los fines establecidos en el presente Reglamento. El acceso a los datos para uso secundario debe contribuir al interés general de la sociedad"*. Dada la mayor sensibilidad de los datos electrónicos de salud, el EEDS introduce normas de gobernanza y salvaguardas más detalladas en las que los ETS desempeñan un papel central como mecanismo clave para facilitar el acceso controlado y garantizar un alto nivel de protección.

Según lo establecido en el Artículo 73, todo uso secundario de datos electrónicos de salud debe realizarse exclusivamente dentro de un ETS regido por un Organismo de Acceso a Datos de Salud[19] (en adelante OADS). Esto significa que los investigadores y entidades investigadoras tienen acceso a los conjuntos de datos pero, según lo establecido en el Artículo 73.2, sin posibilidad de descargar datos personales[20]. Como se detalla en el párrafo 1 del Artículo 73, el EEDS exige estrictas salvaguardas para los ETS, incluyendo: acceso limitado a personas autorizadas listadas en el permiso de datos, protección de última generación contra lecturas, copias o eliminaciones no autorizadas, y un número mínimo de personas identificables autorizadas para introducir, inspeccionar, eliminar o modificar datos. Los ETS deben mantener registros completos y auditables conservados durante al menos un año, restringir a los usuarios solo a los datos necesarios para su propósito aprobado y evitar cualquier exportación de datos personales (solo resultados anonimizados y comprobados pueden salir del entorno)[21].

El artículo 51.1 del EEDS establece las categorías mínimas de datos electrónicos de salud para uso secundario, que, además de los relacionados con los historiales electrónicos de salud, también incluyen otras categorías como datos electrónicos personales de salud generados automáticamente a través de aplicaciones de bienestar o registros de productos medicinales; no obstante, es importante tener en cuenta que el artículo 51.4 establece que *"los Estados miembros podrán introducir medidas más estrictas y garantías adicionales a nivel nacional destinadas a salvaguardar la sensibilidad y el valor de los datos contemplados en el apartado 1, letras f) [datos genéticos, epigenómicos y genómicos humanos], g) [otros datos moleculares humanos, como datos proteómicos, transcriptómicos, metabolómicos, lipidómicos y otros datos ómicos], i) [datos procedentes de aplicaciones de bienestar] y q) [datos de salud procedentes de biobancos y bases de datos asociadas]"*. Este es un criterio adicional para evaluar cuándo los conjuntos de datos (totales o parciales) deben considerarse bajo protección especial.

3. Otras normativas

Otro instrumento legal relevante es el Reglamento de Datos[22], que regula el acceso a datos desde dispositivos conectados y otros intercambios de datos entre empresas. El Reglamento de Datos refuerza el papel de salvaguardas similares a los ETS en el intercambio de datos industriales y

[19] Véase el Capítulo IV "Uso Secundario", Sección 2 "Gobernanza y mecanismos para uso secundario" del EEDS para una descripción detallada del Organismo de Acceso a Datos de Salud.

[20] "(...) *Los organismos de acceso a datos de salud revisarán los datos de salud electrónicos incluidos en una petición de descarga con objeto de garantizar que los usuarios de datos de salud solo puedan descargar datos de salud electrónicos no personales, (...)"*

[21] https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en#:~:text=Data%20processing%20can%20only%20take,these%20stringent%20measures%20are%20essential

[22] Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos) (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=OJ:L_202302854)

de IoT. Aunque no define ETS ni los menciona explícitamente, el artículo 4.6 exige que las partes que comparten datos que contienen secretos comerciales acuerden medidas proporcionales de confidencialidad, estableciendo así el uso de medidas técnicas y organizativas, una disposición que alude a una solución de entorno de tratamiento seguro. En la práctica, esto permite a los titulares de datos exigir que los datos empresariales sensibles se analicen únicamente en un entorno controlado y restringido de acceso y suspender el intercambio si se vulneran las salvaguardias. Por tanto, el Reglamento de Datos respalda implícitamente los ETS como mecanismos para facilitar la portabilidad de datos protegiendo la propiedad intelectual y el conocimiento confidencial.

La legislación sectorial también puede considerarse que refleja, de alguna forma rudimentaria, los principios del modelo ETS. Por ejemplo, bajo el marco legal europeo para el sector de estadística[23] , los investigadores pueden acceder a microdatos confidenciales solo bajo condiciones estrictas (a menudo a través de centros seguros *in situ* o estructuras de instalaciones controladas a distancia); se podría decir que esto anticipa el concepto ETS formalizado posteriormente en la DGA.

B. ETS y cumplimiento de protección de datos

Un ETS es una **infraestructura que permite el acceso y el tratamiento de datos sensibles.** Además, la **gestión y operación del ETS implicará el tratamiento de datos personales para garantizar el correcto funcionamiento** del ETS y, entre otros objetivos, apoyar la responsabilidad proactiva, la privacidad y la seguridad[24].

Según lo establecido en el Artículo 1 de la DGA y en los Artículos 2.1.a) y 2.3 del EEDS, el tratamiento de datos personales dentro de un ETS debe cumplir plenamente con el RGPD. Esta aclaración confirma que el uso del ETS no modifica la asignación de roles y responsabilidades bajo el RGPD, ni exime a los responsables o encargados de sus obligaciones legales. En consecuencia, todos los principios del RGPD aplicables al responsable deben implementarse eficazmente, incluyendo la licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, integridad y confidencialidad, y, en particular, el principio de responsabilidad proactiva consagrado en el Artículo 5.2 del RGPD. Los responsables deben ser capaces de demostrar el cumplimiento de estos principios mediante medidas técnicas y organizativas adecuadas (AEPD, 2023).

La gobernanza adecuada de un ETS implica establecer mecanismos controlados para el acceso a los datos que garanticen el cumplimiento legal y la soberanía digital. Los ETS enfrentan importantes desafíos organizativos, especialmente en relación con las estructuras de gobernanza y la gestión de encargados e intermediarios. Una gobernanza eficaz es esencial para garantizar el cumplimiento de los requisitos legales de protección de datos.

Específicamente para el cumplimiento del RGPD, deberían establecerse marcos de gobernanza integrales para implementar el principio de responsabilidad proactiva, incluyendo roles,

[23] Ver:
- Reglamento (CE) nº 223/2009 del Parlamento Europeo y del Consejo de 11 de marzo de 2009 relativo a la estadística europea y por el que se deroga el Reglamento (CE, Euratom) no 1101/2008 relativo a la transmisión a la Oficina Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico, el Reglamento (CE) no 322/97 del Consejo sobre la estadística comunitaria y la Decisión 89/382/CEE, Euratom del Consejo por la que se crea un Comité del programa estadístico de las Comunidades Europeas (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32009R0223)
- Reglamento (UE) nº 557/2013 de la Comisión, de 17 de junio de 2013, por el que se aplica el Reglamento (CE) no 223/2009 del Parlamento Europeo y del Consejo, relativo a la estadística europea, en lo que respecta al acceso a datos confidenciales con fines científicos, y por el que se deroga el Reglamento (CE) no 831/2002 de la Comisión (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32013R0557)

[24] Por ejemplo, en el caso de infraestructuras informáticas que apoyan el sector sanitario para tratamientos que impliquen historiales electrónicos de salud, recetas electrónicas, etc., también es necesario gestionar los datos de los usuarios de esa infraestructura, desde los datos del personal de TI responsable del desarrollo y mantenimiento de la infraestructura, hasta los datos del personal sanitario y los propios beneficiarios del sistema sanitario, etc.

responsabilidades y mecanismos claramente definidos para garantizar operaciones seguras de tratamiento.

1. Definición de roles en los ETS

El EEDS, en su artículo 74 y su considerando (79), define claramente los roles del RGPD en las actividades de tratamiento relacionadas con los ETS de la siguiente manera:

- El OADS es el responsable de los datos personales tratados en el ETS con el fin de cumplir sus funciones conforme al reglamento EEDS.
- El OADS actúa como encargado de tratamiento del usuario de datos de salud, quién actúa como responsable de los datos electrónicos personales de salud conforme a un permiso de datos emitido en virtud del artículo 68 del EEDS.
- En este último caso, el usuario de datos de salud actúa como responsable de dichas actividades de tratamiento.
- El titular de los datos sanitarios de confianza será considerado como un encargado del usuario de datos de salud cuando proporcione datos a través de un ETS.

Tales roles no se definen en el caso más general de los ETS en el marco de la DGA, y no pueden asumirse que sean uniformes, ya que cada caso requiere una evaluación individual, contextual y detallada que tenga en cuenta las características específicas de la infraestructura definida para cada espacio de datos; aunque las asignaciones de roles establecidas por el EEDS podrían utilizarse como guía. En cualquier caso, el papel del responsable del tratamiento, incluyendo posibles situaciones de corresponsabilidad, debe estar claramente definido y documentado adecuadamente. Esto incluye la aclaración explícita de la responsabilidad de tareas como la gestión de brechas de datos, la respuesta a solicitudes de acceso a datos, la posibilidad de que los interesados ejerzan sus derechos y la provisión de información transparente a las personas.

2. Términos contractuales y asignación de responsabilidades

La identificación precisa de los roles del responsable, corresponsables y encargado, junto con las cláusulas específicas correspondientes, debe reflejarse explícitamente en los acuerdos contractuales entre todas las partes participantes en el ETS, o en cualquier legislación nacional desarrollada al respecto. Los contratos deben definir las operaciones de tratamiento permitidas, prohibir la reutilización no autorizada de datos[25] y garantizar que el proveedor del ETS actúe siguiendo únicamente instrucciones documentadas, así como en cláusulas específicas relativas a los riesgos identificados[26].

En el considerando (60) y el artículo 52.4 del EEDS se establece que *"Las medidas legales, organizativas y técnicas para preservar los derechos de propiedad intelectual e industrial o los secretos comerciales podrían incluir acuerdos contractuales comunes de acceso a datos de salud electrónicos, obligaciones específicas en el permiso de datos en relación con dichos derechos, el tratamiento previo de los datos para generar datos derivados que protejan un secreto comercial,*

[25] En el caso de utilizar servicios de intermediación de datos (definición incluida en el artículo 2.11) de la DGA), el artículo 12.a) de la DGA establece que "os proveedores de servicios de intermediación de datos no podrán utilizar los datos en relación con los que presten sus servicios para fines diferentes de su puesta a disposición de los usuarios de datos y prestarán los servicios de intermediación de datos a través de una persona jurídica distinta"

[26] Una visión general inicial puede encontrarse en la sección III.A del documento del AEPD: "Informe de conclusiones del evento de AEPD-ENISA sobre espacios de datos" [abr 2024] (https://www.aepd.es/documento/informe-de-conclusiones-aepd-enisa.pdf)

pero que sean útiles para el usuario de datos de salud o para la configuración del entorno de tratamiento seguro, de modo que el usuario de datos de salud no pueda acceder a dichos datos".

La gobernanza contractual constituye una piedra angular de la implementación de la gobernanza de un ETS. La redacción de términos y condiciones contractuales plantea consideraciones legales importantes, incluyendo las relacionadas con la asignación de responsabilidades, responsabilidad civil (*liability*), derechos de auditoría, subcontratación, gestión de incidentes y terminación. Estos contratos deben personalizarse para cada caso particular.

En este punto, es importante destacar que el acceso a los datos de salud para fines secundarios no se limita al marco del EEDS ni al uso del ETS. Como se explica en el considerando (52) del EEDS, esta regulación relativa al uso de datos secundarios es *"Sin obstaculizar ni sustituir los acuerdos contractuales u otro tipo de mecanismo existente"*.

3. Terceros y la implementación del ETS

Como se indica en la DGA, el propósito de un ETS es permitir que la entidad que la proporciona garantice el cumplimiento legal y mantenga la soberanía digital sin tener que depender de las garantías proporcionadas por los usuarios de datos. En consecuencia, cuando la entidad responsable de proporcionar el ETS (en el contexto del EEDS, el OADS) depende de terceros para la implementación u operación del ETS[27], dichos acuerdos deben estructurarse de manera que la entidad garantice el cumplimiento legal[28] y preserve la soberanía digital independientemente de cualquier garantía proporcionada por esos terceros. Es importante señalar que un tercero no asume necesariamente el papel de encargado.

De hecho, si nos remitimos de nuevo a la definición de ETS establecida en el artículo 2.20) de la DGA, se identifica la necesidad de *"permitir que la entidad encargada de proporcionar el entorno de tratamiento seguro determine y supervise todas las acciones de tratamiento, incluida la presentación, el almacenamiento, la descarga y la exportación de datos, así como el cálculo de datos derivados mediante algoritmos computacionales"* para, entre otras cosas, garantizar el cumplimiento efectivo de la legislación de la UE y, en particular, del RGPD. Esta circunstancia requiere que la entidad que proporciona el ETS (el OADS en el caso del EEDS) tenga un control genuino y efectivo sobre el ETS. De lo contrario, la finalidad del ETS se vería socavado, ya que las responsabilidades de la entidad que proporciona el ETS se trasladarían efectivamente a un tercero.

Cuando el ETS es implementado por un tercero, será aplicable el cumplimiento de los requisitos aplicables a los encargados según el artículo 28 del RGPD y, cuando corresponda, las disposiciones sobre transferencias internacionales de datos recogidas en el Capítulo V del Reglamento.

Por tanto, las responsabilidades que esta entidad tiene bajo el RGPD (en particular el OADS en el caso de los datos de salud) no pueden transferirse únicamente al tercero mediante salvaguardas contractuales como las que un propio usuario de datos podría proporcionar, ya que, en los términos en que se establecen los requisitos del EEDS y de la propia DGA, éstas no son suficientes.

La implicación de terceros intermediarios como encargados introduce consideraciones adicionales de gobernanza organizativa, ya que la selección de un encargado no puede relajar los estrictos requisitos de control que el ETS impone a los usuarios de datos. Se puede emplear un encargado para llevar a cabo las actividades de gestión del usuario de datos sin acceder a datos sensibles,

[27] Como se describe en el considerando (77) del EEDS, los ETS pueden ser gestionados por entidades externas específicamente contratadas para proporcionar las herramientas técnicas, organizativas e infraestructurales necesarias para realizar las operaciones de tratamiento requeridas.

[28] Como se indica en el considerando (7) del DGA, "creado o supervisado" (en la versión inglesa de la norma: "provided or controlled").

como datos de salud u otros, incluida la propiedad intelectual. Cuando estas entidades, que pueden incluir proveedores externos de nube o servicios, reciben la responsabilidad de tratar datos sensibles, deberían estar sujetas a un control riguroso y total por parte del OADS. Mantener la total transparencia y control en relación con estas entidades sigue siendo un desafío constante, ya que el principio de responsabilidad proactiva sigue aplicándose al responsable incluso cuando algunas actividades de tratamiento se externalizan. En consecuencia, los responsables deben implementar mecanismos efectivos de monitorización, auditoría[29] y capacidades de supervisión para verificar de forma continua que los encargados cumplan con los requisitos regulatorios aplicables.

Según los términos establecidos para los ETS, la certificación de seguridad por terceros por sí sola es insuficiente, ya que no cumple con los requisitos específicos establecidos en las normativas aplicables (específicamente, la DGA y el EEDS para datos de salud). El EEDS enfatiza la necesidad de capacidades de auditoría efectivas y control total; como se indica en elapartado II.A.1, esta noción debe interpretarse como un control efectivo, y no meramente nominal, por parte del OADS. Por tanto, las disposiciones contractuales que definen la autoridad del OADS sobre el ETS deben complementarse con medidas técnicas apropiadas que permitan ejercer eficazmente dicha autoridad en la práctica.

En este sentido, deben tenerse en cuenta dos consideraciones distintas. Primero, debe evitarse la dependencia de un solo proveedor cuando sea posible, asegurando que los componentes ETS puedan ser soportados por proveedores alternativos, reduciendo así la dependencia de un proveedor (ACM, AFM, AP, DNB & RDI, 2026). En segundo lugar, debe considerarse evitar la concentración del control técnico sobre todo el ETS en un solo tercero. Esto puede lograrse distribuyendo funciones críticas entre diferentes componentes y, cuando corresponda, diferentes proveedores, de modo que ningún tercero tenga control técnico sobre el ETS en su conjunto. Estas dos salvaguardas son complementarias, ya que la sustituibilidad del proveedor reduce la dependencia de un proveedor concreto, mientras que la distribución de la arquitectura puede reducir la concentración de control efectivo en un solo tercero. Estas medidas pueden fortalecer el control efectivo del OADS y la resiliencia del ETS, incluso en situaciones que impliquen indisponibilidad del servicio, mantenimiento, restricciones en auditorías u otras circunstancias que afecten a un proveedor individual (incluyendo incluso presiones externas no relacionadas con el propio servicio, como intereses comerciales o coerción externa).

Dado el estado actual del desarrollo tecnológico y la amplia disponibilidad de capacidad computacional escalable y competitiva en costes, se espera que los servicios en la nube se conviertan en una opción especialmente atractiva para proporcionar la infraestructura y las herramientas necesarias para realizar operaciones de tratamiento que involucren datos altamente sensibles[30].

En este contexto, un desafío central es el establecimiento de la confianza en las garantías reclamadas e implementadas por los proveedores de servicios en la nube[31] que operan los ETS. Por ello, conviene

[29] El artículo 73.3 del EEDS establece que "los organismos de acceso a datos de salud se asegurarán de que se realicen auditorías periódicas de los entornos de tratamiento seguros, también por terceros, y adoptarán medidas correctivas con respecto a cualquier deficiencia, riesgo o vulnerabilidad detectados por dichas auditorías en los entornos de tratamiento seguros".

[30] La importancia de la computación en la nube en relación con los desafíos de protección de datos queda aún más subrayada por el hecho de que los dos primeros Códigos de Conducta transnacionales del RGPD adoptados a nivel de la UE se refieren a actividades de tratamiento en la nube; véase CdC en la Nube de la UE (https://eucoc.cloud/en/home) y el CdC de CIETS (https://www.cispe.cloud/code-of-conduct/)

[31] Véase el artículo 6.30) de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32022L2555) (en adelante NIS2, por sus siglas en inglés) para la definición de "servicio de computación en la nube", término equivalente para "servicio en la nube".

mencionar que, antes de continuar, una clasificación de los servicios en la nube podría ser la de "nube pública" y "nube privada" (así como los modelos híbridos[32]), ya que la implementación y el control que se pueden ejercer sobre cada uno es clave en el contexto tratado en este documento.

Los titulares de datos, los organismos de acceso a datos y los usuarios de datos deben poder contar con garantías verificables de que las salvaguardas técnicas, organizativas y contractuales están adecuadamente implementadas y se aplican de forma consistente. Esto requiere transparencia respecto a la arquitectura del sistema y los controles de seguridad, compromisos contractuales sólidos, una asignación clara de responsabilidades y la disponibilidad de auditorías independientes. Por tanto, la confianza no se basa únicamente en promesas contractuales, sino en el cumplimiento demostrable, la supervisión continua y la capacidad de detectar, prevenir y remediar desviaciones de las salvaguardas acordadas. En particular, la decisión de confiar la operación de un ETS a un proveedor de servicios en la nube externo, en lugar de a una institución de investigación u organismo público, requiere una justificación cuidadosa. Por tanto, garantizar que "hacer lo correcto" prevalezca sobre simplemente "hacer lo que es eficiente" requiere una evaluación consciente del operador externo, junto con acuerdos legales, contractuales y técnicos sólidos que repliquen eficazmente o compensen la confianza tradicionalmente depositada en entornos de investigación institucional cuando las operaciones del ETS se delegan a proveedores externos.

Al mismo tiempo, los objetivos y limitaciones inherentes a los ETS pueden entrar en tensión con los modelos de negocio o características operativas de los grandes proveedores de servicios en la nube, incluidos aquellos designados como guardianes de acceso[33], cuya posición de poder económico y tecnológico hace que la garantía efectiva de control sea particularmente compleja[34]. La asimetría de la información y el poder de negociación que caracteriza la relación entre dichos proveedores y sus clientes pueden limitar la capacidad de estos últimos para negociar salvaguardas personalizadas o para obtener suficiente transparencia respecto a los procesos internos y las arquitecturas técnicas. De manera similar, dada la escala, opacidad y alcance global de las operaciones de estos proveedores, no se puede garantizar que las autoridades supervisoras puedan desempeñar sus responsabilidades de supervisión de manera eficaz y sin impedimentos indebidos.

Además, una lista no exhaustiva de características relevantes de un proveedor de servicios externo, ya sea categorizada como guardianes de acceso o no, que pueda aumentar el impacto de los riesgos para la protección de datos y que debe considerarse al analizar dichos riesgos, incluye lo siguiente:

- El tipo de servicios a contratar (por ejemplo, infraestructura, herramientas, servicios de escalabilidad, etc.).
- El tipo de actividades de tratamiento implementadas (gestión de identidad, gestión de usuarios de datos, etc.).
- El grado en que el OADS mantiene el control total y efectivo sobre las operaciones de tratamiento pertinentes.
- Limitaciones en la capacidad del OADS para ejercer auditorías o supervisión efectivas.
- Sumisión a regulaciones y servicios de inteligencia no comunitarios.

[32] Véase el considerando (33) de NIS2.

[33] Véanse los artículos 2.1) y 3 del Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales) (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32022R1925).

[34] Véase por ejemplo la noticia The Guardian "Amazon Web Services outage shows internet users 'at mercy' of too few providers, experts say" [20 de octubre de 2025] https://www.theguardian.com/technology/2025/oct/20/amazon-web-services-aws-outage-hits-dozens-websites-apps

- Si existen transferencias internacionales de datos personales.
- La complejidad de investigar brechas de datos o verificar el cumplimiento de la legislación aplicable, incluido el RGPD.
- El uso de datos de diferentes fuentes en la nube y los riesgos asociados a la vinculación de datos.
- Posición dominante en el mercado.
- Posible discontinuidad de los servicios.
- Dependencia del proveedor o dificultades para migrar a otro proveedor.
- La resiliencia y disponibilidad del proveedor de servicios en la nube.
- La posibilidad de acceso a claves criptográficas o de seudónimo.
- La posibilidad de acceder a la información de autenticación de los usuarios (incluidas las contraseñas).
- El alto nivel de privilegios o poder que ostenta el proveedor de servicios externo.

4. Transferencias internacionales

Deben establecerse medidas para garantizar que las transferencias a terceros países no se realicen a menos que se aprueben de forma efectiva las salvaguardas y condiciones adecuadas, conforme al RGPD. En particular, el artículo 87.2 del EEDS estipula que los datos electrónicos personales de salud *"podrán almacenarse y tratarse en un tercer país, o un territorio o uno o varios sectores específicos dentro de ese tercer país, cuando a dicho país, territorio o sector se aplique una decisión de adecuación adoptada en virtud del artículo 45 del Reglamento (UE) 2016/679"*.

Sin embargo, el cumplimiento de estos requisitos no garantiza necesariamente la soberanía digital ni el control efectivo sobre los datos y el entorno de tratamiento. Incluso cuando el tratamiento en un país fuera del EEE esté cubierto por una decisión de adecuación, la implicación de entidades o infraestructuras sujetas a una jurisdicción no perteneciente al EEE puede plantear consideraciones adicionales respecto a dicho control. Por lo tanto, el cumplimiento de los requisitos del RGPD para transferencias internacionales y la preservación del control efectivo sobre el ETS deben considerarse consideraciones relacionadas pero distintas.

En consecuencia, la ubicación y supervisión del alojamiento del ETS, así como las herramientas habilitadas para trabajar dentro del ETS, deben estar garantizadas contractualmente además de todos los temas tratados en la sección "II.B.3. Terceros y la implementación del ETS". Además, responsabilidades en caso de una brecha de datos personales (ya sea por acceso no autorizado o por la falta de disponibilidad del ETS o cualquiera de sus herramientas[35]) también debe estar claramente definido.

5. Facilitar el ejercicio de los derechos de los interesados

El ETS debe proporcionar mecanismos organizativos y técnicos adecuados para facilitar el ejercicio de los derechos de los interesados conforme al marco aplicable de protección de datos. La

[35] Publicación del blog de AEPD: "Soberanía operativa en tratamientos de datos personales" [febrero 2026] (https://www.aepd.es/prensa-y-comunicacion/blog/soberania-operativa-en-tratamientos-de-datos-personales)

implementación de dichos mecanismos debe basarse en que el tratamiento de datos para uso secundario puede descansar en bases legales distintas al consentimiento, como el cumplimiento de una obligación legal o la realización de una misión en interés público. Dependiendo de la base legal aplicable, la naturaleza del tratamiento y cualquier restricción o derogación aplicable, el ETS debe apoyar eficazmente, cuando sea aplicable, las solicitudes relativas al acceso, rectificación, borrado, restricción del tratamiento, objeción y otros derechos relevantes del interesado. Esto puede incluir interfaces dedicadas para la presentación y seguimiento de solicitudes, mecanismos para verificar/evaluar las solicitudes relevantes, así como procedimientos para implementar las acciones correspondientes, incluyendo cuando los datos ya hayan sido incorporados en conjuntos de datos derivados o resultados analíticos. Cuando un derecho esté restringido o no se aplique bajo el marco legal aplicable, el procedimiento correspondiente debe prever la evaluación y comunicación adecuadas de los motivos aplicables.

6. Privacidad desde el diseño y por defecto

Más allá del sector sanitario, los ETS deberían estar regidos por marcos de gobernanza robustos que integren los principios de protección de datos desde el diseño y por defecto, tal como se consagra en el artículo 25 del RGPD. En este contexto, la distinción conceptual entre "compartir datos" y "acceso a datos" se vuelve especialmente relevante. Aunque el intercambio de datos tradicionalmente implica la transferencia de conjuntos de datos a los usuarios, el acceso a los datos (especialmente en la diferenciación explícita en la DGA) enfatiza la reutilización controlada sin pérdida de control por parte del titular de los datos[36]. Esta distinción es especialmente relevante para la reutilización de ciertas categorías de datos protegidos o sensibles en manos de organismos del sector público, ya que sustenta la confianza, la transparencia y el ejercicio efectivo de los derechos del interesado, que son objetivos centrales del marco de gobernanza de datos de la Unión[37]. Desde la perspectiva de la protección de datos, los ETS deben operacionalizar principios clave del RGPD, como la limitación de la finalidad, la minimización de datos, así como la integridad y confidencialidad, desde el diseño y por defecto[38].

El EEDS exige el cumplimiento del RGPD tanto para usos primarios como secundarios de datos[39], con especial énfasis en las actividades de tratamiento realizadas dentro de un ETS[40]. Los artículos 52.2 a 52.5 del EEDS reconocen que el cumplimiento formal de los requisitos del artículo 73 del EEDS podría no ser suficiente para cualquier dato electrónico de salud que contenga contenido o información protegida por derechos de propiedad intelectual o secretos comerciales. El artículo 52.2 establece que podrían estar *"partes de los conjuntos de datos se ven afectadas y justificarán la necesidad de protección específica de los datos"*, extendiéndose más allá de los datos personales para incluir otros datos sensibles.

Por lo tanto, incluso en el caso de un ETS que cumpla con los requisitos del artículo 73 del EEDS, los OADS deben tener en cuenta el hecho de que varios conjuntos de datos necesitan protección especial:

---

[36] También es destacable que este concepto de conceder acceso a datos sin transferirlos se refleja explícitamente en otra pieza clave de la legislación europea, concretamente el Reglamento de Inteligencia Artificial. El considerado (69) de este reglamento enfatiza que, además de garantizar el cumplimiento de los requisitos de protección de datos durante todo el ciclo de vida de un sistema de IA, debe prestarse especial atención a los enfoques tecnológicos que eviten la transmisión de datos. Específicamente, el considerado destaca "*el uso de una tecnología que permita llevar los algoritmos a los datos y el entrenamiento de los sistemas de IA sin que sea necesaria la transmisión entre las partes ni la copia de los datos brutos o estructurados",* reforzando así la relevancia de modelos basados en acceso que preservan el control de los datos mientras facilitan la innovación.

[37] Considerando (5) de la DGA.

[38] Artículo 73.2 del EEDS.

[39] Artículo 1 y considerando (5) del EEDS

[40] Considerando (77) del EEDS

- Que dicha protección se seleccione para hacer frente a amenazas que surjan desde diversos puntos de vista: secretos comerciales, propiedad intelectual y protección de datos personales.
- Que las medidas de protección pudieran ser legales, organizativas y técnicas. Que los riesgos debían evaluarse desde puntos de vista tan diferentes.
- Y, finalmente, la evaluación puede llegar a establecer que el tratamiento conlleve un riesgo serio e irremediable de infringir derechos de propiedad intelectual o secretos comerciales, por lo que se deberá denegar el acceso a los datos.

Es importante enfatizar la importancia de este asunto. Por ejemplo, un posible uso secundario podría implicar el desarrollo e implementación de políticas de salud pública mediante el tratamiento de datos personales. Dependiendo de los riesgos asociados a dichas políticas, como los que surgen durante una pandemia, debe asegurarse la disponibilidad y la resiliencia (como exige el artículo 32 del RGPD) frente a amenazas físicas, digitales o legales. En este caso, podría surgir un problema de disponibilidad, por ejemplo, debido a un fallo en el suministro eléctrico, en cuyo caso habría que implementar las medidas necesarias. Sin embargo, otro posible riesgo de disponibilidad podría derivar de restricciones legales de uso, como las relacionadas con secretos comerciales, derivadas de una implementación incorrecta de las salvaguardas que el ETS debe establecer respecto a los secretos comerciales y derechos de propiedad intelectual.

Por esta razón, los OADS deben prestar especial atención a garantizar que las salvaguardas requeridas se implementen adecuadamente desde el diseño.

Como se describe en el apartado anterior, un ETS debe considerarse como una infraestructura que facilita el acceso y reutilización responsable de los datos para garantizar el cumplimiento de los requisitos de protección de datos personales. Por tanto, los desafíos técnicos para implementar dicho ETS, desde la perspectiva de la protección de datos, están estrechamente ligados al cumplimiento de las estrictas condiciones de su definición de conformidad al artículo 2 de la DGA, así como al artículo 73 del EEDS.

Sin embargo, todavía no existe un entendimiento común (y mucho menos una estandarización) sobre cómo debe implementarse un ETS en la práctica. Se conocen algunos elementos que se han utilizado[41] para implementar un ETS y todos enfatizan que el acceso a los datos, así como la exportación de datos, están estrictamente controlados[42].

Primero, se deben construir ETS sobre ***principios de seguridad de confianza cero***, donde ningún usuario, dispositivo, aplicación o carga de trabajo es confiable por defecto, independientemente de si opera dentro o fuera del perímetro de la red (NIST, Zero-trust architecture, 2020). Esto se debe a que las arquitecturas de confianza cero refuerzan la resiliencia frente a amenazas cibernéticas cada vez más sofisticadas y aceleradas por IA (ENISA, ENISA's view on Cybersecurity in the Frontier AI Era, 2026). Este enfoque incluye una verificación continua de identidad[43], acceso de privilegios mínimos, autenticación fuerte y monitorización continua para limitar los movimientos laterales.

Para ello, es importante señalar que implementar un ***ETS no es solo una cuestión de seguridad aplicada a la protección de datos***; también se asegurará que ***todos los principios de protección***

[41] Véase https://healthycloud.eu/workshop-elements-of-secure-processing-environments/

[42] La importancia de este asunto se ilustra aún más con el trabajo de la TEHDAS2 Joint Action (https://tehdas.eu/project/), financiada por la UE, que ha desarrollado muy recientemente directrices comunes y especificaciones técnicas para apoyar la implementación armonizada del EEDS, incluyendo especificaciones técnicas que definen los requisitos funcionales y de seguridad fundamentales para los ETS y proporcionan un marco común para su implementación entre los Estados miembros.

[43] Esto es independientemente de si el acceso se concede por un periodo específico (sujeto a renovación) a un investigador o a una institución de investigación, ya que, en cualquier caso, la identidad de la persona que accede al sistema debe ser verificada en todo momento.

de datos, como por ejemplo, la minimización de datos y la limitación de finalidad, ***están efectivamente implementados***. Desde la perspectiva de la ingeniería de protección de datos, un ETS debe abordar tanto la protección de los datos que entran en el entorno de tratamiento (*privacidad de entrada*) y la protección de los individuos contra la identificación individual de los resultados publicados por el medio ambiente (*privacidad de salida*) (ENISA, Engineering Personal Data Sharing, 2024). De hecho, estos principios deben estar presentes en todas las fases del tratamiento. En el caso de un OADS bajo el EEDS que debe implementar un ETS para el tratamiento de datos electrónicos de salud (como la recepción, combinación, preparación y compilación de los datos solicitados a los titulares de datos de salud, así como la pseudonimización o anonimización de los datos), para proporcionar acceso a usuarios de datos estrictamente autorizados, el OADS debería considerar, desde la fase de diseño del ETS, y obviamente mucho antes de que comience cualquier tratamiento, si existen técnicas de ingeniería de protección de datos que puedan utilizarse como facilitadores para asegurar que el OADS pueda apoyar plenamente las tareas deseadas sin tener acceso a los datos sanitarios originales. Si éste es el caso, entonces queda claro que el ETS debe implementarse en consecuencia, ya que por estos medios se garantizará que se cumplan los principios mencionados de protección de datos.

a) Aplicación del principio de precaución desde el diseño

Dadas las características específicas de los ETS, la novedad de su uso y la finalidad para la que se implementan (es decir, facilitar el tratamiento de datos especialmente sensibles), así como los riesgos que pueden identificarse en relación con los derechos y libertades derivados de dicho tratamiento, merece la pena tomarse un momento para reflexionar sobre la aplicación del principio de precaución[44] desde el diseño. Este enfoque se describe en este informe como una consideración metodológica importante y no debe entenderse como un requisito regulatorio específico derivado directamente de la DGA, EEDS o RGPD.

Por lo tanto, una tarea inicial es identificar casos que involucran infraestructuras similares que hayan enfrentado situaciones críticas y analizarlos retrospectivamente para anticipar dichas situaciones. Algunos ejemplos podrían incluir:

- Casos de indisponibilidad del servicio derivados de la detección de posibles infracciones de la legislación de la UE (ya sea mediante auditorías internas[45] o incluso mediante tecnologías innovadoras que exponen vulnerabilidades en el servicio). En tales casos, debe existir un plan de respuesta adaptado a la gravedad de las situaciones que puedan surgir; incluso puede ser necesario tener la opción de acceder a los datos a través de otro ETS completamente independiente (ya sea otra infraestructura u otro operador) para garantizar la continuidad del servicio.

[44] En su "Comunicación de la Comisión sobre el recurso al principio de precaución" (COM(2000)1 final) [febrero de 2000] (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52000DC0001), la Comisión Europea declaró que: "*Aunque en el Tratado sólo se mencione explícitamente el principio de precaución en el terreno del medio ambiente, su ámbito de aplicación es mucho más amplio. Este principio abarca los casos específicos en los que los datos científicos son insuficientes, no concluyentes o inciertos, pero en los que una evaluación científica objetiva preliminar hace sospechar de que existen motivos razonables para temer que los efectos potencialmente peligrosos para el medio ambiente y la salud humana, animal o vegetal pudieran ser incompatibles con el alto nivel de protección elegido*". En este sentido, el EDPS ha destacado la idoneidad de aplicar el principio de precaución como medida preventiva en el caso de operaciones de tratamiento con un impacto significativo o cuando exista incertidumbre sobre cuál podría ser ese impacto (véase "EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data" [19 diciembre 2019] https://www.edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf).

[45] Véase por ejemplo la noticia The Guardian "Office for National Statistics has 'deep-seated' problems and needs an overhaul" [26 de junio de 2025] https://www.theguardian.com/uk-news/2025/jun/26/review-calls-for-10m-overhaul-of-the-office-for-national-statistics

- Casos en los que un usuario de datos puede extraer información detallada de tablas, modelos o estadísticas que, directa o indirectamente, revelan información confidencial (por ejemplo, mediante tablas con atributos demasiado granulares, coeficientes que permiten inferir registros individuales, modelos demasiado específicos o mapas con resolución espacial excesiva). En tales situaciones, revisar los resultados antes de que finalmente estén disponibles para el usuario es crucial para identificar estos problemas e implementar mecanismos de anonimización antes de permitir que el usuario descargue los datos.

- Casos en los que se intenta reconstruir información individual mediante ataques de inferencia (por ejemplo, ejecutando la misma consulta repetidamente, comparando resultados con ligeras modificaciones en las consultas, mediante modelos sucesivos, etc., e incluso cualquiera de estos mediante intentos coordinados entre dos usuarios diferentes). Esta situación podría llevar a la implementación de una revisión manual antes de poner los datos a disposición del usuario y comprobar sus solicitudes previas; o imponiendo un límite al número de consultas que puede realizar un usuario de datos; o imponiendo obligaciones específicas de divulgación de datos a los usuarios.

- Casos de incumplimiento por parte de los usuarios de datos (por ejemplo, uso indebido de credenciales, compartición de cuentas, subida de material no autorizado o incumplimiento de los términos de uso). Estas situaciones podrían minimizarse mediante un seguimiento más detallado de la actividad de los usuarios, lo que podría llevar a la revocación temporal o permanente del acceso e incluso la notificación a la institución de investigación para la que trabaja el usuario de datos.

- Casos de incidentes cibernéticos que generalmente resultan en indisponibilidad de servicios y pueden ser causados, por ejemplo, por *ransomware*, fallos de red o vulnerabilidades de infraestructura. En estos casos, la implementación de medidas de ciberseguridad es un paso fundamental.

- Casos en los que los modelos de IA capaces de detectar vulnerabilidades del sistema se ejecutan en entornos controlados, comprometiendo potencialmente la integridad de la infraestructura y las salvaguardas implementadas[46], lo que puede provocar graves brechas de seguridad con impacto en la protección de datos.

b) Marco de los "Five Safes"

El marco de *"Five Safes"*[47] (Ritchie, 2017) establece un enfoque integral que abarca el diseño y la planificación de soluciones basadas en datos. Se basa en un modelo de protección en capas con cinco "dimensiones de control", conocidas como los *"Five Safes"*, donde cada dimensión debe analizarse colectivamente. Al abordar una pregunta simple pero crítica para cada capa, el marco permite el desarrollo de una metodología estructurada y sistemática. Una fortaleza clave de este enfoque es que múltiples capas deben fallar simultáneamente para que ocurra una brecha real de datos, mitigando así el posible impacto.

[46] Véase Hugging Face "Anatomy of a Frontier Lab Agent Intrusion: A Technical Timeline of the July 2026 Incident" [27 de julio de 2026] https://huggingface.co/blog/agent-intrusion-technical-timeline

[47] Página web oficial del marco de los "Five Safes": https://fivesafes.org/

Safe projects	¿Es apropiado este uso de los datos?	Controles de gestión
Safe people	¿Se puede confiar en que los investigadores lo usen de manera adecuada?	
Safe settings	¿La instalación de acceso limita el uso no autorizado?	
Safe data	¿Existe un riesgo de divulgación en los propios datos?	Controles estadísticos
Safe outputs	¿Los resultados estadísticos no son reveladores?	

Figura 1: Las cinco dimensiones de control del marco de los *"Five Safes"* y las preguntas que plantean. (Ritchie, 2017)

Este enfoque se combina luego con la metodología de evaluación de riesgos propuesta en el siguiente apartado, incluyendo un breve ejemplo en el caso de uso descrito en la sección "IV. Un escenario de caso de uso".

7. Gestión de riesgos de protección de datos

A la hora de definir los principales procesos de gestión que implementan un modelo de gobernanza, la gestión de riesgos desempeña un papel clave. La gestión de riesgos implica la identificación previa de amenazas, seguida de la evaluación de sus niveles de riesgo inherentes para los derechos y libertades de las personas físicas, así como la selección de estrategias de gestión de riesgos basadas en medidas organizativas, legales y técnicas.

En relación con la gestión de riesgos, debe subrayarse la obligación de realizar una Evaluación de Impacto en Protección de Datos (EIPD)[48] conforme al artículo 35 del RGPD. Las EIPD permiten a los responsables identificar y evaluar sistemáticamente los riesgos asociados al tratamiento de datos personales e informar decisiones sobre la implementación de salvaguardas técnicas y organizativas adecuadas basadas en un enfoque basado en riesgos. Dado que los ETS suelen estar destinados a actividades de tratamiento de alto riesgo[49], generalmente se requiere la realización de una EIPD.

En base a los resultados del EIPD, las entidades que actúan como responsables de los tratamientos realizados dentro de un ETS deben seleccionar e implementar técnicas adecuadas de ingeniería de protección de datos antes de que se realice el tratamiento. Medidas como la minimización de datos, la anonimización, el cifrado de datos en reposo, en tránsito y, cuando sea técnicamente factible, en uso, así como controles de acceso estrictos, deben evaluarse cuidadosamente en cuanto a su implementación efectiva, con el objetivo de priorizar la protección de datos preservando la utilidad de los datos para los fines de tratamiento previstos. Además, se requieren medidas adecuadas para facilitar el ejercicio de los derechos de los interesados. La selección y el despliegue de tales medidas deben justificarse a la luz de la gravedad del impacto y probabilidad de los riesgos identificados.

Dentro del marco del EEDS, los ETS deben abordar amenazas relacionadas con la protección de datos y la privacidad, además de secretos comerciales y estadísticos, propiedad intelectual e industrial, seguridad nacional u otros requisitos nacionales. La gestión de riesgos para estos requisitos no debe llevarse a cabo de forma independiente. Es esencial que exista un único marco de gobernanza (con características específicas), junto con la coexistencia de un enfoque unificado de gestión de riesgos que integrando todos los requisitos. De lo contrario, las medidas resultantes pueden ser ineficaces, ineficientes y no garantizar el cumplimiento de los principios de protección de datos.

A la luz de lo anterior y dentro del alcance de este documento guía, esta sección identifica características específicas de los ETS y factores de riesgo relevantes que deben tenerse en cuenta al

[48] Considerando (15) de la DGA.

[49] Grupo "Protección de Datos" del Artículo 29. Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679. (WP 248 rev.01). Adoptado el 4 de abril de 2017. Revisadas por última vez y adoptadas el 4 de octubre de 2017. https://ec.europa.eu/newsroom/article29/items/611236

identificar y gestionar riesgos de protección de datos y privacidad en cada caso concreto. Gestionar riesgos de privacidad incluye evaluar el nivel de riesgo e identificar medidas para mitigar el riesgo inicial.

Por lo tanto, se enumera a continuación varios factores de riesgo específicos de ETS que deben tenerse en cuenta.

- Tratamientos de datos a gran escala[50]. El gran volumen de datos tratados, combinado con las técnicas actualmente disponibles en el mercado, puede reducir la eficacia de los mecanismos de anonimización, aumentando así la probabilidad de reidentificación.
- Características específicas de los datos tratados. La naturaleza particular y la sensibilidad de los datos pueden implicar un mayor impacto potencial en los interesados, dependiendo de las categorías de datos involucradas.
- Inferencia de datos personales inesperados. Existe la posibilidad de inferir nuevos datos personales que no se previeron dentro del alcance de la investigación y que justifiquen el acceso a esos datos.
- Las características específicas de los usuarios que desean acceder a estos datos. En cada contexto específico de la implementación de un ETS, debe evaluarse el tipo de usuarios que se espera que accedan a los datos debido al posible impacto en el nivel de riesgo asociado al tratamiento, así como a otras consideraciones relevantes de protección de datos, como posibles transferencias a terceros países.
- Acceso ilegal o no autorizado a datos personales. La posibilidad de acceso a datos personales sin la debida autorización o en violación de las normas aplicables.
- Filtraciones masivas de datos[51]. En caso de brechas de datos personales a gran escala, pueden producirse consecuencias significativas para los interesados.

Además, se ha identificado un conjunto de factores de riesgo de alto nivel que también deben tenerse en cuenta:

- Cambios en el marco legal. Los desarrollos relacionados, por ejemplo, con transferencias internacionales de datos, pueden tener un impacto significativo en las infraestructuras que implementan espacios de datos.
- Tensiones internacionales y desarrollos geopolíticos. Conflictos como la guerra en Ucrania, incluyendo interrupciones en los servicios prestados por empresas estadounidenses de datos en ciertas jurisdicciones, o la reciente guerra en Oriente Medio, donde se han reportado brechas de datos a gran escala que afectan bases de datos genéticas, ilustran riesgos sistémicos más amplios para la protección de datos.
- Tecnologías disruptivas. La aparición de tecnologías disruptivas, como la computación cuántica (ENISA, Post-Quantum Cryptography: Current state and quantum mitigation, 2021) y estrategias como HNDL[52], puede socavar las salvaguardas técnicas y organizativas existentes.

[50] Grupo "Protección de Datos" del Artículo 29. Directrices sobre los delegados de protección de datos (DPD) (wp243rev.01 Adoptadas el 13 de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017. Páginas 7-8. https://ec.europa.eu/newsroom/article29/items/612048

[51] AEPD. "Orientaciones para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas de datos personales" [marzo 2023] (https://www.aepd.es/documento/orientaciones-riesgo-brechas-masivas-aapp.pdf)

[52] Harvest now, decrypt later (https://en.wikipedia.org/wiki/Harvest_now,_decrypt_later)

- Los modelos de "IA frontera" suponen una amenaza creciente de ciberseguridad y privacidad al acelerar drásticamente la velocidad y sofisticación de los ataques, comprimir el tiempo desde la detección de vulnerabilidades hasta su explotación y desafiar las capacidades tradicionales de defensa (ENISA, ENISA's view on Cybersecurity in the Frontier AI Era, 2026).

- La posibilidad de quedarse atado a proveedores con sede en terceros países[53] en sectores críticos, como la sanidad, puede afectar al modelo de bienestar de la UE, así como a aspectos económicos e incluso de seguridad.

- Crisis contextual. Precedentes históricos, como las guerras balcánicas y la inestabilidad geopolítica, ponen de manifiesto el riesgo de posibles colapsos del Estado de derecho, que podrían tener graves consecuencias para la protección de datos y los derechos fundamentales.

Como se expone en los Considerandos (20) y (4) de la DGA, los datos personales podrían estar inextricablemente vinculados a datos no personales que podrían incluir datos protegidos por secretos comerciales o derechos de propiedad intelectual. En consecuencia, cualquier amenaza a los conjuntos de datos, ya sea derivada de secretos comerciales, de propiedad intelectual o incluso riesgos para la seguridad nacional vinculados a la sensibilidad de los datos que se están tratando, puede representar una amenaza directa para la protección de datos. Estos riesgos deben considerarse de forma holística al realizar una evaluación de riesgos de protección de datos. De hecho, la evaluación de riesgos correspondiente debe reflejar la naturaleza, escala y sensibilidad de los datos en cuestión y no debe limitarse a amenazas dirigidas por actores convencionales o de baja capacidad. En particular, en función del contexto y los riesgos relevantes, el modelo de amenaza puede necesitar considerar actores sofisticados y bien dotados de recursos, incluyendo potencialmente actores a nivel estatal y servicios de inteligencia. Especialmente en los casos en que tales amenazas se consideren razonablemente previsibles, cualquier salvaguardia legal y contractual debe complementarse necesariamente con medidas técnicas sólidas.

Debe realizarse un ejercicio específico para analizar los riesgos de privacidad en cada implementación particular de un ETS, teniendo en cuenta los casos de uso autorizados. También deben analizarse todos los riesgos identificados de protección de datos en función de su impacto derivado en otros derechos y libertades fundamentales.

Todas estas consideraciones expuestas aquí —aparte del hecho de que puede haber otras circunstancias específicas a tener en cuenta en cada caso— podrían incluso llevar a la necesidad de implementar diferentes ETS bajo el control del OADS, dependiendo del tipo de usuarios, del tipo de proyectos a llevar a cabo u otras circunstancias relevantes.

Todos los riesgos identificados requieren la implementación de medidas adecuadas para reducir el nivel de riesgo para la protección de datos personales. De acuerdo con los principios de protección de datos, dichas medidas deben aspirar a garantizar la lealtad, la desvinculabilidad, la transparencia y la intervención, junto con objetivos de (ciber)seguridad como la confidencialidad, integridad, disponibilidad y resiliencia.

Se puede realizar una evaluación de riesgos para cada caso basada en la metodología de Modelado de Amenazas a la Privacidad y Protección de Datos LIINE4DU (AEPD, Introducción a LIINE4DU 1.0: Una nueva metodología para el modelado de amenazas para la privacidad y la protección de datos, 2024), que se basa en un modelo categorizado en las siguientes diez categorías de amenazas:

[53] Véase "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la soberanía tecnológica europea, acompañada de una Estrategia de Código Abierto de la UE" (COM(2026) 503 final) (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52026DC0503)

- Vinculación/ *Linking*: Esta amenaza implica relacionar diferentes datos o actividades del interesado para obtener más información sobre el interesado o sobre un grupo de personas al que pertenece.
- Identificación/ *Identifying*: Esta amenaza implica conocer la identidad de un interesado directamente (a través del tratamiento de información identificable o de filtraciones, por ejemplo) o indirectamente (a través de la deducción o la inferencia, por ejemplo).
- Inexactitud/ *Inaccuracy*: Esta amenaza implica el uso de datos obsoletos, erróneos, incompletos, sesgados o de baja calidad que pueden llevar a decisiones o acciones incorrectas, y a causar inconvenientes o incluso daños al interesado.
- No repudio/ *Non-repudiation*: Esta amenaza implica la capacidad de atribuir una característica o actividad al interesado (algo que sabe, que es, que hace, etc.) cuando esto implica un impacto para sus derechos y libertades fundamentales.
- Exclusión/ *Exclusion*: Esta amenaza implica no atender adecuadamente a un interesado, obstaculizando involuntaria o deliberadamente su participación o implicación en la vida física o digital.
- Detección/ *Detecting*: Esta amenaza implica deducir la existencia de datos o la implicación del interesado en una actividad a través de la observación.
- Brecha de datos/ *Data Breach*: Esta amenaza implica la destrucción, pérdida, alteración, divulgación no autorizada o acceso a datos personales por error, personas de confianza maliciosas o ciberataques.
- Engaño/ *Deception*: Esta amenaza implica intentar influir, coaccionar o manipular intencionalmente al interesado para que tome decisiones no intencionadas, involuntarias y potencialmente dañinas, a menudo en contra de sus propios intereses.
- Divulgación/ *Data Disclosure*: Esta amenaza implica recoger, almacenar, tratar o compartir/ transferir datos personales en exceso.
- Desconocimiento y falta de capacidad para intervenir/ *Unawareness and Unintervenability*: Esta amenaza implica demostrar de manera insuficiente el cumplimiento o informar, involucrar o empoderar a los interesados en el tratamiento de sus datos personales también de manera insuficiente.

Por último, debe enfatizarse que se requiere el cumplimiento del RGPD independientemente del nivel de riesgo asociado a una determinada actividad de tratamiento. Sin embargo, en el contexto del EEDS, el tratamiento con fines secundarios suele implicar tratamientos a gran escala de categorías especiales de datos personales, lo que conlleva que, conforme al artículo 35.3.b) del RGPD, la realización de una Evaluación de Impacto en la Protección de Datos (EIPD) es obligatoria.

En general, integrar correctamente los principios de protección de datos en las prácticas de datos puede ayudar a mitigar los riesgos de mal uso de los datos mientras se crean las condiciones para la innovación responsable, la colaboración y la creación de valor, así como fomentar la confianza entre los individuos (IDGDPT Berlin Group, 2024).

III. CONSIDERACIONES Y MEDIDAS DE IMPLEMENTACIÓN

Sobre la base del análisis anterior, un ETS deberá permitir un tratamiento seguro y respetuoso con la privacidad de los datos personales dentro de un marco legal y técnicamente robusto, superando así con creces un marco tradicional de seguridad. Aunque debe adoptarse un enfoque basado en el riesgo, dependiendo del contexto específico, al decidir cómo se implementará un tratamiento específico dentro del marco de un ETS, siempre debe considerarse que el tratamiento en cuestión debe considerarse de alto riesgo en cuanto al impacto para los derechos y libertades de las personas. Esto, a su vez, requiere algunos requisitos concretos que se establecerán como mínimos, y que se espera que siempre estén vigentes. Estos requisitos derivan de la definición del ETS junto con las aplicaciones relevantes (esperadas) de los ETS según el marco legal vigente, así como con requisitos bien conocidos y establecidos en el contexto de los marcos de gestión de riesgos de seguridad y privacidad (véase, por ejemplo, (NIST, Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5, 2020)).

A. Medidas que se deben aplicar

En este apartado el objetivo es exponer aquellas medidas que podrían considerarse como el establecimiento de un "umbral inferior"; por tanto, el cumplimiento de estos requisitos es necesario pero no necesariamente adecuado. En otras palabras, las medidas incluidas en este catálogo reflejan el nivel mínimo de medidas de protección esperado para el funcionamiento de un ETS, teniendo en cuenta la seguridad y la protección de datos desde el diseño y las obligaciones por defecto aplicables a su función. Sin embargo, su inclusión no debe entenderse como que cada medida individual esté prescrita en términos idénticos o explícitos por una disposición legal específica. Más bien, las medidas traducen los requisitos aplicables en salvaguardas concretas que deben implementarse adecuadamente. Además, la lista aquí establecida describe las medidas en términos generales, requiriendo, en cada caso específico, una implementación adecuada en línea con las circunstancias particulares de ese caso. Estas medidas se presentan de manera tecnológicamente neutral, aunque se proporcionan algunos ejemplos ilustrativos para mayor claridad.

Las medidas propuestas aquí incluyen tanto las relacionadas con operaciones de tratamiento asociadas al funcionamiento del propio ETS, como aquellas directamente relacionadas con los tratamientos soportados por esta infraestructura; en muchos casos, estas medidas cumplirán ambos propósitos, dado que, por ejemplo, la gestión de identidad, los controles de acceso y los registros de acceso son operaciones presentes en ambos tipos de tratamiento, aunque en distintos grados.

1. Gobernanza y responsabilidad proactiva

1. Desarrollo y aplicación de políticas.
2. Mecanismo de autoexclusión (*opt-out*). En el caso de tratar datos sanitarios para uso secundario, se implementarán mecanismos para ejercer el derecho a autoexcluirse, así como para revertirlo.
3. Gestión del consentimiento. En los casos en que la base legal para el tratamiento sea el consentimiento, se implementarán mecanismos que permitan la retirada del consentimiento en cualquier momento.
4. Se implementarán mecanismos para garantizar la trazabilidad de los flujos de datos y conjuntos de datos, con el fin de garantizar la eficacia del ejercicio de los derechos de los interesados.
5. Establecer un enfoque documentado basado en riesgos para determinar los controles y procesos de seguridad específicos que se deben implementar.

6. Implementación de procesos para la evaluación ética y científica del proyecto mediante los cuales el usuario de datos desee acceder al ETS, incluyendo justificación para acceder a datos personales no anonimizados[54] cuando sea aplicable, una evaluación de la necesidad y proporcionalidad, y una revisión de cumplimiento del RGPD, incluyendo EIPD.

7. Procedimientos eficaces bien establecidos para gestionar el acceso de los usuarios y las responsabilidades relevantes. Criterios claros[55] para conceder permisos de acceso, de modo que los usuarios no tengan acceso ilimitado. Los permisos deben concederse tras un proceso exhaustivo de revisión.

8. Implementación de mecanismos para facilitar la revisión de los datos incluidos en una solicitud de descarga con el fin de evaluar el riesgo de reidentificación en el conjunto de datos[56] y así garantizar que los usuarios de datos solo puedan descargar datos no personales del ETS.

9. Mapeo de cumplimiento normativo y verificación continua mediante monitorización y auditoría periódicas.

10. Panel de cumplimiento y métricas.

11. Paneles e interfaces de ejercicio de derechos.

12. Establecer métodos para garantizar que se respeten las normas de soberanía de datos de la UE.

13. Proporcionar la información necesaria del ETS al responsable en los casos en que la entidad responsable del ETS actúe como encargada.

14. Participación del Responsable de Protección de Datos (DPD), o asesores de protección de datos, en todas las etapas del ETS (desde la planificación y desarrollo hasta su implementación, operación e incluso desmantelamiento).

2. Gestión de datos

15. Creación de catálogos[57] de datos y conjuntos de datos disponibles, que serán interoperables.

16. Prevención de pérdida de datos y divulgación no autorizada (esto puede incluir tecnologías de Prevención de Pérdida de Datos (*Data Loss Prevention*, DLP) y/o medidas técnicas u organizativas equivalentes).

17. Garantizar que solo se pongan a disposición dentro del ETS datos adecuados, relevantes y necesarios para los fines autorizados del tratamiento (minimización de datos).

18. Desidentificación efectiva de datos (esto está relacionado con técnicas efectivas de anonimización o posiblemente seudonimización y puede incluir medidas como la eliminación o transformación de identificadores directos, separación de identificadores de variables analíticas, generalización o supresión de atributos, agregación de valores, incluidos valores poco frecuentes, o posiblemente otras técnicas de anonimización u otras técnicas de mejora de la privacidad).

[54] Artículo 67.2.e) del EEDS.

[55] Artículo 68.12 del EEDS.

[56] Esto puede implicar que se revisen, entre otras cosas, celdas que contienen (o que puedan dar lugar) valores atípicos, atributos demasiado granulares, combinaciones peligrosas de variables, coeficientes que permiten inferencias, gráficos demasiado detallados y modelos que podrían revelar información individual. Si se identifica un riesgo, el resultado deberá ser modificado, agregado, eliminado o simplemente no autorizado para su descarga.

[57] La identificación y marcado de ciertos datos y conjuntos de datos es un caso de particular interés para los datos mencionados en los Artículos 51.4 y 52.2 del EEDS.

19. Aplicación de tecnologías estadísticas y de mejora de la privacidad siempre que sea posible.

20. Implementación de mecanismos para asegurar un periodo limitado de disponibilidad de los datos dentro del ETS.

21. Segregar datos y conjuntos de datos según su sensibilidad, finalidad, requisitos de acceso u otras características de riesgo relevantes, incluyendo el almacenamiento o tratamiento separado de datos particularmente sensibles, según se identifique en el catálogo, cuando corresponda.

22. Cifrado de datos en reposo para evitar accesos no autorizados, garantizando la confidencialidad incluso si los sistemas de almacenamiento están comprometidos.

3. Gestión de identidad y control de accesos

23. El acceso debe limitarse a personas autorizadas según lo definido por los permisos de datos correspondientes, que incluirán el flujo de trabajo aprobado para cada caso.

24. Verificación previa de la identidad del usuario (por ejemplo, el centro de investigación), así como de la persona física que actúa en su nombre.

25. Principio de privilegio mínimo (*principle of least privilege*, PoLP). El acceso debe restringirse al nivel mínimo necesario y concederse solo durante el menor tiempo necesario para completar la tarea, asegurando que cada tratamiento sea proporcional y esté limitado por su finalidad.

26. Firma de acuerdos de confidencialidad, protección de datos y uso aceptable entre la entidad responsable de proporcionar el ETS y el usuario de datos[58].

27. Revocación inmediata del acceso tras la finalización del proyecto.

28. Uso de métodos fuertes de identificación y autenticación del usuario (por ejemplo, mediante esquemas seguros de autenticación multifactor (*multi-factor authentication*, MFA), certificados, etc.).

29. Revisión periódica de los permisos de acceso.

4. Seguridad física

30. El acceso a las instalaciones del ETS debe ser controlado y verificado físicamente (por ejemplo, mediante el uso de acreditaciones de seguridad).

31. Locales seguros y segregados con roles definidos y políticas de acceso para evitar accesos físicos no autorizados a dispositivos y datos.

32. Implementación de mecanismos para facilitar el despliegue de las salvaguardas necesarias para cada acceso permitido.

5. Seguridad de redes y comunicaciones

33. Solo se pueden descargar datos no personales o suficientemente anonimizados desde el ETS.

34. Los flujos masivos de datos deben detectarse, auditarse y, de ser necesario, cancelados automáticamente.

[58] Como establece el Artículo 68.12 del EEDS: "Con el fin de reducir los costes y tasas, el OADS también podrá proponer al usuario de datos de salud que almacene el conjunto de datos en un sistema de almacenamiento con capacidades reducidas. Estas capacidades reducidas no deberán afectar a la seguridad del conjunto de datos tratado."

35. Los flujos de datos deben limitarse en el corto y en el largo plazo y estar sujetos a un procedimiento especial.

36. Los datos entrantes deben enrutarse a través de entornos de cuarentena para verificar su autenticidad.

37. Todas las transferencias de datos hacia el SPE y dentro de él deben realizarse de forma segura, utilizando técnicas criptográficas de última generación (con procesos adecuados de gestión de claves) para protegerlas contra el espionaje y las modificaciones no autorizadas. Esto también implica la aplicación de medidas estrictas de seguridad de red (como, por ejemplo, la segmentación de la red o el filtrado del tráfico).

6. Seguridad de sistemas y aplicaciones

38. Los sistemas deben ser reforzados (por ejemplo, endurecimiento del sistema operativo, lista blanca de aplicaciones).

39. Evitar la ejecución o manipulación no autorizada de código.

40. Protección antimalware para detectar, prevenir y eliminar software malicioso como virus y ransomware para proteger sistemas y datos.

41. Cada entorno de tratamiento (instancia del ETS) debe estar separado y aislado de diferentes entornos (para evitar accesos cruzados no autorizados o fugas de datos entre diferentes aplicaciones/conjuntos de datos).

42. Aislamiento del ETS del exterior para evitar que los datos se transfieran de forma incontrolada (por ejemplo, prohibiendo dispositivos USB, bloqueando impresoras, desactivando el portapapeles compartido, impidiendo la sincronización con almacenamiento en la nube y bloqueando el acceso directo a internet).

43. Gestión de parches para actualizar regularmente el software y corregir vulnerabilidades, mejorar la funcionalidad y proteger contra amenazas cibernéticas.

44. Implementar una infraestructura de escritorio virtual (virtual desktop infrastructure, VDI), u otros enfoques equivalentes, para facilitar un acceso seguro, controlado y monitorizado a los datos.

7. Auditoría, registro y seguimiento

45. Mantener registros completos y auditables de todas las operaciones de acceso y otras, incluyendo, entre ellas, los registros de comandos ejecutados y los registros de acceso a archivos.

46. Los registros deben ser monitorizados (rastreo y correlación de actividad del usuario), protegidos (es decir, mediante mecanismos de registro seguros e inviolables y rastreos de auditoría completos) y reportados por separado de los entornos principales.

47. Copia de seguridad de registros.

48. Monitorización y alertas en tiempo real.

49. Paneles de control de eventos de seguridad que incluyen detección de anomalías y análisis de comportamiento para, en particular, detectar accesos no autorizados o de abuso.

50. Deben realizarse auditorías regulares de protección de datos y seguimiento de cumplimiento; en particular, para el sector sanitario, auditorías a los usuarios de datos sanitarios para garantizar el cumplimiento del tratamiento que realizan en el ETS[59], y auditorías internas y de terceros sobre el cumplimiento del ETS con los estándares, especificaciones y requisitos definidos[60].

8. Respuesta a incidentes, recuperación y resiliencia

51. Procedimientos de detección y clasificación de incidentes.

52. Equipo de respuesta a brechas de datos y vías de escalada.

53. Procedimientos de contención, erradicación y recuperación.

54. Mecanismos de copia de seguridad y restauración, incluyendo la creación de copias seguras de datos críticos y pruebas regulares de los procedimientos de restauración de copias de seguridad

55. Procedimientos de revisión y corrección posteriores a una brecha de datos.

56. Protocolos de comunicación y notificación.

57. Garantizar la disponibilidad y resiliencia del ETS en línea con la criticidad del servicio que soporta. Esto podría implicar tener un ETS separado funcionando en paralelo, ya sea en términos de infraestructura y/o del operador.

9. Gestión de terceros

58. Incorporación de la autonomía digital como criterio de calidad en los servicios de TI mediante la imposición de requisitos y criterios específicos y verificables, dando preferencia a soluciones que cumplan con los requisitos de soberanía más estrictos.

59. Evaluación de riesgos del proveedor y debida diligencia. Incluirá la evaluación del riesgo de dependencia del proveedor y, en consecuencia, la adopción de estrategias multi proveedor y el uso de estándares abiertos e interoperabilidad como principio explícito de diseño en la arquitectura de TI.

60. Requisitos contractuales de seguridad (SLAs, permisos, acuerdos, contratos).

61. Seguimiento de la lista de materiales de software (*software bill of materials*, SBOM).

62. Clasificación de proveedores y designación de proveedores críticos.

63. Controles de residencia de datos y de transferencia transfronteriza.

10. Cultura organizativa y formación

64. Formación específica para cada función (desarrolladores, administradores, usuarios).

65. Formación en protección de datos y confidencialidad estadística.

66. Cultura y canales de notificación de incidentes.

[59] De acuerdo con el artículo 73.1.e) del EEDS.

[60] Según se menciona en el artículo 73.3 del EEDS.

67. Campañas de sensibilización que destaquen la importancia de aplicar el principio de precaución en todos sus aspectos a la gestión del SPE, así como a todas las operaciones de tratamiento que éste soporta.

68. Fomento de la autonomía digital y la soberanía tecnológica dentro de la organización.

B. Ingeniería de protección de datos para implementar un ETS

En el apartado anterior, discutimos medidas específicas para abordar riesgos relevantes en el contexto de los ETS. Sin embargo, como se ha señalado anteriormente, estas pueden no ser suficientes, a pesar de su necesidad. En concreto, al implementar un ETS, deben tenerse en cuenta técnicas y protocolos criptográficos avanzados que sean especialmente relevantes para aplicaciones que mejoran o preservan la privacidad; de hecho, tales herramientas pueden facilitar la compartición y la interacción responsable de datos en escenarios donde, sin ellas, la confianza puede ser insuficiente (ENISA, Engineering Personal Data Sharing, 2024). Estas técnicas apoyan inherentemente la realización de la llamada computación segura, que, por definición, constituye un bloque fundamental de construcción de un ETS.

A continuación, presentaremos brevemente, como ejemplos indicativos, casos concretos de técnicas criptográficas avanzadas que proporcionan salvaguardas de protección de datos que se ajustan bien a las propiedades deseadas para un ETS. Por supuesto, ninguna de ellas debe considerarse una panacea, ni todas son siempre posibles o necesarias (ya que, como veremos, cada una tiene sus propias limitaciones). Sin embargo, dado que estas técnicas ofrecen beneficios específicos de protección de datos que van mucho más allá de la seguridad, deben tenerse necesariamente en cuenta a la hora de implementar un ETS.

1. ETS vs TEEs

En primer lugar, debe aclararse desde el principio que el ETS no coincide con un entorno de ejecución confiable (*trusted execution environment*, TEE), independientemente de que, en la práctica, un TEE podría usarse como componente básico para un ETS. Los TEE suelen considerarse enfoques prometedores para implementar la llamada computación confidencial (*confidential computing*) y proteger cargas de trabajo sensibles incluso cuando se ejecutan en proveedores de servicios en la nube no confiables. Los TEE utilizan hardware especializado dentro de la base de computación confiable (TCB) (como sistemas en chip (SoCs) con unidades de gestión de memoria (MMUs) y motores de cifrado de memoria (MEEs)) para establecer un entorno seguro y aislado para ejecutar código sensible. Con estos medios se permite la ejecución segura del código aislándose del sistema operativo, núcleo e hipervisor del sistema anfitrión. Este espacio de ejecución aislado pretende proporcionar fuertes garantías de confidencialidad e integridad, protegiendo datos y procesos de software del sistema comprometido e incluso de amenazas físicas al hardware del servidor. Además, los TEE incorporan una raíz criptográfica de confianza (RoT) dentro del SoC, permitiendo la comprobación remota para verificar tanto la plataforma hardware como la integridad de la instancia TEE (Li, Yang, Chen, Yan, & Zhang, 2025). Por lo tanto, en palabras sencillas, los TEE utilizan una raíz de confianza hardware para permitir el tratamiento de datos con un control de acceso detallado y la protección del código ejecutado, el estado de ejecución y la memoria de los sistemas en la nube (Birrell, et al., 2018), (Sehgal, Bhatt, & Acken, 2020).

Sin embargo, desde el punto de vista de la protección de datos, un TEE tiene limitaciones importantes, principalmente derivadas del hecho de que el funcionamiento interno de los TEE suele ser de código cerrado y opacos, ya que dependen de hardware proporcionado por proveedores específicos, lo que reduce la transparencia; de hecho, incluso los servicios de comprobación remota pueden no ser transparentes. También existen otros problemas, como posibles vulnerabilidades a ataques de canal lateral y limitaciones debido a la memoria y almacenamiento restringidos. Además, los TEE en principio se centran en la seguridad y no en otros principios de protección de datos.

Concluyendo, sobre la base de lo anterior y teniendo en cuenta la definición y el uso de un ETS, los TEE por sí solos no deben considerarse ETS, aunque puedan soportar la implementación de un ETS[61].

2. Cifrado homomórfico

La criptografía tradicional tiene como objetivo transformar los datos originales (es decir, el texto en claro) en una forma ofuscada (es decir, un texto cifrado). La información cifrada parece un conjunto aleatorio de datos y, por lo tanto, cualquier operación entre textos cifrados carece de sentido. Por otro lado, un esquema de cifrado homomórfico (HE) permite además realizar cálculos directamente sobre los textos cifrados, de tal forma que el texto cifrado resultante se corresponde con el resultado de operaciones equivalentes realizadas sobre los textos en claro subyacentes. Esto permite procesar los datos en forma cifrada sin necesidad de descifrarlos. Existen esquemas que permiten realizar operaciones homomórficas de suma o de multiplicación, y también hay esquemas de cifrado totalmente homomórfico (FHE) que permiten ambas operaciones[62].

En el contexto de la implementación de un ETS, el cifrado homomórfico puede servir como base adecuada cuando los usuarios de datos necesitan realizar operaciones sobre valores numéricos. Estos casos prácticos podrían incluir, por ejemplo, la predicción del rendimiento de dispositivos médicos o la monitorización de pacientes con fines de investigación, que se basan en grandes cantidades de datos médicos numéricos. Para ello, un enfoque habitual consiste en aplicar, por ejemplo, la regresión lineal, lo cual puede realizarse sobre valores cifrados de forma homomórfica. De este modo, ninguna parte tiene acceso a los valores numéricos originales; es decir, ni los usuarios de los datos, ni tampoco la entidad intermediaria correspondiente al proveedor de SPE. A continuación, se ofrece una figura ilustrativa[63].

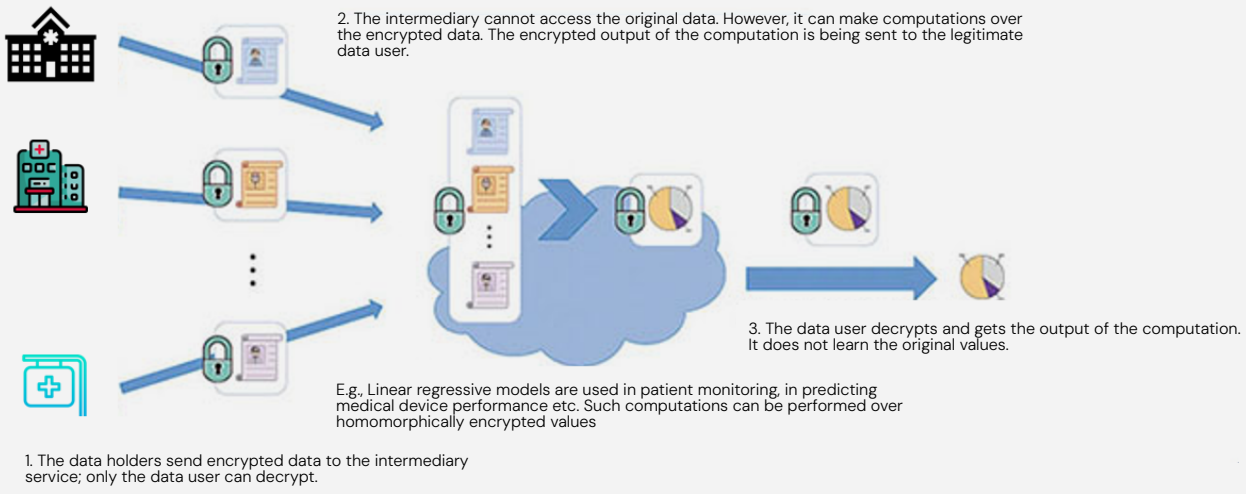


Figura 2: Un ejemplo de cifrado homomórfico para implementar ETS en el sector sanitario

Como última observación, aunque el cifrado totalmente homomórfico (FHE) se ha considerado durante mucho tiempo una funcionalidad compleja y que requiere muchos recursos, con importantes limitaciones prácticas, los avances recientes han demostrado su viabilidad, incluso en escenarios de aplicación más exigentes.

[61] Véase, por ejemplo, el entregable "D4.3 'System Specfication and Arhitecture'" del proyecto JOCONDE (Joint On-demand COmputation with No Data Exchange) (https://cros.ec.europa.eu/book-page/joconde)

[62] Algunos algoritmos permiten comparaciones booleanas, como TFHE (*Torus Fully Homomorphic Encryption*).

[63] Cabe señalar que las operaciones sobre datos cifrados podrían ser realizadas tanto por el intermediario como por los propios usuarios de datos (dentro del entorno del intermediario): en cualquier caso, ninguna entidad puede acceder a los valores originales

3. Computación multi parte segura

Los protocolos de computación multi parte segura (*Secure Multi-Party Computation*, SMPC) son técnicas criptográficas que permiten a varias partes calcular conjuntamente una función a partir de sus entradas privadas sin revelárselas entre sí. Intuitivamente, los protocolos SMPC permiten a las partes obtener conjuntamente un resultado de cálculo autorizado sin tener que revelar sus entradas a las demás; cada parte puede participar en el cálculo sin tener acceso directo a los datos subyacentes de las demás partes. Por lo tanto, la información revelada a una parte se limita al resultado acordado y a cualquier información que pueda inferirse legítimamente a partir de él.

Una característica valiosa de los SMPC es su capacidad para distribuir la confianza y el control entre varias partes que participan en el cálculo, evitando así la dependencia de un único punto de confianza. De hecho, el cálculo requiere la participación de varias partes, mientras que ninguna de ellas tiene acceso a toda la información necesaria para reconstruir las entradas protegidas. Esta forma de control compartido es una característica inherente a los SMPC (aunque también se pueden lograr formas similares de control distribuido mediante otras tecnologías).

Los protocolos SMPC podrían basarse en tecnologías fundamentales como la transferencia inconsciente, los circuitos codificados, los esquemas de compromiso, las pruebas de conocimiento cero, el cifrado homomórfico y el reparto de secretos (Zhou, et al., 2024)[64]. Es interesante señalar que los protocolos SMPC ya han sido considerados para permitir a las organizaciones realizar cálculos estadísticos conjuntos sin intercambiar datos inteligibles[65].

4. Cifrado polimórfico y seudonimización

Los métodos criptográficos tradicionales se basan en el principio de que cada texto cifrado corresponde a una clave de descifrado única. Sin embargo, técnicas más avanzadas relajan esta restricción para permitir una funcionalidad diferente: un texto cifrado — que solo puede ser descifrado por su creador — puede transformarse (o volver a cifrar) de tal manera que solo un destinatario autorizado y específico pueda descifrarlo usando su propia clave. Esta capacidad es una característica fundamental de lo que se conoce como cifrado polimórfico (Verheul, Jacobs, Meijer, Hildebrandt, & Ruiter, 2016). En otras palabras, mediante el cifrado polimórfico, los datos pueden cifrarse de tal manera que no sea necesario fijar *a priori* quién puede descifrar los datos (ENISA, Engineering Personal Data Sharing, 2024). La propiedad importante del cifrado polimórfico es que la entidad que realiza este re-cifrado no tiene acceso a los datos originales, ni a (cualquiera de las) claves de descifrado. Por lo tanto, si tal entidad es un intermediario dentro del marco de un ETS, entonces este intermediario consigue proporcionar acceso solo a usuarios legítimos sin tener acceso a los datos originales.

Sin embargo, el cifrado polimórfico debe considerarse junto con la seudonimización. Como se describe en (Verheul, Jacobs, Meijer, Hildebrandt, & Ruiter, 2016), la entidad responsable del re-encriptado también realiza la seudonimización, es decir, sustituyendo los identificadores de los individuos por seudónimos que parecen aleatorios. Este proceso se aplica directamente a los datos cifrados (por lo que esta entidad aún no accede a los datos originales), asegurando que cuando un usuario autorizado los descifra, reciba información seudonimizada. Además, si el mismo conjunto de datos cifrado se vuelve a cifrar varias veces para diferentes usuarios, los seudónimos resultantes son distintos e invinculables entre usuarios.

---

[64] Véase también el entregable "D2.1 'Technology Survey and Analysis'" del proyecto JOCONDE (Joint On-demand COmputation with No Data Exchange) para un análisis exhaustivo del panorama del SMPC (https://cros.ec.europa.eu/book-page/joconde).

[65] Véase, por ejemplo, el proyecto JOCONDE (Joint On-demand Commission with No Data Exchange), donde se indica explícitamente que Eurostat considera esta posibilidad (https://cros.ec.europa.eu/book-page/joconde); Ricciato, F. 2024, Steps Toward a Shared Infrastructure for Multi-Party Secure Private Computing in Official Statistics, SageJournals, https://doi.org/10.1177/0282423X241235259

Las propiedades anteriores se muestran en la siguiente figura.

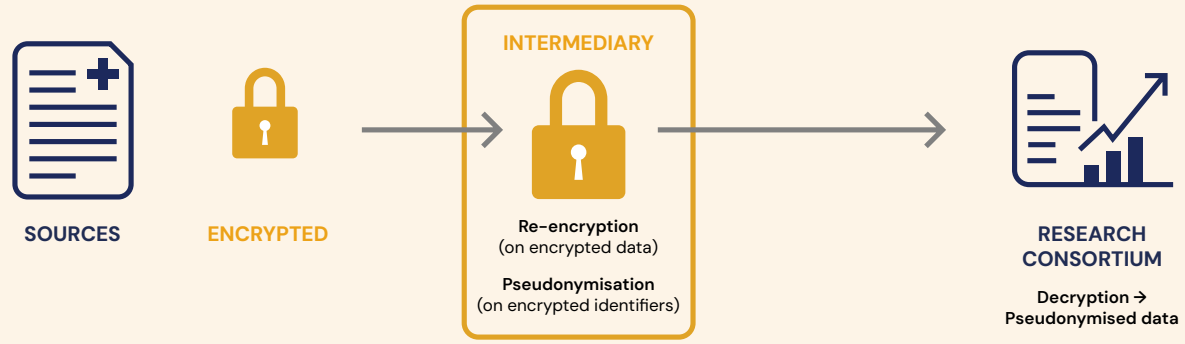


Figura 3: Un diagrama simplificado sobre el cifrado polimófico y la seudonimización

El cifrado polimórfico y la seudonimización ya se han utilizado en el contexto de un estudio a gran escala sobre la enfermedad de Parkinson (van Gastel, Jacobs, & Popma, 2021). Las propiedades mencionadas ilustran su importancia en términos de proporcionar salvaguardas esenciales para un ETS.

Cabe destacar que, en tal entorno, la seudonimización depende de reemplazar identificadores originales por seudónimos. Sin embargo, dependiendo de la estructura y el contenido del conjunto de datos, esta medida por sí sola puede ser insuficiente. Por ejemplo, la reidentificación puede seguir siendo posible por parte del usuario de datos en caso de que el conjunto de datos contenga cuasi-identificadores que permitan eludir la seudonimización (Samarati, 2001). Esto subraya aún más la importancia de aplicar un enfoque exhaustivo y basado en el riesgo al implementar una ETS.

5. Seudonimización ciega

Un proveedor de ETS debe garantizar que los usuarios legítimos tengan acceso a datos que no puedan atribuirse a una persona específica. Para ello, se podrían implementar técnicas robustas de seudonimización – probablemente basadas en algoritmos criptográficos fuertes. Los enfoques típicos de pseudonimización requieren que la entidad que realiza la seudonimización tenga conocimiento del identificador original (ENISA, Pseudonymisation techniques and best practices, 2019), (EDPB, 2025). Sin embargo, existen técnicas basadas, entre otras, en las nociones criptográficas de PRFs (Funciones Pseudo-Aleatorias) ciegas que permiten proporcionar la llamada seudonimización ciega como servicio (Lehmann, 2019), que basta para asegurar las siguientes propiedades:

i. La seudonimización se externaliza a una entidad central (es decir, un proveedor de la nube como un guardián de acceso), aunque completamente "ciega": el proveedor de servicios no conoce ni la información sensible (incluidos los identificadores originales) ni los seudónimos que produce. Los seudónimos son en realidad valores PRF.

ii. Cuando los datos se almacenan en reposo, se ponen seudónimos de forma totalmente invinculable, mientras que los identificadores originales no pueden recuperarse matemáticamente mediante la inversión de seudónimos. La desvinculabilidad se garantiza dividiendo la información sobre individuos en tablas no vinculables.

iii. Cuando se necesitan ciertos subconjuntos de datos para un usuario legítimo de datos, solo entonces se establece el enlace mediante una operación de unión controlada y no transitiva; es decir, solo el usuario legítimo recibirá estos datos seudónimos, de modo que incluso si otro usuario solicita acceder a los datos, la correlación entre estas dos instantáneas diferentes será invinculable.

iv. El operador de unión permite crear, para cualquier persona, el mismo seudónimo irreversible (incluso "a ciegas", mediante una función PRF ciega).

Con este enfoque, los datos se almacenan de forma segura (en el sentido de que se ocultan las identidades y no se permite la identificación individual) en el OADS antes de cualquier solicitud de acceso; para cada una de estas solicitudes, y una vez concedido el acceso, se lleva a cabo "a ciegas" una operación de unión adecuada. Nadie tiene acceso a los datos originales.

Por supuesto, el procedimiento anterior se centra en seudonimizar correctamente los identificadores de los individuos; sin embargo, la ofuscación/enmascaramiento sigue siendo necesaria para los cuasi-identificadores (como en el caso del cifrado polimórfico).

6. Privacidad diferencial

La privacidad diferencial (Dwork, 2006) es un marco riguroso diseñado para proteger la privacidad individual en el análisis de datos introduciendo ruido aleatorio cuidadosamente calibrado en las salidas de las consultas. En términos sencillos, la privacidad diferencial debilita la relación entre la presencia de un individuo en un conjunto de datos y el resultado de un análisis. Es decir, la observación del resultado no debería permitir a un observador determinar con certeza si los datos de un individuo concreto han contribuido a él. Así pues, el resultado tiene por objeto revelar información sobre el conjunto de datos o la población en su conjunto, sin aumentar de forma significativa lo que se puede saber sobre cualquier individuo concreto. De manera más formal, esto garantiza que la inclusión o exclusión de los datos de cualquier individuo concreto en el conjunto de datos tenga un impacto insignificante en el resultado final. El ruido se controla estadísticamente para equilibrar la privacidad y la utilidad: debe ser suficiente para enmascarar las contribuciones individuales, al tiempo que se preserva la precisión global de los datos agregados. Este enfoque es especialmente valioso en escenarios donde se analizan datos sensibles, como historiales médicos o información financiera, y, de hecho, puede ser un enfoque para implementar la medida numerada 8) en el catálogo correspondiente del apartado III.A. Al cuantificar la pérdida de privacidad mediante parámetros, la privacidad diferencial proporciona una medida a implementar para minimizar el riesgo de reidentificación.

Sin embargo, debe señalarse que el equilibrio entre privacidad y utilidad debe considerarse cuidadosamente. Las garantías estrictas de privacidad diferencial pueden requerir (dependiendo del caso) cantidades sustanciales de ruido, lo que podría reducir la utilidad de los datos resultantes. En la práctica, diferentes variantes e implementaciones de privacidad diferencial pueden proporcionar distintos niveles de protección.

7. Aprendizaje federado

El aprendizaje federado (*federated learning*, FL) (EDPS & AEPD, 2025) es una tecnología que mejora la privacidad basada en inteligencia artificial, específicamente en el aprendizaje automático. Permite que múltiples fuentes de datos entrenen colaborativamente un modelo compartido manteniendo los datos descentralizados.

En lugar de centralizar los datos en una sola ubicación:

- Los datos permanecen en los dispositivos de los usuarios.
- Un modelo de aprendizaje automático se distribuye a cada dispositivo.
- Los dispositivos entrenan el modelo localmente.
- Solo las actualizaciones de modelos (por ejemplo, gradientes o pesos) se comparten con un servidor central o de forma colaborativa entre dispositivos.

En lugar de enviar datos en bruto a un servidor central (si existe), cada fuente procesa sus propios datos localmente y solo comparte las actualizaciones del modelo. Sin embargo, a pesar de las ventajas de privacidad del enfoque FL, cabe mencionar que mantener los datos en bruto locales no garantiza por sí solo su protección. Las actualizaciones de modelos pueden codificar información sobre los datos utilizados para el entrenamiento local y, bajo ciertas condiciones, pueden permitir inferir o reconstruir información sobre registros individuales de entrenamiento, por ejemplo debido a efectos de memorización (véase, por ejemplo, la discusión relevante recogida en (Ricciato, 2026) y las referencias en ella). Por lo tanto, las actualizaciones de modelos no deben considerarse automáticamente información anónima o no sensible, y la protección de privacidad ofrecida por FL debe evaluarse a la luz de la arquitectura específica, el modelo de amenazas y las salvaguardas adicionales empleadas.

Por último, es importante señalar que FL no entra necesariamente en conflicto con el requisito de supervisión central de un ETS, siempre que la arquitectura federada esté diseñada de tal manera que el operador ETS mantenga el control y la supervisión centralizados sobre el flujo de trabajo global de los tratamientos[66].

C. Mapeo de amenazas y medidas

A continuación presentamos un marco de trabajo para realizar un análisis exhaustivo de las medidas que deben implementarse para la protección de datos, basado en la metodología LIINE4DU combinada con el marco Five Safe introducido en la sección anterior. Éste se presenta de forma sistemática para que pueda ser de aplicación, y en el apartado "IV. Un caso práctico" se incluye a modo de ejemplo, un análisis de riesgos derivado de la amenaza "Vinculación/ *Linking*" junto con una lista de propuestas de medidas.

Amenazas a la protección de datos	**Medidas que podrían reducir los riesgos asociados para la protección de datos**				
	Safe projects	Safe people	Safe settings	Safe data	Safe outputs
Vinculación / *Linking*					
Identificación / *Identifying*					
Inexactitud / *Inaccuracy*					
No repudio / *Non-repudiation*					
Exclusión / *Exclusion*					
Detección / *Detecting*					
Brecha de datos / *Data Breach*					
Engaño / *Deception*					
Divulgación / *Data Disclosure*					
Desconocimiento y falta de capacidad para intervenir / *Unawareness and Unintervenability*					

Figura 4: Esquema propuesto para identificar medidas adecuadas que minimicen los riesgos derivados de las amenazas identificadas a la protección de datos

[66] Esto también se ha tenido en cuenta en el proyecto TEHDAS2 financiado por la UE relevante – véase D7.4, disponible en https://tehdas.eu/wp-content/uploads/2026/06/d7.4-technical-specification-for-health-data-access-bodies-on-the-implementation-of-secure-processing-environments.pdf

IV. UN CASO PRÁCTICO

A continuación, se presenta un escenario de un caso práctico de un ETS, basado en técnicas de ingeniería de protección de datos.

A. Descripción del escenario

Un consorcio de investigación compuesto por varias instituciones académicas y de salud pública quiere investigar la relación entre la carga alostática (un biomarcador compuesto del estrés crónico) y diversas variables demográficas y socioeconómicas (véase, por ejemplo, (Robertson T., 2016)). Para ello, el estudio busca datos de múltiples titulares de datos de salud y administrativos (por ejemplo, hospitales, registros nacionales de salud, oficinas estadísticas).

El consorcio tiene como objetivo realizar un análisis de regresión lineal con el objetivo de describir la relación entre una variable de resultado (en este caso, la carga alostática, que es la llamada variable dependiente) y una o más variables de exposición (o independientes).

En este caso de uso específico, asumimos como variables independientes[67] la edad, el sexo y el área de residencia (es decir, código postal), así como el estatus socioeconómico (*socioeconomic status*, SES). La regresión lineal pretende calcular una ecuación lineal (es decir, los coeficientes relevantes) que describa eficazmente dicha relación.

De acuerdo con las disposiciones del EEDS, el consorcio de investigación solicita dichos datos (que también incluyen datos de salud, es decir, una categoría especial de datos personales[68]) a través de un OADS, que verifica la consulta y emite un permiso de datos, lo que significa que el consorcio tendrá acceso a la información relevante a través de un ETS.

B. Análisis de riesgos de protección de datos *(relacionado con la vinculación)*

El siguiente subapartado analiza los riesgos de protección de datos utilizando la metodología de LIINE4DU previamente introducida para identificar medidas adecuadas para su implementación en un ETS. Este análisis se centra en facilitar el tratamiento de los datos solicitados asegurando el cumplimiento de los requisitos de privacidad.

Para evitar que el documento resulte excesivamente extenso y mantener la flexibilidad (dado que se trata de una breve introducción al caso sin todos los detalles contextuales), ofrecemos una visión general del análisis de amenazas relacionadas con la vinculación, junto con las medidas de mitigación propuestas. Más concretamente, en lo que respecta a la amenaza de la vinculación, establecemos como requisito que el consorcio no debe acceder a ninguna información que permita vincular a personas con conjuntos de datos externos, lo que a su vez podría dar lugar a la identificación de personas. De hecho, aunque no se requieren identificadores directos para este caso de uso, combinaciones como "edad-sexo-CP-SES", cuando se cruzan con el conjunto de titulares de datos, aún pueden permitir la reidentificación en ciertos escenarios (véase, por ejemplo, (Samarati, 2001), (Sweeney, 2002)). Por lo tanto, dicha información no puede clasificarse como anónima.

A continuación se presentan varias consideraciones preliminares a tener en cuenta para mitigar los riesgos derivados de la amenaza de la vinculación y, en consecuencia, identificar e implementar adecuadamente las medidas necesarias:

[67] También se les conoce como covariables en el análisis de regresión.

[68] Artículo 9 del RGPD.

- Las restricciones de descarga dentro del ETS son insuficientes para mitigar completamente las amenazas de vinculación. El riesgo principal surge cuando los usuarios pueden agrupar datos dentro del entorno, asociando potencialmente diferentes elementos de datos o acciones del usuario.
- Variables como edad, sexo, código postal y estatus socioeconómico son cuasi-identificadores muy significativos. Cuando el consorcio vincula datos de hospitales, registros, oficinas estadísticas y registros administrativos, estas variables (ya sea individualmente o en combinación) pueden señalar individuos o subgrupos muy pequeños.
- El consorcio puede derivar patrones vinculados a nivel de grupo para códigos postales o estratos SES específicos, revelando inadvertidamente información sensible sobre subgrupos protegidos o vulnerables.
- Las repetidas secuencias de regresión, la estratificación y la modelización iterativa pueden agregar de forma acumulativa información específica de subgrupos a lo largo del tiempo, aumentando los riesgos de vinculación, especialmente al producir resultados muy detallados.

Tras este análisis preliminar, se proporciona un ejemplo de algunas medidas identificadas como más adecuadas para este caso entre las listadas en la sección "III.A. Medidas que se deben aplicar".

Amenazas a la protección de datos	Medidas[69] que podrían reducir los riesgos asociados para la protección de datos				
	Safe projects Is this use of the data appropriate?	Safe people Can the researchers be trusted to use it in an appropriate manner?	Safe settings Does the access facility limit unauthorised use?	Safe data Is there a disclosure risk in the data itself?	Safe outputs Are the statistical results non-disclosive?
Linking (Relacionar diferentes datos o actividades del interesado para obtener más información sobre el interesado o sobre un grupo de personas al que pertenece)	6), 7), 14)	25), 26), 64)	31), 32)	15), 16), 17) 18), 19), 20) 21), 22), 33)	8)

Figura 5: Ejemplo de medidas para abordar los riesgos de protección de datos derivados de la vinculación en el caso de uso descrito.

Entre las medidas anteriores, la desidentificación efectiva de de datos (numerada 18) es de gran importancia para mitigar la amenaza de vinculación. La elección de las técnicas adecuadas de desidentificación debe darse teniendo en cuenta las características inherentes del proceso, junto con los riesgos relevantes para los derechos y libertades de las personas. Puede darse el caso de que se pueda garantizar una desidentificación eficaz mediante una técnica avanzada de ingeniería de protección de datos (como también implica la medida numerada 19). Esto se analizará a continuación.

C. Enfoque de ingeniería de protección de datos

El análisis anterior no ha abordado los riesgos relacionados con la vinculación derivados de la gestión y mantenimiento del propio ETS. En otras palabras, de forma similar al requisito del consorcio de investigación, el OADS ni ninguno de sus encargados podrá vincular (o posiblemente identificar) a individuos. Por tanto, si el OADS puede cumplir con sus obligaciones de compartir datos sin acceder a los datos originales, este enfoque debe ser prioritario.

[69] Todos los números de esta tabla se refieren a la lista de todas las medidas mencionadas anteriormente en el apartado "III.A".

Una técnica de ingeniería de protección de datos que podría utilizarse para abordar los desafíos mencionados es la aplicación de cifrado homomórfico (HE) sobre los datos personales originales para realizar regresión lineal sobre datos cifrados. De hecho, recordando las propiedades de HE descritas en el apartado "III.B. Ingeniería de protección de datos para implementar un ETS", los titulares de los datos pueden cifrar homomórficamente sus datos antes de enviarlos al OADS, quien a su vez estará disponible para realizar regresión lineal sin tener acceso a los datos originales: el resultado de este análisis también estará cifrado, al que se dará acceso (o compartido con) al consorcio de investigación. Luego, el consorcio de investigación descifrará este resultado, calculando así los coeficientes; el consorcio de investigación no obtiene acceso a datos personales, ni puede inferir información personal, al tiempo que se cumplen de manera efectiva sus objetivos de investigación.

D. La técnica de ingeniería de protección de datos en detalle

1. Fase 1: acuerdo y configuración

- El consorcio presenta una solicitud de acceso a datos al OADS, detallando el diseño del estudio. El OADS verifica y valida la solicitud, emitiendo un permiso de datos con parámetros específicos, de acuerdo con lo requerido por los fines de uso secundario del EEDS.

- Ésta es la fase en el que el OADS decide la técnica de ingeniería de protección de datos que se utilizará; HE para este caso conceto. En caso de que el HE esté apoyado por un tercero (por ejemplo, un proveedor de tecnologías para la mejora de la privacidad (PET)), dicho tercero se incorporará adecuadamente en esta fase, proporcionando las herramientas criptográficas pertinentes para la configuración de claves y las operaciones criptográficas; de lo contrario, el HDAB se encargará de dicha configuración.

2. Fase 2: gestión de claves criptográficas

- El consorcio de investigación genera[70] un par de claves de cifrado homomórfico:
  - La clave pública se comparte de forma segura con los titulares de los datos (a través del OADS).
  - La clave privada es guardada de forma segura por el consorcio de investigación.

3. Fase 3: enviar los datos cifrados al OADS

- Cada titular de datos cifra los datos solicitados (es decir, puntuación de carga alostática, edad, sexo, código postal, indicadores SES como quintil de ingresos, nivel educativo, etc.)[71] localmente, utilizando la clave pública HE del consorcio y el algoritmo HE correspondiente.

- Los conjuntos de datos cifrados se envían al ETS orquestados por el OADS.
  - Los datos en texto plano nunca salen del titular de datos. Además, ni el OADS ni cualquier otra parte que pueda apoyar el OADS pueden acceder a los datos en texto plano ni a la clave de descifrado.

[70] El OADS, probablemente con la ayuda de un proveedor de PET, debería apoyar al consorcio de investigación en este paso.

[71] Estas variables deben codificarse primero adecuadamente para alimentar posteriormente el algoritmo de regresión lineal.

4. Fase 4: computación segura vía OADS

- El consorcio sube al código de regresión lineal ETS que opera sobre datos cifrados.
  - El OADS deberá comprobar esta entrada proporcionada por el consorcio (por ejemplo, para detectar posibles códigos maliciosos).
- El cálculo se realiza directamente sobre los datos cifrados (debido al HE), sin descifrarlos nunca.

5. Fase 5: compartir resultados

- El OADS devuelve resultados de regresión cifrados (por ejemplo, coeficientes) al consorcio de investigación. Esto se realiza de forma segura, para garantizar la autenticación de entidades y datos.
- El consorcio utiliza su clave privada para descifrar los resultados.
  - Alternativamente, el acceso a resultados cifrados y su descifrado seguro podrían realizarse dentro del ETS, bajo una implementación adecuada que permita un acceso seguro y privado a estos datos. De este modo, el OADS podría verificar que no se remitirán datos personales al consorcio de investigación.

6. Fase 6: análisis e informes

- Los resultados descifrados se interpretan y reportan.
- Ninguna persona es reidentificable por ninguna de las partes.
- Solo se permiten usos secundarios permitidos (por ejemplo, investigación científica).

Los pasos básicos del proceso anterior (es decir, los pasos 3 a 5) se muestran en la siguiente figura.

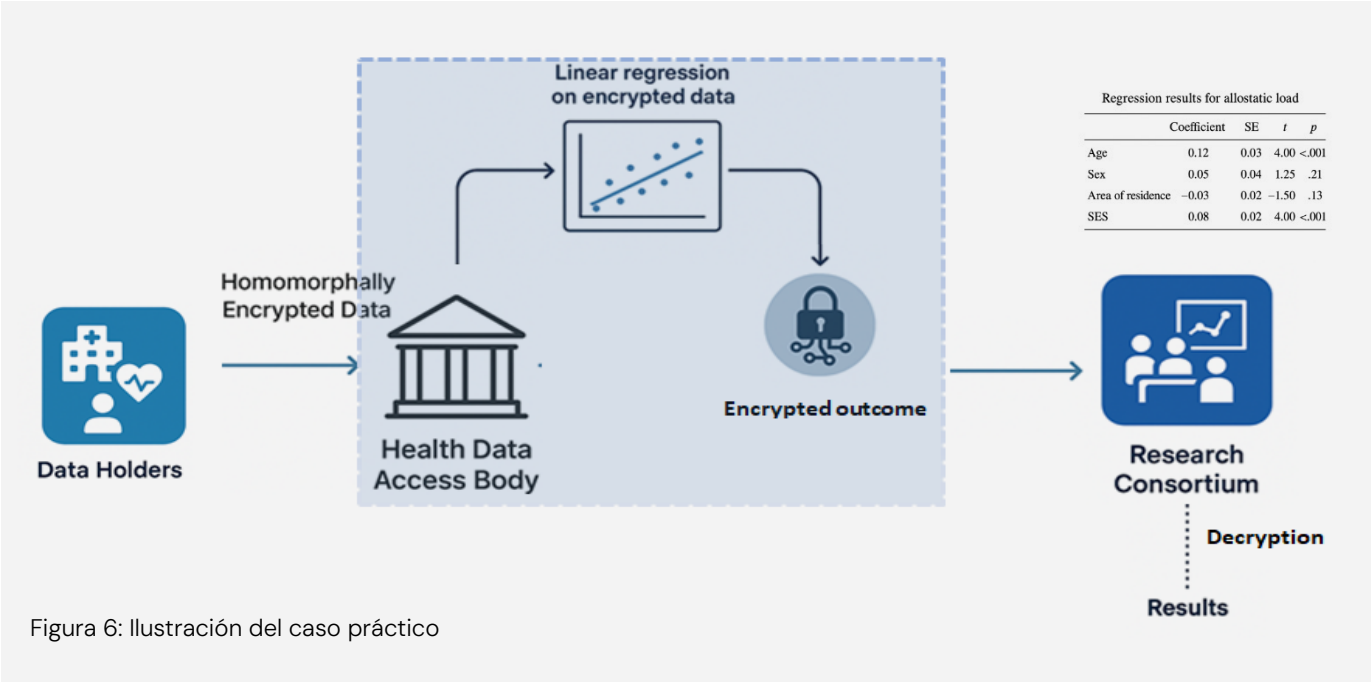


Figura 6: Ilustración del caso práctico

Aunque en este ejemplo el cálculo lo realiza el OADS en nombre del consorcio de investigación, en lugar de directamente por los usuarios dentro del ETS, el modelo sigue siendo coherente con el concepto general de un ETS como mecanismo para permitir el acceso seguro y la reutilización de

datos. En este caso, el acceso seguro se logra mediante la ejecución controlada del cálculo solicitado y la provisión de la salida autorizada, sin conceder a los usuarios de datos acceso a los datos subyacentes. De todos modos, esta técnica de ingeniería de protección de datos también podría adaptarse para permitir que el propio consorcio de investigación realice los cálculos dentro del entorno ETS usando cifrado homomórfico.

De esta manera, ni el proveedor del ETS ni el usuario de datos acceden a ninguna parte de los conjuntos de datos originales; los cálculos son totalmente confidenciales, los datos permanecen siempre cifrados, ni el ETS ni el usuario de datos acceden a información que permita la identificación directa o indirecta de un individuo o incluso inferir información para una persona, mientras que el algoritmo de cifrado también garantiza la integridad de los datos dentro del ETS. Por lo tanto, una implementación adecuada de esta técnica de ingeniería de protección de datos pretende abordar directamente las amenazas relacionadas no solo con la vinculación, sino también con la identificación, no repudio, detección, brecha de datos y divulgación de datos. Además, esta técnica contribuye a aliviar amenazas como la inexactitud (ya que los datos no pueden modificarse dentro del ETS sin que se detecte dicha modificación), así como el engaño y la falta de conocimiento (ya que si los usuarios conocen bien las características del proceso global, no se equivocarán sobre cómo se respetan sus derechos ni serán manipulados en sus elecciones).

Este enfoque de ingeniería de protección de datos también encaja bien con el enfoque de "*Five Safes*". De hecho, esta solución aborda inherentemente el riesgo de divulgación en los datos ("*safe data*"), mientras que los resultados estadísticos no son divulgativos ("*safe output*"). Además, el cifrado homomórfico junto con una gestión adecuada de claves garantiza que se evite el uso no autorizado ("*safe settings*"). Por supuesto, siempre que se establezcan métodos de autenticación adecuados para los investigadores de este consorcio (que es un requisito previo para implementar esta solución), junto con el hecho de que el consorcio no accede a datos personales y que existe una aprobación formal del proyecto y especificación de los propósitos autorizados, datos, usuarios, actividades de tratamiento, duración y resultados, este enfoque está en línea con los principios de "*safe project*" y "*safe people*".

En términos más generales, este ejemplo ilustra que las garantías que ofrece el SPE pueden considerarse uno de los factores relevantes en la evaluación global de equilibrio, junto con la naturaleza y la sensibilidad de los datos, los fines y los intereses que se persiguen mediante la reutilización de los datos, incluido el fomento de la investigación y la innovación, y los riesgos para los derechos y libertades de los interesados.

Por último, es importante señalar que el uso de una tecnología avanzada que mejora la privacidad (como en este ejemplo el cifrado homomórfico) no determina por sí solo los roles respectivos de las partes bajo el RGPD. Cuando el OADS actúa como encargado en relación con el tratamiento realizado dentro del ETS, y la infraestructura técnica es proporcionada por un proveedor de servicios separado, este último puede actuar como subencargado, dependiendo de los roles y responsabilidades respectivas de las partes. En tal caso, también habría que tener en cuenta los requisitos del artículo 28.4 del RGPD relativos a la autorización previa específica o general por escrito del responsable para el compromiso de otro encargado.

V. REFLEXIONES FINALES

Los entornos de tratamiento seguro se están convirtiendo en una piedra angular para permitir la compartición segura de datos en ecosistemas cada vez más interconectados y basados en datos, como los espacios de datos europeos, ya que *"proporcionan las fuentes estructuradas de datos fiables"* y *"son fundamentales para construir un mercado único de datos"*[72]**.** A medida que el panorama de la ciberseguridad sigue evolucionando, impulsado por los avances en inteligencia artificial y la aparición de la computación cuántica, los entornos de tratamiento seguro deben diseñarse con resiliencia, adaptabilidad y seguridad desde el diseño como principios fundamentales.

Un enfoque integral debe combinar salvaguardas técnicas robustas con medidas organizativas adecuadas, implementadas mediante una metodología basada en riesgos que refleje la naturaleza de alto riesgo de muchas operaciones de tratamiento. Esto incluye la adopción de arquitecturas de confianza cero, donde ningún usuario, dispositivo o carga de trabajo es implícitamente confiable, y el acceso se verifica continuamente en función de los principios de identidad, contexto y privilegio mínimo. Para ello, la monitorización continua, los mecanismos sólidos de autenticación y control de acceso son elementos esenciales de este enfoque, asegurando que el ETS opere dentro de una infraestructura que garantice el cumplimiento legal y la soberanía digital para la entidad proveedora, sin depender de garantías de los usuarios de datos, ya sean entidades privadas, organismos públicos o investigadores individuales.

Al mismo tiempo, la seguridad debe complementarse con técnicas avanzadas de ingeniería de protección de datos cuando sea necesario, como el cifrado que mejore la privacidad (por ejemplo, cifrado homomórfico) y el cálculo seguro multi parte. Estas tecnologías mejoran la seguridad al tiempo que apoyan el cumplimiento de los requisitos de protección de datos y permiten la compartición de datos confiable y el tratamiento colaborativo.

Los ETS no son únicamente medidas de protección o seguridad de datos. Como muchas tecnologías de mejora de la privacidad (PET), son tecnologías de doble uso (AEPD, Espacios de Datos, soberanía y protección de datos desde el diseño, 2023) que abordan una serie de desafíos de acceso a datos derivados de requisitos legales, demandas del mercado y otras consideraciones. Los ETS deben entenderse como facilitadores de acceso a datos que sirven a los intereses de diversos interesados, incluidos laboratorios industriales, instituciones de investigación, agencias de seguridad nacional y operadores de infraestructuras críticas.

Más allá de las preocupaciones sobre la protección de datos, la idoneidad de las medidas a implementar en un ETS también puede influir en la disponibilidad de un uso secundario de datos de salud. Por consiguiente, un alto nivel de protección en el marco de los SPE no se limita únicamente a la protección de los datos personales. Por ejemplo, en circunstancias excepcionales (como una pandemia mundial u otras emergencias graves de salud pública), el acceso a datos farmacéuticos o de laboratorio puede resultar indispensable para proteger la vida y la salud pública a gran escala. En tales casos, un enfoque rígido y binario que deniegue automáticamente el acceso podría no ser adecuado.

Por lo tanto, los SPE deben basarse en requisitos procedentes de múltiples fuentes.

Dentro del marco de gobernanza de un SPE, es esencial incluir la figura de un delegado de protección de datos (DPD) o de un asesor en materia de protección de datos. Esta persona debe poseer conocimientos especializados en normativa de protección de datos, comprender las particularidades de las actividades de tratamiento implicadas y ser capaz de identificar y aplicar las medidas

[72] Comunicación de la Comisión al Parlamento Europeo y al Consejo. Estrategia para una Unión de Datos. Desbloqueando datos para la IA (COM(2025) 835 final) [noviembre 2025] (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52025DC0835)

técnicas y organizativas adecuadas para garantizar la protección de datos desde el diseño y de forma predeterminada. Además, el DPP debe supervisar el cumplimiento y gestionar los impactos y riesgos críticos para los derechos y libertades de las personas, haciendo especial hincapié en garantizar que las evaluaciones de impacto relativas a la protección de datos (EIPD) se realicen de forma sistemática, se documenten adecuadamente y se integren de manera efectiva en el diseño y el funcionamiento de las actividades de tratamiento. Dado que cada actividad de tratamiento que se base en una SPE puede conllevar perfiles de riesgo distintos en función de su contexto, naturaleza, alcance y finalidad, las EIPD constituyen el mecanismo clave para determinar y justificar las garantías organizativas y técnicas específicas del contexto, en lugar de basarse en controles uniformes o genéricos.

VI. REFERENCIAS

ACM, AFM, AP, DNB, & RDI. (2026). *Towards digital autonomy - Increased control over digital dependencies*. Authority for Consumers and Markets (ACM). Obtenido de https://www.acm.nl/system/files/documents/towards-digital-autonomy.pdf

AEPD. (2023). *Aproximación a los espacios de datos desde la perspectiva del RGPD*. Obtenido de https://www.aepd.es/documento/aproximacion-espacios-datos-rgpd.pdf

AEPD. (septiembre de 2023). Espacios de Datos, soberanía y protección de datos desde el diseño. Obtenido de https://www.aepd.es/prensa-y-comunicacion/blog/espacios-de-datos-soberania-y-proteccion-de-datos-desde-el-diseno

AEPD. (2024). *Introducción a LIINE4DU 1.0: Una nueva metodología para el modelado de amenazas para la privacidad y la protección de datos*. Obtenido de https://www.aepd.es/guias/nota-tecnica-introduccion-a-liine4du-1-0.pdf

Birrell, E., Gjerdrum, A., R., v. R., Johansen, D., Johansen, B., & Schneider, F. (2018). SGX enforcement of use-based privacy. *Proc. 2018 Workshop Privacy Electronic Society – WPES.18*, (págs. 155–167.).

Dwork, C. (2006). Differential Privacy. *Automata, Languages and Programming. ICALP 2006. 4052*. Lecture Notes in Computer Science, Springer.

EDPB. (2025). *Guidelines 1/2025 on Pseudonymisation (version under public consultation)*. Obtenido de https://www.edpb.europa.eu/public-consultations/guidelines-012025-on-pseudonymisation_en

EDPS, & AEPD. (2025). *TechDispatch: Aprendizaje Federado - Federated Learning*. Obtenido de https://www.aepd.es/guias/tech-dispatch-aprendizaje-federado.pdf

ENISA. (2019). *Pseudonymisation techniques and best practices*. Obtenido de https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

ENISA. (2021). *Post-Quantum Cryptography: Current state and quantum mitigation*. Obtenido de https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

ENISA. (2024). *Engineering Personal Data Sharing*. Obtenido de https://www.enisa.europa.eu/publications/engineering-personal-data-sharing

ENISA. (2026). *ENISA's view on Cybersecurity in the Frontier AI Era*. Obtenido de https://www.enisa.europa.eu/publications/enisas-view-on-cybersecurity-in-the-frontier-ai-era

IDGDPT Berlin Group. (2024). *Working Papes on Data Sharing*. Obtenido de https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20241206-WP-Data-Sharing.pdf?__blob=publicationFile&v=2

Lehmann, A. (2019). ScrambleDB: Oblivious (Chameleon) Pseudonymization-as-a-Service. *Proceedings on Privacy Enhancing Technologies*, (págs. 289-309).

Li, M., Yang, Y., Chen, G., Yan, M., & Zhang, Y. (2025). SoK: Understanding design choices and pitfalls of Trusted Executed Environments. *19th ACM Asia Conference on Computer and Communications Security (ASIA CCS '24)* (págs. 1600-1616). ACM.

NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5*. Obtenido de https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST. (2020). *Zero-trust architecture*. NIST SP 800-207. Obtenido de https://csrc.nist.gov/pubs/sp/800/207/final

Ricciato, F. (2026). Privacy-enhancing or privacy-elusion technology? A critical view of (pseudo) synthetic data based on deep learning. *Journal of Official Statistics*. Obtenido de https://journals.sagepub.com/doi/10.1177/0282423X251412328

Ritchie, F. (2017). The 'Five Safes': A framework for planning, designing and evaluating data access solutions. *Data for Policy 2017*:. Obtenido de https://doi.org/10.5281/zenodo.897821

Robertson T., W. E. (2016). The importance of age, sex and place in understanding socioeconomic inequalities in allostatic load: Evidence from the Scottish Health Survey (2008-2011). *BMC Public Health*, pág. 16:126.

Samarati, P. (2001). Protecting Respondents Identities in Microdata Release. (IEEE, Ed.) *IEEE Transactions on Knowledge and Data Engineering, 13*, págs. 1010-1027.

Sehgal, N. K., Bhatt, P. C., & Acken, J. M. (2020). Future trends in cloud computing. (S. International, Ed.) *Cloud Computing with Security*, págs. 235-259.

Sweeney, L. (2002). k-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10(7)*, págs. 557-570.

van Gastel, B., Jacobs, B., & Popma, J. (2021). Data Protection Using Polymorphic Pseudonymisation in a Large-Scale Parkinson's Disease Study. *J. Parkinsons Dis*.(11(s1)), págs. S19-S25.

Verheul, E., Jacobs, B., Meijer, C., Hildebrandt, M., & Ruiter, J. d. (2016). *Eric Verheul, Bart Jacobs, Carlo Meijer, Mireille HildPolymorphic Encryption and Pseudonymisation for Personalised Healthcare*. Eric Verheul, Bart Jacobs, Carlo Meijer, Mireille Hildebrandt and Joeri de Ruiter (2016), Polymorphic Encryption andCryptology {ePrint} Archive, Paper 2016/411. Obtenido de https://eprint.iacr.org/20

Zhou, I., Tofigh, F., Piccardi, M., Abolhasan, M., Franklin, D., & Lipman, J. (2024). Secure Multi-Party Computation for Machine Learning: A Survey. *IEEE Access*, págs. 53881–53899.


aepd
agencia
española
protección
datos


HELLENIC DATA
PROTECTION AUTHORITY