centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 813

CIBERSEGURIDAD DE ESPACIOS DE DATOS

Abril 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional
CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.04.11 10:46:33 +02'00'

Pº de la Castellana 109, 28046 Madrid

Nipo: 083-24-150-9
Fecha de Edición: abril de 2024

ÍNDICE

1. INTRODUCCIÓN

1.1 Conceptos previos

En la era digital la gestión eficiente de grandes volúmenes de datos se ha convertido en un pilar fundamental para la transformación digital. Los **espacios de datos** permiten a las organizaciones almacenar, procesar, compartir y analizar información a una escala sin precedentes, con independencia de la fuente de los datos y la estructura subyacente. Esta flexibilidad es especialmente valiosa en entornos donde los datos pueden ser tanto estructurados como no estructurados, lo que facilita la inclusión de información diversa y su análisis integral. Sin embargo, con el creciente volumen de datos que manejan las organizaciones y la naturaleza que estos puedan tener, surge una preocupación crucial: la **ciberseguridad.**

La ciberseguridad en espacios de datos se presenta como un **desafío complejo y dinámico**. A medida que las amenazas cibernéticas, tanto genéricas como especialmente dirigidas, evolucionan, es imperativo que las organizaciones y partes interesadas implementen estrategias sólidas para proteger la confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad de sus datos.

La construcción de un mercado único europeo de datos forma parte de la Estrategia Europea de los Datos, siendo los espacios de datos comunes europeos una pieza fundamental en su despliegue, por ello, la Unión Europea tiene entre sus objetivos invertir y desarrollar espacios de datos comunes en sectores económicos estratégicos y de interés público, como pueden ser los sectores salud, energía y financiero, entre otros, buscando la creación de un **mercado único europeo de datos**, donde estos fluyen entre los diferentes Estados Miembros y entre sectores de actividad, de acuerdo con los valores europeos de autodeterminación informativa, privacidad, transparencia, accesibilidad, seguridad y competencia leal.

Estos espacios de datos comunes europeos deben hacer que los datos sean fáciles de encontrar, accesibles, interoperables y reutilizables (principios FAIR), garantizando una protección de los **principios europeos y derechos digitales** y, al mismo tiempo, un alto nivel de ciberseguridad y transparencia, generando un aspecto fundamental como es el de la creación de confianza para todos los intervinientes.

España está alineada con Europa en esta materia, entre los ejes de España Digital 2026 se encuentra la **transición hacia una economía del dato**. Actualmente se está trabajando para promover el entorno propicio para la creación de espacios de datos sectoriales, a través de las distintas iniciativas en materia de datos incluidas dentro del Plan de Recuperación, Transformación y Resiliencia.

Esta guía aborda los **principales aspectos a considerar relativos a la seguridad** para desplegar y operar un espacio de datos.

1.2 Economía del dato

Vivimos en un entorno en constante evolución en el que **los datos crecen de manera exponencial** y son, además, **un componente fundamental de la economía digital**. En este contexto, es necesario desbloquear su potencial para maximizar su valor mediante la creación de oportunidades para su reutilización. Sin embargo, es importante tener en cuenta que ese incremento en velocidad, escala y variedad de los datos supone que asegurar su calidad y protección sea más complicado.

La **economía del dato** evalúa cómo los datos pueden transformar y propulsar la economía en todas sus dimensiones y vertientes, extendiéndose más allá de la mera oferta y demanda de conjuntos de datos. Su alcance trasciende la tecnología y abarca la influencia global que los datos tienen en todos los sectores y actividades, desde la toma de decisiones estratégicas hasta la operación, pasando por la innovación o el desarrollo de nuevas líneas de negocio.

En este escenario de economía del dato surge la necesidad de establecer procesos comunes aplicables a los activos de datos de toda organización a lo largo de su ciclo de vida. Todo tipo de instituciones deben disponer de datos bien gobernados, gestionados y con niveles adecuados de calidad y seguridad, siendo necesaria una metodología de evaluación común que pueda ayudar a una mejora continua de dichos procesos y permita evaluar la madurez de una organización de forma estandarizada.

Las organizaciones que buscan desplegar **con éxito espacios de datos** se enfrentarán a desafíos adicionales. La flexibilidad, la financiación inteligente, la formación adecuada de los profesionales, la interoperabilidad, la proactividad en el cumplimiento de la normativa y la implementación efectiva de procesos de gobierno, gestión y calidad del dato son aspectos clave a abordar. La capacidad de adaptarse a un entorno normativo dinámico y de aprovechar estos elementos será fundamental para el éxito en el despliegue y operación de espacios de datos.

No debe confundirse la gobernanza de los espacios de datos (acuerdos de cooperación y de nivel de servicio y modelos de continuidad) con el gobierno y gestión del dato desplegado por los participantes. Sin la existencia de un gobierno y gestión del dato, difícilmente se podrá disponer de un dato de calidad que ofrecer al espacio de datos.

En este sentido, la Oficina del Dato ha patrocinado, promovido y participado en la generación de las **especificaciones UNE** que desempeñan un papel crucial al proporcionar un **marco de referencia sólido y armonizado para el gobierno, gestión y calidad del dato**, aplicables a todo tipo de organización, facilitando la generación y movilización del dato público y privado impulsando de manera efectiva la economía del dato. Estas especificaciones describen procesos normalizados para el adecuado tratamiento de los datos a lo largo de su ciclo de vida, maximizando la aportación de valor a la estrategia de negocio, minimizando los riesgos inherentes al tratamiento del dato, procedimentando tareas y así evitando trabajos innecesarios, estableciendo marcos homogéneos de referencia y certificación, y facilitando la compartición de información con confianza y soberanía. Se encuentran basadas en estándares internacionales y normas de referencia tales como ISO/IEC 38505, ISO 8000-60, ISO 25012/24/40, COBIT 2019, o DAMA DMBoK2.

Esta familia de especificaciones UNE relativas al dato se compone de:

- **UNE 0077:2023** para el efectivo "Gobierno del dato".
- **UNE 0078:2023** para la adecuada "Gestión del dato".
- **UNE 0079:2023** para la "Gestión de la calidad del dato".
- **UNE 0080:2023** para la "Evaluación del gobierno, gestión y gestión de la calidad del dato".
- **UNE 0081:2023** para la "Evaluación de la calidad del dato".

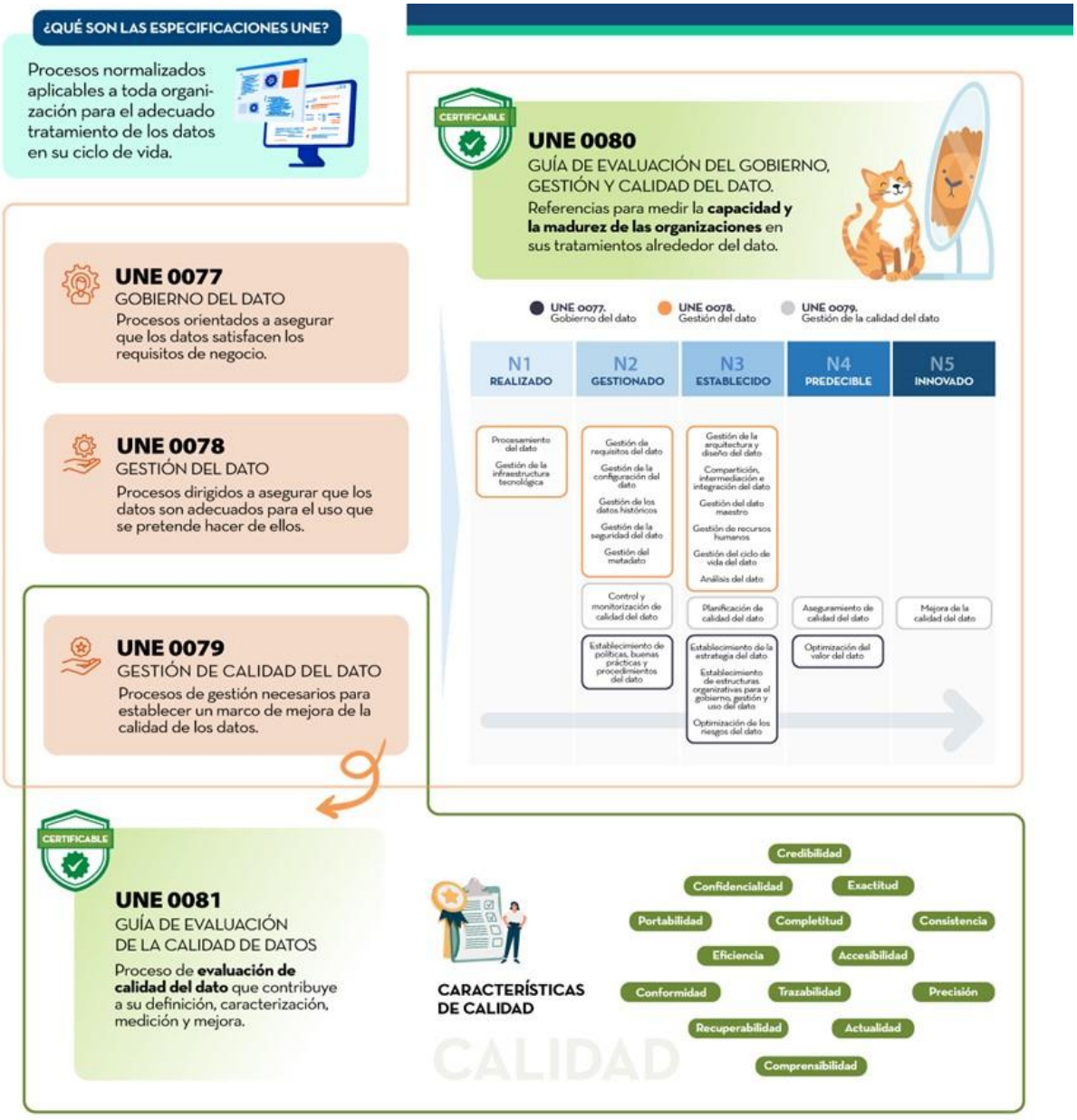

Figura 1. Especificaciones UNE. Fuente: datos.gob.es

Las especificaciones UNE 0077, 0078 y 0079 están concebidas para ser aplicadas de forma conjunta, habilitando un marco de referencia sólido que fomente la adopción de prácticas sostenibles y efectivas alrededor del dato.

Además, es necesaria una metodología de evaluación común que permita una mejora continua de los procesos de gobierno, gestión y gestión de la calidad del dato, así como la medición de la madurez de las organizaciones de forma estandarizada. Para el desarrollo de un marco homogéneo de evaluación del tratamiento que una organización hace de los datos se ha desarrollado la especificación UNE 0080.

Con el objetivo de ofrecer un proceso basado en estándares internacionales que ayude a las organizaciones a utilizar un modelo de calidad y a definir características y métricas de calidad adecuadas, se ha generado la especificación UNE 0081 Evaluación de la calidad del dato que complementa la UNE 0079 Gestión de la calidad del dato.

La especificación UNE 0081, basada en la familia de estándares internacionales ISO/IEC 25000, permite conocer y evaluar la calidad de los datos de toda organización, permitiendo establecer un plan futuro para su mejora, y pudiéndose incluso llegar a certificar su calidad formalmente bajo las características de calidad establecidas en la ISO/IEC 25012.

De esta forma, con las **especificaciones UNE** se **fortalece la calidad y gestión de los datos,** lo que redunda en una mayor y más fácil participación en los mercados de datos, habilitando la comercialización y compartición de datos con soberanía, confianza y seguridad.

1.3 Marco Normativo

El marco jurídico de la Unión Europea en el ámbito de protección de datos es un elemento facilitador para el desarrollo de una Economía del Dato acorde a los valores y principios de la Unión. Los espacios comunes europeos de datos deben **mantener** en todo momento el pleno respeto de los **derechos y principios europeos**, teniendo en cuenta que la protección de las personas físicas en relación con el tratamiento de sus datos personales es un derecho fundamental.

En el ámbito de la utilización de datos en el entorno digital, se está desarrollando un conjunto de normativas tanto a nivel europeo como nacional. Sin embargo, estas normas no alteran el régimen de tratamiento de datos personales para ninguna de las actividades reguladas ni los requisitos de información establecidos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, en adelante, RGPD).

En este sentido, la Estrategia Europea del Dato se despliega a través de diferentes iniciativas legislativas que definen las condiciones y regulaciones para la gestión y reutilización de datos en un espacio de datos, siendo algunas de las normas clave:

- **Reglamento de Gobernanza de Datos (Data Governance Act, en adelante, DGA)**: 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, que regula la reutilización de ciertas categorías de datos en manos de organismos del sector público. Además, define categorías de intervinientes en los espacios de datos, abarcando datos tanto del sector privado como público, estableciendo condiciones y garantías para nuevos modelos de negocio de datos, como los servicios de intermediación y la cesión altruista de datos. Este reglamento complementa la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público, especificando condiciones para la reutilización de datos protegidos por confidencialidad comercial, estadística, derechos de propiedad intelectual o datos personales.

- **Reglamento de Datos (Data Act)**: 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). Complementa al Reglamento de Gobernanza de Datos y amplía los derechos de acceso a datos no personales, dedicando el Capítulo VIII a los requisitos esenciales de interoperabilidad en los espacios de datos.

Asimismo, la aplicación de estas dos regulaciones en materia de datos debe entenderse junto con otras relacionadas:

- **Reglamento de Mercados Digitales**: 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. El Reglamento regula los servicios básicos de plataforma ofrecidos por los Guardianes de Acceso, especialmente aquellos relacionados con servicios de computación en la nube.

- **Reglamento de Servicios Digitales**: Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. El Reglamento establece normas armonizadas sobre la prestación de servicios intermediarios en el mercado interior.

- **Reglamento de Libre Circulación de Datos no Personales**: Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea define las pautas para la libre circulación de datos no personales en la Unión Europea.

- **Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales**: Comunicación de la Comisión al Parlamento Europeo y al Consejo - Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea. Ofrece directrices adicionales sobre el tratamiento de conjuntos de datos mixtos.

- **Conjuntos de datos específicos de alto valor y modalidades de publicación y reutilización**: Reglamento de ejecución (UE) 2023/138 de la Comisión, de 21 de diciembre de 2022, por el que se establecen una lista de conjuntos de datos específicos de alto valor y modalidades de publicación y reutilización. Establece la lista de conjuntos de datos, así como modalidades de publicación y reutilización.
- **Protección de Datos**: Cuando se llevan a cabo tratamientos de datos personales en un espacio de datos, el marco normativo se establece principalmente a través del precitado RGPD que se complementa, a nivel nacional, con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD-GDD).

Esta normativa, junto con la regulación de Inteligencia Artificial, la normativa de ciberseguridad y el marco europeo de interoperabilidad, conforman un conjunto integral que busca regular la gestión de datos en el ámbito europeo, abordando aspectos diversos como la reutilización, la circulación, la intermediación y la publicación de conjuntos de datos específicos.

Adicionalmente a este marco legislativo se están desarrollando reglamentos sectoriales que llegan allí donde la reglamentación horizontal no es capaz de cubrir requisitos específicos de cada sector, como lo es:

- **Datos sanitarios**: Propuesta de Reglamento del Parlamento Europeo y del Consejo, sobre el Espacio Europeo de Datos Sanitarios. Se enfoca específicamente en el ámbito de los datos sanitarios.

Estas propuestas e iniciativas reflejan el compromiso de la Unión Europea en la creación de un marco regulatorio integral para la gestión y utilización de datos en diversos sectores, promoviendo la interoperabilidad y la eficaz implementación de espacios de datos en toda la Unión Europea.

La necesidad de mantener la conformidad y el alineamiento con las regulaciones europeas y nacionales de aplicación requieren una atención continua por parte de las organizaciones participantes en los espacios de datos. Este proceso implica la necesidad de adaptarse a las nuevas normativas, ya que estas pueden tener un impacto significativo en la gestión, compartición y protección de datos en la Unión Europea. Además, en el contexto del sector público y otras entidades obligadas, es necesario implementar las medidas del Esquema Nacional de Seguridad correspondientes a la evaluación del nivel de riesgo. La implementación de estas medidas de seguridad se abordará en detalle en la sección 2.5.

Este marco normativo cada vez más exigente conlleva una mayor responsabilidad y exigencia de cumplimiento para las organizaciones. Se requiere una mayor concienciación y una cultura de seguridad más robusta. Las sanciones y multas por incumplimiento son significativas, aunque, generalmente, no aplicables a las Administraciones Públicas. Asimismo, destaca un énfasis creciente en la notificación de incidentes, así como la necesidad de cooperación y coordinación a nivel nacional e internacional.

1.4 Características de un espacio de datos

Un espacio de datos es un **ecosistema** que permite que diversos actores **compartan datos de manera voluntaria y segura**, siguiendo mecanismos integrados de gobernanza, legales, organizativos, normativos y tecnológicos, dentro de un entorno de soberanía, confianza y seguridad para todos los participantes.

Así, los espacios de datos se conciben como entornos (tecnológicamente) ciberseguros, (digitalmente) soberanos y (funcionalmente) interoperables para compartir y explotar datos, respetando siempre las normas y marcos comunes europeos.

El **concepto de soberanía** es clave, entendiéndose como la capacidad de un participante de mantener el control sobre sus propios datos, expresando los términos y condiciones que regirán sus usos permitidos.

1.4.1 Escenarios de compartición de datos

Considerando que el objetivo principal de un escenario de compartición de datos es satisfacer una necesidad de negocio, hay una **amplia variedad de escenarios de compartición de datos** y, para cada uno de ellos, existe una arquitectura adecuada. En otras palabras, aunque un modelo de gobernanza específico pueda tener diferentes modelos de arquitectura de espacios de datos asociados, no todos los modelos son igualmente apropiados.

A continuación, se propone una clasificación de entornos de compartición que abarca la mayoría de los escenarios. **Se puede considerar que estamos ante un espacio de datos cuando se va más allá de un intercambio bilateral de información**.

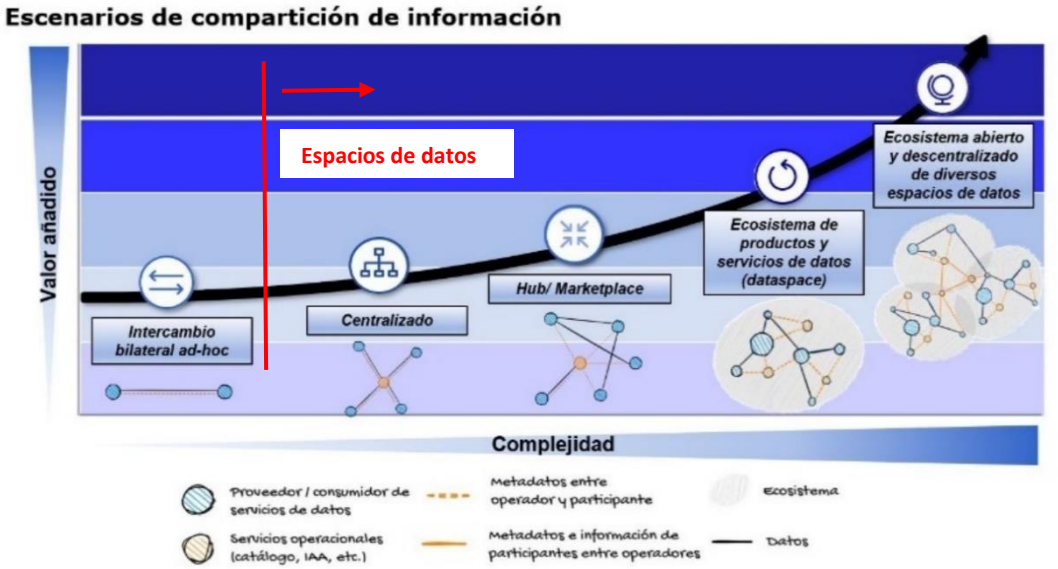

Figura 2. Escenarios de compartición de datos. Fuente: datos.gob.es

El objetivo europeo de constituir espacios federados interoperables de compartición de datos y recursos de computación en diferentes sectores industriales puede considerarse un

objetivo a medio/largo plazo dado que las tecnologías sobre las que se sustenta se encuentran hoy inmaduras. Por ello, **el alcance de esta guía en materia de seguridad se centrará en los modelos centralizados de espacios de datos.**

1.4.2 Ventajas y desafíos del uso de espacios de datos

En general, los espacios de datos ofrecen ventajas significativas a las organizaciones que buscan compartir y explotar grandes volúmenes de datos, pero requieren una **planificación**, **implementación** y **gestión** cuidadosas para garantizar el éxito.

El uso de un espacio de datos presenta una serie de ventajas:

- **Flexibilidad:** permiten la integración sin la necesidad de esquemas de base de datos comunes, posibilitando la conexión de diferentes repositorios de datos distribuidos. Esta flexibilidad promueve la interoperabilidad entre diversas fuentes y sistemas.
- **Escalabilidad:** pueden escalarse fácilmente, lo que permite a las organizaciones almacenar grandes volúmenes de datos. Además, gracias a la descentralización, se pueden añadir nuevas fuentes de datos según sea necesario.
- **Rentabilidad:** suelen ser más rentables que las soluciones tradicionales de almacenamiento de datos.
- **Analítica:** permiten a las organizaciones realizar analíticas avanzadas sobre grandes volúmenes de datos procedentes de múltiples fuentes, lo que permite mejorar el conocimiento y la toma de decisiones.
- **Procesamiento de datos en tiempo real:** pueden procesar datos en tiempo real, lo que permite a las organizaciones tomar decisiones oportunas basadas en información actualizada.

Sin embargo, es importante tener en cuenta que, a su vez, presentan una serie de desafíos que deben abordarse:

- **Complejidad:** pueden ser complejos de configurar y gestionar, requiriendo habilidades y conocimientos especializados para su configuración y mantenimiento, siendo así atractivo para potenciales agresores, ya que existen carencias en capacitación, concienciación y en personal de ciberseguridad.
- **Seguridad:** pueden ser vulnerables a amenazas de seguridad, lo que requiere que las organizaciones implementen fuertes medidas de seguridad para proteger los datos.
- **Ciberseguridad:** de forma más concreta, los espacios de datos pueden ser vulnerables ante ciberamenazas, es decir, amenazas a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de este.
- **Cumplimiento normativo:** requerimientos de cumplimiento normativo crecientemente exigentes en seguridad y protección de datos.
- **Calidad de los datos:** el incremento del volumen de datos en velocidad, escala y variedad implica una mayor dificultad para asegurar su calidad. En situaciones donde

el nivel de calidad del dato es inadecuado y conforme las técnicas analíticas empleadas para procesar conjuntos de datos se vuelven más sofisticadas, los individuos y comunidades pueden verse afectados de nuevas formas. Esto requiere que las organizaciones realicen una sanitización y validación de datos antes de su análisis.

- **Gestión:** pueden ser difíciles de gobernar, lo que requiere que las organizaciones implementen políticas y procedimientos para garantizar que los datos se gestionan de manera efectiva, de la mano de instrumentos como el Esquema Nacional de Seguridad y las especificaciones UNE relativas a los datos.

1.4.3 Claves para la gestión adecuada de un espacio de datos

1	**Gobernanza de datos:** Establecer políticas y procesos de gobernanza para garantizar la integridad y la calidad de los datos en el espacio de datos.
2	**Confidencialidad de los Datos**: Cifrar los datos tanto en reposo como en tránsito para protegerlos contra accesos no autorizados.
3	**Gestión de identidad y control de acceso**: Utilizar una política de gestión de identidad y control de acceso e implementar controles rigurosos para garantizar que solo usuarios autorizados tengan acceso. Esto se logra mediante la definición de roles, accesos, autenticación y autorización adecuadas.
4	**Auditoría y registro**: Registrar y auditar todas las actividades en el espacio de datos para rastrear quién accede a los datos y qué acciones realizan. Esto es fundamental para el cumplimiento normativo y para detectar posibles amenazas de seguridad.
5	**Gestión de versiones y metadatos**: Llevar un control estricto de las versiones de los datos y mantener metadatos detallados para facilitar la búsqueda y la comprensión de los datos almacenados.
6	**Calidad de los datos:** Establecer procesos para garantizar la calidad de los datos, incluida la limpieza, la normalización y la validación de los datos.
7	**Catalogación de datos**: Implementar una herramienta de catalogación de datos que permita a los usuarios encontrar y entender los datos disponibles en el espacio de datos.
8	**Modelo de negocio:** Monitorizar y gestionar las transacciones que ocurren en el seno del espacio de datos así como los costes asociados, ya que puede ser costoso a medida que los volúmenes de datos crecen.
9	**Escalabilidad:** Diseñar la infraestructura del espacio de datos para que sea escalable y pueda manejar grandes cantidades de datos a medida que la organización crece.
10	**Seguridad en el desarrollo**: Incorporar prácticas de seguridad desde el diseño en el desarrollo de aplicaciones y sistemas que interactúen con el espacio de datos.
11	**Cumplimiento normativo**: Asegurarse de cumplir con las regulaciones y normativas aplicables en relación con la privacidad y la protección de datos, como el RGPD y el DGA.

12	**Capacitación y concienciación**: Educar a los usuarios y al personal de la organización sobre las mejores prácticas de seguridad y la importancia de proteger los datos.
13	**Continuidad del negocio**: Implementar un plan de respaldo y recuperación sólido para garantizar la disponibilidad de los datos en caso de fallos o desastres.
14	**Monitorización continua**: Establecer un sistema de monitoreo continuo para detectar y responder rápidamente a posibles amenazas o anomalías en la seguridad.
15	**Colaboración:** Fomentar la colaboración entre equipos de seguridad, operaciones de TIC y equipos de datos para abordar las cuestiones de seguridad de manera integral. La seguridad no es de una organización, sino del conjunto de organizaciones que forman parte del espacio de datos.
16	**Interoperabilidad:** Asegurar la interoperabilidad (a lo largo de 4 niveles: legal, organizativo, semántico y técnico) y las sinergias con otros espacios de datos sectoriales nacionales o europeos.

1.4.4 Buenas prácticas relacionadas con espacio de datos

Adicionalmente al marco normativo indicado en la sección 1.3, existen buenas prácticas que pueden ser de ayuda a las organizaciones a la hora de desplegar un espacio de datos.

La Agencia Española de Protección de Datos ha publicado en mayo del 2023 la Guía **"Aproximación a los espacios de datos desde la perspectiva del RGPD"**. Esta guía recoge medidas que se podrían aplicar para garantizar y poder demostrar la conformidad con la normativa de protección de datos. Estas medidas pueden ser de **carácter jurídico**, **organizativo** y **técnico**.

No obstante, **la Guía de la Agencia Española de Protección de Datos no es un documento de obligado cumplimiento** y su interpretación deberá hacerse sin perjuicio a la normativa sectorial aplicable.

La Oficina del Dato, dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial, ejerciendo su función de dinamizar el gobierno, gestión, compartición y el uso de datos, ha publicado dos **guías de ayuda para la concepción eficaz de espacios de datos y desarrollado un plan de actuaciones para el despliegue de espacios de datos:**

- Guía de evaluación de viabilidad de casos de uso
- Guía de diseño de casos de uso
- Plan de actuaciones para el despliegue de espacios de datos

Estos documentos tienen como propósito ayudar a los posibles creadores de espacios de datos a superar los desafíos típicos al iniciar un caso de uso de compartición de datos. Asimismo, las guías proporcionan orientaciones paso a paso para las diferentes etapas del proceso, ofreciendo plantillas con preguntas específicas para las diversas situaciones que puedan surgir durante su desarrollo.

Es importante entender que el uso de estas guías debe ser iterativo, lo que significa que el proceso debe permitir ajustes y refinamientos continuos. Una vez que se haya confirmado la viabilidad de un escenario particular, se procederá con su diseño detallado, comprendiendo que la dinámica del proceso puede conducir a reconsiderar la etapa inicial de viabilidad. Además, las preguntas formuladas en cada paso pueden conducir a ajustes en pasos anteriores, lo que posibilita una mejora progresiva en todo momento.

El plan de actuaciones proporciona una orientación estratégica y práctica para abordar el despliegue efectivo de espacios de datos en España, sirviendo de referencia para impulsar el desarrollo de nuevos proyectos en sectores estratégicos de la economía nacional. El documento se estructura en tres partes:

- Parte I: Profundiza en la definición de un espacio de datos, se detalla sus principios y dimensiones y se discute la importancia de la gobernanza de estos escenarios, así como se describen varios modelos de espacios de datos.
- Parte II: Se presentan los ejes estratégicos de un plan para el despliegue de los espacios de datos en España.
- Parte III: Se explora la concepción y despliegue de espacios de datos, destacando la importancia de considerar las necesidades de negocio, la escalabilidad y la interoperabilidad. Se enfatiza en la escucha activa del mercado y el conocimiento sectorial para diseñar espacios de datos eficaces. Además, se abordan aspectos como la gobernanza, la calidad de los datos compartidos y la interconexión entre espacios de datos.

2. ASPECTOS DE SEGURIDAD A CONSIDERAR PARA IMPLANTAR Y OPERAR UN ESPACIO DE DATOS

Un espacio de datos debe **garantizar una protección adecuada de la información,** asegurando el control de acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos almacenados.

Los principales riesgos de seguridad a los que se enfrenta cualquier sistema de información son:

- **Control de acceso:** Es esencial controlar quién tiene acceso y garantizar que sólo el personal autorizado puede acceder a los datos. El acceso debe concederse en función de la necesidad de conocer y debe revocarse inmediatamente cuando ya no sea necesario.
- **Protección de la información:** Se deben establecer mecanismos de protección adecuados y proporcionales en función del análisis de riesgos, teniendo en cuenta el impacto que tendría en la organización un incidente que afectara a la seguridad de la información tratada o los servicios prestados.
- **Gobernanza, privacidad y cumplimiento:** Se deben tratar los datos con responsabilidad para evitar el daño reputacional que supondría una brecha de

seguridad de los mismos. Debe tenerse en cuenta la normativa de aplicación, así como posibles normativas sectoriales. Debe haber políticas claras comunicadas a todos los empleados, así como promover la calidad de los datos y el uso ético de los datos sensibles.

En consecuencia, para una adecuada protección de los datos se deberán establecer medidas de seguridad que contemplen los acciones relativas a los aspectos de **prevención, disuasión, protección, detección, reacción y recuperación.**

Estos aspectos de seguridad están alineados con el apartado 3.6 de la Especificación UNE 0078:2023, cuyo propósito es asegurar que la organización es capaz de **mantener los niveles de privacidad y seguridad** adecuados para el dato, especialmente para aquellos que son más sensibles.

Dicho lo anterior, a continuación, se describen las **actividades que se deben realizar para desplegar y operar un espacio de datos:**

1. Identificar los tipos de datos que integrarán el espacio de datos.
2. Conocer el ciclo de vida del dato.
3. Definir el modelo de gobernanza: Políticas de acceso y uso de la información.
4. Conocer las amenazas potenciales.
5. Implementar medidas de seguridad adecuadas.
6. Desarrollar un sistema de monitorización continua.
7. Diseñar un plan de respuesta para posibles incidentes.
8. Establecer un plan de respaldo y recuperación – continuidad del negocio.

Todo ello requiere **fomentar la colaboración** entre equipos de seguridad, operaciones de TIC y equipos de datos para abordar las cuestiones de seguridad de manera integral.

2.1 Identificar los tipos de datos

Para una adecuada gestión de un espacio de datos lo primero es saber qué **tipos de datos va a contener**, de manera que se garantice la confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad de estos:

- **Identificar y clasificar los datos:** crear una forma eficaz y eficiente de identificar y clasificar los datos por contenido, escenarios de uso, tipos y posibles grupos de usuarios.
- **Calificación de la información:** establecer niveles de clasificación atendiendo al impacto que para su privacidad o seguridad tendría un incidente que los comprometiera.
- **Catalogación de datos:** implementar una herramienta de catalogación de datos que permita a los usuarios encontrar y entender los datos disponibles en el espacio de datos.
- **Garantizar la calidad de los datos,** a través de una metodología de evaluación de estos que ayude en el proceso de mejora continua.

2.2 Conocer el ciclo de vida del dato

Debe estar claro **cómo se van a usar los datos y su ciclo de vida,** ya que las medidas de seguridad deben ser acordes a cada una de las fases:

- Ingesta de datos
- Almacenamiento de datos
- Procesamiento y transformación de datos
- Acceso y uso de datos
- Desactivación y eliminación de datos

2.3 Definir el modelo de gobernanza

De acuerdo con la definición del Data Spaces Support Centre (DSSC), el principal cometido de la gobernanza de un espacio de datos es la creación de un marco formado por «*un conjunto de principios, estándares, políticas (incluyendo regulaciones) y prácticas que aplican a la creación, administración y operación de un espacio de datos con un determinado alcance, que cuente con mecanismos para forzar su cumplimiento y para la resolución de conflictos*».

Es esencial identificar quién va a **tener acceso a los datos** y en qué **fase de su ciclo de vida**, estableciendo las condiciones bajo las cuales se accederá a dicha información. Los aspectos a considerar son los siguientes:

- **Gobernanza de datos**, se deben establecer políticas y procesos de gobernanza de datos para garantizar la integridad y la calidad de los datos almacenados.

- **Mínimo privilegio**, de forma que se permita el acceso solo a los datos necesarios para llevar a cabo tareas específicas.
- **Control de acceso**, basado en roles definidos, garantiza que el personal autorizado tenga acceso a datos pertinentes, asegurando la confidencialidad y protegiendo contra accesos no autorizados.
- **Identificación y supervisión de terceros**, asignando identidades de forma única a los usuarios para permitir una trazabilidad clara de las acciones realizadas, lo que permite la rendición de cuentas o "accountability" y ayuda en la gestión de incidentes.
- **Capacitación y concienciación.** Educar a los usuarios y al personal de la organización sobre las buenas prácticas de seguridad y la importancia de proteger los datos contribuye a crear una cultura de seguridad robusta. La concienciación sobre la responsabilidad compartida en la protección de la información es esencial para mitigar posibles amenazas y asegurar un uso adecuado de los datos almacenados.

2.4 Conocer las amenazas potenciales

Las principales amenazas a un espacio de datos son:

- **Acceso no autorizado.** Referido al acceso no autorizado a datos. Esto puede ocurrir si no se implementan adecuadamente los controles de acceso y la autenticación.
- **Fugas de datos.** Las filtraciones de datos pueden ocurrir cuando los datos se exponen o comparten de manera inapropiada, ya sea debido a errores humanos o a vulnerabilidades en la seguridad.
- **Ciberataques genéricos.** Como cualquier sistema de información, los espacios de datos pueden ser blanco de ataques, como ataques de fuerza bruta, ataques de inyección de SQL, ataques de phishing y otros.
- **Malware y ransomware.** La introducción de malware o ransomware en un espacio de datos puede cifrar o dañar los datos, resultando en pérdida de información y extorsión.
- **Robo de credenciales.** La adquisición de códigos de acceso de forma no legítima puede dar lugar a accesos no autorizados y al robo de datos confidenciales almacenados en un espacio de datos.
- **Detección y respuesta inadecuadas.** La falta de sistemas efectivos para detectar amenazas y responder de manera adecuada puede permitir que las amenazas pasen desapercibidas o que no se gestionen de manera efectiva.
- **Vulnerabilidades en la seguridad.** Las vulnerabilidades en los sistemas, aplicaciones o infraestructuras utilizadas para el espacio de datos pueden ser explotadas por actores maliciosos.

- **Falta de gobernanza de datos.** La ausencia de una sólida gobernanza de datos puede resultar en la mala gestión de la información y la pérdida de control sobre quién accede a ella y cómo se utiliza.
- **Errores humanos.** Incluyen acciones accidentales, como la eliminación equivocada de datos o la configuración incorrecta de permisos, pudiendo causar problemas de seguridad y pérdida de datos.
- **Incumplimiento normativo.** La falta de cumplimiento de regulaciones de privacidad y protección de datos, como el RGPD, puede resultar en sanciones legales y daños a la reputación de la organización.
- **Ataques internos.** Los empleados o personas con acceso autorizado pueden representar una amenaza si abusan de sus privilegios o si llevan a cabo actividades maliciosas.
- **Inconsistencia y calidad de datos.** La falta de control sobre la calidad y la consistencia de los datos puede resultar en decisiones erróneas basadas en información incorrecta.

Sin perder de vista las **nuevas amenazas con capacidades de Inteligencia Artificial:**

- Reconocimiento
- Automatización de ataques
- Movimientos laterales y escalado de privilegios
- Exfiltración y cifrado

2.5 Medidas de seguridad

Una vez identificados los tipos de datos, cómo se usan, los usuarios y las principales amenazas, se deben establecer **medidas de seguridad adecuadas y proporcionales** en función de un análisis de riesgos, teniendo en cuenta el impacto que tendría en la organización un incidente que afectara a la seguridad de los datos o información tratada.

La protección se realizará implementando las **medidas generales y específicas** del Esquema Nacional de Seguridad (ENS) que correspondan con la **categoría de seguridad** de los sistemas de información implicados en el espacio de datos. Estas medidas incluirán el marco organizativo, operacional y medidas de protección y estarán orientadas a garantizar que la organización pueda cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias cuando utiliza el espacio de datos. Por ello, se tendrán en cuenta los siguientes principios básicos:

- **Seguridad como proceso integral.** La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información

- **Gestión de la seguridad basada en los riesgos.** El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua, permitiendo el mantenimiento de un entorno controlado minimizando los riesgos a niveles aceptables.
- **Prevención, detección, respuesta y conservación.** La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.
- **Existencia de líneas de defensa.** El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad compuesta por medidas de naturaleza organizativa, física y lógica.
- **Vigilancia continua.** La vigilancia continua permite la detección de actividades o comportamientos anómalos y su oportuna respuesta.
- **Reevaluación periódica**. La evaluación permanente del estado de la seguridad de los activos permite medir su evolución, detectar vulnerabilidades e identificar deficiencias de configuración.
- **Diferenciación de responsabilidades.** En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.

A continuación, se exponen las principales medidas del ENS a implementar desde la planificación hasta la desactivación y eliminación del espacio de datos, incluyendo la revisión, mejora continua y los planes de respuesta a incidentes, respaldo y recuperación.

Es responsabilidad de cada uno de los partícipes en el espacio de datos, así como del operador de la plataforma, **la determinación de la categoría de seguridad conforme** a lo indicado en el Capítulo VII y Anexo I del ENS **y la adopción de las medidas de seguridad y**/o refuerzos aplicables para garantizar la seguridad de la información en línea con lo indicado en el Anexo II del ENS.

Planificación y Diseño		
Medida	**Descripción**	**Referencia ENS**
Evaluación de riesgos	Realizar una evaluación detallada de los riesgos asociados a los datos que se almacenarán en el espacio de datos y definir las medidas de seguridad necesarias.	Principio básico del ENS Análisis de riesgos **[op.pl.1]** Protección de la cadena de suministro **[op.ext.3]**
Políticas de seguridad	Establecer políticas de seguridad que aborden la clasificación de datos, los controles de acceso y las mejores prácticas de cifrado.	Política de seguridad **[org.1]** Normativa de seguridad **[org.2]** Procedimientos de seguridad **[org.3]** Proceso de autorización **[org.4]**
Seguridad por diseño	Integrar la seguridad desde el principio en la arquitectura y el diseño del espacio de datos: • Aislamiento • Segmentación • Refuerzo de plataforma en la nube	Arquitectura de seguridad **[op.pl.2]** Dimensionamiento / gestión de la capacidad **[op.pl.4]** Protección de servicios en la nube **[op.nub.1]**

	• Perímetro de red • Seguridad basada en host	Separación de flujos de información en la red **[mp.com.4]** Desarrollo de aplicaciones **[mp.sw.1]** Aceptación y puesta en servicio **[mp.sw.2]**

Adquisición y Configuración		
Medida	**Descripción**	**Referencia ENS**
Selección de tecnología segura	Elegir tecnologías y plataformas que sean seguras y cumplan con los requisitos de cifrado y autenticación: • Zero trust • Protección perimetral • DLP	Adquisición de nuevos componentes **[op.pl.3]** Componentes certificados **[op.pl.5]** Perímetro seguro **[mp.com.1]**
Configuración segura	Configurar los sistemas y servicios del espacio de datos siguiendo las mejores prácticas de seguridad, como deshabilitar características innecesarias y aplicar parches de seguridad.	Inventario de activos **[op.exp.1]** Configuración de seguridad **[op.exp.2]** Gestión de la configuración de seguridad **[op.exp.3]** Mantenimiento y actualizaciones de seguridad **[op.exp.4]** Interconexión de sistemas **[op.ext.4]**

Ingesta de Datos		
Medida	**Descripción**	**Referencia ENS**
Validación de datos	Implementar controles para validar la calidad y la integridad de los datos antes de ingresarlos al espacio de datos. Calificar los datos.	Protección de la confidencialidad **[mp.com.2]** Protección de la integridad y de la autenticidad **[mp.com.3]** Datos personales **[mp.info.1]** Calificación de la información **[mp.info.2]**
Cifrado de datos en tránsito	Utilizar protocolos seguros para cifrar los datos mientras se transmiten hacia el espacio de datos.	Criptografía **[mp.si.2]** Protección de claves criptográficas **[op.exp.10]**

Almacenamiento y procesamiento		
Medida	**Descripción**	**Referencia ENS**
Cifrado de datos en reposo	Almacenar los datos en el espacio de datos en formato cifrado para protegerlos contra el acceso no autorizado.	Criptografía **[mp.si.2]** Protección de claves criptográficas **[op.exp.10]**
Control de acceso:	Utilizar políticas de control de acceso y autenticación para limitar quién puede acceder a los datos y realizar operaciones en el espacio de datos.	Control de acceso **[op.acc]** Identificación **[op.acc.1]** Requisitos de acceso **[op.acc.2]** Segregación de funciones y tareas **[op.acc.3]** Mecanismo de autenticación (usuarios externos) **[op.acc.5]** Mecanismo de autenticación (usuarios de la organización) **[op.acc.6]** Proceso de gestión de derechos de acceso **[op.acc.4]** Registro de la actividad **[op.exp.8]**
Gestión de claves	Implementar una sólida gestión de claves para garantizar la seguridad de las claves de cifrado.	Protección de claves criptográficas **[op.exp.10]**

Gestión de metadatos		
Medida	**Descripción**	**Referencia ENS**
Control de metadatos	Proteger los metadatos que describen los datos en el espacio de datos, ya que también pueden ser valiosos para los atacantes.	Datos personales **[mp.info.1]** Marcado de soportes **[mp.si.1]** Limpieza de documentos **[mp.info.5]** Vigilancia **[op.mon.3]**
Registro de cambios	Llevar un registro de cambios en los metadatos para detectar y responder a cambios no autorizados.	Gestión de cambios **[op.exp.5]**

Acceso y uso		
Medida	**Descripción**	**Referencia ENS**
Auditoría y monitorización	Establecer registros de auditoría para rastrear el acceso y las actividades de usuario en el espacio de datos. Registros de actividad, buscando patrones anormales. Supervisión de terceros.	Registro de la actividad **[op.exp.8]** Contratación y acuerdos de nivel de servicio **[op.ext.1]** Protección de la cadena de suministro **[op.ext.3]** Sistema de métricas **[op.mon.2]** Detección de intrusión **[op.mon.1]** Vigilancia **[op.mon.3]** Protección de servicios y aplicaciones web **[mp.s.2]** Protección de la navegación web **[mp.s.3]**
Capacitación y concienciación	Educar a los usuarios y administradores sobre las políticas de seguridad y las mejores prácticas de uso seguro de datos.	Caracterización del puesto de trabajo **[mp.per.1]** Deberes y obligaciones **[mp.per.2]** Concienciación **[mp.per.3]** Formación **[mp.per.4]** Protección de la navegación web **[mp.s.3]**

Mantenimiento y actualización		
Medida	**Descripción**	**Referencia ENS**
Parches y actualizaciones	Mantener al día todos los sistemas y software relacionados con el espacio de datos mediante la aplicación de parches de seguridad.	Mantenimiento y actualizaciones de seguridad **[op.exp.4]** Gestión de cambios **[op.exp.5]** Protección frente a código dañino **[op.exp.6]**
Evaluaciones de seguridad	Realizar pruebas regulares de penetración y evaluaciones de seguridad para identificar y remediar vulnerabilidades.	Pruebas periódicas **[op.cont.3]** Medios alternativos **[op.cont.4]**

Desactivación y eliminación		
Medida	**Descripción**	**Referencia ENS**
Eliminación segura	Cuando se retire el espacio de datos, asegurarse de eliminar los datos de manera segura y de acuerdo con las políticas de retención y purga.	Borrado y destrucción **[mp.si.5]**

Plan de Respuesta a Incidentes, respaldo y recuperación – continuidad del negocio		
Medida	**Descripción**	**Referencia ENS**
Plan de respuesta a incidentes, respaldo y recuperación	Desarrollar y mantener un plan de respuesta a incidentes que detalla cómo se deben abordar las brechas de seguridad si se producen. Respaldo y recuperación. Continuidad del negocio.	Gestión de la configuración de seguridad **[op.exp.3]** Gestión de incidentes **[op.exp.7]** Registro de la gestión de incidentes **[op.exp.9]** Análisis de impacto **[op.cont.1]** Plan de continuidad [**op.cont.2]** Copias de seguridad **[mp.info.6**] Protección de la navegación web **[mp.s.3]** Protección frente a la denegación de servicio **[mp.s.4]**

Revisión y Mejora Continua		
Medida	**Descripción**	**Referencia ENS**
Revisión y mejora continua	Realizar revisiones regulares de la seguridad del espacio de datos y ajustar las medidas de seguridad según sea necesario para hacer frente a las amenazas emergentes	Mantenimiento y actualizaciones de seguridad **[op.exp.4]** Gestión de cambios **[op.exp.5]** Protección frente a código dañino **[op.exp.6]**

En el caso particular de que se trate de un espacio de datos en la nube, se deberán adaptar estas medidas para una solución en la nube. La guía CCN-STIC-823 *Utilización de Servicios en la Nube* recoge los aspectos que deberían de contemplarse para la adopción de la nube como paradigma tecnológico para la disposición de servicios con unas garantías de seguridad adecuadas, acordes con el ENS.

2.6 Sistema de vigilancia continua

La monitorización permite una mejora continua de la gestión y seguridad integral del espacio de datos. Debe llevarse a cabo en diferentes ámbitos e **incluir a terceros**:

- **Monitorización continua**: Establecer un sistema de monitorización continuo para detectar y responder rápidamente a posibles amenazas o anomalías en la seguridad.
- **Automatización** de la detección de comportamiento anómalo.
- **Auditoría y Registro**: Registrar y auditar todas las actividades en el espacio de datos para rastrear quién accede a los datos y qué acciones realizan.
- **Auditorías periódicas y pruebas de penetración** para garantizar que se cumplen todos los requisitos de ciberseguridad y que todas las medidas de seguridad están actualizadas y son adecuadas. Esto es fundamental para el cumplimiento normativo y para detectar posibles amenazas de seguridad.
- **Cumplimiento Normativo**: Asegurarse de cumplir con las regulaciones y normativas aplicables en relación con la privacidad y la protección de datos, como el RGPD.

2.7 Plan de respuesta a incidentes

La implementación de un plan de respuesta a incidentes es esencial para la gestión efectiva de cualquier amenaza a la seguridad en un espacio de datos. Este **plan integral** debe incluir la **detección temprana**, **investigación**, **respuesta** y **minimización del impacto**.

- Para lograr una **detección temprana,** se establecen sistemas de monitoreo continuo y alertas automáticas para identificar actividades sospechosas.
- En la fase de **investigación**, se designa un equipo especializado que lleva a cabo una evaluación exhaustiva y recopila evidencia forense para comprender la naturaleza y el alcance del incidente.
- La **respuesta** se basa en acciones predefinidas para abordar incidentes específicos, mientras que la **minimización del impacto** se centra en mitigar los efectos adversos.
- Tras efectuar una respuesta, comienza la fase de **recopilación de información del incidente**, revisar los eventos de seguridad y determinar los activos internos que han sufrido el intento de ataque. Esta información tendrá que ir debidamente documentada, así como las acciones llevadas a cabo en el momento de su detención.
- **Restauración de los sistemas** y servicios siguiendo un plan establecido y finalmente la **resolución y cierre del incidente** determinando el impacto del ciberataque y reforzando las políticas y medidas de seguridad necesarias

Un aspecto fundamental del plan es la **definición clara de roles y responsabilidades**, asegurando una **respuesta coordinada y eficiente**, así como la notificación oportuna y gestión de brechas de seguridad si ocurren. Este plan de respuesta estará **alineado con lo previsto en el artículo 33 del ENS** y la Instrucción Técnica de Seguridad y guías de aplicación correspondientes.

2.8 Plan de respaldo y recuperación – continuidad del negocio

La implementación de un plan de respaldo y recuperación sólido es esencial para **garantizar la disponibilidad** de los datos en situaciones de fallos o desastres.

Este plan debe contemplar la creación regular de **copias de seguridad** de los datos almacenados en el espacio de datos, **asegurando su integridad y consistencia,** así como indicar los controles para el acceso autorizado a dichas copias de respaldo. En función de la categorización de seguridad de la información, podría ser necesario realizar **copias regulares de seguridad de la configuración del sistema**.

Además, se deben establecer procedimientos claros para la rápida recuperación de los datos en caso de pérdida o corrupción. Esto implica la **designación de ubicaciones** de respaldo seguras, preferiblemente fuera del sitio principal, y la **validación periódica** de la efectividad de las copias de seguridad mediante pruebas de recuperación.

La implementación de un plan de respaldo y recuperación no solo **asegura la continuidad operativa**, sino que también minimiza los tiempos de inactividad y preserva la integridad de los datos frente a eventos imprevistos.

2.9 Certificación de la Conformidad con el ENS

Una forma reconocida de garantizar que se dispone del mínimo requerido de seguridad en los espacios de datos es mediante la certificación acreditada de los sistemas de información en los que se apoyan.

El proceso de certificación consiste en que una entidad tercera independiente, que tenga acreditada su competencia técnica e imparcialidad, realice una auditoría de Certificación de la Conformidad respecto a algún framework de seguridad de la información, o ciberseguridad, reconocido.

Un posible framework certificable, al que ya hemos dedicado apartados previos en esta guía, es el Esquema Nacional de Seguridad. Las Certificaciones de Conformidad con el ENS las pueden otorgar los siguientes organismos de certificación que se basarán internamente entre otras, en la norma ISO/IEC 17065:2012:

- Una Entidad de Certificación (EC) acreditada por la Entidad Nacional de Acreditación (ENAC).
- Un Órgano de Auditoría Técnica (OAT) del Sector Público, reconocido por el Centro Criptológico Nacional (CCN), en su ámbito de competencias.
- En determinados casos específicos, directamente el CCN.

La Certificación de Conformidad puede realizarse en cualquiera de las tres posibles categorías para un sistema de información (BÁSICA, MEDIA o ALTA) de forma estándar, o en base a un Perfil de Cumplimiento Específico que pueda llegar a aprobarse por el CCN en virtud de sus competencias.

3. CONCLUSIONES

No hay duda de que los **datos son un activo fundamental** para las empresas. Procesados de manera adecuada, generan grandes ventajas competitivas, tanto en la toma de decisiones como en la generación de nuevos productos y servicios, habilitando tecnologías como la Inteligencia Artificial.

El intercambio de datos **impulsa la eficiencia en las cadenas de suministro**, favoreciendo un desarrollo de productos más rápido e innovador. Al compartir sus datos, las organizaciones también se benefician del acceso a datos de terceros, que pueden ser de gran utilidad en diversos campos: desde el entrenamiento de sistemas de machine learning, hasta el enriquecimiento de analíticas internas. A ello hay que sumar también beneficios a nivel de transparencia y reputación.

Para que este intercambio de datos se realice de una manera segura es **necesario contar con entornos seguros y controlados donde exista una gobernanza clara, como los espacios de datos.**

Los espacios de datos se han convertido en pilares fundamentales para el **almacenamiento, intercambio y análisis de información** en diversos campos, desde la investigación científica hasta la toma de decisiones empresariales.

Ante este escenario de economía del dato, es necesario que toda esta información que formará parte del espacio de datos, esté bien gobernada, gestionada y con el nivel de calidad adecuado. Para ello, las **especificaciones UNE** relativas al dato proporcionan un marco de referencia sólido y armonizado.

Además, deberá tenerse en cuenta el marco normativo al que está sujeto los datos, como es el RGPD, el Reglamento de Datos o el Reglamento de Gobernanza de Datos, entre otros, conformando un conjunto integral para la regulación de la gestión de datos en el ámbito europeo.

También, las organizaciones deben **abordar los riesgos de seguridad y cumplimiento** asociados a los espacios de datos, empezando por crear una forma eficaz y eficiente de identificar y clasificar los datos por contenido, escenarios de uso, sensibilidad a la privacidad y seguridad, tipos y posibles grupos de usuarios con un catálogo que permita la búsqueda y recuperación de datos. También debe haber un método conveniente para separar los datos que se quieren conservar de los que se quieren eliminar.

La **calidad del dato** resulta muy importante en este aspecto, ya que tiene un impacto directo en la compartición de datos entre organizaciones, siendo una variable clave en el éxito del nuevo paradigma de los espacios de datos. Cuando los datos son de alta calidad, se crea un entorno propicio para el intercambio de información precisa y consistente, lo cual permite a las organizaciones colaborar de manera más efectiva, fomentando la innovación y el desarrollo conjunto de soluciones.

Es esencial que las organizaciones **cuenten con personal** con conocimientos adecuados no sólo para crear sino para gestionar un espacio de datos de forma continua.

Ante la cuestión de qué requisitos de seguridad deben cumplir los espacios de datos, estos se resumen en los que aplican a cualquier sistema de información, es decir, una gestión adecuada de los **controles de acceso**, **protección de la información** y **establecimiento de políticas** que permitan una adecuada gobernanza, gestión de la privacidad y supervisión del cumplimiento.

Esta gestión se traduce en la **implantación de las medidas de seguridad** del Esquema Nacional de Seguridad acordes a su categoría de seguridad, en el marco organizativo (políticas, normativa y procedimientos), operacional (planificación, control de acceso, explotación…) y de protección (gestión del personal, protección de los equipos perímetro seguro…) orientadas a garantizar que la organización pueda cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias cuando utiliza un sistema de información.

Se debe contemplar la posibilidad de que los espacios de datos puedan acogerse a un **Perfil de Cumplimiento Específico**, lo que posibilitaría implantar las medidas de seguridad necesarias y adaptadas a su caso particular y además disponer de guías de configuración.

ANEXO: REFERENCIAS

1. ENISA. Health Threat Landscape: Health Sector. [En línea] 05 de Julio de 2023. https://www.enisa.europa.eu/publications/health-threat-landscape.

2. Marín, Jose Luis. Buenas prácticas para medir el impacto de los datos abiertos en Europa. [En línea] Julio de 2023. https://datos.gob.es/sites/default/files/doc/file/informe-buenas-practicas-es.pdf.

3. CCN. Servicios CCN-CERT Sector Salud. [En línea] 19 de Junio de 2018. https://www.ccn-cert.cni.es/es/pdf/documentos-publicos/i-encuentro-salud/2946-servicios-ccn-cert-sector-salud/file?format=html.

4. AEPD. Aproximación a los espacios de datos desde la perspectiva del RGPD. [En línea] Mayo de 2023. https://www.aepd.es/documento/aproximacion-espacios-datos-rgpd.pdf.

5. CCN. Ciberamenazas Sector Salud. [En línea] 19 de Junio de 2018. https://www.ccn-cert.cni.es/es/pdf/documentos-publicos/i-encuentro-salud/2949-ciberamenazas-sector-salud/file?format=html.

6. DOUE. 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. [En línea] 4 de mayo de 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679.

7. BOE. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. [En línea] 5 de diciembre de 2018. https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf.

8. —. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. [En línea] 4 de mayo de 2022. https://www.boe.es/buscar/pdf/2022/BOE-A-2022-7191-consolidado.pdf.

9. Gartner. 2023 Technology Adoption Roadmap for Security and Risk Management. [En línea] 22 de septiembre de 2022.

10. —. Building Data Lakes Successfully - Part 1 - Architecture, Ingestion, Storage and Processing. [En línea] 7 de octubre de 2020. https://www.gartner.com/en/documents/3991474.

11. —. Building Data Lakes Successfully - Part 2 - Consumption, Governance and Operationalization. [En línea] 7 de octubre de 2020. https://www.gartner.com/en/documents/3991480.

12. eSecurity Planet. Security Considerations for Data Lakes. [En línea] 11 de agosto de 2022. https://www.esecurityplanet.com/applications/data-lake-security/.

13. Open Data Science. Best practices for datalake security. Open Data Science. [En línea] 22 de mayo de 2023. https://opendatascience.com/best-practices-for-data-lake-security/.

14. MAETD. Proyecto Espacio Nacional Datos Salud. [En línea] https://espanadigital.gob.es/lineas-de-actuacion/data-lake-sanitario.

15. NIST. NIST SP 800-207A. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments. [En línea] Septiembre de 2023. https://csrc.nist.gov/pubs/sp/800/207/a/final.

16. —. NIST SP 800-207A. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments. [En línea] 18 de abril de 2023. https://csrc.nist.gov/pubs/sp/800/207/a/ipd.

17. UNE. UNE 0077:2023 Gobierno del Dato. [En línea] marzo de 2023. https://tienda.aenor.com/norma-une-especificacion-une-0077-2023-n0071116.

18. —. UNE 0078:2023 Gestión del Dato. [En línea] marzo de 2023. https://tienda.aenor.com/norma-une-especificacion-une-0078-2023-n0071117.

19. —. UNE 0079:2023 Gestión de la Calidad del Dato. [En línea] marzo de 2023. https://tienda.aenor.com/norma-une-especificacion-une-0079-2023-n0071118.

20. —. UNE 0080:2023 Guía de Evaluación del Gobierno, Gestión y Gestión de la Calidad del Dato. [En línea] junio de 2023. https://tienda.aenor.com/norma-une-especificacion-une-0080-2023-n0071383.

21. —. UNE 0081:2023 Guía de Evaluación de la Calidad de un Conjunto de Datos. [En línea] septiembre de 2023. https://tienda.aenor.com/norma-une-especificacion-une-0081-2023-n0071807.

22. ENISA. Cloud Security for Healthcare Services. [En línea] 18 de enero de 2021. https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services.

23. —. Deploying Pseudonymisation Techniques. [En línea] 24 de marzo de 2022. https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques.

24. DOUE. 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. [En línea] 22 de diciembre de 2023. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32023R2854.

25. European webinar on developments in the data spaces of the future. [En línea] 19 de mayo de 2023. https://datos.gob.es/en/noticia/european-webinar-developments-data-spaces-future.

26. Oficina de Publicaciones de la Unión Europea. European data spaces and the role of open data. [En línea] 20 de noviembre de 2023. https://op.europa.eu/en/publication-detail/-/publication/70d01867-8ce1-11ee-8aa6-01aa75ed71a1/language-en.

27. La importancia de desplegar espacios europeos de datos. [En línea] 30 de marzo de 2022. https://datos.gob.es/es/blog/la-importancia-de-desplegar-espacios-europeos-de-datos.

28. Data Spaces Support Centre. DSSC Glossary. [En línea] marzo de 2023. https://dssc.eu/space/Glossary/55443460/DSSC+Glossary+%7C+Version+1.0+%7C+March+2023.

29. DOUE. Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos. [En línea] 3 de junio de 2022. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32022R0868.

30. International Data Spaces Association. Design Principles for Data Spaces. [En línea] abril de 2021. https://design-principles-for-data-spaces.org/.

31. Dato, Oficina del. Plan de actuaciones para el despliegue de espacios de datos. [En línea] Marzo de 2024. https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2024/OdD-Plan_actuaciones_despliegue_espacios_datos_v1-0.pdf.

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL