CCN-CERT

BP/31

Recomendaciones de Protección del Dato en la Nube: Soberanía Digital

INFORME DE BUENAS PRÁCTICAS

MAYO 2024

ccn-cert centro criptológico nacional

20 ANIVERSARIO Centro Criptológico Nacional

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Fecha de edición: mayo de 2024

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

Índice

1. Objetivo de este documento

Esta guía pretende ofrecer una visión general actualizada, junto con algunas recomendaciones, respecto a las soluciones y recursos tecnológicos que típicamente ofrecen los proveedores de servicios en la Nube (CSP, Cloud Service Provider), así como revisar el estado del arte de la tecnología y soluciones de los proveedores hiperescalares, para garantizar la soberanía digital, incluyendo los aspectos relativos a la confidencialidad, integridad y disponibilidad de los datos.

Con tal propósito, la guía describe las distintas medidas técnicas, organizativas y contractuales que los CSP deben cumplir para mitigar los escenarios de riesgo asociados con este tipo de soluciones. Los riesgos, que se describen contemplan distintos escenarios relacionados con la seguridad lógica y física, la privacidad, así como ciertos aspectos regulatorios aplicables en la Unión Europea.

Sin ser una guía exhaustiva, sí pretende ser un documento de referencia para que los líderes técnicos y de negocio puedan encontrar el balance necesario para innovar y, al tiempo, cumplir con los requisitos de seguridad en la Nube. Esta Guía debe ser consultada de manera complementaria a las guías publicadas por el Centro Criptológico Nacional, en particular, la CCN-STIC-823 (Utilización de servicios en la Nube).

2. Ransomware, resiliencia y seguridad

La norma ISO/IEC 19941:2017[1] define la informática en la Nube como el paradigma que permite el acceso a la red a un conjunto escalable y elástico de recursos físicos compartibles, o recursos virtuales con aprovisionamiento de autoservicio y administración bajo demanda. Algunos ejemplos de recursos incluyen servidores, sistemas operativos, redes, software, aplicaciones y equipos de almacenamiento.

El proveedor de servicios en la Nube debe poseer una infraestructura robusta y segura, uno o varios centros de datos independientes y separados físicamente en distintas zonas, contando un equipamiento suficientemente sobredimensionado (hiperescalar), y del que puede ofrecer instancias a sus usuarios de manera individualizada, creando automáticamente recursos tecnológicos de todo tipo mediante código, sin virtualmente limitaciones, ni en número ni en capacidades (Computación, Inteligencia Artificial, soluciones de seguridad, Comunicaciones Satélite y 5G, Análisis masivos de datos, almacenamiento en multitud de formatos, bases de datos, redes de telecomunicaciones, etc.). En todo caso, el uso de la Nube introduce nuevas arquitecturas y paradigmas de seguridad que es necesario contemplar adecuadamente.

1. https://www.iso.org/obp/ui/#iso:std:iso-iec:19941:ed-1:v1:en

2. Ransomware, resiliencia y seguridad

La provisión de tecnologías en Nube es un modelo que permite el acceso por red, de forma segura y bajo demanda, a un conjunto de recursos tecnológicos configurables. Estos recursos pueden ser suministrados y desplegados rápidamente permitiendo, gracias a la automatización en la gestión de los servicios, la autogestión y el autoservicio. Las Administraciones Públicas españolas de manera creciente se están beneficiando de este nuevo paradigma tecnológico, pese a que requiere de una adecuada formación y conocimiento que le permita comprender qué modelo de seguridad en la Nube es el idóneo para cada necesidad.

En definitiva, el propósito es que los servicios en la Nube estén soportados por arquitecturas que por un lado ofrezcan la seguridad necesaria, el cumplimiento de la legislación, la protección y la soberanía del dato y, por otro lado, dispongan de las funcionalidades necesarias que soporten la estrategia de negocio para poder innovar y reducir el 'time-to-market'. Conseguido este equilibrio entre la seguridad, el cumplimiento, los objetivos, el crecimiento del negocio y la innovación o transformación digital, se consigue ofrecer al usuario la flexibilidad, agilidad, escalabilidad y costes de elección según sus necesidades, además de ofrecer la nube pública la ventaja de ayudar a las organizaciones a poder avanzar en sus objetivos de sostenibilidad.

Es precisamente esta multiplicidad de opciones la que obliga a quienes pretenden beneficiarse de los servicios en la Nube a estudiar con detenimiento las diferentes ofertas del mercado, junto a los requerimientos de negocio propios, su correspondiente análisis de riesgo con el fin de poder seleccionar la solución y salvaguardas adecuadas que mejor se adapten a su apetito del riesgo, salvaguardando la conformidad con las disposiciones de la legislación vigente.

3. Conceptos básicos sobre tecnologías en nube[2]

El modelo de tecnologías en Nube permite el acceso bajo demanda, desde cualquier ubicación física con acceso a Internet, a un conjunto de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios en general) que pueden ser solicitados y liberados de manera inmediata, con mínimo esfuerzo en su gestión.

3.1 Definición de Nube pública, privada e híbrida

3.1.1 Nube pública

Una Nube pública es un modelo de computación en la Nube en el que la infraestructura de TI, como los servidores, las redes y los recursos de almacenamiento, se ofrecen como recursos virtuales accesibles a través de Internet.

Tradicionalmente, las organizaciones tenían que adquirir y autoadministrar la infraestructura necesaria para ejecutar las aplicaciones. Su configuración y mantenimiento eran costosos, y las capacidades de computación avanzadas permanecían fuera del alcance de muchas organizaciones. La nube pública resolvió estos desafíos al hacer que los recursos de TI fueran accesibles como servicios completamente administrados.

2. Véase Guía de Seguridad de las TIC CCN-STIC 823

Así, un proveedor externo mantiene el hardware, el software relevante y las licencias en una red de centros de datos distribuida territorialmente. La entidad usuaria puede acceder exclusivamente a lo que necesita bajo demanda y a cualquier escala desde cualquier dispositivo que elija. Su organización puede usar la nube pública para acceder a tecnologías de vanguardia y emergentes, tales como servicios de inteligencia artificial (IA), tecnologías de registro distribuido o el internet de las cosas (IoT), lo que aumenta la velocidad y la adopción de los avances tecnológicos y contribuye a mejorar la prestación de servicios y la satisfacción de los clientes.

3.1.2 Nube privada

Una Nube privada es aquella en la que la infraestructura necesaria está dedicada a un cliente o inquilino (tenant) específico, es decir, no se comparten recursos con terceros, con independencia de que esa infraestructura subyacente para proporcionar recursos sea propiedad, gestionada y mantenida por la propia organización (on-premise), o externalizada en un CSP.

El término *nube privada* se introdujo para establecer una distinción entre estos entornos en la Nube sobre una infraestructura bajo el control único de la organización (sean internos o externos dedicados) y los servicios de *nube pública* proporcionados por proveedores externos sobre una infraestructura compartida (multi tenant).

3.1.3 Nube híbrida

Una nube híbrida es una configuración en la que una organización utiliza tanto la Nube pública como la privada. Alberga un diseño de infraestructura de TI que integra recursos de TI dedicados (habitualmente, internos de la organización) con la infraestructura y los servicios de proveedores de Nube. Con una Nube híbrida, se puede almacenar los datos y ejecutar las aplicaciones en varios entornos diferenciados.

Las organizaciones suelen adoptar estrategias de Nube híbrida para superar las limitaciones de la Nube privada, lo que les permite seguir utilizando su centro de datos local existente, accediendo a la Nube pública según sea necesario. Asimismo, la Nube híbrida le permiten alterar sin problemas las cargas de trabajo entre diferentes entornos. Cuando las organizaciones se quedan sin recursos de computación en el centro de datos interno, amplían las capacidades al pasar la carga de trabajo extra a servicios externos en la Nube de terceros. La *ampliación en la Nube* es una forma adecuada y rentable de admitir cargas de trabajo que presentan patrones de demanda variables o picos de demanda estacionales.

3.2 Características esenciales de la Nube

3.2.1 Autoservicio bajo demanda

En esta modalidad, y desde un panel de control, el cliente del servicio en la Nube puede unilateralmente gestionar la provisión de recursos de nube a medida que los necesite, tales como potencia de cómputo, espacio de almacenamiento, capacidad de la base de datos, todo ello sin requerir ninguna intervención humana por parte del proveedor, siempre dentro de los parámetros de la licencia de uso contratada.

Es habitual que la configuración de los servicios se realice a través de un navegador convencional, accediendo a un panel de control web, donde el administrador puede realizar todas las operaciones necesarias para solicitar servicios en Nube y administrarlos. Esta característica permite que cualquier operación en la Nube se realice mediante una llamada API, lo que posibilita un alto grado de automatización y monitorización de todas las peticiones en la Nube.

3.2.2 Pago por uso

Bajo esta modalidad, el cliente que consume un servicio en la Nube solo paga por los servicios individuales que necesita durante el tiempo que los utilice, sin necesidad de formalizar contratos a largo plazo ni someterse a licencias complejas. Se dice que son similares al concepto de tarifas de agua y electricidad porque solo se paga por lo que se consume y una vez que se cancela el servicio, no se aplican costos adicionales ni cuotas de cancelación.

3.2.3 Reducción de costes

Otra de las características de la Nube es la reducción de costes que supone frente a la informática tradicional. Esto se debe principalmente a la innovación y la automatización que supone la utilización de las tecnologías e infraestructura de la Nube. Las economías de escala en aquellos proveedores hiperescalares provoca que los precios sean más contenidos y competitivos. La innovación en el hardware, como pueden ser las CPUs, tarjetas de red y otros componentes, así como la automatización que ofrecen los servicios de la Nube, consiguen reducir constantemente los precios que se ofertan al cliente.

3.2.4 Acceso global

Los servicios están disponibles en Internet y se accede a ellos mediante mecanismos estándar que permiten el uso de clientes ligeros, tales como teléfonos móviles, tabletas, portátiles y estaciones de trabajo, no siendo necesaria ninguna instalación de software especializado para su gestión.

Ello permite que cualquier tipo de dispositivo pueda ser un medio de acceso a este entorno tanto para su gestión como para su uso.

3.2.5 Conjunto de recursos dedicados a un cliente o compartidos

Como hemos señalado, los recursos donde se ejecutan instancias de computación pueden ser dedicados a un cliente o compartidos entre varios de ellos; por ejemplo, un centro de datos dentro de determinada unión supranacional (como la UE), o estado (como España), dedicado exclusivamente para determinados clientes específicos, o para un conjunto de clientes concretos pertenecientes, por ejemplo, a un gobierno o una institución. El cliente concreto podría estar ejecutando cargas en la Nube privada, pública o híbrida.

En el caso de la Nube privada las instancias estarían compartidas únicamente entre el mismo tipo de clientes.

En el caso de la Nube pública existen dos posibilidades:

- Aquella en la que un cliente ejecuta en un mismo servidor instancias virtualizadas y compartidas entre otros clientes, y donde los recursos de software y hardware se apoyan en mecanismos de aislamiento lógico para proteger sus datos.
- Aquella en la que algunos proveedores de Nube pública ofrecen instancias de servidores dedicados (sin virtualización) donde el cliente puede ejecutar en el precitado servidor una instancia, con o sin virtualización, aislada completamente de otros clientes, evitando así el aislamiento lógico del hardware y software y aumentando la protección de los datos.

La adopción de uno u otro modelo puede ser a costa de sacrificar el acceso a tecnologías más avanzadas de Nube pues normalmente esto ocurre en el modelo de IaaS. Por norma general, los proveedores de nube publican y actualizan continuamente sus innovaciones tecnológicas, de forma que estén disponibles de manera inmediata. La opción de Nube privada o restringida implica la renuncia al acceso a tecnologías disponibles en la Nube pública utilizada por una creciente mayoría de organizaciones de diversos sectores.

3.2.6 Elasticidad y escalabilidad

Los recursos informáticos del proveedor de la Nube permiten prestar servicios bajo demanda a múltiples organizaciones cliente; recursos físicos y virtuales que son asignados, desasignados y reasignados dinámicamente de acuerdo a la demanda de los usuarios de los servicios, lo que hace posible que las capacidades contratadas puedan ser elásticamente aumentadas o disminuidas, en algunos casos automáticamente, para escalar rápidamente los servicios contratados según la demanda que los usuarios tienen de ellos.

Así, desde la perspectiva del cliente de servicios en la Nube, las capacidades de recursos disponibles pueden parecer ilimitados, pudiendo ser provisionados en cualquier cantidad y en cualquier momento, siempre dentro de los acuerdos contractuales y de facturación del servicio consumido.

Todo ello significa, en definitiva, que los recursos demandados son escalables, es decir, se puede inicialmente contratar una determinada cuota de servicio y crecer de forma progresiva, dependiente de la demanda requerida, según las necesidades del cliente, con total inmediatez, sin tener que mantener una interacción humana entre proveedor y cliente, gracias al alto grado de automatización de los procesos y sistemas que ofrece el proveedor de nube.

3.2.7 Innovación y aceleración digital

La Nube ofrece innovación al cliente gracias a una continua Investigación y Desarrollo y a la propia competitividad entre proveedores de la Nube, que se encuentran constantemente desarrollando nuevos servicios y tecnología y mejorando su eficiencia, propiciando que el cliente se beneficie directamente, reduciendo su 'time-to-market' y convirtiendo rápidamente sus ideas en oportunidades que le permitan acelerar su desarrollo digital.

3.2.8 Resiliencia

El uso de la Nube permite aumentar la resiliencia de IT, observable desde ambos lados de la responsabilidad compartida. Por un lado, el proveedor ofrece una infraestructura compuesta por instalaciones y redes (hardware y software) redundantes, que permite la recuperación de desastres y la disponibilidad hasta un nivel de SLA acordado bajo contrato. Por otro lado, el cliente ha de saber cómo utilizar esta infraestructura para configurar sus soluciones desplegadas en la nube para poder cumplir con sus requisitos de resiliencia. El grado de automatización de los proveedores de la Nube suele ofrecer mayor resiliencia que un centro de datos tradicional.

3.2.9 Seguridad

Una seguridad sólida es crucial para sustentar la transformación digital y la innovación. Los prestadores de servicios en la Nube ofrecen ayuda a las organizaciones para desarrollar y convertir la seguridad, la identidad y el cumplimiento en facilitadores empresariales clave. Los proveedores en la Nube consideran la seguridad una de sus máximas prioridades, diseñando infraestructuras de Nube más seguras, automatizando la seguridad para crear un entorno que impulse la velocidad y agilidad requerida por sus clientes, apoyándose en socios del proveedor y una amplia cartera de soluciones de seguridad. Varios informes de IDC y Gartner[3] señalan que la seguridad en la Nube es mayor que la de un centro de datos tradicional, algo que se puede demostrar mediante las múltiples certificaciones y estándares de seguridad, nacionales e internacionales, que los proveedores de la Nube pública obtienen y mantienen.

3.2.10 Supervisión del servicio

Como hemos señalado, los servicios de computación en la Nube se pueden gestionar automáticamente, optimizando su uso mediante la monitorización y la gestión automatizada, lo que permite una utilización eficiente de la infraestructura. Sin embargo, el uso de los recursos también puede ser consultado, supervisado y controlado por el cliente, proporcionando una mayor transparencia, tanto para el proveedor como para el consumidor del servicio utilizado.

3. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

La supervisión permite, como característica derivada, el pago por uso de los servicios contratados en la Nube, lo que permite una adaptación fácil a las cambiantes necesidades de la organización sin comprometerse a dedicar presupuestos excesivos, y mejorando la capacidad de respuesta ante los cambios que se puedan ir produciendo.

3.2.11 Sostenibilidad

La sostenibilidad, entendida como la capacidad de satisfacer las necesidades del presente sin comprometer las del futuro, propias o colectivas, es un objetivo crucial para la sociedad. Entre sus beneficios se encuentran un planeta más saludable, recursos naturales mejor conservados y una economía más resiliente.

En este contexto, mover cargas de trabajo a la Nube puede ser una decisión estratégica para las empresas que buscan contribuir a la sostenibilidad. La Nube ofrece una serie de ventajas que se traducen en un menor impacto ambiental:

- **Eficiencia energética:** Los centros de datos de la nube están diseñados para optimizar el consumo energético, utilizando tecnologías de última generación y fuentes de energía renovable.
- **Reducción de residuos:** La nube elimina la necesidad de adquirir y mantener hardware propio, lo que reduce la cantidad de residuos electrónicos generados.
- **Escalabilidad:** La nube permite ajustar los recursos informáticos a la demanda real, evitando el consumo innecesario de energía.
- **Flexibilidad:** La nube facilita la adopción de prácticas sostenibles, como el auto apagado de servidores en momentos de baja actividad o escalado cuando así sea necesario.

En definitiva, mover las cargas de trabajo a la Nube no solo beneficia a las empresas en términos de costes y eficiencia, sino que también les permite contribuir a un futuro más sostenible.

3.3 Modelos de servicio en la computación en la Nube

Los diferentes modelos de servicio se vinculan al papel que juega el proveedor que suministra los servicios en la Nube respecto a las diferentes capas que conforman la solución, como puedan ser la red, el almacenamiento, los servidores físicos, la virtualización, los sistemas operativos de las máquinas virtuales, el middleware, las aplicaciones y los datos.

Los clientes de servicios en la Nube pueden decidir hasta qué nivel o capa deciden delegar en el proveedor los servicios requeridos. Se muestra a continuación una imagen simplificada que no tiene en cuenta conceptos como cifrado por parte del CSP y/o el CSC, ni la capa superior consistente en los propios datos llevados a la Nube.

Se consideran tres (3) modelos básicos de servicio en la Nube:

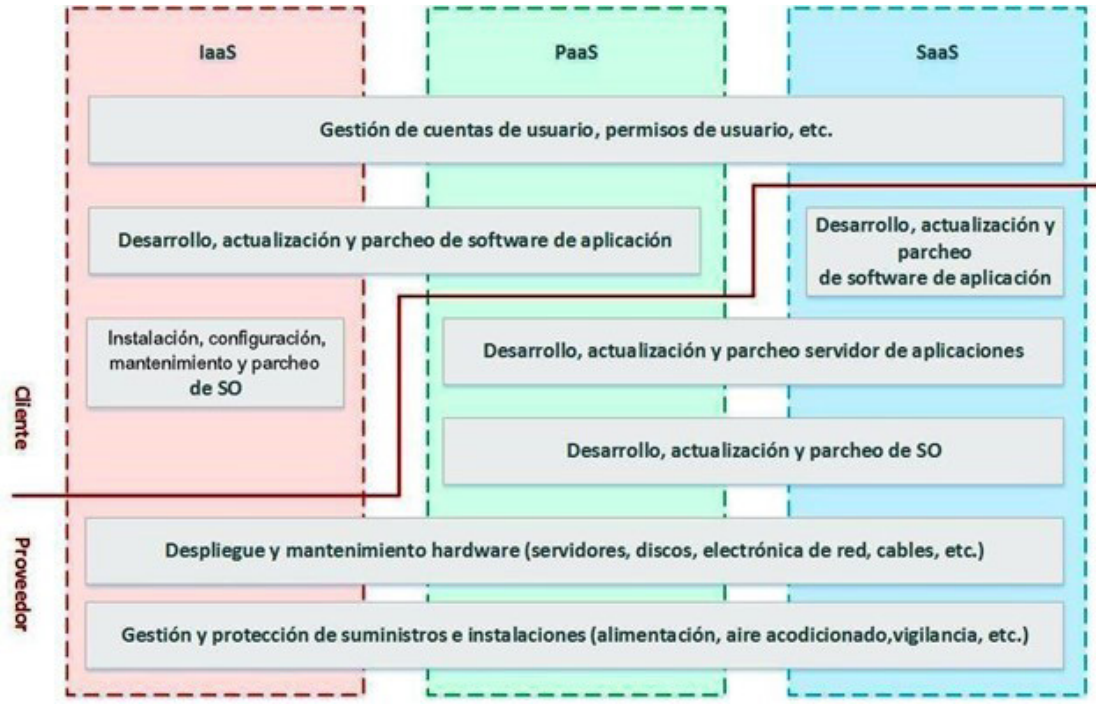


Figura 1.- Responsabilidad en cada uno de los modelos de servicio

3.3.1 Infraestructura como servicio (IaaS)

La infraestructura como servicio, que a veces se abrevia IaaS, contiene los bloques de creación fundamentales para la TI en la nube. Por lo general, permite acceder a las características de conexión en red, a los equipos (virtuales o en software dedicado) y al espacio de almacenamiento de datos. La infraestructura como servicio ofrece el mayor nivel de flexibilidad y control de la administración en torno a los recursos de TI y guarda el mayor parecido con los recursos de TI existentes con los que muchos departamentos de TI y desarrolladores están familiarizados, pero no permite aprovechar al máximo los potenciales ahorros que se obtendrían reduciendo la operación necesaria de la infraestructura transfiriéndola a un tercero.

Este modelo de servicio de computación en la Nube en el caso de IaaS consiste en contratar uno o varios servidores virtuales, compartidos o dedicados, a lo sumo incluyendo el sistema operativo. En esos servidores, el cliente alojará sus aplicaciones y/o bases de datos en el espacio contratado.

En este modelo, el proveedor de servicios en la Nube se limita a mantener el hardware y los suministros y a supervisar que los servidores virtuales funcionen correctamente desde el punto de vista de la disponibilidad del servicio; sin acceso al contenido de la información que se aloja en la instancia del servidor. El cliente dispone de mecanismos para subir y bajar datos y aplicaciones de forma totalmente autónoma y segura.

3.3.2 Plataforma como servicio (PaaS)

En este modelo, las plataformas como servicio eliminan la necesidad de las compañías de administrar la infraestructura subyacente (normalmente, hardware y sistemas operativos) y le permiten centrarse en la implementación y la administración de sus aplicaciones. Esto contribuye a mejorar su eficacia, pues no tienen que preocuparse del aprovisionamiento de recursos, la planificación de la capacidad, el mantenimiento de software, los parches, ni ninguna de las demás tareas que conlleva la ejecución de su aplicación.

En este modelo ocurre exactamente igual que en el IaaS: el proveedor se limita a gestionar la plena funcionalidad de los servicios subyacentes sin acceso a los datos del cliente.

3.3.3 Software como servicio (SaaS)

En este modelo, el software como servicio proporciona un producto completo que el proveedor del servicio ejecuta y administra. En la mayoría de los casos, quienes hablan de software como servicio en realidad se refieren a aplicaciones de usuario final. Con SaaS, no tiene que pensar en cómo se mantiene el servicio ni en cómo se administra la infraestructura subyacente. El cliente del servicio únicamente debe preocuparse por cómo utilizar ese sistema software concreto.

Un ejemplo común de una aplicación SaaS es un programa de correo electrónico basado en la web que le permite enviar y recibir mensajes sin tener que administrar la incorporación de características ni mantener los servidores y los sistemas operativos en los que se ejecuta el programa de correo electrónico. El cliente tendrá que pagar una cuota de alquiler o licencias de uso, siendo únicamente responsable de configurar correctamente la aplicación para implementar los controles de configuración y operación necesarios para la protección de sus datos.

En este modelo puede que el proveedor de servicio SaaS no disponga de infraestructura propia y tenga que subcontratarla a un proveedor de servicios IaaS o PaaS, por lo que puede entrar en juego el conocido como régimen de subcontratación o cadena de suministro.

En este modelo ocurre exactamente igual que en el IaaS: el proveedor se limita a gestionar la plena funcionalidad de los servicios subyacentes sin acceso a los datos del cliente por parte del proveedor SaaS.

3.4 Responsabilidad compartida según el tipo de servicio utilizado

Podemos hablar de seguridad “de” la nube y seguridad “en” la nube, en función del modelo de servicio elegido. En la figura 1 puede observarse que existe un balanceo de responsabilidad entre cliente y proveedor.

Seguridad *de* la nube. El CSP será responsable del mantenimiento y seguridad de los servicios que provea al cliente, así como de cumplir aquellos acuerdos de nivel de servicio y contractuales que se establezcan. Abarcará la seguridad del hardware, el software, las redes y las instalaciones que operan los servicios en la Nube, así como la conformidad con la regulación legal que resulte aplicable a este tipo de servicios.

Seguridad *en* la nube. La responsabilidad del cliente estará limitada a la operativa, gestión, configuración y seguridad de los servicios que despliegue sobre la Nube que no sean propiedad del CSP (por ejemplo, un sistema operativo virtualizado en el modelo de IaaS), así como de las configuraciones que establezca, en base a las funcionalidades que le ofrezca el proveedor dependiendo del tipo servicio y del modelo de servicio en la Nube (IaaS, PaaS, SaaS) que haya contratado, además de la responsabilidad de la conformidad legal de los servicios desplegados en la Nube.

3.5 Modelos de despliegue en la computación en la Nube

Se consideran tres (3) modelos de despliegue en la computación en la nube, con posibles variantes en alguno de ellos.

3.5.1 Despliegue en Nube privada

La Nube privada es la que crea la propia organización para alojar su información a través de servidores virtuales y funcionalidades de autoaprovisionamiento y orquestación, a los que se accede por Internet.

Este modelo de despliegue, en consecuencia, es el que menos se diferencia de las soluciones clásicas de centros de proceso de datos residentes en las organizaciones usuarias. Con esta alternativa se renuncia a la mayor parte de las ventajas que ofrece la Nube. Se incurre en gastos fijos altos, independientemente del uso que se haga de la Nube, a la vez que se hace más difícil cumplir con la optimización del uso energético y del empleo de energías renovables, que son más propios de la nube pública.

3.5.2 Despliegue como Nube Pública

La Nube pública es aquella en que un proveedor de servicios en la Nube pone a disposición del mercado sus plataformas e infraestructuras para que sus diferentes clientes alojen sus datos. La infraestructura hardware y software, según el modelo de servicio elegido, es compartida entre los diferentes clientes (multi-tenant) o dedicada de forma separada entre ellos (single-tenant).

En otras palabras, single-tenant y multi-tenant son dos modelos de implementación de soluciones en la Nube por parte de los proveedores. La diferencia principal es que single-tenant ofrece una instancia de servidor no compartida con otros clientes, mientras que multi-tenant permite compartir un servidor entre distintos clientes, pero dentro del mismo se crean varias instancias de software individuales y seguras gestionadas por cada cliente.

El modelo multi-tenant es considerado más escalable, eficiente y económico que el single-tenant, pero ofrece una superficie mayor de exposición, por lo que, conscientes de ello, los CSP deben adoptar medidas de seguridad más robustas que en un single-tenant.

NOTA: Algunos autores consideran el 'single tenant' como un caso particular de Nube privada, en vez de considerarlo como uno de Nube pública, restringiendo esta última a lo que se conoce como 'multi-tenant'. Esta concepción ha sido la empleada en el apartado 3.3 de definiciones de esta guía.

3.5.3 Despliegue como Nube híbrida

La Nube híbrida es una mezcla de ambas, privada y pública, según las aplicaciones, la naturaleza de determinados datos a tratar y el contexto de la organización. Los despliegues como Nube híbrida también pueden llegar a incluir infraestructura heredada en instalaciones propias.

Para que un despliegue se considere como Nube híbrida, los diferentes entornos de Nube deben estar estrechamente interconectados entre sí, operando como una infraestructura combinada.

4. Soberanía digital y sus requisitos

4.1 Definición de soberanía digital

El concepto de soberanía digital varía en su definición, pero en esencia trata de indicar que el dato está sujeto a las leyes y estructuras de gobernanza del país y de la organización propietaria del dato[4]. Se centra en el control sobre el dato, su ubicación y el acceso al mismo, la infraestructura, el software y el cumplimiento regulatorio necesario para crear y operar el mundo digital[5]. Sin embargo, la soberanía digital también contempla otros aspectos como la transformación digital, la resiliencia, la innovación y la competitividad, además de tener un fuerte componente geopolítico.

La aproximación al cumplimiento de la soberanía digital depende de distintos factores que los Estados reguladores, empresas y proveedores han de considerar. Por un lado, están los riesgos inherentes de seguridad y privacidad y por otro lado está la ventaja competitiva que las tecnologías como la nube ofrecen al negocio para ayudarles a innovar y competir en un mercado libre, digital y global.

La presente sección describe cuáles son los distintos requisitos de soberanía digital, para describir posteriormente medidas técnicas, organizativas y contractuales para cumplir con estos requisitos que ofrece cada proveedor considerado. Con ello se ofrece al lector de esta guía las distintas opciones y medidas que pueden utilizar en el ámbito de la soberanía digital.

---

4. https://d1.awsstatic.com/whitepapers/Whitepaper_Overcoming_the_Tension_Between_Data_Sovereignty_and_Accelerated_Digital_Transformation_2022.pdf

5. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

4.2 Requisitos de soberanía digital

La soberanía digital contempla distintos requisitos, debiendo el usuario de esta guía analizar y valorar cuáles deben ser las medidas técnicas, organizativas, contractuales y regulatorias necesarias para cumplir con ellos, teniendo en cuenta el coste/beneficio, los objetivos de negocio y las políticas y regulaciones que la organización ha de cumplir.

Tanto el usuario como el proveedor de nube están sujetos a legislación vigente que en función de la clasificación de datos que requiere el usuario de la Nube (datos personales, sensibles o clasificados) han de cumplir (Reglamento General de Protección de datos, Esquema Nacional de Seguridad o Ley de Secretos Oficiales, entre otros). En la práctica, puede requerirse su aplicación como una combinación de varias de las precitadas normas jurídicas. Adicionalmente, también hay otras legislaciones que aplican como es la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. La legislación vigente o, en su caso, las cláusulas contractuales contemplan los siguientes requisitos que se detallan en los siguientes apartados de este capítulo:

- **Territorialidad de los datos y posibles transferencias Internacionales:** que reflejará la territorialidad de los Centros de Datos (CPD) donde se ubicará la información del cliente que contrata servicios en la Nube.
- **Jurisdicción a la que se someten las partes bajo contrato:** el contrato debe reflejar a qué legislación se someterá el tratamiento de los datos en relación al cliente, reseñando el mayor número de datos identificativos de cada organización para que el cliente no se encuentre en indefensión cuando requiera hacer valer sus derechos.
- **Limitación de responsabilidad:** son las obligaciones contractuales respectivas de cada parte (CSP y cliente), debiendo protegerse de aquellas que representen un riesgo significativo para ellos.
- **Transferencia de control o portabilidad de datos:** esta cláusula prevé una situación de cambio de control en el CSP donde, ante tales cambios, el cliente tiene el derecho de portar sus datos a otro CSP.
- **Nivel de servicio:** representa la comprensión entre el cliente y el CSP sobre el nivel esperado del servicio que se va a entregar y, en caso de que el proveedor falle en entregar dicho servicio al nivel especificado, fija la indemnización para el cliente.

- **Cláusula de rescisión:** protege al cliente frente al CSP, en caso de una degradación o incumplimiento grave del nivel de servicio (ANS/SLA) esperado y contratado.
- **Confidencialidad:** deben contemplarse las obligaciones del CSP en lo referente a la confidencialidad, es decir, que el CSP no revelará los datos de sus clientes a terceras personas no autorizadas.
- **Propiedad intelectual:** se refiere a la debida protección a los derechos de propiedad intelectual o industrial, derechos de autor, patentes, marcas y diseño industrial.
- **Cumplimiento de la cadena de suministro:** el CSP debe de cumplir de forma transparente, ofreciendo suficientes garantías respecto a las medidas de seguridad técnicas, organizativas y contractuales de los datos a lo largo de toda la cadena de suministro, de acuerdo a la legislación y los contratos vigentes.
- **Notificación de incidencias:** esta cláusula debe definir claramente los mecanismos de notificación de incidencias, especialmente los incidentes de seguridad, entre el CSP y el cliente.
- **Resolución anticipada:** esta cláusula se refiere a la resolución anticipada por parte del cliente del servicio, ya sea por incumplimiento de los ANS/SLA por parte del CSP, o por cualquier otra circunstancia, como puede ser haber encontrado una oferta mejor.

NOTA: Todas estas cláusulas se estudian en profundidad en el anexo al final de esta guía.

4.3 Real Decreto 311/2022, de 3 de mayo

Desde el Centro Criptológico Nacional (CCN), desarrollando las disposiciones del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), se ha establecido una estrategia basada en la responsabilidad compartida y la definición conjunta de mecanismos de seguridad en los entornos en la Nube.

Tanto el proveedor como el cliente requieren realizar un análisis de riesgos previo que ayude a mitigar todos los riesgos, sin olvidar los acuerdos contractuales incluyendo las cláusulas o requisitos descritos en el apartado 4.2 de esta guía. En este sentido, el ENS sirve de base para poder ayudar a establecer una estrategia y un marco de control basado en la creación de Perfiles de Cumplimiento Específicos (PCE) de la seguridad, que permitan trasladar la confianza a las organizaciones, ya pertenezcan al sector público o al privado, en el ámbito de aplicación del ENS.

Figura 2.- Estrategia de seguridad en la nube

4.3.1 Exigencia de cumplir con el ENS

Se debe establecer y certificar el cumplimiento de unos niveles mínimos de seguridad de acuerdo a lo dispuesto en el ENS. Tratándose de llevar a la Nube información con algún tipo de restricción en su manejo por su sensibilidad o clasificación, se deberá exigir una Certificación de Conformidad con el ENS de categoría ALTA del sistema propiedad del CSP donde se alojan los servicios ofrecidos o, de existir, un Perfil de Cumplimiento Específico para una solución concreta en la Nube, todo ello, de conformidad con el preceptivo análisis de riesgos previo que la entidad responsable del tratamiento de los datos debe realizar.

Las soluciones que se despliegan en la nube requieren algunas consideraciones en el momento de contratación y uso de los servicios en la Nube. Estas consideraciones, tratadas desde el prisma del ENS, estarán recogidas en la guía *CCN-STIC 823* Utilización de Servicios en la Nube, así como en otras guías CCN-STIC más específicas orientadas a soluciones.

El análisis de riesgos realizado deberá contemplar la utilización de componentes de seguridad software o hardware en el entorno, y la necesidad de contar, o no, con algún tipo de aprobación o certificación formal para los mismos.

4.3.2 Perfil de Cumplimiento Específico (PCE)

Mediante la Certificación de Conformidad con el ENS en categoría ALTA, quedarán aseguradas las líneas base de seguridad en el empleo de servicios en la nube. Sin embargo, las amplias posibilidades de personalización y configuración que pueden llegar a proporcionar los servicios en nube podrían limitar la capacidad de implantación de medidas de seguridad por parte del CSP, no pudiendo responsabilizarse en algún caso de la configuración definida por el cliente del servicio en la Nube (CSC).

Dentro de la gestión de relaciones con proveedores (Supplier Relationship Management – SRM) orientada a CSC y CSP, cabe señalar:

- **El CSP** conoce los compromisos de seguridad que adquiere con el CSC en base a la Certificación de Conformidad con el ENS de que dispone, de su categoría y de los servicios comprendidos en el alcance, y siempre de conformidad con los requisitos de seguridad expresados por el cliente.

- **El CSC** elige determinados servicios de un CSP en base a su perfil de riesgo, pero no es suficiente con la elección del binomio CSP/Servicios contratados, sino que además debe seguir las guías de configuración segura, también designadas como de bastionado, que proporcionan los CSP para algunos de sus servicios, ya se trata de las Guías publicadas por el CCN o directamente por el propio CSP, de no existir las anteriores.

Esta responsabilidad de ambas partes, los compromisos adoptados por el CSP en base a su Certificación de Conformidad con el ENS y las acciones que el CSC deberá llevar a cabo para asegurar la seguridad de los servicios contratados dentro de sus posibilidades de configuración, podrán ser recogidos en un **Perfil de Cumplimiento Específico, validado por el CCN**, y sus guías de configuración de seguridad asociadas, donde se establezcan qué aspectos de seguridad serán responsabilidad del CSP y cuales corresponderán o serán parametrizables por el CSC.

Junto a la adopción de dicho Perfil de Cumplimiento Específico (PCE), se deberá contar con un análisis que contemple los principales riesgos a los que está sometido el sistema, así como las medidas de seguridad necesarias para su mitigación.

El PCE contendrá una Declaración de Aplicabilidad que detallará la relación de las medidas de seguridad que serán de aplicación y responsabilidad del CSC, yendo acompañada de las Guías de Configuración segura necesarias para que el CSC pueda implementar aquellas configuraciones de seguridad requeridas en el servicio en nube cuya implantación sea responsabilidad del propio CSC.

Como se ha señalado, este PCE deberá ser validado por el Centro Criptológico Nacional para asegurar que se salvaguarden los estándares de seguridad recogidos en el ENS, y será publicado como Perfil de Cumplimiento Específico validado para determinadas soluciones o servicios ofrecidos por los CSP a los que resulte de aplicación.

4.3.3 Mecanismos de vigilancia

Junto a la publicación del Perfil de Cumplimiento Específico (PCE), el servicio en la nube deberá disponer de mecanismos de vigilancia de la superficie de exposición que permitan la monitorización del estado de situación y cumplimiento de las medidas de seguridad recogidas en la Declaración de Aplicabilidad.

Este PCE, junto con las configuraciones de seguridad definidas, y habiendo implementado los mecanismos de vigilancia provistos por el CSP, deberá permitir la reproducción de un escenario de seguridad que garantice el almacenamiento y tratamiento de información sensible o con cierto grado de clasificación en la nube de manera segura.

Es importante comprender que un CSP suele disponer de un variado elenco de organizaciones cliente, con diferentes requerimientos de seguridad, disponiendo de soluciones adaptadas a las necesidades de todos ellos. El Catálogo de Productos y Servicios de Seguridad de las TIC publicado por el CCN, o la adecuada aplicación de las medidas específicas del ENS (como la [op.nub], por ejemplo), o la observancia de las Guías CCN-STIC, contemplan las medidas de seguridad que se consideran más adecuadas.

Evidentemente, cualquier modificación de las medidas de seguridad adoptadas por el CSP que impacte en el PCE relacionado, será previamente validada por el CCN, antes de su explotación comercial en el ámbito del ENS.

4.3.4 Escenarios de Nube segura

El conjunto de instrucciones (por ejemplo, guías, procedimientos o código fuente) necesarias para la implementación de cualquier escenario de seguridad en la nube, así como cualquier mecanismo que permita la reproducción automatizada de un escenario en la nube, serán validados por el CCN y, en su caso, publicados junto al PCE.

Adicionalmente, y dada la rápida evolución de las amenazas que afectan a los sistemas de información, el CSP deberá contar con la capacidad de adaptarse a cualquier escenario que presente un riesgo de seguridad durante todo el tiempo de vida del servicio en nube, garantizando la implantación de medidas de seguridad de acuerdo a la legislación vigente.

En aquellos aspectos de seguridad donde, de acuerdo al preceptivo análisis de riesgos, un CSP haya identificado a partir de un momento dado riesgos graves de seguridad en el servicio que no puedan ser mitigados mediante la implementación de las medidas de seguridad recogidas en el PCE al que se acoja, se deberán implementar en su defecto aquellas medidas compensatorias que permitan mitigar los nuevos riesgos eficazmente, siendo notificadas al CCN dichas medidas a efectos de poder adaptar el PCE en el caso de ser necesario.

4.3.5 Soluciones de apoyo del Centro Criptológico Nacional

Una buena práctica complementaria a todo lo proporcionado por los CSP en aras a la Soberanía Digital de sus clientes de Computación en la Nube es, por ejemplo, implementar soluciones de protección del dato por sí mismo, como es la solución CARLA del CCN. CARLA es una herramienta orientada a la protección y trazabilidad del dato, con independencia de donde se encuentre éste, ya sea en modo local o en la Nube.

La organización cliente de servicios en la Nube define para cada documento, o conjunto de éstos, quiénes tienen derecho de acceder a él en claro. Al estar todos los documentos etiquetados de forma transparente (siempre que se disponga de un agente nominal y de la correspondiente autorización se accederá directamente al documento), una vez retirado el permiso de acceso por la organización propietaria del mismo, el documento no puede descifrarse y, en consecuencia, ser accedido con independencia de dónde se encuentre. En consecuencia, los documentos no podrán ser leídos por terceros ante una hipotética brecha de seguridad con fuga de datos.

4.4 Legislación aplicable sobre seguridad de la información

En España, con afectación al sector público y al sector privado que le aporta soluciones o le presta servicios, disponemos de al menos dos (2) normas jurídicas que determinan, entre otros aspectos, las medidas de seguridad a aplicar a los sistemas de información que soportan los servicios y la información manejada por éstos, en función de determinadas circunstancias.

4.4.1 Ley de Secretos Oficiales (LSO)

4.4.1.1 Introducción a la LSO

La importancia que tiene la protección de la información clasificada (IC), para aquellas organizaciones que la custodien o la traten en sus sistemas de información, está regulada en la Ley 9/1968, de 5 de abril, sobre secretos oficiales (LSO), modificada por la Ley 48/1978, de 7 de octubre y desarrollada por el Decreto 242/1969, de 20 de febrero.

La información clasificada es asimismo tratada en la Estrategia de Seguridad Nacional, donde se reconoce que esta información es un objetivo fundamental para los servicios de inteligencia hostiles, para grupos terroristas que tienen por objetivo la amenaza a nuestra seguridad y la desestabilización de nuestro sistema democrático, y para otros países con intereses económicos o comerciales en competencia con los de nuestra industria.

En España, las *materias clasificadas* (denominación adoptada por la LSO) pueden tener los grados SECRETO y RESERVADO, existiendo asimismo *materias de reserva interna*, que pueden adoptar los grados CONFIDENCIAL y DIFUSIÓN LIMITADA.

4.4.1.2 Criterios de externalización en la Nube

En primera instancia, distinguiremos dos (2) posibilidades distintas basadas en el grado de la información que pretendemos externalizar a un CSP:

- Sistemas que manejan información de los grados (SECRETO, RESERVADO o CONFIDENCIAL). Utilizando como referencia la *Guía CCN-STIC-301 Medidas de Seguridad de las TIC a Implementar en Sistemas Clasificados.*

- Sistemas que manejan información de DIFUSIÓN LIMITADA (DL) que podrían equipararse inicialmente en cuánto a medidas de seguridad requeridas, a falta de realizar el preceptivo análisis de riesgos, con los sistemas que manejan información sensible del ENS de categoría ALTA.

Si combinamos estas dos (2) posibilidades con los modelos de despliegue existentes en la Computación en la Nube, obtenemos hasta cuatro (4) escenarios distintos:

- **Escenario nº 1 - Sistema que maneja IC de grado superior a DL y Nube privada:** si la Nube privada es titularidad de la organización cliente y no compartida con terceras organizaciones (single-tenant), aun no siendo equivalente a desarrollar con infraestructura propia en una Zona de Acceso Restringido (ZAR) de la organización que contrata, podría considerarse adecuada dicha externalización con cautelas contractuales y acreditación de la ZAR del CSP contratado.

- **Escenario nº 2 - Sistema que maneja IC de grado DL y Nube privada:** si la Nube privada es titularidad de la organización cliente y no compartida con terceras organizaciones (single-tenant), aun no siendo equivalente a desarrollar con infraestructura propia en un área segura del Organismo que contrata, podría considerarse adecuada dicha externalización con cautelas contractuales y acreditación del establecimiento adjudicatario o, en su defecto, aportando la certificación del ENS en categoría ALTA de la zona segura que contiene la infraestructura privada y los datos, ya que hemos visto que, a falta de conocer el Plan de Tratamiento de Riesgos (PTR) proveniente del preceptivo análisis de riesgos realizado, pueden considerarse equivalentes sistemas que manejan información clasificada del grado DL y sistemas de categoría ALTA del ENS.

- **Escenario nº 3 - Sistema que maneja IC de grado DL y Nube pública:** este escenario de Nube pública (multi-tenant), por analogía entre los sistemas que manejan IC de grado DL y los sistemas de categoría ALTA del ENS, se contempla en la medida de seguridad **[op.nub.1] Protección de servicios en la Nube** del Anexo II del RD 311/2022, de 3 de mayo, por el que se regula el ENS, que deberá cumplirse junto al resto de medidas que sean de aplicación.

- **Escenario nº 4 - Sistema que maneja IC de grado superior a DL y Nube pública:** este escenario de Nube pública (multi-tenant) no se contempla en primera instancia en los sistemas que manejan IC de grado SECRETO, RESERVADO o CONFIDENCIAL, salvo autorización expresa por parte de la Autoridad de Acreditación del Sistema.

Algunos proveedores de Nube pública ofrecen regiones single-tenant, por ejemplo, empleadas en nubes gubernamentales *SECRET* y *TOP SECRET*. También puede ofrecer 'dedicated local zones' que consisten en zonas completamente aisladas y ubicadas en España. En cualquier caso, estas contrataciones para su aplicación específica a sistemas que manejan información clasificada en un grado superior a DL deben consultarse previamente a la Autoridad de Acreditación del Sistema.

4.4.2 Esquema Nacional de Seguridad (ENS)

4.4.2.1 Introducción al ENS

El ordenamiento jurídico español posee el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), que afecta a los sistemas de información de todo el sector público sin excepción, así como a los proveedores que le aportan soluciones o le prestan servicios competenciales apoyados en medio electrónicos.

El ENS pretende proteger los sistemas de información que soportan los servicios públicos, junto a la información sensible que éstos manejan, aplicando medidas de seguridad en función del preceptivo análisis de riesgos respecto a la seguridad, y de la categoría de dichos sistemas. Dicha categoría puede ser BÁSICA, MEDIA o ALTA.

Como se contempla en la medida de seguridad **[mp.info.2] Calificación de la información,** para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas. El valor a emplear en el caso de información de materias no clasificadas sería USO OFICIAL para información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.

En definitiva, se han de establecer medidas de seguridad específicas, en función del nivel de seguridad de la información de que se trate, o de su calificación, en relación al tratamiento realizado respecto a ella. Como consecuencia, es necesario adoptar criterios o una escala de calificación (o clasificación, si se trata de información clasificada en base a la LSO o tratados internacionales) que permitan ajustar los requisitos de seguridad a dichos criterios. Un ejemplo puede ser calificar la información como 'USO OFICIAL", a la vez que determinar algún ámbito de distribución o difusión de la misma, como puede ser información 'pública', 'de uso interno', 'restringida', etc.

4.4.2.2 Criterios de externalización en la Nube

Los CSP, cuando actúan como proveedor de servicios del sector público, o de sus proveedores, deben cumplir con las disposiciones del ENS. Dicho cumplimiento se evidencia disponiendo de la preceptiva Certificación de Conformidad con el ENS, con independencia de disponer de otras certificaciones en base a estándares internacionales como son, por ejemplo, las normas ISO. En la actualidad existe un importante elenco de CSP certificados del ENS, muchos de ellos en categoría ALTA.

El propio RD 311/2022, por el que se regula el ENS, dispone en su anexo II de la medida de seguridad **[op.nub.1] Protección de servicios en la nube,** específica para servicios prestados en esta modalidad, donde se detallan los requisitos base y refuerzos obligatorios que se deben adoptar según la categoría del sistema de las establecidas por el ENS.

Cabe señalar que el hecho de que un CSP haya obtenido la Certificación de Conformidad con el ENS para categoría ALTA no significa que necesariamente cualquier servicio que ofrezca lo esté, del mismo modo que una certificación contra una versión antigua del ENS puede estar obsoleta en algunos aspectos, todo ello por dos (2) razones:

- La primera es el concepto de 'alcance' de la certificación del proveedor, que podría estar circunscrito a determinado subconjunto de la totalidad de servicios ofrecidos por el CSP: si el cliente de la Nube elige otros servicios excluidos, éstos no estarán amparados por el Certificado de Conformidad con el ENS del CSP.

- La segunda corresponde al concepto de 'catálogo de servicios', que implica el cumplimiento con el ENS para determinada categoría si el cliente de la Nube contrata al menos una serie de servicios (como puede ser la elección de dos CPD en diferentes zonas para la prestación del servicio de Nube, junto a la opción de replicación entre ambos a efectos de disponibilidad): si el cliente no contrata algún servicio necesario del catálogo, no cumplirá con el ENS al no cumplir con todos los requisitos que determina la norma.

4.5 Legislación de protección de datos personales y relacionada

4.5.1 Reglamento General de Protección de Datos (RGPD)

La Computación en la Nube, en función de la zona geográfica o jurisdicción donde se encuentren los CPD del CSP y, en consecuencia, los datos de la organización cliente, podría implicar una Transferencia Internacional de Datos (TID).

En relación a las transferencias de datos personales a terceros países u organizaciones internacionales, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) señala, en su artículo 45 sobre transferencias basadas en una decisión de adecuación, que podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate, garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

En el momento de redacción de estos párrafos, la Comisión Europea ha reconocido que catorce (14) países proporcionan una protección adecuada: Andorra, Argentina, Canadá (solo para organizaciones sujetas a la ley PIPEDA), Islas Feroe, Guernsey, Israel, Isla de Man, Japón, Jersey, Nueva Zelanda, República de Corea, Suiza, Reino Unido en virtud del RGPD y LED, Estados Unidos (organizaciones comerciales que participan en el Marco de Privacidad de Datos UE-EE.UU.) y Uruguay.

Con excepción del Reino Unido, estas decisiones de adecuación no abarcan los intercambios de datos que se rigen por el artículo 36 de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

Existen otras posibilidades de legitimar TID, como son que el tercer país u organización internacional ofrezcan garantías adecuadas, aportadas mediante instrumentos de los relacionados en el art. 46 del RGPD sobre transferencias mediante garantías adecuadas (Normas corporativas vinculantes, cláusulas tipo, autorización de la Autoridad de Control, códigos de conducta, etc.).

4.5.2 Ley 40/2015, de 1 de octubre, de Régimen jurídico del sector público

Mediante el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, se introduce un nuevo art. 46 bis sobre ubicación de los sistemas de información y comunicaciones para el registro de datos en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con implicación directa sobre la Computación en la Nube.

El precitado artículo obliga a que, por motivos de seguridad pública, los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión del censo electoral, los padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de los usuarios del sistema nacional de salud, así como los correspondientes tratamientos de datos personales, se ubiquen y presten dentro del territorio de la Unión Europea. Asimismo, establece que solo puedan ser cedidos a terceros países cuando estos cumplan con las garantías suficientes que les permitan haber sido objeto de una decisión de adecuación de la Comisión Europea, o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

4.5.3 Ley 39/2015, de 1 de octubre, del Procedimiento administrativo común de las administraciones públicas

De la misma forma, mediante el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, se introduce el nuevo apartado 3, que se añade tanto al artículo 9 como al artículo 10 de la Ley 39/2015, de 1 de octubre, establece la obligatoriedad de que, en relación con los sistemas previstos en la letra c) del apartado 2 de los artículos 9 y 10, los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en territorio español en caso de que se trate de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Salvo las excepciones que se introducen en la ley, estos datos no podrán ser objeto de transferencia a un tercer país u organización internacional y, en cualquier caso, se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

5. Espacios de datos

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

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

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

Para ampliar información sobre los espacios de datos, que frecuentemente se apoyarán en la Nube, puede consultarse la guía **"CCN-STIC 813 Ciberseguridad de Espacios de Datos".**

6. Medidas técnicas, organizativas y contractuales de cada CSP

Los siguientes apartados describen las medidas consideradas por distintos proveedores de Nube pública, privada, o híbrida, para el cumplimiento de los requisitos de soberanía digital anteriormente descritos, así como su visión al respecto, todo ello con el propósito de facilitar la toma de decisión al lector de esta guía.

A la vista de la ingente documentación aportada por los distintos proveedores, los epígrafes siguientes son consecuencia de un significativo ejercicio de síntesis y simplificación. En consecuencia, recomendamos contactar con los propios CSP para obtener información adicional más detallada que la que aquí se resume, por orden alfabético.

6.1 Amazon Web Services (AWS)

En AWS la seguridad es la principal prioridad. AWS ofrece un conjunto de más de 300 herramientas de ciberseguridad en la nube. AWS admite 143 estándares de seguridad y certificaciones de cumplimiento, entre los que se encuentra el nivel alto de ENS RD 311/2022 que se recertifica cada año, cumpliendo además con las exigencias de tenercuenta con 8 guías CCN-STIC, así como la cualificación en 2024 de más de una docena de servicios de seguridad, almacenamiento y virtualización en el Catálogo de Productos y Servicios. Todo ello evidencia el compromiso y cumplimiento riguroso de los requisitos y estándares de agencias de seguridad y cumplimiento por todo el mundo.

AWS fue el primer proveedor de nube hiper-escalable en anunciar en junio de 2021 la creación de una nueva región de AWS en España, ofrece ocho regiones existentes (España, Irlanda, Frankfurt, Londres, París, Estocolmo, Milán, y Zúrich) y en 2023 AWS anuncio la creación de la nube soberana para la Unión Europea.

La soberanía ha sido una prioridad para AWS desde el principio de su creación en 2006 y prueba de ellos son las distintas regiones, soberanas por diseño que AWS ha creado en distintos países, incluyendo España, cumpliendo con las exigencias regulatorias nacionales, y siendo el primer proveedor de servicios en la nube que permitía que sus clientes controlaran la ubicación, movimiento y acceso de sus datos. El enfoque en materia de soberanía digital de AWS que se anunció en 2022 con el "Compromiso de Soberanía Digital de AWS" consiste en seguir haciendo que la nube de AWS sea soberana por diseño, comprender las necesidades y los requisitos cambiantes tanto de los clientes como de los reguladores, y a adaptarnos e innovar rápidamente para satisfacerlos sin reducir el rendimiento, la innovación, la seguridad o la escalabilidad que ofrece la nube de AWS. Aunque no existe una definición única de soberanía digital, tras escuchar a los clientes, reguladores y socios, la soberanía digital, AWS lo ha condensado en varios temas principales:

La soberanía del dato incluye:

- **Control sobre la ubicación y procesamiento de los datos:** El cliente tiene el control sobre la ubicación y procesamiento de sus datos.
- **Control verificable sobre el acceso a los datos:** El cliente requiere asegurarse de que ni AWS ni ningún gobierno extranjero puedan acceder a sus datos en la nube.
- **La capacidad de cifrar todo en cualquier lugar:** El cliente requiere funciones y controles para cifrar o encriptar sus datos tanto en tránsito como en reposo o mientras están almacenados en la memoria.

La soberanía operacional incluye:

- **Resiliencia y capacidad de supervivencia:** El cliente quiere asegurarme de que puede mantener las operaciones a pesar de la inestabilidad geopolítica (por ejemplo, la influencia extranjera), los desastres naturales o los fallos técnicos.
- **Independencia:** El cliente quiere que sus industrias y sectores compitan y prosperen. Quiere contribuir al tejido económico y social de su país mediante el desarrollo de capacidades técnicas e infraestructura.

Control sobre la ubicación y procesamiento de los datos

Los clientes tienen la opción de desplegar sus datos en cualquiera de las seis regiones existentes en la Unión Europea entre la que se encuentra la de región España que cumple con el nivel Alto del ENS.

Determinan dónde se almacenará el contenido del cliente, incluido el tipo y la región geográfica del almacenamiento.

El cliente elige el estado de seguridad de su contenido. AWS ofrece a sus clientes características de cifrados líderes en el sector para proteger su contenido en tránsito y en reposo, y le proporcionamos la opción de gestionar sus propias claves de cifrado dentro o fuera de la nube.

El cliente puede gestionar el acceso a su contenido, a los servicios y recursos de AWS a través de los usuarios, grupos, permisos y credenciales que están siempre bajo su control. AWS no puede por diseño acceder a sus contenidos datos y existen múltiples validaciones independientes de auditores que lo acreditan.

Control verificable sobre el acceso a los datos

El sistema AWS NITRO ha reinventado la virtualización de Amazon EC2 para para restringir el acceso a los datos de los clientes mediante hardware y software especializados para proteger los datos ante el acceso externo durante el procesamiento en EC2. Nitro proporciona sólidos límites de seguridad física y lógica, y está diseñado para hacer cumplir las restricciones de modo que nadie, ni siquiera en AWS, pueda acceder a las cargas de trabajo de los clientes en EC2. AWS no tiene rutas de acceso secundarias o alternativas a los sistemas host de EC2 de Nitro. Prueba de ellos son las auditorías realizadas por CCN CPSTIC, así como NCC Group. Esto permite manejo datos sensibles y clasificados.

La capacidad de cifrar todo en cualquier lugar

AWS Key Management Service (AWS KMS) fue el primer servicio de un proveedor de nube en validado por CCN en CPSTIC y está acreditado bajo FIPS 140-2. AWS KMS permite crear, administrar y controlar claves criptográficas en las aplicaciones y en servicios de AWS mediante un control centralizado de las claves criptográficas que se utilizan para proteger los datos.

Los clientes puedan cifrarlo todo en cualquier lugar con claves de cifrado gestionadas dentro o fuera de la nube de AWS mediante un HSM externo mediante la funcionalidad del External Key Store (XKS) de AWS KMS. AWS ha cualificado los servicios de cifrado bajo CPSTIC, así como FIPS 140-2 y existen números proveedores como Thales, Entrust, Fortanix, DuoKey o HashiCorp que ofrecen implementaciones de XKS.

Resiliencia y capacidad de supervivencia

AWS ofrece la más alta disponibilidad de red, mayor que cualquier proveedor de nube. La región de AWS en España fue construida desde cero, mantenidas solo por personal de AWS, y sin compartir su infraestructura con terceros. La región está compuesta por varias zonas de disponibilidad (AZ), que son particiones totalmente aisladas entre ellas. Para aislar mejor los problemas y lograr una alta disponibilidad, los clientes pueden realizar particiones de las aplicaciones y ubicarlas en varias AZ de la misma región de AWS. Las AZ están físicamente separadas entre sí por una distancia significativa de muchos kilómetros, aunque todas están dentro de un rango de 100 km (60 millas) de separación. Adicionalmente AWS ofrece:

- Las zonas locales de AWS que ubican el cómputo, el almacenamiento, la base de datos y otros servicios selectos de AWS más cerca de los usuarios finales.
- Zonas locales dedicadas que ofrecen las mismas características que las zonas locales, pero son creadas para el uso exclusivo por un único cliente o comunidad.
- AWS Outposts brinda servicios, infraestructura y modelos operativos nativos de AWS a prácticamente cualquier centro de datos, espacio de coubicación o instalación local.
- **AWS Wavelength:** implementan infraestructura de AWS que integran servicios de cómputo y almacenamiento de AWS dentro de los centros de datos de los proveedores de telecomunicaciones en el borde de las redes 5G.

AWS anunció en octubre del 2023 el lanzamiento de la Nube Soberana Europea de AWS, una nueva nube independiente para la Unión Europea, diseñada para ayudar a las organizaciones del sector público y a los clientes de sectores altamente regulados a satisfacer sus necesidades de soberanía en constante evolución. La Nube Soberana Europea de AWS será independiente y separada de otras Regiones actuales, con una infraestructura ubicada íntegramente dentro de la Unión Europea y con la misma seguridad, disponibilidad y rendimiento que los clientes obtienen en las Regiones actuales.

AWS Ofrece Landing Zones (LZ) específicas para el cumplimiento regulatorio o el uso de datos clasificados como el LZ del ENS o el Security Accelerator LZ. Los LZ despliegan automáticamente arquitecturas seguras que cumplen con los controles de seguridad específicos para el cumplimiento normativo. Adicionalmente existen una amplia variedad de socios de AWS que ofrecen soluciones soberanas de LZ.

6. Medidas técnicas, organizativas y contractuales de cada CSP

AWS ofrece mediante el programa Global Security & Compliance Acceleration para el ENS la validación de socios de AWS con experiencia en la seguridad de AWS, así como en el cumplimiento del ENS. El CCN ha adoptado este mecanismo para indicar en su página web el número de entidades implementadoras de las guías CCN-STIC que demuestran tener esta competencia.

AWS en colaboración con el CCN, Telefonica Tech, Indra y T-System han formado alianzas conjuntas para apoyar en la ciberseguridad y cumplimiento soberano de las administraciones públicas.

Independencia

AWS proporcionan transparencia en cuanto a los servicios que implican la transferencia de datos de los clientes y no utiliza los datos de los clientes, ni obtiene información a partir de éstos, con fines de marketing o publicidad.

Los clientes disponen de un Contrato de Usuario del Servicio, Acuerdo de Encargado del Tratamiento, Acuerdos de Nivel de Servicio (ANS/SLA), Política de Uso Aceptable y Licencia de Propiedad Intelectual. Los términos de servicio de AWS establecen que el personal de AWS no tiene acceso a los datos de los clientes y distintas certificaciones nacionales e internacionales realizadas por auditores independientes lo acreditan.

Mediante el contrato de AWS pueden utilizar todos los servicios de AWS para procesar los datos personales. El código de conducta CISPE validado por el EDPB y aprobado por la Autoridad Francesa de Protección de Datos (CNIL) certifica 107 servicios de AWS que garantizan a las organizaciones que su proveedor de servicios de infraestructura en la nube cumple los requisitos correspondientes a un procesador de datos de acuerdo con el RGPD.

Los centros de datos de AWS en España se gestionan mediante la empresa Data Service S.L.U de AWS y no utiliza ninguna subcontratación por lo que son gestionadas exclusivamente por personal de AWS cualificado, cumpliendo con las regulaciones y jurisdicción nacional.

AWS ofrece mecanismos y créditos gratuitos para poder migrar los datos y aplicaciones de clientes a otros entornos fuera de AWS.

La Ley CLOUD no otorga a las fuerzas del orden de los Estados Unidos un acceso ilimitado o sin restricciones a los datos. Las fuerzas del orden de los Estados Unidos solo pueden solicitar contenido a los proveedores de servicios en dos circunstancias: (1) con el consentimiento del cliente o (2) con una orden judicial emitida por un tribunal de los Estados Unidos de conformidad con los procedimientos penales de los Estados Unidos.

La Ley es neutral en materia de cifrado y no puede obligar a los proveedores de servicios a descifrar las comunicaciones o los datos del cliente. Adicionalmente es importante señalar que AWS no tiene acceso a las llaves de cifrado controladas y almacenadas en HSM que cumplen con FIPS 140-2 nivel 3.

Históricamente, AWS ha recibido muy pocas solicitudes de las fuerzas del orden de los Estados Unidos y es transparente informando públicamente el número de solicitudes que recibimos y procesamos. A fecha del presente documento ninguna solicitud dio lugar a la divulgación al gobierno de EE. UU. de datos de contenido empresarial o gubernamental ubicados fuera de los Estados Unidos.

Los servicios de nube hibrida de AWS ofrecen una experiencia coherente que satisfagan los requisitos y casos de uso específicos donde sea que la necesite el cliente, desde la nube hasta las instalaciones y en la periferia.

6.2 Google Cloud

Como ya se ha explicado anteriormente, la definición de Soberanía Digital no es única y no consiste únicamente en aplicar una serie de medidas tecnológicas.

Google, además de lanzar su propuesta tecnológica de Soberanía Digital, que se esboza en este apartado, ha llevado a cabo otras acciones en iniciativas que se enmarcan dentro de un plan estratégico para mejorar e incrementar la Soberanía Digital en España, pues aportan valor añadido a la capacidad del país para controlar su propio destino digital.

El concepto de Nube Abierta[6] de Google Cloud tiene una relevancia especial cuando se habla de Soberanía Digital. La apuesta que hace Google en el código abierto (open source) añade capacidades únicas de Soberanía Digital como:

- Transparencia en el código fuente de muchos de los servicios que se ejecutan.
- Flexibilidad para implementar (y migrar si es necesario) cargas de trabajo esenciales en plataformas de nubes públicas o fuera de ellas.

6. https://cloud.google.com/open-cloud

- Flexibilidad para desarrollar y ejecutar apps desde cualquier lugar.
- Autonomía y control sobre la infraestructura y los datos.
- Aumenta la supervivencia de los datos y reduce el 'vendor lock-in' o dependencia del proveedor.

La Seguridad 'en la nube' y la seguridad 'de la nube' son la prioridad según Google. No obstante, en este documento no se detallan las medidas y soluciones de seguridad que están disponibles para los clientes que deciden traer sus cargas de trabajo a Google. Servicios de seguridad como firewalls, Computación Confidencial, gestores de clave, HSM, cifrado en reposo, en tránsito y en uso, proxificación de API, capacidad de elegir la región donde se ubican las cargas de trabajo, fuertes políticas de organización sobre el control de acceso, los roles, los usuarios, medias anti DDoS, DLP, monitorización, controles sobre redes privadas, … son medidas que forman parte del catálogo básico de seguridad de Google Cloud Platform[7].

Este documento incluye únicamente las soluciones que se han desarrollado específicamente para dotar a los datos de sus clientes de servicios en la Nube de capacidades de soberanía digital.

6.2.1 Enfoque de Google Cloud respecto a Cloud Act

Al igual que otras empresas de tecnología y comunicaciones, Google recibe solicitudes de gobiernos y tribunales de todo el mundo para obtener información sobre los clientes. Google Cloud ha desarrollado un proceso transparente, justo y exhaustivo que cumple las mejores prácticas internacionales en lo que respecta a solicitudes de acceso a datos por parte de organismos gubernamentales, incluyendo solicitudes de acceso a datos en base a la Cloud Act. Google proporciona una respuesta caso por caso, teniendo en cuenta diferentes circunstancias, requerimientos legales, acuerdos con clientes y políticas de privacidad.

7. https://cloud.google.com/solutions/security

Google fue el primer proveedor de nube en publicar informes periódicos de transparencia[8] sobre las solicitudes gubernamentales de información del cliente, que incluye solicitudes de acceso a datos en base a la US Cloud Act. Google cuenta con políticas y procedimientos operativos sólidos y otras medidas organizativas implementadas, que protegen contra solicitudes ilegales o excesivas de datos por parte de las autoridades públicas:

Redirección: Si Google recibe una solicitud de una Agencia Gubernamental para obtener datos de clientes de la nube en base a la Cloud Act, Google informa al gobierno que debe emitir la solicitud directamente a la organización (i.e. al cliente). Este enfoque está alineado con la política del gobierno de los EE. UU (Departamento Justicia de US). y las obligaciones contractuales y compromisos entre Google y el cliente.

Evaluación de la validez jurídica: si, no obstante, el gobierno obliga a Google a responder a una solicitud de datos de clientes, un equipo dedicado de abogados de Google y personal especialmente capacitado revisará cuidadosamente la solicitud para verificar que sea legal, proporcionada y satisfaga los requisitos de Google y sus políticas. Google mantiene un equipo dedicado, especializado y multifuncional para evaluar y procesar solicitudes de datos de los usuarios respetando la ley y protegiendo la privacidad y la seguridad de los usuarios.

Todas las solicitudes de datos de usuario deben ser procesadas y aprobadas por los miembros del equipo antes de que cualquier dato esté disponible. Todas las solicitudes se manejan de acuerdo con la ley y las políticas y procedimientos de Google. Además, Google se opone a la solicitud, la limita o la modifica en caso de considerar que es demasiado amplia, desproporcionada o incompatible con la ley aplicable; Google se opone directamente si la considera ilegal[9].

Aviso al cliente (customer notice) y transparencia: Google notificará al cliente antes de que sus datos sean divulgados, a menos que dicha notificación esté prohibida por la ley, pudiera obstruir a una autoridad pública una investigación, o provocar la muerte o daños físicos graves a una persona.

8. https://transparencyreport.google.com/user-data/enterprise
9. https://services.google.com/fh/files/misc/government_requests_for_cloud_customer_data_google.pdf

Cuando la notificación previa por Google está prohibida según la ley aplicable, es política de Google notificar al cliente cuando eventualmente se levanta cualquier prohibición, como cuando una ley o un tribunal ordena la divulgación o el período de prohibición ha expirado. Esta notificación habitualmente se envía al cliente de Google Cloud.

Acción judicial del cliente: Google, en la medida permitida por la ley y por los términos de la solicitud gubernamental, cumplirá con las solicitudes razonables de un cliente con respecto a sus esfuerzos para oponerse a una solicitud, como por ejemplo que el cliente presente una objeción a la divulgación ante la autoridad competente, tribunal y proporcionando una copia de la objeción a Google.

Si Google notifica al cliente de una situación de solicitud gubernamental de datos del cliente y el cliente posteriormente presenta una objeción a la divulgación ante un tribunal apropiado y proporciona una copia de la objeción a Google, Google no proporcionará los datos en respuesta a la solicitud.

6.2.2 Propuesta tecnológica de soberanía digital

Una vez se ha visto que la propuesta de Soberanía Digital no consiste únicamente en una propuesta tecnológica, en este apartado se explica la propuesta tecnológica de Soberanía Digital de Google Cloud, la cual no consiste únicamente en elegir controles ya existentes desde hace años y exponerlos como solución de Soberanía. El enfoque ha sido desarrollar una solución tecnológica nueva, con productos y servicios nuevos, innovando en cómo es posible en la Nube obtener niveles de seguridad e independencia superiores en muchos casos a los obtenidos en despliegues on-premise.

La propuesta debe ser modular y escalable, permitiendo a los usuarios elegir en un catálogo el nivel de Soberanía Digital que necesita para cada uno de sus servicios, sin tener que invertir de más, pero permitiendo los niveles máximos de Soberanía Digital en los servicios que así lo requieran sin renunciar por ello a la innovación y la escalabilidad.

Google entiende que la solución ofrecida en la Nube debe basarse en un catálogo de productos y servicios con el objetivo de permitir a los usuarios hospedar, desde información pública a información clasificada del más alto nivel, pasando por los niveles intermedios, adecuando el coste y complejidad a cada uno de los casos.

Los diferentes niveles de información y la recomendación de cómo aproximar una solución con productos y servicios de Google Cloud es la siguiente:

	Pública	Sector Público ENS	Sin Clasificar Uso Oficial	Difusión Limitada	Confidencial+
GCP	✓	—	—	—	—
GCP-ENS	✓	✓	—	—	—
Controles Regionales	✓	✓	✓	—	—
Controles Soberanía	✓	✓	✓	✓	—
GDCH	✓	✓	✓	✓	✓

Figura 4.- Soluciones diferenciadas en función de los niveles de sensibilidad de la información

En la propuesta de Soberanía Digital de Google en España hay dos (2) líneas diferenciadas que se detallan a continuación, una primera propuesta conectada y una segunda, para cargas de trabajo fuertemente reguladas, completamente desconectadas. En los puntos siguientes se describen de forma abreviada las propuestas:

6.2.3 Soberanía digital conectada

La propuesta conectada de Google Cloud consiste en una serie de productos y servicios nuevos desarrollados específicamente para dotar a los usuarios de capacidades de Soberanía Digital sin renunciar a la innovación, capacidades tecnológicas y economía de escala de la Nube pública.

6.2.3.1 Disponer de un partner de confianza

En la propuesta tecnológica, el partner de confianza juega un papel importante ya que es responsable de varios puntos clave de la propuesta:

- **Gestor de claves externas:** Mantiene en sus centros de datos bajo su absoluto control el gestor de claves con las que se cifran los datos en la Nube. El CSP no tiene acceso ni control en ningún momento sobre esas claves.

Control de las operaciones: Controla, autoriza y monitoriza todas las operaciones del personal del CSP sobre la infraestructura que soporta datos de cliente.

Soporte local: Proporciona soporte desde España y en español para los clientes del CSP en España. Esto permite que el prestador de servicios en la Nube ni siquiera sea consciente en muchos casos de posibles incidencias que puedan tener sus clientes ya que son solucionados de forma completamente autónoma por el partner de confianza.

6.2.3.2 Solución tecnológica

Como se decía anteriormente, la solución tecnológica de Soberanía Digital debe ser una solución modular y escalable que permite adecuar la complejidad a los requisitos de soberanía que cada cliente necesite.

Para concretar la solución tecnológica propuesta por Google, se enumeran a continuación cada uno de los productos y servicios exclusivamente diseñados para proporcionar Soberanía Digital, de menor a mayor nivel de requisitos.

Google Cloud Platform (GCP)

Los clientes de servicios en la Nube cuyos requisitos sean únicamente el hospedar información pública o corporativa sin ningún requisito de Soberanía Digital pueden utilizar la nube pública de GCP en su configuración predeterminada con alto nivel de seguridad, servicio e innovación.

Las medidas de seguridad implementadas por defecto en GCP incluyen cifrado por defecto en todo momento de todos los datos de cliente, alta disponibilidad, sistemas de monitorización permanente, la mejor protección anti DDoS, sistemas anti ransomware, Chronicle SIEM/SOAR, VirusTotal, Mandiant, etc.

Google Cloud Platform (GCP-ENS)

Cuando el cliente de servicios en la Nube necesite cumplir con los requisitos del Esquema Nacional de Seguridad, la solución no puede ser más sencilla ya que se implementa sobre GCP, utilizando todos los mecanismos de protección anteriores y mejorando la seguridad y cumplimiento con la configuración necesaria para cumplir con las disposiciones del ENS incluidas las de categoría ALTA.

Cabe reseñar, por su importancia, que el ámbito de aplicación de la Certificación de Conformidad con el ENS de Google Cloud incluye todos los centros de proceso de datos de GCP en el mundo, así como un gran número de servicios, incluyendo servicios de Soberanía Digital e Inteligencia Artificial.

6.2.3.3 Controles regionales

Este servicio incrementa el nivel de Soberanía, seguridad y confidencialidad de los datos e implementa diferentes controles sobre la nube pública. Además de garantizar el cumplimiento de categoría Alta con el ENS añade:

- Controles de residencia en la Unión Europea para que los datos siempre se mantengan dentro de los límites de la UE.
- Transparencia de acceso, permitiendo a los clientes una total visibilidad sobre las operaciones del personal de Google sobre la infraestructura que soporta sus sistemas.
- Restricciones de TLS que permiten garantizar la máxima seguridad en los datos en tránsito.
- Restricciones de uso de servicios sin garantías de residencia.
- Claves gestionadas por el cliente en la Nube para cifrar los datos. (CMEK).
- Transparencia de acceso a las claves (monitorización sobre el uso de claves criptográficas)
- 'Confidential Compute' - Cifrado en uso.
- Controles de VPC, capa perimetral de protección de datos sensibles.
- Soporte de Google con personal en la Unión Europea.

6.2.3.4 Controles de soberanía

Sobre los Controles Regionales, se construyen los Controles de Soberanía, incluyendo todos los controles establecidos sobre la Nube pública y manteniendo el nivel de cumplimiento del ENS de categoría ALTA.

- **Gestión Externa de Claves:** Permite gestionar las claves de cifrado de la información de forma externa a la nube, de forma que Google no puede acceder a la información en ningún momento porque está protegida a nivel criptográfico.
- **Justificación de acceso a las claves:** Ofrece la posibilidad de definir (externamente a Google) los motivos por los cuales es posible acceder a una clave, habilitando y deshabilitando claves de forma autónoma a Google Cloud.
- **BYOID:** Permite utilizar identidades ya existentes, externas, con los servicios de soberanía.

Para el nivel de soberanía conectada más elevado, interviene el partner de confianza según se ha detallado en apartados anteriores. El partner de confianza ofrece los siguientes controles y garantías:

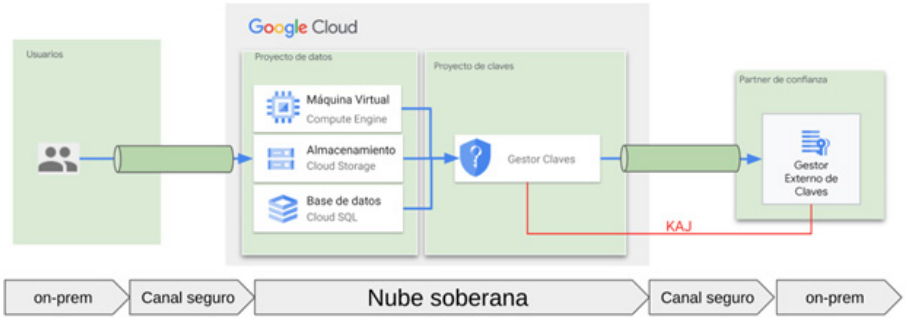
- **Gestión externa de claves:** A través de un servicio gestionado, el partner de confianza ofrece la gestión de las claves externas con todas las garantías, incluyendo la justificación de acceso a las claves y la monitorización del uso de dichas claves.
- **Soporte desde España y en español:** El partner de confianza ofrece soporte especializado de manera que el personal de Google no accede a los servicios, ni siquiera ante problemas de los clientes en España.
- **Control de Acceso:** Cuando el personal de Google Cloud (personal siempre ubicado en la Unión Europea) necesite realizar alguna operación que pueda conllevar un acceso a sistemas de cliente, necesitará una aprobación previa, firmada criptográficamente con una clave externa, antes de poder acceder a la operación.
- **Gestión de claves Externas:** La Gestión de claves externas a través del Cloud EKM[10] External Key Manager) es una pieza fundamental de nuestra propuesta tecnológica de Soberanía Digital conectada. Cloud EKM está incluido en el Catálogo CPSTIC (CCN-STIC-105) en mayo de 2023.

10. https://cloud.google.com/kms/docs/ekm

Cloud EKM permite crear y gestionar claves de forma completamente externa a GCP, en el centro de proceso de datos del partner de confianza y utilizar esas claves para cifrar la información en la nube. De esta forma, la información en la plataforma de GCP se cifra con una clave que no está en la nube, permitiendo al cliente o al partner controlar quién, cuándo y para qué se accede a dicha clave y por ende a la información que protege.

El EKM permite crear claves para cifrado simétrico y claves asimétricas para firma digital, todo fuera de la nube en todo momento. Otra de las funcionalidades de EKM es el KAJ (Key Access Justification) o Justificación de Acceso a las Claves. KAJ permite definir en el gestor externo de claves, los motivos o razones por las que se permite el acceso a las claves en un momento dado, permitiendo al cliente o partner definir cuando Google puede acceder a cada una de las claves y para qué.

El diagrama siguiente muestra a muy alto nivel, de cómo se podría utilizar el cifrado externo en tres (3) servicios distintos, como ejemplo.



6.2.4 Soberanía digital desconectada

Para los clientes con necesidades reguladas como el uso de información clasificada (del grado Confidencial o superior) Google Cloud ha creado, dentro de Google Distributed Cloud, su versión desconectada:

6.2.4.1 Google Distributed Cloud Hosted (GDCH)

Según Google, a diferencia de otras soluciones de otros fabricantes que pueden parecer similares, GDCH es una nube completamente desconectada, diseñada para ejecutar cargas de trabajo sensibles, que admiten clientes con estrictos requisitos de residencia de datos, seguridad y privacidad. GDCH no requiere conexión con el CSP o con cualquier otra red para su funcionamiento.

GDCH incluye el hardware, software, plano de control local y herramientas operativas necesarias para implementar, operar, escalar y proteger una nube administrada completa. Los clientes de sectores regulados, como el gubernamental, los servicios financieros, la atención médica y la fabricación, tienen la capacidad de cumplir con las prioridades empresariales y ayudar a modernizar incluso sus cargas de trabajo más sensibles o confidenciales.

Funciones principales de GCDH

Las funciones principales de GDCH incluyen:

- **Aislamiento total:** GDCH no requiere conectividad a Google Cloud ni a la Internet pública para administrar la infraestructura, los servicios, las API o las herramientas, y está diseñado para permanecer perpetuamente.
- **Servicios en la nube integrados:** GDC Hosted ofrece servicios avanzados en la nube, incluidas muchas de nuestras tecnologías de datos y aprendizaje automático, soluciones de Inteligencia Artificial, OCR, Speech-to-Text y habilita un catálogo de aplicaciones de proveedores de software independientes (ISV) a través de nuestro mercado.
- **Ecosistema abierto:** Se diseñó en torno a la estrategia de nube abierta de Google Cloud. Se basa en la API de Kubernetes y usa componentes de código abierto líderes de la industria en la plataforma y los servicios administrados.
- **Opciones flexibles de hardware:** proporciona a los clientes una flexibilidad líder en el sector para el hardware, lo que incluye procesamiento generalizado y GPU. Los clientes pueden comenzar con tan solo cuatro bastidores y crecer a medida que crecen sus cargas de trabajo.
- **Operaciones configurables:** El modelo operativo se puede configurar para adaptarse a las necesidades únicas de cada cliente.

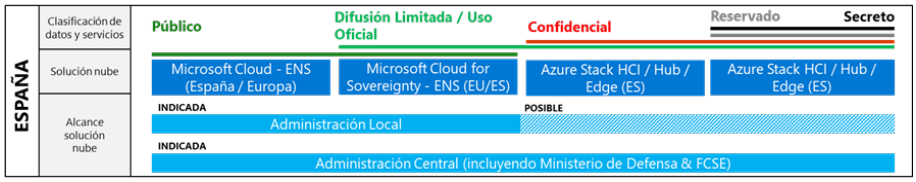
6.3 Microsoft Cloud

6.3.1 Introducción

Microsoft lleva más de 35 años en España y ha realizado diferentes inversiones en formación, digitalización y mejora del ecosistema de empresas tecnológicas. Fue el primer proveedor Cloud en obtener el certificado de conformidad para Esquema Nacional de Seguridad (2016) y recientemente ha obtenido la renovación **(RD 311/2022)** categoría ALTA siendo los primeros y únicos en incluir un servicio de Ciberseguridad apoyado por Inteligencia Artificial.

6.3.2 Medidas técnicas para la Soberanía Digital

La propuesta de soberanía digital de Microsoft sigue una línea basada en los niveles de clasificación de la información. La aproximación es proporcionar la mayor seguridad e innovación posible para cada nivel de clasificación con soluciones Cloud.



Esta aproximación según el nivel de clasificación de la información permite en cada caso adaptarse a las necesidades de los CSC añadiendo las salvaguardas desarrolladas por los equipos de ingeniería y alineadas con los requisitos de las diferentes regulaciones para dotar de mayor seguridad y transparencia.

6.3.2.1 Microsoft Cloud

Microsoft Azure, Microsoft 365, Microsoft 365 para Educación, Microsoft Dynamics 365 y Microsoft Power Platform han sido auditados y encontrados **conforme con las exigencias del Real Decreto 311/2022 del 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, cumpliendo con las disposiciones definidas en la categoría ALTA.**

Microsoft dispone de más de 170 servicios Cloud bajo el alcance de dicho certificado de conformidad, incluyendo servicios de Computación, Almacenamiento, Redes, Gestión de claves, Productividad, Seguridad, Inteligencia Artificial y los servicios utilizados por la solución Microsoft Cloud for Sovereignty. Dentro del alcance de dicho certificado de conformidad también se sitúan todas las regiones ubicadas en la UE + AELC (incluyendo la región de Madrid – España).

6.3.2.2 Microsoft Cloud for Sovereignty (ENS)

Microsoft Cloud for Sovereignty es una nueva solución Cloud disponible de forma general para todos los clientes desde diciembre de 2023. Esta solución se compone de diferentes piezas desarrolladas y disponibles exclusivamente para clientes que requieren soluciones de soberanía digital. Microsoft Cloud for Sovereignty proporciona diferentes activos:

- Herramienta para el despliegue y configuración de la Landing Zone Soberana (SLZ) para restringir y configurar servicios y regiones y aplicar conjuntos de políticas mapeadas con las normativas existentes.
- Herramienta para la gestión del ciclo de vida de la Landing Zone Soberana (SLZ) que permite hacer evaluaciones previas al despliegue, identificar redundancias, conflictos y elementos fuera de política, así como monitorizar la integridad de configuración.
- Conjuntos de políticas mapeadas a la normativa y estándares de la industria existentes, incluyendo el ENS nivel ALTO (disponible a partir 17/05/2024)[11].
- Herramientas de vigilancia de cumplimiento de dichas políticas a través de Defender for Cloud proporcionando un sistema de puntuación de cumplimiento.
- Gestión de claves dedicada (single tenant) mediante Azure Key Vault Managed HSM (FIPS 140-2 Level 3) con control total del dominio de seguridad por parte del partner / CSC, y sacando al CSP (Microsoft) de la cadena de custodio al mismo tiempo que se garantizan los SLAs de Microsoft Cloud y se evitan los problemas de seguridad que tiene la interconexión con sistemas externos.
- Computación confidencial a través de Azure Confidential Computing para la protección de datos y código, así como de máquinas virtuales completas mientras están en uso.

11. https://learn.microsoft.com/es-es/azure/governance/policy/samples/built-in-initiatives#regulatory-compliance

- Logs de transparencia[12] para dar visibilidad de las operaciones que realizan los ingenieros de Microsoft. Se cubren tanto las operaciones requeridas por el partner / CSC como las operaciones realizadas por el CSP (Microsoft). Todos los accesos quedan registrados informando de la suscripción, día/hora de acceso, servicio accedido, rol del ingeniero, localización (lugar de trabajo) del ingeniero y tiempo de acceso. Esta información además es accesible durante 90 días.

Tercero en confianza

Para la solución de Microsoft Cloud for Sovereignty Microsoft propone la figura del tercero en confianza, el partner. Este, se encarga de operar los servicios de los CSC proporcionados por el CSP (Microsoft Cloud).

- Opera la infraestructura Cloud del cliente.
- Da soporte técnico al cliente.
- Gestiona las claves de cifrado a través del servicio de Azure Key Vault Managed HSM, teniendo el control total del dominio de seguridad donde se almacenarán dichas claves de cifrado y sacando así a al CSP (Microsoft) de la cadena de custodio.
- Gestiona la Landing Zone Soberana (SLZ) del cliente, sus políticas el acceso a los logs de transparencia.

6.3.2.3 Azure Stack HCI / Hub / Edge

Para los niveles de clasificación más altos, Microsoft dispone de tres tipos de servicios para entornos de Cloud híbrida/privada.

- **Microsoft Azure Stack HCI (Hiperconvergente)** y que es líder en el cuadrante de infraestructura híbrida distribuida de Gartner[13]. Permite ejecutar cualquier aplicación, máquina virtual o carga de trabajo basada en contenedores en cualquier lugar con una experiencia coherente con el plano de control de Azure en modalidad semi-desconectada (es necesaria una conexión cada 30 días). Dispone de servicios de Inteligencia Artificial en contenedores incluyendo servicios de IA Generativa.

12 https://learn.microsoft.com/en-us/industry/sovereignty/transparency-logs#details-covered-in-transparency-logs
13. https://azure.microsoft.com/es-es/blog/microsoft-recognized-as-a-leader-in-2023-gartner-magic-quadrant-for-distributed-hybrid-infrastructure/

- **Microsoft Azure Stack Hub** amplía Azure para ejecutar aplicaciones en el entorno local (centros de datos propios del CSC) pudiendo desplegar servicios de Azure en su centro de datos en modalidad totalmente desconectada. Azure Stack Hub está aprobado para su uso por el Organismo de Certificación del CCN-CERT[14]. Dispone de servicios de Inteligencia Artificial en contenedores incluyendo servicios de IA Generativa.

- **Microsoft Azure Stack Edge** extiende las capacidades de Azure Stack, permitiendo ejecutar las cargas de trabajo y obtener información en el perímetro, donde se crean los datos, usando hardware como servicio específico. Incluye formatos resistentes (*ruggedized*) y también está certificado por el Organismo de Certificación del CCN-CERT[15]. Dispone de servicios de Inteligencia Artificial en contenedores incluyendo servicios de IA Generativa.

6.3.3 Medidas organizativas

Microsoft dispone de un marco organizativo basado en políticas de seguridad, procedimientos de operación, procesos internos y adecuación a estándares de mercado para garantizar la seguridad de los clientes. A continuación, detallamos dichas medidas:

6.3.3.1 Control de los datos

- Microsoft solo usa los datos de sus clientes para proporcionarle los servicios acordados y con los fines relacionados con la prestación de dichos servicios.

- No comparte los datos de los CSC con anunciantes ni para acciones de marketing. Esta política está respaldada por los acuerdos de servicio y la adopción del código internacional de buenas prácticas para privacidad en la nube, ISO-IEC 27018.

- Microsoft se rige por estrictos estándares de privacidad y seguridad y elimina los datos de los CSC de los sistemas bajo su control, sobrescribe los recursos de almacenamiento antes de reutilizarlos y purga o destruye el hardware retirado.

14. https://aka.ms/AzureStackOc
15. https://aka.ms/AzureStackOc

6.3.3.2 Residencia y seguridad del dato

- El CSC siempre decide en que región de Microsoft Cloud ubicar sus datos (dispone de más de 65 regiones en todo el mundo, incluida la región de Madrid - España).
- El CSC decide los mecanismos de cifrado que utiliza en los servicios de Microsoft Cloud.
- El CSC define los roles y permisos (RBAC) para sus servicios en Microsoft Cloud.
- Para los servicios correspondientes a la iniciativa EU Data Boundary[16], Microsoft almacena y trata los datos del CSC y datos personales dentro de la UE.
- Microsoft protege los datos de sus clientes en reposo (sus centros de datos), en tránsito (entre el CSC y Microsoft, y entre los centros de datos de Microsoft) y en uso (si así lo contrata el CSC) con un cifrado avanzado.

6.3.5 Medidas contractuales

6.3.5.1 Reglamento General de Protección de Datos (RGPD)

Microsoft se compromete a cumplir con el RGPD. Dichos compromisos contractuales de Microsoft con respecto al RGPD (Términos del RGPD) se encuentran en el anexo al **Addendum de Protección de Datos denominado "Términos de conformidad con el Reglamento General de Protección de Datos de la Unión Europea"[17]**. Mediante dichos términos Microsoft se compromete a los requisitos de los encargados del tratamiento en el Artículo 28 del RGPD y otros artículos relativos.

6.3.5.2 Clarifying Lawful Oversees Use of Data (CLOUD Act)

Microsoft como cualquier empresa que opere en EEUU, incluidas las europeas, está sujeta al cumplimiento de la ley Clarifying Lawful Oversees Use of Data (CLOUD Act). A través del CLOUD Act se puede solicitar contenido a los proveedores de servicios solo cuando el sujeto haya dado su consentimiento o con una orden judicial, o de conformidad con un acuerdo bilateral previamente acordado.

---

16. https://learn.microsoft.com/es-es/privacy/eudb/eu-data-boundary-learn
17. https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=31

El CLOUD Act no proporciona acceso sin restricciones a los datos personales. Microsoft adopta una serie de compromisos contractuales con respecto a esta ley:

- Microsoft defiende los datos de sus clientes a través de directivas y procesos claramente definidos y establecidos, compromisos contractuales y, si fuera necesario, los tribunales. En primer lugar, **redirigiendo cualquier solicitud de datos por parte del gobierno al cliente.**
- Si Microsoft recibe una solicitud de datos que pertenecen a un cliente, **se lo notificará de forma inmediata y le proporcionará una copia de la solicitud a menos que esté legalmente prohibido hacerlo.**
- Además, Microsoft **empleará todos los esfuerzos legales para impugnar el requerimiento** de revelación sobre la base de cualquier deficiencia legal relativa a la legislación del requirente o sobre la base de cualquier conflicto con la legislación de la Unión Europea o con la legislación del Estado Miembro aplicable.
- En el caso de que, tras haber seguido los pasos descritos en los puntos anteriores, Microsoft o cualquiera de sus filiales siguiese obligada a revelar datos personales y siguiendo las condiciones establecidas en la Addendum de Protección de Datos[18], **Microsoft indemnizará a un interesado con respecto a los daños materiales y no materiales** que se le ocasionen como consecuencia de una revelación, por parte de Microsoft, de datos personales del interesado que hayan sido transferidos en respuesta a un requerimiento procedente de una autoridad pública u organismo gubernamental no perteneciente a la Unión Europea o al Espacio Económico Europeo en infracción de las obligaciones de Microsoft bajo el Capítulo V del RGPD.
- Microsoft no otorga y nunca ha otorgado acceso a datos personales de clientes de sector público y sector empresarial de la UE. Y tampoco proporciona a ningún gobierno las claves de cifrado de Microsoft ni la capacidad de romper sus mecanismos de cifrado.

6.4 Oracle

6.4.1 Nube soberana de la Unión Europea

La propuesta de Oracle respecto a la soberanía digital está orientada hacia la solución **EU Sovereign Cloud**, la cual ofrece a los clientes acceso a más de cien servicios iguales a los de la nube pública comercial de Oracle.

18. https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=31

Se pueden ejecutar las mismas aplicaciones y cargas de trabajo en Oracle EU Sovereign Cloud, sin precisarse nuevas competencias ni procesos operativos.

Actualmente, hay dos (2) regiones de EU Sovereign Cloud, una en España y la otra en Alemania. **Ambas son independientes de las regiones de nube comerciales y gubernamentales de Oracle.** Esta arquitectura en la nube de la UE independiente simplifica y fortalece la soberanía y los controles digitales.

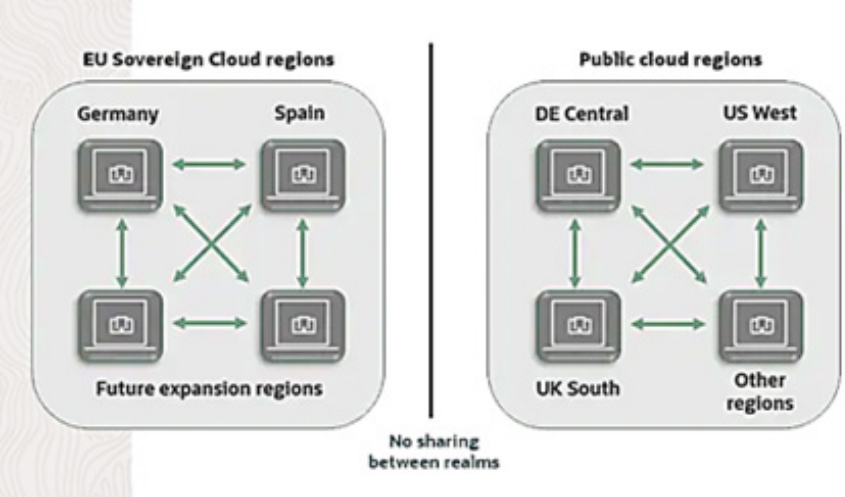


Figura 6.- Distinción entre EU Sovereign Cloud regions y Public Cloud regions

6.4.2 Ventajas de la Nube soberana

Los despliegues de los clientes son más rápidos y asumen menos riesgo con la residencia de datos y la contención en la UE por defecto, sin depender su configuración de herramientas basadas en políticas complejas.

Los clientes pueden utilizar las dos regiones en la Nube de Madrid y Frankfurt, separadas ambas por unos 1.500 km, para la redundancia y la recuperación ante desastres. Cada región de Oracle Cloud tiene al menos tres dominios de errores, que son agrupaciones de hardware que forman centros de datos virtuales para ofrecer una alta disponibilidad local y resiliencia a fallos de hardware y red.

El **dominio EU Sovereign Cloud** se diferencia de otras ofertas de Nube al ser un dominio diseñado para datos de la UE, ubicado en la UE, operado en su totalidad por residentes de la UE y con acceso físico y lógico restringido a residentes de la UE.

El personal de Oracle que proporciona soporte al cliente, soporte del centro de datos y operaciones del centro de datos se encuentra en toda la UE. El hardware y los activos utilizados para EU Sovereign Cloud son propiedad, operados y gestionados por una entidad jurídica independiente.

6.5 Otros proveedores de Nube pública, privada o híbrida

Futuras actualizaciones de esta guía están abiertas a otros prestadores de servicios en la Nube (CSP) con la finalidad de aportar su conocimiento y puntos de vista respecto a la soberanía digital en cuanto a mecanismos de protección de los datos en la Nube para mantener el control sobre los mismos.

Anexo 1. Cláusulas contractuales y computación en la nube

1.1 Introducción

La computación en la Nube representa un cambio respecto al modelo tradicional de entrega de servicios de TI. Una parte importante del éxito de la migración hacia la Nube es la formalización del contrato o contratos (prestación de servicios, acceso a datos personales, etc.) entre el proveedor (CSP) y la organización cliente (CSC).

1.1.1 Regulación contractual de la prestación del servicio

Cualquier prestación de servicios, y la computación en la Nube no deja de serlo, requiere que se regule mediante un contrato la relación entre el CSP y el CSC (en este caso, el contratante). Distinguiremos:

- **Las cláusulas del contrato,** que deben definir claramente la posición de cada una de las partes, así como sus responsabilidades y obligaciones, habitualmente incluyendo cuestiones relativas a la seguridad de la información del cliente que es custodiada por el proveedor.

- **Los términos de uso,** que se encargan de definir las especificaciones técnicas más importantes relacionadas con la entrega y la calidad del servicio. Suelen estar recogidas en documentos llamados Acuerdos de Nivel de Servicio (ANS o SLA por sus siglas en inglés) y entre otras cuestiones establecen los niveles de rendimiento y disponibilidad garantizados por el proveedor.

Si bien los contratos comerciales siempre se negocian, en el caso de los CSP a menudo no suele existir tal acercamiento de posiciones. Los CSP suelen mostrar claramente en un portal web las condiciones en las que prestan su servicio y es el cliente el que debe adherirse a ellas (contratos de adhesión). En consecuencia, un buen consejo es negociar el contrato siempre que sea posible o, en su defecto, estudiar cuidadosamente cada una de las cláusulas propuestas por los diferentes proveedores, hasta encontrar el acuerdo que mejor satisfaga las necesidades del cliente.

Los clientes de los CSP pueden diferir en tipología (organizaciones pertenecientes al sector público o al sector privado), tamaño (sector privado de µPYMES a grandes empresas; sector público de pequeños a grandes organismos) y utilización del servicio (clientes que aportan elevado volumen de negocio y clientes relativamente irrelevantes a efectos de facturación), lo que determinará su capacidad de negociar. Este aspecto es muy relevante desde el punto de vista legal, ya que la futura relación entre un CSP y sus clientes estará regulada por medio del precitado contrato. Debido a la falta de regulaciones específicas, las funciones y obligaciones recíprocas se establecerán en cláusulas generales de contratación, elaboradas de manera unilateral por el CSP y aceptadas por los clientes sin modificación (comúnmente), o negociadas en acuerdos específicos.

Conviene destacar que incluso cuando un cliente no puede negociar diferentes condiciones de un contrato con un CSP específico, el cliente todavía es libre de elegir entre las diferentes ofertas del mercado. Por tanto, en el caso de una pequeña organización, las recomendaciones que siguen respecto a cláusulas contractuales específicas deben entenderse como facilitadores de elección entre las diferentes ofertas del mercado.

1.1.2 Análisis detallado de cada cláusula

1.1.2.1 Conformidad con el ENS

Si los servicios alojados en Nube participan de las competencias de la entidad pública contratante, es imperativo que los sistemas de información en los que se sustentan tales servicios sean conformes con lo dispuesto en el ENS, en los niveles de seguridad en cada dimensión y en la categoría de seguridad que la entidad contratante haya determinado previamente.

Lo anterior implica la necesidad de verificar que los sistemas concernidos del CSP poseen la correspondiente Declaración de Conformidad con el ENS (solo aplicable a sistemas de información de categoría Básica) o la Certificación de Conformidad con el ENS (obligatoria para sistemas de categorías Media y Alta). En este último caso, de no poseer la Certificación, dichos sistemas habrán de ser evaluados por una Entidad de Certificación del ENS acreditada por ENAC que confirme dicho cumplimiento, de conformidad con lo dispuesto en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, tras haber superado satisfactoriamente una Auditoría de Seguridad, regulada en la Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

1.1.2.2 Seguridad de la información y protección de Datos personales

Debe prestarse especial atención a esta cláusula cuya finalidad es asegurar que el CSP puede proporcionar suficientes medidas de seguridad, tanto técnicas como organizativas, a los tratamientos sobre datos personales que lleve a cabo en base a la prestación de sus servicios, a la vez que garantice el cumplimiento de la legislación del cliente en la materia (como puede ser el RGPD y la LOPDGDD).

Para mayor garantía, sería bueno se hiciera constar en el contrato de prestación de servicios que el CSP dispone de certificaciones de seguridad de la información (por ejemplo, del ENS) quizá complementada por la ISO/IEC 27018:2019 Código de Prácticas para la protección de la Información de Identificación Personal (PII) en la nube o cualquier otro estándar internacional. Debe prestarse especial atención al alcance de la certificación, el cual debe cubrir el conjunto de servicios que se contratan, ya que todas las normas permiten certificaciones parciales. Debe recordarse que las certificaciones obtenidas por un CSP no son eternas, estando sometidas a un proceso de renovación cada cierto tiempo en base a una auditoría realizada por una entidad de certificación (EC) acreditada (en España por ENAC) y, respecto a las normas ISO, auditorías de seguimiento anuales. Esto significa que debería verificarse anualmente que el CSP mantiene las certificaciones necesarias.

Habitualmente, además de una cláusula referida a protección de datos en el contrato de prestación de servicios con el CSP, se suscribe un contrato adicional de Encargado del Tratamiento específico, para dar cumplimiento al art. 28 del RGPD que señala *"1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado"*.

1.1.2.3 Territorialidad de los datos y posibles transferencias Internacionales

Esta cláusula reflejará la territorialidad de los Centros de Datos (CPD) donde se ubicará la información del cliente que contrata servicios en la Nube.

Si dicha transferencia es a un tercer país como, por ejemplo, fuera del EEE (Espacio Económico Europeo), puede tener importantes consecuencias legales, ya que se considerará una transferencia internacional de datos. En dicho caso únicamente se consideraría factible si se dispone de una Decisión de Adecuación en base al art. 45 del RGPD sobre transferencias internacionales de datos, que señala *"1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica".*

Según la Comisión Europea, a la redacción de esta guía, hay 14 países que han sido reconocidos como adecuados para la transferencia de datos personales desde la UE: Andorra, Argentina, Canadá (solo para organizaciones sujetas a la ley PIPEDA), Islas Feroe, Guernsey, Israel, Isla de Man, Japón, Jersey, Nueva Zelanda, Suiza, Uruguay, Reino Unido y EE.UU. (para el marco de privacidad de datos UE-EE.UU., que entró en vigor el 10 de julio de 2023). Debe tenerse en cuenta que estas Decisiones de Adecuación pueden ser revisadas o revocadas por la Comisión Europea en cualquier momento si considera que el nivel de protección ya no es suficiente.

1.1.2.4 Legislación aplicable

La legislación aplicable es el conjunto de leyes y normas a las que debe ajustarse el contrato entre el CSP y el CSC.

Cada país tiene restricciones y requerimientos específicos amparados en legislación aplicable a los datos, principalmente si son de naturaleza personal.

El contrato debe reflejar a qué legislación se someterán los datos y sus tratamientos en relación al cliente, que actúa en calidad de Responsable del Tratamiento ('Data Controller' en inglés). El CSP, por su parte, actúa como Encargado del Tratamiento ('Data Processor' en inglés).

1.1.2.5 Jurisdicción a que se someten las partes

Otro aspecto relevante es la jurisdicción aplicable en relación a discrepancias entre las partes (CSP y cliente) durante el ciclo de vida del contrato que regula la prestación de servicios en la Nube. Dada la universalidad de muchos CSP, debe quedar reflejado en dicha cláusula a qué jurisdicción se someten las partes, así como reseñar los máximos datos identificativos de cada organización para que el cliente no se encuentre en indefensión cuando requiera hacer valer sus derechos.

Téngase en cuenta que pueden devenir en nulas cláusulas de previsión en materia de responsabilidad, en función de la ley aplicable que rija el contrato. Si la legislación es de corte anglosajón, acepta limitaciones de responsabilidad de los CSP y en su caso determina una compensación económica en base a la cuantía desembolsada por el cliente en la contratación del servicio. Si la legislación es de corte continental, permite la limitación de responsabilidad por negligencia, pero no por culpa o dolo.

No siempre resulta sencillo lograr que la jurisdicción recaiga en el propio país. En la práctica, la decisión definitiva termina por depender de la capacidad de negociación de las partes, de modo que el CSP o CSC que goce de una posición preponderante, termina imponiendo las condiciones que le sean más convenientes.

1.1.2.6 Confidencialidad

Deben contemplarse las obligaciones del CSP en lo referente a la confidencialidad, es decir, que no revelará nuestros datos a terceras personas. La cláusula recogerá que todo el personal empleado o colaborador (técnico, administrativo, de apoyo o de mantenimiento) del CSP que por cuestiones de operativa del CPD tenga o pueda tener acceso a los datos del cliente, habrá firmado una cláusula de confidencialidad. El CSP, por tanto, responderá ante cualquier actuación dolosa o negligente de éstos. Este aspecto queda garantizado si el CSP dispone de la Certificación de Conformidad con el ENS, pero no está de más que quede reflejado en el contrato.

Otro de los puntos clave a tener en cuenta en la cláusula de confidencialidad, es la limitación de los Supuestos en los que el proveedor del servicio podrá revelar la información a terceros. Aunque la jurisdicción que vaya a regir el contrato podrá contener previsiones específicas en este sentido, resulta conveniente limitar la revelación de datos a efectos de cumplir obligaciones legales o de requerimientos de autoridades competentes.

En cualquier caso, debería hacerse constar que la revelación de datos o información ha de ser la mínima necesaria para cumplir con cualesquiera obligaciones legales o requerimientos. Siempre que sea posible, el CSP se comprometerá a notificar lo antes posible al cliente tal revelación de datos, indicándole qué datos ha revelado y a quién lo ha hecho. Otra cuestión es que los datos del cliente del servicio estén cifrados en todo momento.

1.1.2.7 Propiedad intelectual e industrial

La cláusula de propiedad intelectual e industrial es importante tenerla en cuenta. En su acepción más amplia sujeta a derecho, se refiere a los denominados derechos de autor, patentes, marcas y diseño industrial.

Para generalizar, puede referirse a que todo el trabajo que se ha realizado durante el ciclo de vida del contrato de servicios en la Nube, apoyándose en las utilidades que el CSP proporciona, son propiedad intelectual del cliente o de terceros que le han cedido el derecho de uso mediante las correspondientes licencias. Ha de quedar estipulado que los datos, App (aplicaciones), BB.DD. (Bases de Datos), y demás herramientas software que el cliente ha ubicado en la infraestructura del CSP, son de su propiedad.

Según el modelo de entrega de servicios en la Nube que se haya contratado, puede ser más o menos difícil de determinar:

- **Infraestructura como Servicio (IaaS).** Dicho modelo de entrega, equivale a contratar el aprovisionamiento de servidores virtuales completamente vacíos. Solo disponen del sistema operativo. Por tanto, todo su contenido será del cliente. Al CSP no le corresponde derecho alguno.

- **Plataforma como Servicio (PaaS).** En este caso, además del sistema operativo suele incorporar una BB.DD., utilitarios de programación, "web services", etc. Todas las aplicaciones que desarrolle el cliente con esas herramientas de programación, otras aplicaciones que adicione y los datos asociados, serán de su propiedad y no generaran derecho alguno a favor del CSP.

- **Software como Servicio (SaaS).** En este caso, el cliente se limita a utilizar una aplicación o conjunto integrado de ellas en la Nube. Por tanto, serán solo de su propiedad el contenido que allí almacene: Datos, metadatos, etiquetado de recursos y tal vez los scripts permitidos para automatización, entre otros posibles.

A modo de resumen esta cláusula asegura que el acuerdo de servicio no implique nunca la cesión de ningún derecho de propiedad intelectual a favor del CSP, que ha de comprometerse a no efectuar ningún tratamiento, ceder o facilitar el acceso a los contenidos del cliente, en favor de terceros, ya sea de forma parcial o en su totalidad, en ninguna forma ni por ningún medio.

1.1.2.8 Limitación de responsabilidad

Al revisar sus obligaciones contractuales respectivas, las partes (CSP y cliente) deben proteger aquellas que representen un riesgo significativo para ellos, mediante la inclusión en este apartado de cláusulas económicas de remediación u obligaciones de indemnizar caso de incumplimiento de la otra parte de sus obligaciones contractuales, o que se produzcan desviaciones en el nivel de servicio.

Si no es posible, al menos deben revisarse y evaluarse cuidadosamente las cláusulas estándar que ha incluido el CSP en su contrato y que normalmente eximen o limitan su responsabilidad.

De forma general, salvo aquellas cuestiones que puedan quedar fuera del ámbito de control o voluntad del proveedor del servicio, el CSP debería responsabilizarse frente al cliente de cualesquiera daños o perjuicios que pudieran surgir a consecuencia de la suscripción del contrato de prestación de servicios en la Nube.

1.1.2.9 Transferencia de control

Esta cláusula prevé una situación de cambio de control en el CSP, motivada por ejemplo por una compra, absorción o fusión empresarial. Podría redactarse de forma que, en dicho supuesto, el nuevo gestor que ofrecerá los servicios contratados en la Nube se obligue a heredar las actuales condiciones contractuales, o bien el cliente tenga la potestad de rescindir el contrato.

No obstante, el cese o rescisión voluntaria del acuerdo de servicio, tal vez por parte del CSC, también debería preverse de forma análoga a esta cláusula.

1.1.2.10 Cadena de subcontratación

En el caso de que estemos contratando una aplicación en la Nube, tipo SaaS, puede darse el caso que lo hagamos con un proveedor de software independiente ("software house" o desarrollador de software) y éste no disponga de infraestructura virtual debiendo subcontratarla. Si es así, en al Acuerdo de Encargado de Tratamiento (lo firman la empresa cliente y el proveedor SaaS) debe figurar que el Encargado del tratamiento (el proveedor SaaS) subcontrata los servicios a un proveedor de IaaS o PaaS, indicando el nombre de la empresa subcontratada (El CSP donde se almacenarán los datos). Por tanto, puede producirse una subcontratación en cadena con otros terceros. Representa una sucesiva realización de tratamientos por encargo, donde alguno de los proveedores que prestan el servicio puede estar ubicado fuera del territorio de la UE, en uno de los llamados terceros países.

Para que la subcontratación en cadena de servicios sea legítima y acorde al ordenamiento jurídico europeo (especialmente de Protección de Datos), el cliente que actúa como Responsable del Tratamiento, queda obligado a exigir la suscripción de un contrato de tratamiento por encargo, donde se disponga que el proveedor del servicio (Encargado del Tratamiento) solamente actuará siguiendo las instrucciones del Responsable del Tratamiento que es objeto del servicio. Si además el proveedor del servicio se encuentra ubicado en un tercer país, será preciso verificar que dicho país está amparado por una Decisión de Adecuación de la Comisión Europea.

Mediante el contrato de tratamiento por encargo o de "Encargado del tratamiento", según dispone el art. 28 del RGPD, un Responsable del Tratamiento establecido en la UE, traslada sucesivamente a los diferentes CSP que intervienen, el compromiso respecto a las condiciones y garantías que deben aportar para asegurar el nivel de protección de los datos personales, adecuado a las disposiciones del RGPD.

El art. 28 del RGPD señala no solo la necesidad del contrato de Encargado del Tratamiento señalando *"3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable", sino que también dispone "2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios"*. El apartado 3 del mismo artículo detalla el contenido mínimo que debe tener dicho contrato.

Adicionalmente, dicho contrato de tratamiento por encargo debería recoger que el CSP se comprometa a formalizar dicho tipo de acuerdos con todas las terceras empresas que intervengan en la prestación del servicio y así sucesivamente, informando inmediatamente si se prevé variación respecto a las mismas.

1.1.2.11 Resolución anticipada por incumplimiento de los ANS/SLA, o incluso libremente

Esta cláusula protege al cliente frente al CSP, caso de una degradación o incumplimiento del nivel de servicio (ANS/SLA) esperado y contratado por el cliente. Es aconsejable que el cliente se proteja estableciendo una posible rescisión del contrato por dichas causas, independientemente de pactar indemnizaciones.

Asimismo, debería estar prevista la cancelación o finalización del contrato por cualquier otra circunstancia como, por ejemplo, la intención de migrar a otro CSP que le ofreciera mejores condiciones al cliente.

Debe dejarse clara la propiedad de la información y demás aplicaciones que el cliente haya ubicado en el CLOUD (ver cláusula de Propiedad Intelectual).

Debe pactarse un retorno ordenado de la información, a ser posible estableciendo un formato estándar para los datos, fijando un período transitorio que posibilite migrar en tiempo adecuado los datos y aplicaciones a otro CSP o, en su caso, a un CPD local. Dicho proceso de finalización de servicios deberá prever y detallar un formato de intercambio, que haga viable la extracción sin que se resienta la integridad de los datos. Resultaría útil que el CSP estuviese contractualmente obligado a cooperar en el marco de una migración de datos a la nueva infraestructura que indique el cliente. Todo ello, a ser posible, de forma gratuita.

Una vez la información esté replicada en su nueva ubicación, deberá garantizarse el proceso de borrado seguro de la misma en el CSP que se abandona, que elimine toda posible brecha posterior de seguridad. Dicha situación futura, cuando deje de estar en vigor la relación contractual que une al cliente con el CSP, no puede comprometer de ninguna manera la responsabilidad sobre los datos. Debe prestarse atención a posibles legislaciones que obliguen al proveedor a conservar los datos cierto tiempo pese haber finalizado la relación.

Siempre es recomendable que el cliente tenga una cláusula en el contrato, que le permita rescindir el mismo sin necesidad de alegar razón, mediante el envío de un preaviso con una antelación razonable y pactada. Esta previsión es relevante en contratos que tienen como sustento de la prestación de servicios a la tecnología que, si bien carece de interés para el CSP, su influencia es crucial en el cliente. Nadie garantiza que un proveedor puntero hoy, lo siga siendo dentro de varios años. Si dicha cláusula no es aceptada por el CSP, al menos debe identificarse cualquier penalización o exigencia de pago íntegro del servicio caso de resolución unilateral anticipada, que se contemple en las condiciones generales de contratación.

1.1.2.12 Acuerdos de Nivel de Servicio

Los acuerdos de nivel de servicio (ANS / SLA) más que una cláusula contractual suele ser una adenda al contrato o un documento específico.

No se puede gestionar el nivel de servicio, si no se han suscrito previamente un SLA / ANS con el CSP, al igual que no pueden suscribirse si previamente el cliente del servicio no ha definido sus Requerimientos de Nivel de Servicio (SLR). Caso de adscribirse un ANS estándar del CSP, al cliente igualmente debe verificar que cumpla sus requerimientos del SLR.

El National Institute of Standards and Technology (NIST) define un Acuerdo de Nivel de Servicio como: *"Un SLA representa la comprensión entre el cliente y el CSP sobre el nivel esperado del servicio que se va a entregar y, en caso de que el proveedor falle en entregar dicho servicio al nivel especificado, la compensación disponible para el cliente".*

Algunos CSP ya contemplan el seguimiento del cumplimiento de los SLAs mediante un conjunto estándar de indicadores que pueden consultarse a través de un panel de control o cuadro de mando unificado desde el portal del cliente, o bien mediante el envío de informes periódicos al cliente por correo electrónico.

Una vez que se ha migrado a la Nube, el cliente tiene la responsabilidad de velar que los términos del SLA se están cumpliendo y que los indicadores clave de rendimiento (KPI) son monitorizados. Serán los KPI quienes reflejen con precisión el rendimiento en curso. Una vez que el cliente ha definido y desarrollado los parámetros de los KPI, puede trabajar con el CSP para crear alertas cuando el rendimiento caiga por debajo de un rango aceptable. Mediante el análisis de la causa, el rendimiento podrá irse optimizando de forma continua.

Es aconsejable que, a la contratación del servicio en la Nube, ya se dispone de definiciones de KPIs propios o estándares. Así podrán añadirse inicialmente como un anexo al contrato, que vincule al CSP al cumplimiento de los SLA, en base a valores tangibles. Su incumplimiento puede conllevar penalizaciones pactadas en el contrato.

Recordar que los indicadores de nivel de servicio han de ser específicos, medibles, alcanzables y realistas.

Marcos y estándares sobre las "mejores prácticas" de TI como puede ser ITIL, definen una completa Gestión del Nivel de Servicio, que es bueno consultar previamente a la contratación.

1.1.2.13 Notificación de incidencias

Esta cláusula debe definir claramente los mecanismos de notificación de incidencias, especialmente las de seguridad, entre el CSP y el cliente. Deben definirse interlocutores concretos y formas de comunicación, de forma armonizada con la medida de seguridad [op.nub.1] del Anexo II del RD 311/2022, de 3 de mayo.

Debe prestarse especial consideración en definir el tiempo máximo que puede transcurrir desde que ocurre o se descubre la incidencia, hasta que es fehacientemente notificada. También es importante definir si el cliente dispondrá de acceso a consultar por algún medio el registro de logs, transacciones y accesos que afecten al entorno de sus propios datos.

De forma adicional, puede preverse el caso de incurrir en costes financieros o de reputación por parte del cliente, motivados por un incidente de seguridad del CSP, las posibles compensaciones económicas y la designación de un árbitro neutral para evaluarlo. Puede darse el caso de que, por requerimientos legales, se deba avisar a terceros mediante notificaciones específicas, dado que el cliente actúa como Responsable del Tratamiento.

Centro Criptológico Nacional

20 ANIVERSARIO

CCN-CERT centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es