centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 823

Uso seguro de Servicios en la Nube en el marco del ENS



Noviembre 2026

Edita:

centro criptológico nacional

© Centro Criptológico Nacional, 2026

centro criptológico nacional
Firmado digitalmente por CCN
Fecha: 2026.11.16 15:34:21 +01'00'

Fecha de Edición: noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN 4
1.1 OBJETIVO DE LA GUÍA 4
1.2 ALCANCE Y DESTINATARIOS 4
1.3 MARCO NORMATIVO Y MARCO DE REFERENCIA 5
1.4 ESTRUCTURA Y CONTENIDO DE LA GUÍA 6
2. CONCEPTOS 7
2.1 MODELOS DE SERVICIO 7
2.2 MODELOS DE DESPLIEGUE 9
2.3 CONSIDERACIONES GENERALES PARA CADA MODELO DE DESPLIEGUE EN EL CONTEXTO DEL SECTOR PÚBLICO 10
3. ESTRATEGIA DE ADOPCIÓN DE SERVICIOS EN LA NUBE 12
3.1 CUMPLIMIENTO NORMATIVO Y SEGURIDAD EN LA NUBE 12
3.2 SOBERANÍA DEL DATO 14
3.3 GOBERNANZA Y RESPONSABILIDAD COMPARTIDA 18
3.3.1 ROLES Y RESPONSABILIDADES 19
3.3.2 RELACIÓN CON EL PROVEEDOR DE SERVICIOS EN LA NUBE 21
3.3.3 SUPERVISIÓN 23
3.4 CONTRATACIÓN DE SERVICIOS EN LA NUBE 24
4. SEGURIDAD EN EL CICLO DE VIDA DEL SERVICIO EN LA NUBE 27
4.1 PLANIFICACIÓN Y ANÁLISIS DE RIESGOS 27
4.2 EVALUACIÓN Y ADOPCIÓN DE SOLUCIONES TECNOLÓGICAS 29
4.3 IMPLEMENTACIÓN SEGURA 30
4.4 MONITORIZACIÓN, AUDITORÍA Y MEJORA CONTINUA 32
4.5 GESTIÓN DE INCIDENCIAS Y CONTINUIDAD DEL SERVICIO 34
4.6 FINALIZACIÓN DEL SERVICIO Y REVERSIBILIDAD 35
ANEXO A — ACRÓNIMOS 37
ANEXO B — MATRIZ DE RESPONSABILIDAD 39
ANEXO C — TRAZA NORMATIVA ENS-REGLAMENTO DE EJECUCIÓN (UE) 2024/2690 PARA PROVEEDORES DE SERVICIOS DE COMPUTACIÓN EN NUBE 46

1. INTRODUCCIÓN

1.1 Objetivo de la guía

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), establece **los principios básicos** y **los requisitos mínimos** necesarios para una protección adecuada de la información tratada y de los servicios prestados por las entidades del sector público. En este contexto, el uso de servicios en la nube representa un paradigma tecnológico que debe alinearse plenamente con las exigencias del ENS para garantizar la seguridad de los sistemas de información.

Cabe recordar que el ENS no solo es de aplicación a los **sistemas de información del sector público, sino también a aquellos del sector privado que, en virtud de una relación contractual, presten servicios competenciales a las entidades del sector público**, tal y como establece el artículo 2.3 del citado Real Decreto 311/2022. Asimismo, cualquier organización, independientemente de su naturaleza jurídica, puede optar por aplicar voluntariamente el ENS como marco de referencia para mejorar la seguridad de sus sistemas.
La externalización creciente de servicios TIC hacia entornos de computación en la nube plantea nuevos retos en materia de **seguridad**, **gobernanza** y **cumplimiento normativo**. Aspectos como la correcta **identificación y asignación de responsabilidades** entre la entidad usuaria y el proveedor de servicios en la nube, una adecuada **gestión de riesgos**, la inclusión de **cláusulas contractuales específicas** y la **elaboración de Declaraciones de Aplicabilidad** adaptadas al entorno de servicios en la nube se vuelven esenciales para garantizar un uso seguro y conforme al ENS.

El objetivo de la presente guía es proporcionar un marco de referencia técnico y normativo para el uso seguro de servicios en la nube por parte de las entidades del sector público, así como de los proveedores que les prestan dichos servicios. La guía aborda aspectos clave a lo largo de todo el ciclo de vida de un servicio en la nube, como la **planificación estratégica**, la **contratación**, la **implantación de medidas de seguridad**, la **supervisión continua**, la **gestión de incidentes** y la **finalización y reversibilidad del servicio**. Todo ello, en coherencia con las disposiciones del ENS y del resto del marco normativo vigente en materia de seguridad de la información.

1.2 Alcance y destinatarios

La presente guía está dirigida a todas aquellas **entidades del sector público que utilicen, estén considerando utilizar o presten servicios en la nube** en el ejercicio de sus competencias, así como a aquellas **entidades privadas que proporcionen servicios en la nube a entidades del sector público o que se sirvan de servicios en la nube para tal prestación** y que, por tanto, se encuentran bajo el ámbito de aplicación del ENS.
La guía se estructura siguiendo el **ciclo de vida del servicio en la nube**, desde su planificación hasta su reversibilidad. Adicionalmente, se incorporan una serie de anexos de apoyo. La finalidad última es facilitar a las entidades públicas y a sus proveedores la utilización de servicios en la nube con garantías de seguridad, cumplimiento y confianza.

1.3 Marco normativo y marco de referencia

La presente guía se enmarca dentro del conjunto de normas y estrategias aplicables al uso de servicios en la nube en el sector público, incluyendo, entre otras, las siguientes:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Reglamento (UE) 2016/679, General de Protección de Datos (RGPD).
- Directiva (UE) 2022/2555 (NIS2), relativa a medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.
- Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad (ENI) en el ámbito de la Administración Electrónica.
- Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento Europeo de Inteligencia Artificial).
- Ley de Contratos del Sector Público: Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, en los aspectos desarrollados en la presente Guía.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en lo relativo a la ubicación dentro del territorio de la Unión Europea de los sistemas de información y comunicaciones destinados al tratamiento de determinadas categorías de datos (artículo 46 bis, introducido por el Real Decreto-ley 14/2019, de 31 de octubre).
- Estrategia de Servicios en la Nube Híbrida para las Administraciones Públicas.
- Esquema Europeo de Certificación de Ciberseguridad para Servicios Cloud (EUCS)
- Plan de Digitalización de las Administraciones Públicas.

La presente relación no tiene carácter exhaustivo, pudiendo ser de aplicación otras disposiciones normativas, especialmente de carácter sectorial, que deberán ser

consideradas atendiendo al ámbito de actividad y a las particularidades de los servicios en la nube objeto de adopción.

Este marco normativo proporciona el contexto legal y estratégico necesario para garantizar que el uso de servicios en la nube se realice de forma segura y conforme a los principios de legalidad, proporcionalidad, responsabilidad, trazabilidad, seguridad por defecto y por diseño, y vigilancia continua, establecidos por el ENS.

1.4 Estructura y contenido de la guía

La presente guía se organiza con el objetivo de proporcionar un marco claro y práctico para el uso seguro de servicios en la nube, abordando tanto los **aspectos conceptuales y estratégicos** como los **operativos y de seguridad** a lo largo de todo el **ciclo de vida de dichos servicios**.

El documento se articula en cuatro epígrafes principales, complementados por anexos de apoyo.

El **epígrafe 1** recoge las disposiciones introductorias de la guía: su objetivo, el alcance y los destinatarios, el marco normativo y de referencia aplicable, y la presente descripción de la estructura del documento.

En el **epígrafe 2** se introducen los conceptos y los elementos fundamentales necesarios para comprender el desarrollo de la guía, describiendo los **modelos de servicio en la nube** y los **modelos de despliegue**, con el fin de establecer una base común que facilite una interpretación homogénea del resto del documento, así como consideraciones generales para cada modelo de despliegue en el contexto del sector público.

En el **epígrafe 3**, se desarrolla la **estrategia de adopción de servicios en la nube**, abordando los factores clave que deben guiar la toma de decisiones desde un enfoque estratégico, orientado a responsables públicos y decisores. Se tratan, entre otros, el cumplimiento normativo y la seguridad en la nube, la soberanía del dato y la jurisdicción aplicable, así como los aspectos de gobernanza, la responsabilidad compartida, la definición de roles y responsabilidades, la relación con el proveedor de servicios en la nube (CSP), la supervisión de los servicios contratados y la contratación de soluciones en la nube.

El **epígrafe 4** se centra en la **seguridad a lo largo del ciclo de vida del servicio en la nube**, abordando su adopción como un **proceso continuo**, y no como una decisión puntual. Se analizan las distintas fases del ciclo de vida, incluyendo la planificación y el análisis de riesgos, la evaluación y adopción de soluciones tecnológicas, la implementación segura, la monitorización y auditoría, la gestión de incidencias y la continuidad del servicio, y la finalización del servicio y la reversibilidad, aspectos esenciales para evitar dependencias tecnológicas y garantizar el control sobre la información a largo plazo.

Finalmente, la guía se completa con una serie de **ANEXO** A — ACRÓNIMOS, que recopilan información de apoyo, incluyendo acrónimos, una matriz de responsabilidades por modelo de servicio y trazas normativas.

Estructura general de la guía

Esta estructura permite al lector consultar la guía de forma transversal o secuencial, en función de sus responsabilidades y necesidades, sirviendo tanto como documento de referencia general como herramienta de apoyo en proyectos concretos de uso de servicios en la nube.

2. CONCEPTOS

En este epígrafe se definen los conceptos fundamentales empleados en la guía, estableciendo un marco terminológico común que facilite la comprensión y aplicación de las recomendaciones posteriores. Se abordan los **modelos de servicio** y **modelos de despliegue** en la nube, así como las principales consideraciones específicas que deben tenerse en cuenta en el contexto del sector público.

A efectos de esta guía, se utiliza preferentemente el término nube para referirse a los servicios de *cloud computing*. Las expresiones en inglés solo se emplean en siglas ampliamente conocidas o denominaciones oficiales para facilitar su comprensión. Por ejemplo, *Cloud Service Provider (CSP)* se refiere al proveedor de servicios en la nube. De igual modo, *Cloud Service Customer (CSC)* designa a la entidad usuaria o cliente que consume los servicios en la nube, en contraposición al proveedor que los ofrece.

2.1 Modelos de servicio

Los modelos de servicio en la nube se distinguen por el alcance de las responsabilidades asumidas respectivamente por el proveedor de servicios en la nube (*Cloud Service Provider,* **CSP**) y por la entidad cliente (*Cloud Service Customer*, **CSC**). Esta distinción es clave para establecer correctamente las obligaciones contractuales en materia de seguridad y cumplimiento normativo.

Desde una perspectiva tanto contractual como de gestión del riesgo, es esencial identificar con precisión el **modelo de servicio que se va a contratar**, ya que de ello dependen aspectos clave como el grado de personalización posible, el esfuerzo operativo requerido, el cumplimiento de requisitos legales y, en especial, la **asignación de responsabilidades en materia de seguridad.**

Cada modelo de servicio establece **cómo se gestionan las distintas capas del servicio** (infraestructura física y virtual, plataforma de software, aplicaciones y datos) y quién es responsable de cada una. Esta distribución de responsabilidades debe quedar **claramente definida** en el contrato y sus anexos técnicos (por ejemplo, en el Acuerdo de Nivel de Servicio – SLA).

Además, es necesario establecer mecanismos que permitan supervisar y verificar el cumplimiento de dichas responsabilidades durante toda la vigencia del servicio, ya sea mediante la Declaración de Aplicabilidad de seguridad u otros instrumentos equivalentes que aporten evidencias de la correcta implantación de los controles de seguridad pactados.

Los principales modelos de servicio en la nube son los siguientes:

- **Infraestructura como Servicio (*Infrastructure as a Service*, IaaS):** en este modelo el proveedor (CSP) ofrece recursos de infraestructura tales como capacidad de procesamiento, almacenamiento y redes. El cliente (CSC) despliega y gestiona sobre dicha infraestructura sus propios sistemas operativos, aplicaciones y datos. El CSP es responsable de la seguridad y disponibilidad de la infraestructura subyacente (instalaciones físicas, hardware, red física y capa de virtualización). Por su parte, el CSC asume la responsabilidad de la configuración segura, la gestión y actualización de los sistemas operativos que instala, de sus aplicaciones, la gestión de usuarios y accesos, así como de proteger la información tratada en la nube.

  Dentro de este ámbito han surgido modalidades especializadas como los **Contenedores como Servicio (Container as a Service, CaaS)**, en las que el CSP proporciona plataformas gestionadas para la ejecución y orquestación de contenedores. En estos casos, el proveedor asume responsabilidades adicionales relacionadas con la gestión de la infraestructura y de los servicios de orquestación, mientras que el CSC mantiene la responsabilidad sobre las aplicaciones desplegadas, las imágenes de contenedor utilizadas, su configuración de seguridad y la protección de los datos tratados. Aunque presentan características propias, estos servicios pueden considerarse una evolución o especialización de los modelos basados en infraestructura, situándose habitualmente entre IaaS y PaaS.

- **Plataforma como Servicio (*Platform as a Service*, PaaS):** el CSP ofrece una plataforma que incluye la infraestructura, el sistema operativo, las herramientas de ejecución y otros componentes necesarios para desplegar aplicaciones. El CSC no gestiona la infraestructura ni el sistema operativo, que son responsabilidad del CSP. En este modelo, el CSP debe garantizar la seguridad de la infraestructura y de la plataforma, mientras que el CSC es responsable del desarrollo seguro, configuración y protección de las aplicaciones y de la información tratada.

  Como evolución de este modelo han aparecido los servicios de **Funciones como Servicio (Function as a Service, FaaS) o entornos serverless**, en los que el CSP proporciona un entorno completamente gestionado para la ejecución de funciones o componentes de código bajo demanda. En estos servicios, el proveedor administra tanto la infraestructura como la plataforma de ejecución y los mecanismos de escalados asociados, mientras que el CSC conserva la responsabilidad sobre el código desarrollado, la configuración de las funciones, la gestión de identidades y permisos y la protección de la información procesada. Aunque presentan un mayor nivel de abstracción que los servicios PaaS tradicionales, comparten los mismos principios de responsabilidad compartida y pueden considerarse una modalidad especializada de dicho modelo.

- **Software como Servicio (*Software as a Service*, SaaS):** el CSP suministra aplicaciones completas accesibles, normalmente, a través de Internet, gestionando íntegramente la infraestructura subyacente, la plataforma y el propio software. El CSC no administra los componentes técnicos del servicio (no tiene que instalar ni mantener la aplicación en servidores propios), pero es

responsable de la correcta configuración del servicio, de la gestión de los usuarios y permisos, de la protección de la información introducida o tratada en la aplicación y del cumplimiento de la normativa que sea aplicable en el uso del servicio.

A medida que se avanza desde IaaS hacia modelos de mayor nivel de abstracción, como PaaS o SaaS, aumenta el alcance de los servicios gestionados por el CSP y disminuye la carga operativa asumida por el CSC. No obstante, esta reducción de responsabilidades técnicas no implica una transferencia completa de las obligaciones en materia de seguridad, gestión de riesgos o cumplimiento normativo, que continúan siendo compartidas entre ambas partes conforme a las condiciones del servicio contratado.

Con independencia del modelo de servicio adoptado o de la externalización de determinadas funciones en terceros, el CSC **mantiene en todo momento** la **responsabilidad última sobre la seguridad** de la información y el cumplimiento de la normativa aplicable. El modelo de responsabilidad compartida no exime al cliente de sus obligaciones; supone que el proveedor asume parte de las funciones (entre ellas, ciertas medidas de seguridad), mientras que la entidad usuaria sigue siendo responsable de su correcta definición, supervisión y cumplimiento.

2.2 Modelos de despliegue

Los modelos de despliegue definen cómo se organizan y ponen a disposición las infraestructuras y servicios tecnológicos (servidores, almacenamiento, redes y aplicaciones) en función de quién los controla y con quién se comparten:

Nube pública: la nube pública es un modelo en el que los recursos informáticos son propiedad de un proveedor externo y se ofrecen a múltiples clientes bajo un esquema de pago por uso. Los servicios son compartidos (modelo multi-tenant) y altamente escalables. El proveedor se encarga de la gestión, el mantenimiento y la seguridad de la infraestructura subyacente.

Nube privada: la nube privada es una infraestructura dedicada exclusivamente a una organización. Puede estar ubicada en las instalaciones propias (*on-premise*) o alojada por un tercero, pero su uso es exclusivo. Ofrece mayor control, personalización y, en algunos casos, mayor adecuación a requisitos normativos estrictos.

Nube híbrida: la nube híbrida combina los modelos de nube pública y privada, que permanecen como entidades distintas pero interconectadas, permitiendo compartir datos y aplicaciones. Está diseñada para aprovechar las ventajas de ambos modelos, como el mayor control de la nube privada y el menor coste o la escalabilidad de la nube pública.

Es habitual en organizaciones que desean mantener información sensible en entornos privados y aprovechar la flexibilidad de la nube pública para cargas variables.

2.3 Consideraciones generales para cada modelo de despliegue en el contexto del sector público

El uso de servicios en la nube en el sector público debe abordarse mediante un análisis integral que contemple su impacto en la seguridad de la información, el cumplimiento normativo, la eficiencia económica, la gobernanza y la soberanía del dato. La elección del modelo de despliegue (nube privada, pública o híbrida) deberá realizarse en función de estos factores y de forma coherente con la categorización del sistema conforme al ENS, el análisis de riesgos y los requisitos específicos del servicio.

A continuación, se presentan las principales características y aspectos a considerar para cada modelo de despliegue, sin perjuicio de que su idoneidad deba evaluarse en cada caso concreto.

Nube privada:

- Puede permitir **un mayor grado de control[1] sobre la configuración, operación y medidas de seguridad**, especialmente en entornos donde la entidad gestiona directamente la infraestructura o dispone de capacidades de administración sobre la misma.
- Permite establecer condiciones más restrictivas en relación con **la localización del dato, su tratamiento y los mecanismos de acceso**, en función del diseño del entorno.
- Requiere la asunción, total o parcial, de las **tareas de operación, mantenimiento y seguridad**, dependiendo del modelo de servicio y del grado de externalización.
- Puede implicar **mayores costes de inversión y operación**, especialmente en entornos *on-premise*, así como la necesidad de gestionar el ciclo de vida tecnológico de la infraestructura.
- La escalabilidad, resiliencia y capacidad de evolución tecnológica dependerán de las capacidades del entorno y del modelo de servicio.

Nube pública

- El nivel de control de la entidad usuaria sobre la infraestructura y los servicios depende del **modelo de servicio contratado (IaaS, PaaS o SaaS)**, siendo progresivamente menor a medida que aumenta el nivel de abstracción.
- Proporciona **alta escalabilidad y elasticidad**, facilitando la adaptación a variaciones de demanda.
- Permite un modelo económico basado en **pago por uso**, reduciendo la inversión inicial en infraestructura.
- Requiere analizar la **localización del dato y la jurisdicción aplicable**, en relación con los requisitos de soberanía del dato y cumplimiento normativo.

[1] El nivel de control efectivo dependerá del modelo de servicio utilizado (IaaS, PaaS o SaaS) y de las condiciones de provisión del servicio.

- Implica el uso de **entornos compartidos (*multi-tenant*)**, lo que exige evaluar los mecanismos de aislamiento lógico y segregación de clientes.
- Puede introducir **dependencia tecnológica del proveedor (*vendor lock-in*)**, siendo relevante considerar portabilidad y reversibilidad del servicio.
- La capacidad de **configuración de controles de seguridad** puede estar condicionada por el modelo de servicio y las restricciones del proveedor.
- Deben establecerse mecanismos de **monitorización, supervisión y auditoría, distribuidos entre proveedor y entidad usuaria** según el modelo de responsabilidad aplicable.

Nube híbrida

- Permite **la combinación de entornos de nube privada y nube pública**, facilitando una asignación flexible de sistemas, servicios y datos en función de criterios de seguridad, cumplimiento, eficiencia y optimización de recursos.
- Facilita la **segmentación de cargas de trabajo**, permitiendo ubicar cada componente en el entorno más adecuado según su criticidad, sensibilidad o variabilidad de demanda, en coherencia con el análisis de riesgos y la categorización del sistema.
- Permite **optimizar el equilibrio entre control y escalabilidad**, manteniendo entornos de mayor control para sistemas críticos y aprovechando la elasticidad de la nube pública para cargas variables o menos sensibles.
- Requiere establecer mecanismos **adecuados de interoperabilidad e integración segura** entre entornos, incluyendo aspectos de identidad, red, datos y monitorización.
- Permite una **gobernanza unificada de la seguridad**, mediante la definición de políticas coherentes aplicables de forma transversal a los distintos entornos.
- Facilita la **adaptación progresiva de los sistemas a la nube**, permitiendo estrategias de migración gradual o coexistencia de arquitecturas tradicionales y nube.
- Requiere definir claramente el **modelo de responsabilidades entre entornos y proveedores**, en función de los servicios utilizados y del grado de externalización.
- Permite mejorar **la resiliencia arquitectónica**, al distribuir servicios y cargas entre distintos entornos, reduciendo dependencias únicas.

En determinadas estrategias de uso de servicios en la nube en el ámbito del sector público, como la **Estrategia de Servicios en la Nube Híbrida para las Administraciones Públicas**[2], se contempla la distribución de cargas de trabajo en función de su criticidad, sensibilidad y requisitos normativos. En este contexto, los entornos de nube privada o de mayor control suelen emplearse para sistemas que gestionan información sensible o soportan procesos críticos, mientras que la nube pública se utiliza, principalmente,

[2] https://espanadigital.gob.es/sites/espanadigital/files/2025-05/2022_12_Estrategia_Cloud_AAPP.pdf

como complemento para cargas de trabajo con menores requisitos de protección o mayor variabilidad en la demanda.

No obstante, esta aproximación debe entenderse como un criterio de referencia, cuya aplicación concreta dependerá del análisis de riesgos, de la categorización del sistema conforme al Esquema Nacional de Seguridad y de las características específicas de cada servicio.

Consideraciones comunes

Con independencia del modelo de despliegue adoptado, deberán tenerse en cuenta las siguientes consideraciones:

- La **responsabilidad última** sobre la seguridad de la información **corresponde a la entidad del sector público**, de acuerdo con el ENS.
- El uso de servicios en la nube no exime del cumplimiento normativo, sino que **requiere adaptar los mecanismos de control y supervisión**.
- La seguridad efectiva dependerá de la **correcta configuración, gestión y supervisión de los servicios**, y no exclusivamente del modelo de despliegue seleccionado.
- Resulta imprescindible **realizar un análisis de riesgos específico**, que permita determinar la idoneidad del modelo y las medidas de seguridad necesarias.
- Deberán establecerse mecanismos adecuados de gobernanza, control y seguimiento, en particular en entornos con múltiples proveedores o modelos de servicio.

En consecuencia, la selección del modelo de nube deberá basarse en **criterios técnicos, organizativos y normativos**, alineados con el **análisis de riesgos y la categorización del sistema**, evitando decisiones basadas exclusivamente en factores económicos o de conveniencia tecnológica.

3. ESTRATEGIA DE ADOPCIÓN DE SERVICIOS EN LA NUBE

El uso de servicios en la nube en el sector público requiere una planificación estratégica que garantice el cumplimiento de la normativa vigente y la protección de los datos públicos. En este epígrafe, se presentan los pilares principales de dicha estrategia: desde las **exigencias legales y de seguridad**, pasando por la **soberanía del dato**, la **elección del modelo de nube adecuado según la sensibilidad de la información**, hasta una adecuada **gobernanza con responsabilidades compartidas** y las consideraciones para la **contratación** exitosa del servicio.

3.1 Cumplimiento normativo y seguridad en la nube

La **seguridad** y el **cumplimiento normativo** constituyen la base de cualquier estrategia de nube en la Administración. Antes de migrar servicios o datos a la nube, la entidad pública debe asegurarse de que se respetan todas las leyes y normativas aplicables, con

especial atención a las derivadas del ENS y a las relativas a protección de datos personales, servicios esenciales, etc.

El uso de servicios en la nube **exige salvaguardar la seguridad y el control sobre los datos** para mantener la autonomía estratégica y la confianza en los servicios públicos digitales. A continuación, se resumen los principales marcos normativos y requisitos que deben considerarse en materia de cumplimiento:

- **Esquema Nacional de Seguridad (ENS)**: Real Decreto 311/2022, de 3 de mayo. El ENS requiere **categorizar los sistemas de información según la valoración de la información manejada y de los servicios que soporta**, realizar **análisis de riesgos** e implantar medidas de seguridad adecuadas según el Anexo II del RD según la categoría del sistema (BÁSICA, MEDIA o ALTA) o de los niveles de las dimensiones de seguridad (BAJO, MEDIO o ALTO), todo ello con el objetivo de **garantizar la protección de los sistemas de información, asegurando la confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad de los datos**.

  Adicionalmente, relacionado con los servicios en la nube, existen **guías CCN-STIC** relacionadas con la configuración de seguridad y consideraciones.

- **Reglamento General de Protección de Datos (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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 - RGPD) y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**: Cuando la entidad pública utiliza servicios en la nube para tratar **datos de carácter personal**, **debe firmarse un contrato de encargado del tratamiento con el proveedor** (según el artículo 28 del RGPD) que establezca claramente las obligaciones de éste en materia de privacidad y seguridad.

  Asimismo, la LOPDGDD complementa al RGPD en el ordenamiento español, reforzando aspectos como: la protección de los derechos digitales, las obligaciones de los responsables y encargados del tratamiento, y el régimen sancionador, aspectos que deberán ser tenidos en cuenta de la definición de la estrategia de uso de servicios en la nube.

- **Esquema Nacional de Interoperabilidad (ENI):** Real Decreto 4/2010, de 8 de enero**. Garantiza que los sistemas de** información del sector público puedan compartir información y conocimiento, y trabajar conjuntamente de forma **coherente**. En el contexto de la nube, el ENI implica que las soluciones contratadas **deben permitir la integración y el intercambio de información con las entidades usuarias** de manera interoperable. Es decir, las aplicaciones en la nube deben ajustarse a estándares abiertos, protocolos y formatos comunes que faciliten la comunicación entre entidades y que eviten crear silos. Cumplir el ENI en la nube supone, entre otros, evitar dependencias de formatos propietarios cerrados, garantizar que se puedan extraer y compartir datos con terceros legítimos, y que los servicios ofrezcan APIs u otras interfaces normalizadas para interoperar. De este modo, el uso de la nube no comprometerá la interconexión entre entidades públicas ni la prestación integral de servicios al ciudadano.

- **Directiva NIS2**: 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 (NIS2), así como la normativa nacional que resulte de su transposición. Esta directiva establece un marco normativo de referencia en materia de ciberseguridad en la Unión Europea. Los proveedores de servicios de computación en la nube están identificados en el Anexo I como sectores de alta criticidad, incluidos en el ámbito de aplicación del Reglamento de Ejecución (UE) 2024/2690 de la Comisión.
- **Contratos del Sector Público**: Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, en los aspectos desarrollados en la presente Guía.

Estos marcos normativos, junto con otras guías y normas sectoriales específicas, constituyen el entorno regulatorio que debe regir cualquier migración o uso de servicios en la nube. La estrategia de uso de la nube deberá asegurar que los servicios se prestan con el nivel de **seguridad, privacidad y fiabilidad** requerido. Los siguientes epígrafes profundizarán en cómo abordar aspectos concretos como la soberanía del dato, la elección del modelo adecuado según sensibilidades, la gobernanza y la contratación, siempre manteniendo la conformidad con las normativas mencionadas.

3.2 Soberanía del dato

La soberanía del dato constituye un principio esencial en el uso de servicios en la nube, al estar directamente relacionada con el control efectivo de la información, el cumplimiento normativo y la adecuada gestión de riesgos. Este concepto hace referencia a la capacidad de la entidad responsable de la información y del tratamiento de los datos para garantizar que estos permanecen protegidos y sometidos a un marco jurídico compatible con los principios del ordenamiento jurídico español y europeo, con independencia del modelo de servicio o despliegue adoptado.

La soberanía del dato no depende de un único factor, sino de la **interacción de múltiples jurisdicciones concurrentes**, que deben analizarse de forma conjunta en cualquier estrategia de uso de servicios en la nube. Entre los elementos más relevantes destacan los siguientes:

a) Localización física de los datos

Hace referencia al lugar en el que los datos son almacenados y procesados, incluidas las copias de seguridad y los registros de actividad. Este factor condiciona qué autoridades territoriales tienen acceso o competencia sobre la información y qué normativa o medidas legales pueden aplicarse en función de la ubicación de las infraestructuras.

b) Jurisdicción del proveedor del servicio

Incluye las obligaciones legales derivadas del país en el que el proveedor está establecido, así como las aplicables a su matriz o grupo empresarial. Este aspecto resulta especialmente relevante en proveedores globales, ya que pueden estar sujetos a legislaciones nacionales con alcance extraterritorial que permitan a

determinadas autoridades solicitar acceso a datos, incluso cuando estos se encuentren almacenados fuera de dicho país.

c) Jurisdicción del responsable del tratamiento

En el ámbito del sector público, las entidades actúan como responsables del tratamiento, lo que implica la plena aplicación del Reglamento General de Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) y el Esquema Nacional de Seguridad (ENS), con independencia de la ubicación de los datos o del proveedor del servicio.

En consecuencia, el hecho de que una actividad esté sujeta al RGPD no excluye la posible aplicación simultánea de normativas extranjeras, pudiendo producirse conflictos de jurisdicción que deben ser identificados y evaluados desde la perspectiva del riesgo.

En este mismo contexto, debe considerarse lo dispuesto en la **Ley 9/2017, de Contratos del Sector Público (LCSP)**, en su redacción vigente tras las modificaciones introducidas por el **Real Decreto-ley 14/2019, de 31 de octubre**, que incorpora previsiones específicas aplicables a aquellos contratos cuya ejecución implique el tratamiento de datos personales por cuenta del responsable del tratamiento.

En estos supuestos, de conformidad con lo establecido en el artículo 122.2 de la LCSP, los pliegos de cláusulas administrativas particulares deberán incluir, entre otras, obligaciones orientadas a garantizar el control sobre la localización y las condiciones de prestación del servicio. En particular, cuando la ejecución del contrato requiera el tratamiento de datos personales por el contratista por cuenta del responsable del tratamiento, el adjudicatario deberá declarar, con carácter previo a la formalización del contrato, la **ubicación de los servidores y el lugar desde el que se prestarán los servicios asociados**, así como **comunicar cualquier modificación que se produzca durante la vigencia del contrato**.

Asimismo, en los términos previstos en la normativa de contratación pública y, en particular, en relación con el régimen de subcontratación recogido en el artículo 215 de la LCSP, los licitadores deberán indicar en su oferta si tienen previsto recurrir a la **subcontratación de los servicios asociados al tratamiento**, identificando el perfil empresarial de los subcontratistas. Estas previsiones refuerzan las exigencias de control sobre la **jurisdicción efectiva del tratamiento de los datos**, así como sobre la cadena de prestación del servicio, aspectos que resultan especialmente relevantes en entornos de computación en la nube.

Desde el punto de vista del riesgo, la utilización de proveedores de servicios en la nube sujetos a legislaciones de terceros países puede introducir riesgos específicos para la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, entre los que destacan:

- La posibilidad de acceso a los datos por parte de autoridades extranjeras en virtud de normativa local o extraterritorial.

- Limitaciones en la capacidad de la entidad pública para ser informada de dichos accesos o para oponerse a los mismos.
- Dificultades para garantizar el cumplimiento efectivo de los principios, derechos y garantías establecidos en el RGPD.
- Pérdida de control efectivo sobre la información y sobre los mecanismos de protección aplicados.

Estos riesgos deberán ser identificados, analizados y evaluados en el análisis de riesgos del sistema de información (véase epígrafe **4.1 Planificación y análisis de riesgos**), en coherencia con los principios del ENS, especialmente los relativos a la gestión de riesgos, la diferenciación de responsabilidades y el control de accesos, y adoptando las medidas de seguridad correspondientes.

En relación con la localización, y sin perjuicio de las obligaciones específicas en materia de transparencia y control sobre la ubicación de la infraestructura recogidas en la normativa de contratación pública (Ley 9/2017, de Contratos del Sector Público) anteriormente indicadas, se recomienda, como principio general, que el almacenamiento y tratamiento de los datos del sector público se realice dentro del Espacio Económico Europeo (EEE), especialmente cuando se trate de información valorada para la dimensión de confidencialidad en nivel MEDIO o ALTO. Esto favorece la aplicación directa del RGPD y del marco normativo europeo, reduce la exposición a conflictos jurisdiccionales y facilita las labores de supervisión y control por parte de autoridades europeas competentes. En este sentido, la determinación de la localización efectiva del tratamiento deberá abordarse desde una perspectiva conjunta que integre **cumplimiento normativo, gestión del riesgo y control de la cadena de prestación del servicio**, especialmente en entornos de computación en la nube.

Esta recomendación general resulta independiente de la obligación legal específica establecida en el artículo 46 bis de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, introducido por el Real Decreto-ley 14/2019, de 31 de octubre, conforme al cual los sistemas de información y comunicaciones destinados al censo electoral, los padrones municipales de habitantes y otros registros de población, los datos fiscales relacionados con tributos propios o cedidos, y los datos de los usuarios del sistema nacional de salud, así como los correspondientes tratamientos de datos personales, deberán ubicarse y prestarse, en todo caso, dentro del territorio de la Unión Europea.Cuando resulte necesario tratar datos personales fuera del EEE, o permitir el acceso a dichos datos desde terceros países, incluidos supuestos de soporte técnico, administración remota o intervención de subencargados, deberá analizarse si existe una **transferencia internacional de datos** y cumplirse los requisitos establecidos en el RGPD. Ello incluye, entre otros, la existencia de una decisión de adecuación adoptada por la Comisión Europea o la aplicación de garantías adecuadas, tales como cláusulas contractuales tipo u otros mecanismos previstos en la normativa. Adicionalmente, deberán tenerse en cuenta las disposiciones específicas de la LOPDGDD y, cuando proceda, realizar evaluaciones de impacto relativas a la protección de datos y a las transferencias internacionales, de acuerdo con las recomendaciones de las autoridades de control.

Por otra parte, la preservación de la soberanía del dato deberá materializarse mediante la incorporación de garantías específicas en los procesos de contratación, así como mediante la definición de medidas técnicas y organizativas adecuadas. En particular, deberán considerarse al menos los siguientes aspectos:

a) Control de la localización del dato

Los contratos deberán especificar las ubicaciones autorizadas para el almacenamiento y procesamiento de la información, priorizando centros de datos situados en la Unión Europea, y restringiendo cualquier cambio de ubicación sin autorización expresa de la entidad contratante.

b) Transparencia ante requerimientos legales

El proveedor deberá comprometerse a notificar sin dilación cualquier solicitud de acceso a datos por parte de autoridades, especialmente cuando proceda de jurisdicciones extracomunitarias, permitiendo a la entidad pública adoptar las medidas legales oportunas.

c) Protección criptográfica de la información

Se exigirá el uso de mecanismos de cifrado robustos para la protección de los datos en tránsito y en reposo, conforme a las recomendaciones del CCN. Se priorizará que la gestión de las claves criptográficas permanezca bajo el control de la entidad pública o se realice mediante dispositivos seguros (por ejemplo, módulos hardware de seguridad, HSM, cualificados).

d) Capacidades de auditoría y supervisión

Deberán establecerse derechos de auditoría que permitan a la entidad usuaria verificar el cumplimiento de las medidas de seguridad por parte del proveedor, incluyendo evaluaciones independientes, revisiones periódicas y pruebas técnicas.

e) Control de accesos y subcontratación

El contrato deberá definir claramente las condiciones de acceso a la información por parte del personal del proveedor y de terceros, limitando privilegios, garantizando la trazabilidad de las actuaciones y regulando la subcontratación bajo las mismas obligaciones de seguridad y confidencialidad.

Por lo tanto, la soberanía del dato debe considerarse un criterio transversal en todas las fases del ciclo de vida del servicio en la nube y en la toma de decisiones estratégicas, incluyendo:

- La selección del modelo de servicio (IaaS, PaaS, SaaS).
- La elección del modelo de despliegue (público, privado o híbrido).
- La selección del proveedor.
- La categorización del sistema conforme al ENS.
- La definición de controles de seguridad y medidas de protección asociadas.

En particular, deberá evaluarse con especial rigor la idoneidad del uso de la nube en función del análisis de riesgos, pudiendo requerirse soluciones que garanticen un mayor control sobre la infraestructura, la localización de los datos y la jurisdicción aplicable.

En definitiva, la soberanía del dato no debe entenderse únicamente como una cuestión de cumplimiento formal, sino como la capacidad real para mantener el control efectivo sobre su información, garantizando su protección frente a accesos no autorizados y asegurando su tratamiento conforme al marco jurídico europeo y a los principios del Esquema Nacional de Seguridad.

3.3 Gobernanza y responsabilidad compartida

El uso de servicios en la nube requiere un marco de gobernanza sólido, que defina de forma clara los roles, responsabilidades y mecanismos de control, asegurando el cumplimiento de las obligaciones en materia de seguridad de la información por parte de la entidad usuaria y del proveedor del servicio.

Este marco debe integrarse en la estructura organizativa existente y alinearse con el ENS, adaptando los procesos internos para contemplar las particularidades de los entornos en la nube, especialmente en lo relativo a la externalización de servicios y al modelo de responsabilidades compartidas. Por lo tanto, adoptar servicios en la nube no consiste solo en cuestiones técnicas o contractuales, sino también en establecer una **gobernanza** adecuada. Una correcta gobernanza implica definir **políticas, procedimientos y estructuras organizativas** para gestionar estos servicios de forma segura y eficaz.

En este contexto, la entidad deberá disponer de una Política de Seguridad de la Información que establezca los principios y directrices generales en materia de seguridad, en línea con el marco organizativo del ENS. Dicha política debe ser conocida por toda la organización y servir de referencia para el uso de servicios en la nube, garantizando que su uso es coherente con los requisitos de seguridad definidos a nivel corporativo.

Asimismo, deberá desarrollarse normativa interna que regule el uso de servicios en la nube, estableciendo criterios claros sobre su utilización, incluyendo, entre otros aspectos:

- Tipología de servicios autorizados.
- Condiciones de uso aceptable.
- Tipos de información que pueden ser tratados en función de su calificación.
- Requisitos de acceso y uso desde distintos entornos o dispositivos.
- Medidas de seguridad a aplicar.

Esta normativa deberá ser coherente con las medidas del ENS en materia de marco organizativo y contribuir a una utilización homogénea y controlada de los servicios en la nube dentro de la organización.

Igualmente, será necesario definir y documentar los procedimientos de seguridad asociados a la gestión de los servicios en la nube, incluyendo los procesos de alta, modificación y baja de servicios, así como las actividades de operación, supervisión y control. Estos procedimientos deberán identificar claramente las responsabilidades de las distintas unidades implicadas.

En entornos en la nube adquiere especial relevancia el establecimiento de un proceso formal de autorización para la incorporación de nuevos servicios o la modificación de los existentes. Este proceso deberá contemplar, al menos:

- La evaluación previa de riesgos.
- La verificación del cumplimiento normativo aplicable.
- La validación por parte de los responsables competentes (Información, Servicio y Seguridad).
- La definición del modelo de responsabilidades entre la entidad usuaria y el proveedor.

Este enfoque permite garantizar que el uso de servicios en la nube se realiza de forma controlada, evitando la incorporación de soluciones no autorizadas y reduciendo los riesgos asociados a prácticas como la utilización de servicios en la nube al margen de los procedimientos establecidos.

En todo caso, la externalización de servicios en la nube no implica la transferencia de la responsabilidad sobre la seguridad de la información, que seguirá recayendo en la entidad cliente, conforme a lo establecido en el Esquema Nacional de Seguridad. La gestión adecuada del modelo de responsabilidad compartida requerirá, por tanto, una definición clara de las funciones y obligaciones de cada parte, que deberá reflejarse tanto en la gobernanza interna como en los acuerdos contractuales con el proveedor.

3.3.1 Roles y responsabilidades

La utilización de servicios en la nube requiere definir de forma clara las responsabilidades asumidas por la entidad usuaria y por el proveedor del servicio, estableciendo mecanismos de coordinación y supervisión adecuados. Esta delimitación resulta esencial para garantizar la aplicación efectiva de las medidas de seguridad, el cumplimiento normativo y la correcta gestión del riesgo asociado al servicio.

En los entornos en la nube adquiere especial relevancia el modelo de **responsabilidad compartida,** mediante el cual las funciones y obligaciones en materia de seguridad, operación y cumplimiento se distribuyen entre el cliente del servicio y el proveedor del servicio en la nube. La distribución concreta de dichas responsabilidades dependerá, entre otros factores, del modelo de servicio contratado (IaaS, PaaS o SaaS), del alcance de los servicios externalizados y de las condiciones contractuales establecidas.
La adopción de este modelo no implica la transferencia de la responsabilidad última sobre el servicio, la seguridad de la información ni el cumplimiento de la normativa aplicable, que continuará correspondiendo a la entidad cliente como responsable de la información tratada. En consecuencia, el **CSC deberá**:

- Determinar los requisitos de seguridad aplicables al servicio.
- Evaluar los riesgos asociados al uso del entorno en la nube.
- Supervisar el cumplimiento de las obligaciones asumidas por el CSP.
- Verificar que las medidas de seguridad implantadas resultan adecuadas al nivel de riesgo y a la categorización del sistema.

Por su parte, el **CSP deberá** garantizar la seguridad y operación de aquellos componentes, capacidades o servicios que se encuentren bajo su ámbito de control, proporcionando además la información, mecanismos y capacidades necesarias para que el CSC pueda ejercer sus responsabilidades de seguridad y supervisión. La distribución de responsabilidades variará en función del modelo de servicio contratado. De forma general:

- En entornos IaaS, el CSP asume principalmente la seguridad de la infraestructura física y de virtualización, mientras que el CSC mantiene la responsabilidad sobre sistemas operativos, configuraciones, aplicaciones y datos.
- En servicios PaaS, el CSP amplía su ámbito de responsabilidad a la plataforma y componentes middleware, manteniendo el CSC el control sobre aplicaciones, configuraciones y datos.
- En soluciones SaaS, el CSP gestiona la mayor parte de los componentes tecnológicos del servicio, mientras que el CSC conserva responsabilidades relacionadas con la gestión de identidades, configuración funcional, protección de la información y uso adecuado del servicio.



Distribución orientativa de responsabilidades en función del modelo de servicio

Esta distribución deberá concretarse para cada servicio contratado, identificando de forma precisa las responsabilidades técnicas, organizativas y operativas de cada parte, así como los mecanismos de coordinación y supervisión asociados.

A efectos de la presente guía, los modelos CaaS (Containers as a Service) y FaaS (Functions as a Service) se consideran variantes especializadas de los modelos IaaS y PaaS respectivamente. En consecuencia, las referencias realizadas en esta guía a los modelos IaaS y PaaS se entenderán extensibles a dichas modalidades, sin perjuicio de las particularidades técnicas y de seguridad específicas que puedan derivarse de su utilización. En cuanto a la asignación de responsabilidades, deberá realizarse tomando como referencia el modelo principal del que derivan, ajustando contractualmente aquellas responsabilidades específicas asociadas a la gestión de contenedores, orquestadores, funciones, componentes software y servicios de ejecución gestionados por el proveedor.

La definición insuficiente o ambigua de responsabilidades puede generar situaciones en las que determinados controles de seguridad no sean implantados o supervisados adecuadamente, por asumir incorrectamente que corresponden a la otra parte. Por ello, resulta recomendable formalizar esta distribución mediante matrices de responsabilidad, acuerdos de nivel de servicio y documentación contractual específica.

Como medida de carácter práctico para facilitar la correcta asignación y seguimiento de responsabilidades, resulta recomendable desarrollar la **Declaración de Aplicabilidad** incorporando una estructura que permita identificar, de manera explícita, la titularidad de cada medida de seguridad, tomando como referencia el ANEXO B — MATRIZ DE RESPONSABILIDAD. En particular, puede optarse por una configuración en la que se distinga entre aquellas medidas cuya responsabilidad corresponde de forma exclusiva al CSC, aquellas cuya responsabilidad primaria recae en el CSP, y aquellas otras cuya implantación y supervisión requiere la participación de ambas partes en el marco del modelo de responsabilidad compartida. Este enfoque permite disponer de una visión clara y consolidada de la distribución de responsabilidades, facilitando tanto la implantación efectiva de las medidas de seguridad como las labores de seguimiento, supervisión y auditoría del cumplimiento, reduciendo el riesgo de omisiones o solapamientos en la asignación de responsabilidades.

3.3.2 Relación con el proveedor de servicios en la nube

El establecimiento de una relación segura, transparente y fiable con el proveedor de servicios en la nube constituye un elemento fundamental de la gobernanza de la seguridad en entornos en la nube. Dicha relación debe articularse mediante acuerdos contractuales sólidos, mecanismos de interlocución definidos y criterios de exigencia verificables, garantizando en todo momento el cumplimiento del Esquema Nacional de Seguridad y de la normativa de protección de datos aplicable. Las cláusulas contractuales deberán reflejar, entre otros, los siguientes aspectos:

- **Alcance de la responsabilidad de ambas partes.**

  Con carácter previo a la formalización de cualquier acuerdo, la entidad cliente deberá determinar qué medidas de seguridad corresponden al CSP, cuáles al CSC y cuáles son de responsabilidad compartida. Esta distribución depende directamente del modelo de servicio contratado (IaaS, PaaS o SaaS) y deberá quedar reflejada en la Declaración de Aplicabilidad, elaborada sobre la base del análisis de riesgos previo, el nivel de seguridad por dimensión y la categorización del sistema.

- **Punto de Contacto designado.**

  En los servicios externalizados, el CSP deberá designar formalmente un Punto o Persona de Contacto (POC) para la seguridad de la información tratada y del servicio prestado, que cuente con el apoyo de los órganos de dirección, que canalice y supervise el cumplimiento de los requisitos de seguridad y las comunicaciones relativas a la seguridad de la información y la gestión de incidentes. Esta designación deberá quedar documentada contractualmente y estar disponible con carácter previo al inicio efectivo de la prestación.

- **Acuerdos contractuales**.

  La relación con el proveedor de servicios en la nube deberá formalizarse mediante los correspondientes instrumentos contractuales conforme a la Ley 9/2017, de Contratos del Sector Público, que constituye el marco a través del cual se concretan y hacen exigibles las obligaciones en materia de seguridad, protección de datos, niveles de servicio y supervisión. En este sentido, los pliegos deberán reflejar de forma expresa la distribución de responsabilidades, las medidas de control y los mecanismos de seguimiento necesarios para garantizar el cumplimiento de los requisitos establecidos en el Esquema Nacional de Seguridad y en la normativa aplicable.
  Los acuerdos contractuales suscritos con el CSP deberán contemplar, como mínimo, los siguientes aspectos:

  - Exigencia de conformidad con el ENS, en los niveles de seguridad en cada dimensión y en la categoría de seguridad del sistema, incluyendo el Certificado de Conformidad vigente. Contrato de encargado del tratamiento, conforme al artículo 28 del Reglamento General de Protección de Datos (RGPD) y a la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).
  - Cláusulas sobre protección de datos personales, que incluyan la finalidad del tratamiento, la limitación en el acceso, los requisitos de subcontratación y las garantías exigibles en caso de transferencias internacionales de datos.
  - Acuerdo de Nivel de Servicio (SLA), con indicadores medibles y verificables de disponibilidad, rendimiento, soporte técnico y tiempos de respuesta ante incidentes.

- Certificaciones de seguridad reconocidas, según corresponda al nivel de riesgo del servicio y la categoría del sistema.
- Medidas de seguridad técnicas y organizativas requeridas, debidamente detalladas y alineadas con la declaración de aplicabilidad del sistema.
- Obligaciones de confidencialidad, extensivas al personal del CSP y a sus posibles subcontratistas.
- Derecho de auditoría y supervisión por parte de la entidad contratante o de terceros designados por ella.
- Notificación de incidentes y brechas de seguridad, con indicación expresa de los plazos máximos y los canales de comunicación habilitados.
- Garantías de reversibilidad del servicio y condiciones para la recuperación y portabilidad de la información al término del contrato.
- Régimen de subcontratación controlada, con obligación de aprobación previa por parte del CSC.
- Régimen de penalizaciones y consecuencias ante el incumplimiento de las obligaciones de seguridad, incluyendo responsabilidades, medidas correctoras y causas de resolución contractual.

Se recomienda mantener un registro actualizado de los acuerdos suscritos con cada CSP que recoja, como mínimo: datos identificativos del proveedor y del POC designado; descripción del servicio contratado y modelo de servicio; nivel de riesgo asignado al proveedor; obligaciones de seguridad del CSP y métodos de verificación acordados; cláusulas críticas de seguridad (SLA, subcontratación, penalizaciones y condiciones de reversibilidad); y estado de las certificaciones y acreditaciones vigentes.

Este registro facilitará la gestión del ciclo de vida contractual y el seguimiento descrito en el **epígrafe 3.3.3**.

3.3.3 Supervisión

De conformidad con el artículo 37 del ENS, relativo a los mecanismos de control, cada entidad titular de sistemas de información deberá establecer los mecanismos necesarios para garantizar de forma efectiva el cumplimiento del ENS. Esta obligación se extiende a los servicios externalizados en la nube, respecto de los cuales la entidad mantiene en todo momento la responsabilidad última sobre la seguridad del sistema.

Conforme al artículo 13 del ENS, **el Responsable de Seguridad** determina las decisiones para satisfacer los requisitos de seguridad, supervisa la implantación de las medidas correspondientes y reporta sobre el estado de cumplimiento. En entornos en la nube, esta función supervisora se proyecta tanto sobre los controles implementados por la propia entidad como sobre aquellos que, por el modelo de responsabilidad compartida, recaen sobre el CSP. La supervisión no puede delegarse al proveedor: es siempre responsabilidad de la entidad cliente del servicio.

Además, en los servicios externalizados, el CSP deberá contar con un POC debidamente designado para canalizar y supervisar las comunicaciones relativas a seguridad y la gestión de incidentes en el ámbito del servicio. Esta función podrá recaer en el Responsable de Seguridad del CSP o en el interlocutor designado a tal efecto, siempre que disponga del apoyo organizativo necesario y de capacidad efectiva de coordinación. La supervisión de los servicios en la nube deberá integrarse en los mecanismos de seguimiento del contrato previstos en la normativa de contratación pública, asegurando que el cumplimiento de los niveles de servicio, de las medidas de seguridad y de las obligaciones asumidas por el proveedor pueda ser verificado de forma continua durante toda la vigencia del contrato.

La supervisión del servicio en la nube deberá articularse mediante, al menos, los siguientes mecanismos:

- Revisión periódica del cumplimiento de los SLA y de los indicadores clave de rendimiento (KPI) definidos contractualmente.
- Acceso y análisis de registros de actividad (logs), eventos de seguridad e informes del servicio proporcionados por el CSP.
- Ejercicio del derecho de auditoría reconocido contractualmente, mediante la revisión de evidencias objetivas del cumplimiento de las medidas de seguridad exigidas.
- Seguimiento de incidentes de seguridad notificados por el CSP, verificando los plazos y los procedimientos establecidos.

Los resultados de la supervisión deberán retroalimentar el proceso de mejora continua, descrito en el **epígrafe 4.4**, permitiendo la actualización de controles y la revisión del análisis de riesgos.

3.4 Contratación de servicios en la nube

La externalización de servicios en la nube conlleva una distribución de responsabilidades entre el CSP, el CSC o, de forma compartida, entre ambos, en función del modelo de servicio contratado. No obstante, el CSC mantiene la responsabilidad última sobre el sistema de información y debe garantizar que dichas responsabilidades estén claramente identificadas y formalizadas en los instrumentos contractuales.

Con carácter previo a la contratación, es imprescindible definir con precisión el alcance del servicio, con el fin de evitar ambigüedades o lagunas en la asignación de responsabilidades que pudieran derivar en riesgos para la seguridad de la información o en incumplimientos normativos.

En primer lugar, el Responsable de Seguridad deberá categorizar el sistema que se pretende externalizar, tomando como base las valoraciones realizadas por los Responsables de la Información y del Servicio, de conformidad con el procedimiento del Anexo I del ENS. La categoría determinará las medidas exigibles al CSP y el nivel de certificación requerido.

Con carácter previo a la redacción de los pliegos de condiciones técnicas, el responsable de compras o contratación deberá recabar el asesoramiento del Responsable de Seguridad para la definición de los requisitos de seguridad exigibles a los licitadores, conforme al artículo 19 del ENS. Cuando el prestador vaya a tratar datos personales por cuenta de la entidad, deberá consultarse igualmente al Delegado de Protección de Datos.

La contratación de servicios en la nube en el sector público deberá ajustarse a lo dispuesto en la Ley 9/2017, de Contratos del Sector Público, que establece el régimen jurídico aplicable a la preparación, adjudicación y ejecución de los contratos. En este contexto, la definición del objeto del contrato, la determinación de las condiciones de ejecución y la inclusión de requisitos en materia de seguridad, protección de datos y localización de la información deberán abordarse de forma específica en los pliegos, garantizando su coherencia con el Esquema Nacional de Seguridad y con el resto del marco normativo aplicable.

El Informe 13/2021 de la Junta Consultiva de Contratación Pública del Estado califica los servicios en la nube principalmente como contratos de suministro[3]. La **Nota sobre la Calificación Jurídica de los Contratos de Prestación de Servicios en la Nube y su contratación centralizada**, emitida en 2021 por la Dirección General de Racionalización y Centralización de la Contratación (DGRCC) del Ministerio de Hacienda, establece que los servicios en la nube (SaaS, PaaS, IaaS) son suministros aptos para la contratación centralizada.

Asimismo, el Sistema Dinámico de Adquisición SDA 25/2022, impulsado por el Ministerio de Hacienda, constituye el marco de contratación centralizada de referencia para la adquisición de software por la Administración General del Estado. Para los servicios en la nube, resulta de especial relevancia su epígrafe III.2.3, relativo a los medios admisibles para la acreditación de la seguridad.

En el contexto del SDA 25/2022, la acreditación de la seguridad de programas suministrados en modalidad de servicios en la nube presenta particularidades respecto a las soluciones tradicionales “on-premise”. A diferencia de estas últimas, donde la evaluación puede centrarse en el producto software de forma aislada, en el modelo de servicios en la nube, la seguridad debe considerarse de manera integral, abarcando tanto el software como la infraestructura sobre la que se presta el servicio. Esta diferencia se fundamenta en el modelo de responsabilidad compartida, en el que el proveedor asume una parte significativa de los controles de seguridad.

En este sentido, el epígrafe III.2.3 establece que la acreditación de la seguridad deberá realizarse mediante evidencias objetivas reconocidas, tales como:

- Certificación conforme al Esquema Nacional de Seguridad (ENS), adecuada a la categoría del sistema.

[3] https://www.hacienda.gob.es/dgpatrimonio/junta%20consultiva/informes/informes2021/2021-13racionalizacion.pdf

- Inclusión en el Catálogo de Productos y Servicios STIC del Centro Criptológico Nacional (Guía CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación).
- Certificaciones equivalentes reconocidas por el CCN.
- Esquemas de certificación europeos aplicables a servicios en la nube.

Asimismo, cuando se exija una certificación de seguridad aplicable al servicio en la nube, deberá verificarse que el alcance de dicha certificación cubre el servicio prestado en su conjunto y no únicamente componentes aislados. En el caso de productos o servicios de seguridad incluidos en el CPSTIC, deberá distinguirse entre la certificación o conformidad del servicio en la nube y la evaluación específica del producto o servicio de seguridad que se integre en dicho servicio. Finalmente, se requiere que las certificaciones se mantengan vigentes durante toda la duración del contrato, garantizando así la continuidad del nivel de seguridad exigido.

Para una contratación con garantías de seguridad de un servicio en la nube, los pliegos de condiciones técnicas deberán recoger, como mínimo:

- Descripción detallada del servicio: modelo de servicio (IaaS, PaaS o SaaS) y modelo de despliegue (nube pública, privada o híbrida).
- Subcontratación: condiciones, requisitos y necesidad de aprobación previa por parte del CSC.
- Finalización del servicio: plazos y condiciones para la extinción del contrato, cambio de proveedor o resolución por incumplimiento, incluyendo el régimen de reversibilidad.
- Mecanismos de supervisión, control y auditoría que permitan al CSC verificar el cumplimiento de los requisitos de seguridad y de las obligaciones contractuales.
- Localización geográfica de los servidores y recursos físicos que van a tratar la información. Cuando el CSP vaya a tratar datos personales, deberán estar ubicados en el Espacio Económico Europeo o en países con decisión de adecuación reconocida por la Comisión Europea, conforme al artículo 45 del RGPD.
- Gestión de accesos: mecanismos de control de acceso, autenticación y autorización aplicables al personal de ambas partes.
- Protección de la información, identificación de las medidas de seguridad del ENS exigibles al CSP, distribuidas de forma coherente con el modelo de servicio contratado.
- Acuerdos de nivel de servicio: niveles de servicio medibles y verificables, con penalizaciones o medidas correctoras ante incumplimiento.

No obstante, cabe destacar que el Catálogo de Productos y Servicios STIC del Centro Criptológico Nacional (Guía CCN-STIC 105: Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación) incluye servicios de seguridad en la nube, entendidos estos como productos que, en lugar de estar

desplegados *on-premise*, se encuentran en la nube. Por ello, en los sistemas de categoría MEDIA o ALTA, estos servicios de seguridad deberán estar incluidos en el CPSTIC, de acuerdo con lo establecido en [op.pl.5].

4. SEGURIDAD EN EL CICLO DE VIDA DEL SERVICIO EN LA NUBE

De conformidad con el artículo 36 del ENS, las especificaciones de seguridad se incluirán en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

El uso seguro de servicios en la nube exige integrar la seguridad en todas las fases del ciclo de vida, desde la planificación hasta la extinción del servicio, sobre la base del principio de responsabilidad compartida con el CSP. Este enfoque integral abarca el diseño, la contratación, la configuración, la explotación y la finalización del servicio, incluyendo las garantías de devolución y supresión segura de la información.

El ciclo de vida abarca desde la planificación y el análisis de riesgos del uso o migración de servicios a la nube; la evaluación y adopción de soluciones tecnológicas para determinar el modelo de despliegue y de servicio más idóneo, así como la selección y contratación del proveedor; la implementación segura del servicio; la monitorización, auditoría y mejora continua; la gestión de incidencias y continuidad del servicio; hasta la finalización del servicio con reversibilidad garantizada.

Nota sobre las referencias al Anexo II del ENS: *Las referencias a artículos y medidas concretas del Anexo II que aparecen a lo largo de este epígrafe no constituyen una relación exhaustiva. Todas las medidas del Anexo II del ENS son de aplicación en función de la categoría del sistema y de lo establecido en la Declaración de Aplicabilidad. Las referencias incluidas identifican aquellas medidas de especial relevancia en el contexto de los servicios en la nube, con el fin de orientar su aplicación práctica.*

4.1 Planificación y análisis de riesgos

La decisión de adoptar o migrar servicios a la nube debe sustentarse en un **análisis de riesgos formal y documentado**, no únicamente en consideraciones económicas o tecnológicas. Esta fase tiene como objetivo determinar si el modelo de nube es adecuado para el sistema en cuestión y, en caso afirmativo, bajo qué condiciones.

La entidad deberá categorizar el sistema conforme al procedimiento del Anexo I del ENS, identificando los activos presentes, las dimensiones de seguridad relevantes y el nivel correspondiente para cada información y servicio. Las valoraciones se expresarán, según proceda, en los niveles BAJO, MEDIO o ALTO, sin perjuicio de aquellos supuestos en los que una dimensión pueda no resultar aplicable. Esta valoración será realizada y aprobada formalmente por los Responsables de la Información y del Servicio. A partir de la valoración máxima obtenida en cualquier dimensión, el Responsable de Seguridad determinará la categoría del sistema (BÁSICA, MEDIA o ALTA).

A partir de los resultados de la categorización, se elaborará la Declaración de Aplicabilidad, seleccionando las medidas del Anexo II del ENS junto con los refuerzos que procedan. Este documento, aprobado formalmente por el Responsable de

Seguridad, establecerá qué medidas aplican al CSP, cuáles al CSC y cuáles son compartidas. La categoría y las medidas identificadas se propagarán a todos los elementos del sistema, incluidos los de un CSP contratado o de una cadena de subcontratación.

El **análisis de riesgos** [op.pl.1] identificará las amenazas a las que están expuestos los servicios y la información, en función de la categoría del sistema. Si del análisis resultara necesario implantar medidas adicionales, estas se incorporarán a la Declaración de Aplicabilidad. El mismo criterio se aplicará para definir la arquitectura de seguridad [op.pl.2].

Entre las amenazas específicas del entorno en la nube que deben considerarse se encuentran las siguientes:

- Pérdida de confidencialidad: atendiendo a la clasificación de la información (datos personales, información sensible o estratégica). A este respecto, la información valorada con nivel ALTO en alguna dimensión de seguridad solo debería tratarse o almacenarse en entornos de nube pública cuando el análisis de riesgos, las garantías contractuales, la certificación aplicable y las medidas técnicas implantadas aseguren un nivel de protección adecuado.
- Pérdida de control: derivada de la transferencia de la gestión al CSP, que puede limitar la capacidad de supervisión directa de la entidad.
- Cumplimiento normativo: tanto en materia de seguridad de la información como de integridad de los datos.
- Aspectos jurisdiccionales asociados a la ubicación de los datos, incluidas copias de seguridad y registros de actividad (*logs*), en los términos del **epígrafe 3.2 Soberanía del dato**.
- Dependencia tecnológica (*lock-in*): cuando se identifiquen servicios críticos con dependencias significativas, el impacto se considerará alto y la mitigación será obligatoria.
- Recuperación de datos: deberá establecerse una política de recuperación ante desastre que contemple los escenarios de fallo del CSP.

Cuando el servicio en la nube se acomode a un **Perfil de Cumplimiento Específico** validado y publicado por el CCN, la entidad al elaborar la Declaración de Aplicabilidad para un determinado sistema deberá evaluar si puede optar a ese perfil y, en su caso, adaptar la Declaración de Aplicabilidad al mismo.

El proceso de **adquisición de nuevos componentes** [op.pl.3] requerirá verificar su coherencia con la arquitectura de seguridad, los riesgos identificados y las necesidades técnicas, formativas y presupuestarias.

Respecto al **dimensionamiento y gestión de la capacidad** [op.pl.4], dado su impacto presupuestario, deberá planificarse con antelación suficiente. En entornos en la nube, el dimensionamiento puede ser dinámico.

Tras esta fase de **planificación y análisis de riesgos**, se estará en disposición de evaluar la idoneidad de los modelos en la nube y establecer los criterios para determinar si resultan adecuados, en función de si se trata de servicios no críticos o escalables, de la necesidad de elasticidad o alta disponibilidad, o bien del riesgo asociado a sistemas críticos o información sensible.

Ámbito	Referencia en el ENS
Análisis de riesgos	Análisis de riesgos [op.pl.1]
Arquitectura de seguridad	Arquitectura de seguridad [op.pl.2]
Adquisición de componentes	Adquisición de nuevos componentes [op.pl.3]
Dimensionamiento y capacidad	Dimensionamiento / gestión de la capacidad [op.pl.4]
Declaración de aplicabilidad	Artículo 28 — Cumplimiento de los requisitos mínimos
Perfiles de cumplimiento específicos	Artículo 30 — Perfiles de cumplimiento específicos

4.2 Evaluación y adopción de soluciones tecnológicas

Una vez definidos los criterios en la fase de planificación, se procederá a evaluar y seleccionar la opción tecnológica más adecuada —nube pública, privada (*on-premise* u hospedada) o híbrida— atendiendo a los requisitos de seguridad, el cumplimiento normativo y la soberanía del dato. En cuanto al modelo de despliegue, se atenderá a lo indicado en el **epígrafe 2.2** de la presente guía.

La selección del CSP se realizará de acuerdo con [op.ext.1] e incluirá, como mínimo, **la evaluación de los siguientes aspectos**:

- Certificación vigente conforme al ENS, o a un Perfil de Cumplimiento Específico reconocido por el CCN, verificando que el alcance del certificado cubre los sistemas que prestarán el servicio y con una categoría igual o superior a la del sistema.
- Historial de incidentes de seguridad, transparencia y capacidad de respuesta.
- Riesgo de dependencia tecnológica (lock-in): costes de salida, herramientas de exportación de datos y compatibilidad multicloud.

Además de lo establecido en el **epígrafe 3.4**, los contratos deberán contemplar cláusulas específicas orientadas a la portabilidad y la reversibilidad:

- Derecho a exportar datos en formato estándar e interoperable.
- Obligación de asistencia en la migración y prohibición de formatos propietarios sin alternativa.
- Obligaciones de elaboración de informes periódicos sobre el estado del servicio y la seguridad.

- Costes de salida limitados o predefinidos, y periodo de transición garantizado.

Una vez iniciada la prestación, deberá establecerse un sistema rutinario de medición del cumplimiento de las obligaciones contractuales conforme a [op.ext.2], que incluya el procedimiento para neutralizar desviaciones fuera del margen de tolerancia acordado y los mecanismos de coordinación ante incidentes.

Ámbito	Referencia en el ENS
Aplicabilidad del ENS a proveedores que prestan servicios al sector público	Artículo 2 — Ámbito de aplicación
Selección y contratación del proveedor	Contratación y acuerdos de nivel de servicio [op.ext.1]
Seguimiento y cumplimiento de las obligaciones del servicio	Gestión diaria [op.ext.2]
Protección de la cadena de suministro TIC	Protección de la cadena de suministro [op.ext.3]
Uso de productos y componentes con garantías de seguridad	Componentes certificados [op.pl.5]

4.3 Implementación segura

Durante la fase de implantación o despliegue del servicio en la nube deberán implementarse las medidas de seguridad correspondientes del **Anexo II del ENS**, de acuerdo con la Declaración de Aplicabilidad y con el análisis de riesgos realizado, garantizando una configuración segura desde el inicio de la prestación del servicio.

Se aplicará una **configuración segura** conforme a [op.exp.2], eliminando servicios innecesarios y minimizando la superficie de exposición. Esto incluye:

- Hardening de sistemas operativos: permisos, políticas de contraseñas y parcheado.
- Segmentación de redes y configuración de dispositivos perimetrales.
- Bastionado de aplicaciones, navegadores y servidores web.
- Cifrado de datos y control de accesos en bases de datos.

La **gestión continua de la configuración** se realizará conforme a [op.exp.3], asegurando la aplicación de los principios de mínima funcionalidad y mínimo privilegio, y manteniendo registros auditables de cualquier modificación.

También se mantendrá un control continuo de los cambios realizados en el sistema conforme a la **gestión de cambios** [op.exp.5], planificando los mismos para reducir el impacto sobre la prestación de los servicios afectados, registrando las peticiones de cambio, y determinando si son relevantes para la seguridad del sistema mediante un análisis de riesgos. Los cambios que impliquen un riesgo de nivel ALTO deberán ser

aprobados, explícitamente, de forma previa a su implantación, por el Responsable de la Seguridad.

La **gestión de identidades y accesos** se articulará conforme a las medidas del marco de control de acceso [op.acc] del ENS, prestando especial atención a:

- Gestión centralizada de identidades.
- Autenticación multifactor (MFA) conforme al nivel de riesgo y la categoría del sistema.
- Principio de mínimo privilegio en la asignación de derechos de acceso.
- Revisión periódica de privilegios y desactivación de cuentas inactivas o de personal que cesa.

Asimismo, deberán implementarse los controles técnicos derivados del modelo de responsabilidad compartida, incluyendo el cifrado de datos en tránsito y en reposo, la gestión de claves criptográficas y la configuración de registros de actividad, para garantizar la trazabilidad completa de las operaciones.

Con el objeto de evitar la dependencia operativa total del proveedor (*lock-in*), deberán **documentarse la arquitectura y las configuraciones del sistema**, y mantenerse copias de los datos y de la configuración actualizadas.

Los sistemas que suministran servicios en la nube a organismos del sector público deberán cumplir las medidas de seguridad aplicables en función del modelo prestado (SaaS, PaaS o IaaS) conforme a [op.nub.1.1] y a las guías CCN-STIC que resulten de aplicación.

Cuando se utilicen servicios de terceros, los sistemas que los soportan deberán ser conformes con el ENS o cumplir las medidas de la guía CCN-STIC correspondiente, que incluirá requisitos sobre [op.nub.1.2]:

- Auditoría de pruebas de penetración (pentesting).

  Auditorías de pruebas de penetración que verifiquen la ausencia de vulnerabilidades que pudieran comprometer la información o el servicio.

- Transparencia.

  El CSP deberá proporcionar al CSC visibilidad sobre sus herramientas de seguridad, el tipo de virtualización utilizada, el nivel de segregación de datos y aplicaciones, los mecanismos de borrado seguro, la ubicación geográfica de los datos y el acceso a los registros de actividad.

- Cifrado y gestión de claves.

  El servicio deberá disponer de mecanismos criptográficos que permitan que la información del usuario esté protegida, en tránsito y en reposo, para que no pueda ser leída o modificada en caso de acceso ilegítimo. Los mecanismos criptográficos deberán cumplir con lo especificado en la guía CCN-STIC 807 Criptología de Empleo en el ENS.

Las claves no deben estar almacenadas en la infraestructura del CSP sin control del cliente, o bien deben custodiarse en módulos de seguridad de hardware (HSM) o bien en el gestor de claves criptográficas proporcionado por el CSP, ambos cualificados por el CCN e incluidos en el Catálogo de Productos de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC).

- Jurisdicción de los datos

  El CSP informará sobre la ubicación geográfica de los datos, incluidas las copias de seguridad y los registros de actividad, tanto antes como durante la prestación del servicio.

Para sistemas de categoría MEDIA y ALTA, **los servicios en la nube de terceros deberán estar certificados** bajo la Metodología de Evaluación de Productos en la Nube (CICLON) u otra metodología reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las TIC [op.nub.1.r1]. Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5]. Para sistemas de categoría ALTA, además, la configuración de seguridad deberá realizarse conforme a la **guía CCN-STIC de Configuración de Seguridad Específica** que resulte de aplicación [op.nub.1.r2].

Ámbito	Referencia en el ENS
Configuración segura por defecto	Configuración de seguridad [op.exp.2]
Configuración de seguridad	Gestión de la configuración de seguridad [op.exp.3]
Gestión de cambios	Gestión de cambios [op.exp.5]
Control de accesos	Control de acceso [op.acc]
Mecanismos criptográficos	Protección de claves criptográficas [op.exp.10]
Servicios en la nube	Protección de servicios en la nube [op.nub.1]
Uso de productos y componentes con garantías de seguridad	Componentes certificados [op.pl.5]

4.4 Monitorización, auditoría y mejora continua

De conformidad con el artículo 27 del ENS referente a la mejora continua del proceso de seguridad, el proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua, aplicando los criterios y métodos reconocidos en la práctica nacional e internacional.

En entornos en la nube, la monitorización presenta la particularidad de que parte de la visibilidad sobre el sistema recae en el CSP. Por ello, es imprescindible que los acuerdos contractuales garanticen al CSC el acceso a los registros, métricas e informes necesarios para ejercer su función supervisora.

El sistema estará sujeto **a monitorización continua** conforme a las medidas del grupo [op.mon] del ENS, con ejecución de acciones predeterminadas ante situaciones de compromiso identificadas en el análisis de riesgos. Para la vigilancia efectiva podrán emplearse herramientas nativas del proveedor, sistemas SIEM (*Security Information and Event Management*) , herramientas CASB (*Cloud Access Security Broker*) o herramientas CSPM (*Cloud Security Posture Management*).

La **detección de intrusión** [op.mon.1] deberá articularse teniendo en cuenta el modelo de despliegue y el nivel de gestión que corresponda a cada parte: en servicios IaaS o PaaS, la responsabilidad sobre las capas contratadas recae en el CSC; en SaaS, debe exigirse contractualmente al CSP. En todos los casos, la capa de infraestructura física y virtualización es responsabilidad del CSP.

Una vez migrado el servicio, **el CSC es responsable de verificar el cumplimiento de los SLA y monitorizar los KPI acordados** conforme a [op.mon.2]. Dichos indicadores deben ser específicos, medibles, alcanzables y realistas, y deberán permitir configurar alertas automáticas cuando el rendimiento caiga por debajo del umbral acordado.

El sistema dispondrá de **recolección automática de eventos de seguridad** [op.mon.3] y, según la categoría, de capacidades adicionales de correlación, análisis dinámico de vulnerabilidades y detección de amenazas avanzadas. Las inspecciones periódicas incluirán verificación de configuración, análisis de vulnerabilidades y pruebas de penetración.

Con el fin de evitar ambigüedades en el modelo de responsabilidad compartida, se distinguen los siguientes ámbitos:

- **Aspectos a revisar en el CSP**: disponibilidad e integridad de la infraestructura gestionada por el proveedor, cumplimiento de certificaciones y acreditaciones, aplicación de parches y actualizaciones en la capa bajo su control, elaboración de informes periódicos de seguridad y gestión de incidentes en su perímetro.
- **Aspectos a revisar en el CSC**: configuración segura del entorno contratado, gestión de identidades y accesos de los usuarios propios, monitorización de la actividad de los usuarios internos, cumplimiento de la Declaración de Aplicabilidad y verificación del SLA.

En cuanto a la **mejora continua de la seguridad del sistema**, los registros y datos de monitorización y auditoría servirán de base para la actualización de controles, la adaptación a nuevas amenazas y la revisión periódica del análisis de riesgos. Los informes de auditoría serán remitidos al Responsable del Sistema y al Responsable de Seguridad. Este último analizará dichos informes y elevará sus conclusiones al Responsable del Sistema, quien adoptará las medidas correctoras que resulten oportunas.

Asimismo, se realizará el **mantenimiento y actualizaciones de seguridad** conforme [op.exp.4], por personal debidamente autorizado, atendiendo a las especificaciones de los fabricantes, incluyendo un seguimiento continuo de los anuncios de defectos, y

disponiendo de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones.

Ámbito	Referencia en el ENS
Detección de intrusión	Detección de intrusión [op.mon.1]
Sistema de métricas e indicadores	Sistema de métricas [op.mon.2]
Vigilancia y recolección de eventos	Vigilancia [op.mon.3]
Registro de actividad	Registro de la actividad [op.exp.8]
Mejora continua	Artículo 27 — Mejora continua del proceso de seguridad
Actualizaciones de seguridad	Mantenimiento y actualizaciones de seguridad [op.exp.4]

4.5 Gestión de incidencias y continuidad del servicio

De conformidad con el artículo 26 del ENS, los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

El CSC deberá incorporar en sus **planes de gestión de incidentes y de continuidad** del negocio los procedimientos de actuación ante incidentes que involucren al CSP. Esta coordinación deberá quedar recogida contractualmente: el CSP estará obligado a notificar los incidentes en los plazos del SLA y a restaurar los servicios en el tiempo acordado.

Un incidente en el CSP puede generar: interrupción de servicios críticos, compromiso de información y datos sensibles, incumplimientos normativos o contractuales e impacto operativo, económico o legal.

El artículo 7 del Reglamento de Ejecución (UE) 2024/2690 de la Comisión Europea, de 17 de octubre de 2024, detalla los casos en que un incidente puede considerarse significativo en proveedores de servicios de computación en nube.

La notificación al CERT competente se realizará conforme al artículo 33 del ENS, la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad y la guía CCN-STIC correspondiente. Asimismo, se deberá tener en cuenta la normativa aplicable para efectuar las notificaciones a las autoridades competentes que correspondan.

Se recomienda adoptar con el CSP las siguientes prácticas: simulacros y ejercicios conjuntos sobre el plan de gestión de incidentes, definición de canales de comunicación y procedimientos de escalado, mecanismos de intercambio seguro de información durante la crisis, y documentación de lecciones aprendidas tras cada incidente.

El sistema deberá disponer de un **análisis de impacto** [op.cont.1] que determine los requisitos de disponibilidad de cada servicio y los elementos críticos para su prestación. Para sistemas con disponibilidad ALTA, deberá desarrollarse un **plan de continuidad** [op.cont.2], sometido a **pruebas periódicas** [op.cont.3] y con **medios alternativos**

disponibles [op.cont.4], sometidos a las mismas garantías de seguridad que los originales.

La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera.

Se dispondrá de un **proceso integral para hacer frente a los incidentes** conforme a [op.exp.7]. Para sistemas de categoría MEDIA y ALTA, este proceso integral deberá incluir: medidas urgentes de contención, asignación de recursos para investigación, notificación a los responsables afectados y medidas para evitar la reincidencia. Todas las actuaciones se registrarán conforme a [op.exp.9].

Ámbito	Referencia en el ENS
Continuidad de la actividad	Artículo 26 — Continuidad de la actividad
Análisis de impacto	Análisis de impacto [op.cont.1]
Plan de continuidad	Plan de continuidad [op.cont.2]
Pruebas periódicas	Pruebas periódicas [op.cont.3]
Medios alternativos	Medios alternativos [op.cont.4]
Gestión de incidentes	Gestión de incidentes [op.exp.7]
Actuaciones relacionadas con la gestión de incidentes	Registro de la gestión de incidentes [op.exp.9]
Notificación de incidentes	Artículo 33 — Capacidad de respuesta a incidentes de seguridad

4.6 Finalización del servicio y reversibilidad

Para garantizar el cierre seguro del servicio en la nube, con recuperación completa de los datos, portabilidad, borrado completo de la información y revocación de accesos, el CSC deberá contar con planes de salida que contemplen la terminación por vencimiento natural del contrato, la resolución por incumplimiento y supuestos de fuerza mayor.

En cuanto a la **reversibilidad**, deberá garantizarse la recuperación completa de los datos al término de la relación contractual, habiendo regulado previamente: el formato de los datos y los plazos para su devolución, la utilización de un formato interoperable que facilite el traspaso a la entidad o a un nuevo proveedor, y la coordinación de acciones para una transición ordenada sin afectar a la operativa.

La dependencia tecnológica (*lock-in*) es uno de los mayores riesgos para la reversibilidad y debe mitigarse desde la contratación mediante: un Plan de Reversibilidad probado y validado, la validación de la migración antes del cierre efectivo del servicio y la verificación del borrado de datos en la infraestructura del CSP.

Una vez finalizado el contrato, el CSP deberá ejecutar las acciones necesarias para la **transferencia del conocimiento y de la información del servicio**, devolviendo toda la

información a la entidad o a quien esta designe, en el plazo y formato establecidos en el pliego, mediante una planificación que contemple los medios seguros necesarios, las acciones de contingencia y los riesgos del proceso. Deberá también contarse con un Plan de Recuperación ante Desastres para el supuesto de terminación abrupta de la relación.

En lo referente al **borrado seguro de los datos**, el CSC deberá estar informado de los mecanismos de borrado seguro que aplicará el CSP al término del contrato. Se requerirán: certificado de devolución o destrucción de información sensible, revocación de todos los accesos otorgados al CSP y eliminación de configuraciones asociadas, y destrucción o revocación de las claves criptográficas utilizadas durante la prestación.

Todo **el proceso de finalización deberá quedar documentado**, permitiendo la extracción de lecciones aprendidas, la elaboración del informe de cierre del servicio y la evaluación del estado de seguridad al término de la relación contractual, y todo ello deberá formar parte del acuerdo contractual entre el CSC y el CSP.

Ámbito	Referencia en el ENS
Borrado y destrucción segura de soportes	Borrado y destrucción [mp.si.5]
Copias de seguridad y recuperación	Copias de seguridad [mp.info.6]
Gestión de claves al cierre	Protección de claves criptográficas [op.exp.10]
Gestión de accesos al cierre	Control de acceso [op.acc]

ANEXO A — ACRÓNIMOS

API	Interfaz de Programación de Aplicaciones (Application Programming Interface)
CaaS	Contenedores como Servicio (Container as a Service)
CASB	Cloud Access Security Broker
CCN	Centro Criptológico Nacional
CERT	Equipo de Respuesta a Emergencias Informáticas (Computer Emergency Response Team)
CICLON	Metodología de Evaluación de Productos en la Nube del CCN
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y Comunicación
CSC	Entidad usuaria o cliente (Cloud Service Customer)
CSP	Proveedor de servicios en la nube (Cloud Service Provider)
CSPM	Gestión de la Postura de Seguridad en la Nube (Cloud Security Posture Management)
DGRCC	Dirección General de Racionalización y Centralización de la Contratación del Ministerio de Hacienda
DNS	Sistema de Nombres de Dominio (Domain Name System)
EEE	Espacio Económico Europeo
ENI	Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad
ENS	Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
EUCS	Esquema Europeo de Certificación de Ciberseguridad para Servicios Cloud
FaaS	Funciones como Servicio (Function as a Service)
HSM	Módulo de Seguridad de Hardware (Hardware Security Module)
IaaS	Infraestructura como Servicio (Infrastructure as a Service)
KPI	Indicador Clave de Rendimiento (Key Performance Indicator)
LCSP	Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
MFA	Autenticación Multifactor (Multi-Factor Authentication)
NIS2	Directiva (UE) 2022/2555, relativa a medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión

PaaS	Plataforma como Servicio (Platform as a Service)
PCE	Perfil de Cumplimiento Específico
POC	Punto de contacto (Point of Contact)
RGPD	Reglamento (UE) 2016/679, General de Protección de Datos
SaaS	Software como Servicio (Software as a Service)
SDA	Sistema Dinámico de Adquisición
SIEM	Security Information and Event Management
SLA	Acuerdo de Nivel de Servicio
STIC	Seguridad de las Tecnologías de la Información y Comunicación
TIC	Tecnologías de la Información y Comunicación
UE	Unión Europea

ANEXO B — MATRIZ DE RESPONSABILIDAD

La siguiente tabla representa, a modo orientativo, una matriz de responsabilidades en la que se indica sobre quién recae principalmente la responsabilidad de implementar las medidas del Anexo II del ENS en entornos en la nube, en función de la modalidad de servicio.

La matriz se circunscribe a los modelos de servicio IaaS, PaaS y SaaS. Conforme a lo establecido en el **3.3.1,** las modalidades de CaaS y FaaS se consideran especializaciones de los modelos IaaS y PaaS respectivamente, por lo que la distribución de responsabilidades deberá analizarse de forma específica, tomando como referencia el reparto descrito para dichos modelos, sin perjuicio de las particularidades de cada implementación.

Aunque el CSC mantiene en todo momento la responsabilidad última sobre la seguridad de la información y el cumplimiento de la normativa aplicable, la asignación de responsabilidades en la implementación de las medidas responde al modelo de responsabilidad compartida descrito en la presente guía. La distribución concreta deberá quedar reflejada en la Declaración de Aplicabilidad y en los acuerdos contractuales suscritos con el CSP.

ID	Medida	IaaS	PaaS	SaaS	Explicación breve
org.1	Política de seguridad	CSC	CSC	CSC	El CSC define su política de seguridad, el CSP debe cumplirla en el ámbito del servicio prestado.
org.2	Normativa de seguridad	CSC	CSC	CSC	La normativa interna es responsabilidad del CSC.
org.3	Procedimientos de seguridad	COMP	COMP	COMP	Cada parte define sus procedimientos en su ámbito, la coordinación entre ellos es compartida.
org.4	Proceso de autorización	COMP	COMP	COMP	Las autorizaciones sobre los recursos propios corresponden a cada parte según su capa de responsabilidad.
op.pl.1	Análisis de riesgos	COMP	COMP	COMP	Cada parte realiza el análisis de riesgos en su ámbito; el CSC es responsable del análisis global del sistema.

ID	Medida	IaaS	PaaS	SaaS	Explicación breve
op.pl.2	Arquitectura de seguridad	CSC	COMP	CSP	En IaaS el CSC diseña la arquitectura completa. En PaaS es compartida. En SaaS el CSP define la arquitectura base y el CSC la adapta a su uso.
op.pl.3	Adquisición de nuevos componentes	COMP	COMP	CSP	El CSC define los requisitos, el CSP aporta los componentes certificados que integran el servicio. En IaaS y PaaS la adquisición de componentes propios corresponde al CSC.
op.pl.4	Dimensionamiento / gestión de la capacidad	COMP	COMP	CSP	En SaaS el CSP garantiza la capacidad y elasticidad del servicio. En IaaS y PaaS el CSC también planifica y gestiona la capacidad de los recursos que contrata.
op.pl.5	Componentes certificados	COMP	COMP	COMP	Tanto el CSP como el CSC deben emplear componentes con las garantías de seguridad exigibles en su respectivo ámbito.
op.acc.1	Identificación	CSC	CSC	CSC	El CSC es responsable de la identificación de sus usuarios, con independencia de la infraestructura de identidad que proporcione el CSP.
op.acc.2	Requisitos de acceso	CSC	COMP	COMP	El CSC define las políticas de acceso, en PaaS y SaaS el CSP aplica los controles técnicos correspondientes.
op.acc.3	Segregación de funciones y tareas	CSC	COMP	COMP	El CSC define la segregación funcional. En PaaS y SaaS el CSP participa en su implementación técnica, al controlar las capas sobre las que el CSC no tiene acceso directo.

ID	Medida	IaaS	PaaS	SaaS	Explicación breve
op.acc.4	Proceso de gestión de derechos de acceso	CSC	COMP	COMP	El CSC gestiona los derechos de sus usuarios finales, en PaaS y SaaS comparte con el CSP la gestión de los controles técnicos de acceso.
op.acc.5	Mecanismo de autenticación (usuarios externos)	CSC	COMP	COMP	La responsabilidad principal sobre la gestión de identidades y políticas de acceso recae en el CSC, aunque el CSP puede proporcionar la infraestructura de autenticación.
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	CSC	COMP	COMP	La responsabilidad principal sobre credenciales y políticas de acceso recae en el CSC, aunque el CSP puede proporcionar servicios de identidad.
op.exp.1	Inventario de activos	COMP	COMP	COMP	El CSC inventaría los recursos que despliega y utiliza (usuarios, datos, configuraciones). El CSP gestiona los activos subyacentes de la infraestructura.
op.exp.2	Configuración de seguridad	CSC	COMP	COMP	El CSC configura la seguridad en su entorno, el CSP gestiona la configuración de su infraestructura.
op.exp.3	Gestión de configuración de seguridad	CSC	COMP	COMP	La gestión de la configuración es del CSC en su capa, en PaaS y SaaS se coordina con el CSP.
op.exp.4	Mantenimiento y actualizaciones de seguridad	CSC	COMP	CSP	En IaaS el CSC es responsable de las actualizaciones de sistemas operativos, middleware y aplicaciones. En PaaS el CSP gestiona la plataforma y el CSC su código y dependencias. En SaaS el CSP asume el mantenimiento completo del servicio; el CSC se limita a la configuración y uso seguro.

ID	Medida	IaaS	PaaS	SaaS	Explicación breve
op.exp.5	Gestión de cambios	CSC	COMP	CSP	En IaaS el CSC gestiona los cambios en su entorno. En PaaS es compartida. En SaaS el CSP gestiona los cambios sobre la plataforma y la aplicación.
op.exp.6	Protección frente a código dañino	CSC	COMP	CSP	En IaaS el CSC es responsable de la protección en su capa de software. En PaaS es compartida. En SaaS el CSP protege la infraestructura y la aplicación.
op.exp.7	Gestión de incidentes	COMP	COMP	COMP	La gestión de incidentes es siempre coordinada. El CSC mantiene la responsabilidad de notificación a las autoridades competentes.
op.exp.8	Registro de la actividad	CSC	COMP	COMP	El CSC es responsable del registro de la actividad de sus usuarios. El CSP registra la actividad de la infraestructura bajo su control.
op.exp.9	Registro de gestión de incidentes	COMP	COMP	COMP	Cada parte registra las actuaciones en su ámbito. La coordinación del registro global corresponde al CSC.
op.exp.10	Protección de claves criptográficas	CSC	COMP	COMP	El CSC es responsable de la gestión de sus claves. En SaaS, cuando el servicio lo permita, el CSC debe gestionar sus propias claves. El CSP gestiona las claves de su infraestructura.
op.ext.1	Contratación y acuerdos de nivel de servicio	CSC	CSC	CSC	El CSC establece los contratos y SLA. El CSP asume las obligaciones derivadas de los mismos.
op.ext.2	Gestión diaria	COMP	COMP	COMP	La gestión operativa diaria es compartida en función de las responsabilidades de cada parte.
op.ext.3	Protección de la cadena de suministro	COMP	COMP	COMP	Cada parte es responsable de la seguridad de su propia cadena de suministro.

ID	Medida	IaaS	PaaS	SaaS	Explicación breve
op.ext.4	Interconexión de sistemas	CSC	COMP	CSP	En IaaS el CSC configura y gestiona las interconexiones. En PaaS es compartida. En SaaS el CSP gestiona la interconexión y el CSC tiene una implicación mínima.
op.nub.1	Protección de servicios en la nube	COMP	COMP	COMP	Ambas partes deben proteger los servicios en la nube.
op.cont.1	Análisis de impacto	CSC	CSC	CSC	El CSC realiza el análisis de impacto sobre sus servicios y procesos.
op.cont.2	Plan de continuidad	COMP	COMP	COMP	Los planes de continuidad deben coordinarse entre CSC y CSP. El CSC es responsable de su plan global.
op.cont.3	Pruebas periódicas	COMP	COMP	COMP	Las pruebas de continuidad se realizan en coordinación con el CSP, según lo establecido contractualmente.
op.cont.4	Medios alternativos	COMP	COMP	COMP	Ambas partes deben disponer de medios alternativos en su ámbito para garantizar la continuidad del servicio.
op.mon.1	Detección de intrusión	CSC	COMP	CSP	En IaaS el CSC implementa los mecanismos de detección en su capa (sistemas operativos y aplicaciones); el CSP cubre la infraestructura. En PaaS es compartida. En SaaS el CSP asume la detección; el CSC se limita a la revisión de los registros disponibles y la gestión de usuarios.
op.mon.2	Sistema de métricas	COMP	COMP	COMP	Ambas partes definen y supervisan métricas en su ámbito de responsabilidad.

ID	Medida	IaaS	PaaS	SaaS	Explicación breve
op.mon.3	Vigilancia	CSC	COMP	CSP	En IaaS el CSC implementa la vigilancia en su capa. En PaaS es compartida. En SaaS el CSP asume la vigilancia de la infraestructura y la aplicación; el CSC supervisa la actividad de sus usuarios.
mp.if.1-7	Protección de instalaciones e infraestructuras	CSP	CSP	CSP	En nube pública u hospedada, la seguridad física de las instalaciones es responsabilidad del CSP en todos los modelos. En nube privada *on-premise*, esta responsabilidad recae íntegramente en el CSC.
mp.per.1-4	Gestión del personal	COMP	COMP	COMP	Cada parte gestiona la seguridad de su propio personal.
mp.eq.1-4	Protección de equipos	COMP	COMP	COMP	Cada parte protege los equipos bajo su control. Los equipos del CSC (puestos de trabajo, dispositivos) son siempre responsabilidad del CSC.
mp.com.1-4	Protección de las comunicaciones	CSC	COMP	COMP	La red física subyacente es siempre del CSP en nube pública. No obstante, el CSC mantiene responsabilidades propias en todos los modelos: en IaaS configura y gestiona su perímetro virtual, en PaaS y SaaS es responsable del cifrado en tránsito de sus comunicaciones, la autenticación mutua, el control de acceso a las APIs y la configuración de sus propias conexiones.
mp.si.1-5	Protección de soportes de información	COMP	COMP	COMP	El CSP gestiona los soportes físicos subyacentes. El CSC define las políticas de clasificación, borrado y retención, y es responsable de los soportes bajo su control directo.

ID	Medida	IaaS	PaaS	SaaS	Explicación breve
mp.sw.1-2	Protección de aplicaciones informáticas	CSC	COMP	CSP	En IaaS el CSC es responsable de la seguridad de sus aplicaciones. En PaaS es compartida. En SaaS el CSP asegura la aplicación, el CSC aplica sus políticas de uso seguro.
mp.info.1-6	Protección de la información	COMP	COMP	COMP	Ambas partes protegen la información en su ámbito. El CSC es siempre responsable de la clasificación, el tratamiento y el control de acceso a su información.
mp.s.1-4	Protección de servicios	CSC	COMP	CSP	En IaaS el CSC es responsable de la protección de los servicios que despliega. En PaaS es compartida. En SaaS el CSP protege el servicio; el CSC aplica sus políticas de uso.

Leyenda:

- **CSC** -> La responsabilidad principal de implementación recae en el cliente del servicio en la nube.
- **CSP** -> La responsabilidad principal de implementación recae en el proveedor del servicio en la nube.
- **COMP** -> Responsabilidad compartida: ambas partes intervienen en la implementación, debiendo quedar delimitada su distribución concreta en la Declaración de Aplicabilidad y en el contrato.

La presente matriz constituye un marco de referencia para la asignación de responsabilidades en materia de seguridad entre el CSC y el CSP. No obstante, la concreción de las obligaciones específicas, incluidos los acuerdos de nivel de servicio (SLA), los compromisos de cumplimiento y las responsabilidades asociadas, deberán establecerse de forma expresa en los contratos o acuerdos que regulen la prestación del servicio. Estos acuerdos tendrán carácter vinculante y prevalecerán en aquellos aspectos que requieran un mayor nivel de detalle o adaptación al servicio contratado, sin menoscabo de las responsabilidades que correspondan al CSC como responsable del cumplimiento del ENS y de la normativa vigente

ANEXO C — TRAZA NORMATIVA ENS-REGLAMENTO DE EJECUCIÓN (UE) 2024/2690 PARA PROVEEDORES DE SERVICIOS DE COMPUTACIÓN EN NUBE

La siguiente tabla presenta la correspondencia entre los requisitos técnicos y metodológicos aplicables a los proveedores de servicios de computación en nube, establecidos en el Reglamento de Ejecución (UE) 2024/2690 de la Comisión, y las disposiciones equivalentes del Esquema Nacional de Seguridad (ENS), incluyendo el articulado aplicable y las medidas de seguridad concordantes recogidas en su Anexo II.

Nota: La correspondencia incluida en este anexo tiene carácter orientativo y no constituye una equivalencia jurídica plena entre el ENS y el Reglamento de Ejecución (UE) 2024/2690, ni sustituye el análisis individualizado de cumplimiento que deba realizarse para cada sistema, servicio, proveedor o contrato.

Artículos del Reglamento	Artículos y medidas del ENS concordantes
Artículo 2 Requisitos técnicos y metodológicos	Medidas recogidas en esta tabla Art. 14. Análisis y gestión de los riesgos [op.pl.1] Análisis de riesgos Art. 28. Cumplimiento de los requisitos mínimos [mp.info.1] Datos personales
Artículo 3 Incidentes significativos **Artículo 4 Incidentes recurrentes** **Artículo 7 Incidentes significativos con respecto a los proveedores de servicios de computación en nube**	Art. 25. Incidentes de seguridad [op.exp.7] Gestión de incidentes [op.exp.9] Registro de la gestión de incidentes Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad
1.1 Política sobre la seguridad de las redes y sistemas de información	Art. 12. Política de seguridad y requisitos mínimos de seguridad Art. 27. Mejora continua del proceso de seguridad [org.1] Política de Seguridad [org.2] Normativa de Seguridad [org.3] Procedimientos de seguridad
1.2 Roles, responsabilidades y autoridades	Art. 11. Diferenciación de responsabilidades Art. 13. Organización e implantación del proceso de seguridad [org.1] Política de Seguridad [op.acc.3] Segregación de funciones y tareas

Artículos del Reglamento	Artículos y medidas del ENS concordantes
2.1 Marco de la gestión de riesgos	Art. 7. Gestión de la seguridad basada en los riesgos Art. 14. Análisis y gestión de los riesgos [op.pl.1] Análisis de riesgos [op.ext.3] Protección de la cadena de suministro [op.mon.2] Sistema de métricas
2.2 Control del cumplimiento	Art. 10. Vigilancia continua y reevaluación periódica Art. 28. Cumplimiento de los requisitos mínimos CAPÍTULO IV. Seguridad de los sistemas: auditoría, informe e incidentes de seguridad (artículos 31, 32, 33 y 34)
2.3 Revisión independiente de la seguridad de la información y las redes	Art. 31. Auditoría de la seguridad Guía CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
3.1 Política de gestión de incidentes	Art. 25. Incidentes de seguridad Art. 33. Capacidad de respuesta a incidentes de seguridad Art. 34. Prestación de servicios de respuesta a incidentes de seguridad a las entidades del sector público [op.exp.7] Gestión de incidentes [op.exp.9] Registro de la gestión de incidentes [op.cont.2] Plan de continuidad [op.mon.1] Detección de intrusión [op.mon.2] Sistema de métricas [op.mon.3] Vigilancia

Artículos del Reglamento	Artículos y medidas del ENS concordantes
3.2 Supervisión y registro	Art. 10. Vigilancia continua y reevaluación periódica Art. 21. Integridad y actualización del sistema Art. 24. Registro de actividad y detección de código dañino [op.exp.8] Registro de la actividad [op.mon.1] Detección de intrusión [op.mon.3] Vigilancia [op.acc.1] Identificación
3.3 Notificación de sucesos	Art. 25. Incidentes de seguridad Art. 33. Capacidad de respuesta a incidentes de seguridad Art. 34. Prestación de servicios de respuesta a incidentes de seguridad a las entidades del sector público Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad [op.exp.7] Gestión de incidentes [op.exp.9] Registro de la gestión de incidentes
3.4 Evaluación y clasificación de sucesos	Art. 25. Incidentes de seguridad [op.exp.7] Gestión de incidentes [op.exp.9] Registro de la gestión de incidentes
3.5 Respuesta ante incidentes	Art. 33. Capacidad de respuesta a incidentes de seguridad Art. 34. Prestación de servicios de respuesta a incidentes de seguridad a las entidades del sector público [op.exp.7] Gestión de incidentes [op.cont.3] Pruebas periódicas
3.6 Revisiones posteriores al incidente	Art. 33. Capacidad de respuesta a incidentes de seguridad [op.exp.9] Registro de la gestión de incidentes

Artículos del Reglamento	Artículos y medidas del ENS concordantes
4.1 Plan de continuidad de las actividades y de recuperación en caso de catástrofe	Art. 26. Continuidad de la actividad [op.cont.1] Análisis de impacto [op.cont.2] Plan de continuidad [op.cont.3] Pruebas periódicas [op.cont.4] Medios alternativos [op.ext.3] Protección de la cadena de suministro
4.2 Gestión de las copias de seguridad y las redundancias	[mp.info.6] Copias de seguridad [op.cont.3] Pruebas periódicas [op.cont.4] Medios alternativos
4.3 Gestión de crisis	Art. 26. Continuidad de la actividad [op.cont.2] Plan de Continuidad
5.1 Política de seguridad de las cadenas de suministros	Art. 2. Ámbito de aplicación Art. 15. Gestión de personal Art. 16. Profesionalidad Art. 19. Adquisición de productos de seguridad y contratación de servicios de seguridad Art. 23. Prevención ante otros sistemas de información interconectados [op.ext.1] Contratación y acuerdos de nivel de servicio [op.ext.2] Gestión diaria [op.ext.3] Protección de la cadena de suministro [op.ext.4] Interconexión de sistemas [op.pl.4] Dimensionamiento / gestión de la capacidad
5.2 Directorio de proveedores y prestadores de servicios	Art. 13. Organización e implantación del proceso de seguridad [op.ext.*] Recursos externos

Artículos del Reglamento	Artículos y medidas del ENS concordantes
6.1 Seguridad en la adquisición de servicios TIC o productos TIC	Art. 19. Adquisición de productos de seguridad y contratación de servicios de seguridad Art. 21. Integridad y actualización del sistema [op.pl.3] Adquisición de nuevos componentes [op.pl.5] Componentes certificados [op.ext.1] Contratación y acuerdos de nivel de servicio [op.ext.2] Gestión diaria [op.exp.4] Mantenimiento y actualizaciones de seguridad
6.2 Ciclo de vida del desarrollo seguro	Art. 36. Ciclo de vida de servicios y sistemas [mp.sw.1] Desarrollo de aplicaciones [mp.sw.2] Aceptación y puesta en servicio [op.exp.4] Mantenimiento y actualizaciones de seguridad [mp.info.1] Datos personales
6.3 Gestión de configuraciones	Art. 10. Vigilancia continua y reevaluación periódica Art. 20. Mínimo privilegio Art. 21. Integridad y actualización del sistema Art. 30. Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras [op.exp.2] Configuración de seguridad [op.exp.3] Gestión de la configuración de seguridad
6.4. Gestión de cambios, reparaciones y mantenimiento	[op.exp.5] Gestión de cambios
6.5 Pruebas de seguridad	[op.nub.1] Protección de servicios en la nube [op.exp.5] Gestión de cambios [op.mon.3] Vigilancia
6.6 Gestión de parches de seguridad	Art. 21. Integridad y actualización del sistema [op.exp.4] Mantenimiento y actualizaciones de seguridad

Artículos del Reglamento	Artículos y medidas del ENS concordantes
6.7 Seguridad de las redes	Art. 10. Vigilancia continua y reevaluación periódica Art. 22. Protección de información almacenada y en tránsito Art. 23. Prevención ante otros sistemas de información interconectados [op.pl.2] Arquitectura de seguridad [mp.com.1] Perímetro seguro [mp.com.2] Protección de la confidencialidad [mp.com.3] Protección de la integridad y de la autenticidad
6.8 Segmentación de la red	Art. 23. Prevención ante otros sistemas de información interconectados [op.pl.2] Arquitectura de seguridad [mp.com.1] Perímetro seguro [mp.com.2] Protección de la confidencialidad [mp.com.3] Protección de la integridad y de la autenticidad [mp.com.4] Separación de flujos de información en la red
6.9 Protección frente a los programas informáticos maliciosos y no autorizados	Art. 24. Registro de actividad y detección de código dañino [mp.s.1]Protección del correo electrónico [op.exp.2] Configuración de seguridad [op.exp.6] Protección frente a código dañino [op.exp.3] Gestión de la configuración de seguridad

Artículos del Reglamento	Artículos y medidas del ENS concordantes
6.10 Gestión y divulgación de las vulnerabilidades	Art. 8. Prevención, detección, respuesta y conservación Art. 10. Vigilancia continua y reevaluación periódica Art. 21. Integridad y actualización del sistema Art. 34. Prestación de servicios de respuesta a incidentes de seguridad a las entidades del sector público [op.pl.2] Arquitectura de seguridad [op.exp.3] Gestión de la configuración de seguridad [op.mon.3] Vigilancia [mp.s.2] Protección de servicios y aplicaciones web
7 Orientaciones y procedimientos para evaluar la eficacia de las medidas de gestión de riesgos de ciberseguridad	Art. 7. Gestión de la seguridad basada en los riesgos Art. 10. Vigilancia continua y reevaluación periódica Art. 27. Mejora continua del proceso de seguridad Art. 31. Auditoría de la seguridad [op.mon.2] Sistema de métricas [org.2] Normativa de seguridad [org.3] Procedimientos de seguridad
8.1 Mejora de la sensibilización y prácticas básicas de ciberhigiene	[mp.per.3] Concienciación [mp.eq.1] Puesto de trabajo despejado [mp.eq.2] Bloqueo de puesto de trabajo [mp.s.3] Protección de la navegación web
8.2 Formación en seguridad	Art 15. Gestión de personal Art. 16. Profesionalidad [mp.per.4] Formación
9 Criptografía	Art. 10. Vigilancia continua y reevaluación periódica Art. 27. Mejora continua del proceso de seguridad [op.exp.10] Protección de claves criptográficas [mp.si.2] Criptografía [mp.info.3] Firma electrónica

Artículos del Reglamento	Artículos y medidas del ENS concordantes
10.1 Seguridad de los recursos humanos	Art 15. Gestión de personal [mp.per.1] Caracterización del puesto de trabajo [mp.per.2] Deberes y obligaciones [mp.per.3] Concienciación [mp.per.4] Formación [org.4] Proceso de autorización [op.acc.1] Identificación [op.acc.2] Requisitos de acceso
10.2 Comprobación de antecedentes	Art 15. Gestión de personal Art. 16. Profesionalidad [mp.per.1] Caracterización del puesto de trabajo
10.3 Terminación o cambio de los procedimientos de contratación	[org.2] Normativa de seguridad [mp.per.2] Deberes y obligaciones
10.4 Procedimiento disciplinario	[org.2] Normativa de seguridad [mp.per.2] Deberes y obligaciones
11.1 Política de control de accesos **11.2 Gestión de derechos de acceso** **11.3 Cuentas privilegiadas y cuentas de administración del sistema** **11.4 Sistemas de administración** **11.5 Identificación** **11.6 Autenticación** **11.7 Autenticación de múltiples factores**	Art. 17. Autorización y control de los accesos Art. 18. Protección de las instalaciones Art. 20. Mínimo privilegio [op.acc.*] Control de acceso [op.exp.2] Configuración de seguridad
12.1 Clasificación de activos	Art. 40. Categorías de seguridad [op.exp.1] Inventario de activos [op.pl.1] Análisis de riesgos [op.pl.2] Arquitectura de seguridad
12.2 Gestión de activos	[mp.si.4]. Transporte [mp.si.5] Borrado y destrucción

Artículos del Reglamento	Artículos y medidas del ENS concordantes
12.3 Política de soportes extraíbles	Art. 22. Protección de información almacenada y en tránsito [org.3] Procedimientos de seguridad [org.4] Proceso de autorización [mp.eq.3] Protección de dispositivos portátiles [mp.eq.4] Otros dispositivos conectados a la red [mp.si.2] Criptografía
12.4 Inventario de activos	[op.exp.1] Inventario de activos
12.5 Depósito, devolución o supresión de activos al término de la relación laboral	[mp.si.5] Borrado y destrucción
13 Seguridad medioambiental y física	Art. 2. Ámbito de aplicación Art. 18. Protección de las instalaciones [mp.if.*] Protección de las instalaciones e infraestructuras