Compra de servicios en la nube en el sector público

Manual: incluye un ejemplo de texto de licitación para un Acuerdo marco de nube

Avisos

Este documento se proporciona solo para fines informativos. No se ha desarrollado según las disposiciones legales de los procesos de adquisición pública de ninguna región en particular. Los clientes de servicios en la nube son responsables de realizar sus propias evaluaciones independientes de la información contenida en este documento y de cualquier uso de los productos o servicios del proveedor de nube. Este documento no genera ninguna garantía, representación, compromiso contractual, condición ni afirmación.

Los documentos y textos de ejemplo no se deben interpretar como un asesoramiento, una orientación ni un consejo legal. Los clientes de servicios en la nube deben consultar a sus asesores jurídicos para conocer sus responsabilidades en virtud de la ley aplicable en su propio país. CISPE excluye expresamente toda garantía, responsabilidad o daños asociados que puedan derivarse de, o estén relacionados con, la información proporcionada en este documento.

Acerca de CISPE

Cloud Infrastructure Services Providers in Europe (CISPE, Proveedores de servicios de infraestructura de nube en Europa,https://cispe.cloud) es un grupo independiente del sector sin ánimo de lucro. Representamos a los proveedores de servicios de infraestructura de nube en Europa y trabajamos con el sector y los dirigentes políticos para proporcionar orientación y formación sobre los servicios en la nube y su papel en el sector, la vida pública y la sociedad en general.

Nuestros miembros, cada vez más numerosos, incluyen empresas que operan en todos los países de la Unión Europea con sedes globales en 16 países europeos. La asociación está abierta a las empresas siempre que declaren que al menos uno de sus servicios cumple los requisitos del Código de conducta de protección de datos de CISPE. Nosotros:

- Defendemos los beneficios de las políticas de adquisición pública centradas en la nube dentro de la Unión Europea y de los Estados miembros de la Unión Europea.
- Promovemos requisitos de seguridad y estándares técnicos coherentes en toda la Unión Europea.
- Apoyamos unos requisitos de privacidad globales con un código de conducta.
- Trabajamos para mantener el mercado de la infraestructura de nube de la Unión Europea abierto, competitivo y sin monopolios comerciales.
- Evitamos compromisos injustificados de supervisión de contenidos en el marco legal de la Unión Europea.

Nuestros miembros ofrecen y mantienen los "componentes informáticos básicos" esenciales que permiten al gobierno, las autoridades locales y los negocios crear sus propios sistemas y ofrecer servicios esenciales a miles de millones de ciudadanos. Con esta función, contribuimos en el desarrollo de tecnologías y servicios de vanguardia que incorporan inteligencia artificial (IA), objetos conectados, vehículos autónomos y 5G, así como de la próxima generación de tecnología de conectividad móvil.

Código de conducta de los servicios de infraestructura en la nube

El código de CISPE es anterior a la aplicación del Reglamento general de protección de datos (RGPD) de la Unión Europea. Se adapta a los estrictos requisitos del RGPD, lo que permite a los proveedores de infraestructuras de nube cumplir la normativa y ofrecer un marco robusto para que los clientes puedan seleccionar proveedores de servicios en la nube y confiar en sus servicio. El código de conducta de CISPE ha declarado más de 100 servicios proporcionados por más de 30 empresas con sede en más de 16 Estados miembros de la Unión Europea y utilizados por millones de usuarios finales y consumidores. https://cispe.cloud/code-of-conduct/

CISPE y el sector público

CISPE participa en el debate de la política pública y trabaja para garantizar un mejor conocimiento del papel, la contribución y el potencial del sector de infraestructuras de nube en Europa.

Si bien el modelo de compra pública debe condicionar el proceso de adopción y uso de la informática en la nube, la adquisición de servicios en la nube difiere de la mayoría de las adquisiciones tecnológicas tradicionales conocidas por el sector público. Conviene reconsiderar los enfoques de adquisición: CISPE está animando a los dirigentes políticos de la Unión Europea a desarrollar un enfoque más ambicioso y con visión de futuro en la Unión Europea basado en iniciativas políticas "centradas en la nube", lo que contribuye a impulsar el crecimiento de un mercado único de infraestructura de nube en Europa y a apuntalar los objetivos de crecimiento del Mercado único digital (DSM).

Este manual se ha diseñado para proporcionar orientación y apoyo de utilidad a las autoridades públicas a la hora de adquirir servicios en la nube.

Más información
Miembros de CISPE: https://cispe.cloud/members
Consejo ejecutivo: https://cispe.cloud/board-of-directors
Servicios de informática en la nube declarados en virtud del código de conducta de CISPE: https://cispe.cloud/publicregister

Índice

Resumen y finalidad de este manual

La finalidad de este **manual de compra de servicios en la nube** es proporcionar orientación a aquellos clientes de la nube que deseen comprar servicios en la nube mediante un proceso de adquisición competitivo (**Licitación de servicios en la nube**), pero que carecen de experiencia para redactar un Acuerdo marco de nube.

Este documento se proporciona solo para fines informativos. No se ha desarrollado según las disposiciones legales de los procesos de adquisición pública de ninguna región o país en particular.

En este manual también se incluye la redacción de criterios de selección adicionales para **pedidos abiertos** o **minilicitaciones** cuando se realiza la compra a partir de un Acuerdo marco de nube. Las secciones del manual se organizan a modo de una licitación de TI genérica. La licitación genérica de ejemplo y el texto de los criterios de selección están acompañados por comentarios que ayudan a comprender por qué una licitación de nube difiere de una licitación de TI tradicional.

> ***"Servicios en la nube"*** *hace referencia a todas las tecnologías de la nube y a los servicios relacionados a los que el usuario final necesita acceder. Incluye los servicios de consultoría, profesionales o administrados necesarios para apoyar y ejecutar la migración a la nube y mantener las cargas de trabajo en la nube, además de la propia infraestructura de nube, así como servicios de marketplace en la nube, como los productos de software como servicio (SaaS).*

La aparición de la informática en la nube como opción por defecto de la TI del sector público ofrece la oportunidad de modernizar las estrategias de adquisición existentes. Los procesos de adquisición centrados en la nube permiten a las entidades del sector público extraer todos los beneficios de la nube, como el acceso a innovaciones punteras, aumento de la velocidad y la agilidad, la mejora de la posición de seguridad y la gestión del cumplimiento normativo, al tiempo que logran una mayor eficacia y ahorros en los costes.

Los métodos de adquisición de TI tradicionales para la compra de hardware, software y centros de datos no son aplicables a la compra de servicios en la nube. Todos los enfoques de precios, gestión de contratos, términos y condiciones, seguridad, requisitos técnicos y acuerdos de nivel de servicio, entre otros, cambian en un modelo en la nube, por lo que el uso de métodos de adquisición existentes reduce o elimina en última instancia los beneficios que proporciona la nube.

Uno de los métodos más efectivos de adquisición de servicios en la nube en el sector público es el **Acuerdo marco de nube**, una adjudicación a varias organizaciones de una selección de nubes entre las que los compradores afiliados a la organización de compras que reúnen los requisitos pueden adquirir tecnologías de la nube y servicios asociados que cubran sus necesidades y se adapten a ellas. Como vehículo de lo contratación de nube, dichos acuerdos marco hacen posible la compra de servicios en la nube de manera eficiente y eficaz, de manera que las organizaciones de compras y las entidades de usuario final pueden acceder a una amplia gama de servicios en la nube y, en última instancia, obtener todos los beneficios de la nube: agilidad, beneficiarse de las enormes economías de escala, escalabilidad para lograr una mejor disponibilidad con un coste más bajo, amplitud de funcionalidad, ritmo de innovación y capacidad de expansión a nuevas regiones geográficas.

Tenga en cuenta que **este documento se centra en la compra de las tecnologías de nube Infraestructura como servicio (IaaS) y Plataforma como servicio (PaaS) que proporciona el *Cloud Infrastructure Service Provider (CISP,* Proveedor de servicios de infraestructura en la nube).** Estas tecnologías de la nube se pueden comprar directamente del CISP o a través de un distribuidor del CISP. *Se requieren algunas consideraciones adicionales en la licitación para los distribuidores de servicios de marketplace en la nube (PaaS y SaaS) y los servicios de consultoría de nube.*

Tenga en cuenta asimismo que este documento no cubre todos los aspectos de la creación de un marco de adquisición de nube de extremo a extremo. Existen muchos otros documentos del sector y de los analistas que cubren cuestiones como prácticas recomendadas de adquisición de la nube, cómo presupuestar la nube o la gestión de la nube, entre otros, por lo que recomendamos encarecidamente que tengan en cuenta este asesoramiento y documentos durante el desarrollo de una estrategia global de adquisición de la nube.

La **Tabla 1** siguiente proporciona un esquema del manual de licitación de servicios en la nube y la ubicación del texto de licitación de ejemplo de cada componente en una licitación de servicios en la nube.

Tabla 1: resumen de las secciones del manual de licitación de servicios en la nube

Sección	Información general y texto de licitación de ejemplo
1.0 Información general de un acuerdo marco de nube	Visión general del modelo de acuerdo marco de nube (lotes, cómo competir y contratación)
2.0 Descripción general de la licitación de servicios en la nube	Texto de licitación genérico general que cubre las secciones siguientes, junto con comentarios que explican los motivos de la estructura y el texto de licitación de servicios en la nube.
2.1 Configuración de una licitación de servicios en la nube	2.1.1 Introducción y objetivos estratégicos 2.1.2 Calendario de respuesta a la licitación 2.1.3 Definiciones 2.1.4 Descripción detallada del modelo de compra y competición dentro del acuerdo marco 2.1.5 Requisitos mínimos del licitante: administrativos
2.2 Técnicos	2.2.1 Requisitos mínimos 2.2.2 Comparación entre proveedores 2.2.3 Contratación
2.3 Seguridad	2.3.1 Requisitos mínimos 2.3.2. Comparación entre proveedores 2.3.3 Contratación
2.4 Precios	2.4.1 Requisitos mínimos 2.4.2 Comparación entre proveedores
2.5 Configuración y condiciones de ejecución del contrato	2.5.1 Términos y condiciones 2.5.2 Cómo seleccionar entre los adjudicatarios por proyecto 2.5.3 Incorporación y baja
3.0 Prácticas recomendadas y lecciones aprendidas	3.1 Gestión de la nube 3.2 Elaboración de un presupuesto para la nube

Sección	Información general y texto de licitación de ejemplo
	3.3 Conocimiento del modelo empresarial basado en socios 3.4 Intermediarios en la nube 3.5 Recursos y estudio de mercado previo a la licitación
Apéndice A: Requisitos técnicos para la comparación entre licitantes	Lista de requisitos genéricos de tecnología de nube para pedidos abiertos o minilicitaciones
Apéndice B: demostración	Script de ejemplo de un producto de tecnología de nube que muestra la calificación (demostraciones de nube como parte de un pedido abierto o una minilicitación)

1.0 Información general de un acuerdo marco de nube

Un acuerdo marco de nube bien diseñado posibilita la compra de servicios en la nube de manera que tanto las organizaciones del sector público como los proveedores de nube que participen en el se vean beneficiados. Entre los beneficios de un acuerdo marco de nube bien diseñado se incluyen:

- **Carácter cooperativo:**
    - La unión de varias organizaciones para realizar pedidos con requisitos similares resulta conveniente y eficaz, y reduce los costes, al tiempo que simplifica el proceso de pedido. Establece una manera efectiva de agrupar la demanda de tecnologías de la nube y servicios en la nube comunes de varias organizaciones del sector público, como pueden ser las soluciones de marketplace y los servicios de consultoría.
- **Amplia gama de servicios en la nube:**
    - Puede incluir todos los servicios de consultoría, profesionales o administrados para apoyar y ejecutar de forma integral la migración a la nube y soportar las cargas de trabajo en la nube, así como las tecnologías de la nube proporcionadas por el CISP y los servicios de marketplace.
    - Estas tecnologías de la nubepueden adquirirse directamente del CISP o a través de un distribuidor del CISP.
- **Gestión de contratos:**
    - Unifica las distintas organizaciones o compradores en torno a unos términos y condiciones comunes y la adjudicación de un contrato maestro único, en lugar de uno diferente para cada organización.
    - También es beneficioso para los proveedores, dado que proporciona un proceso de adquisición, unas condiciones y un mecanismo de pedido estándar en lugar de uno diferente para cada organización del sector público.
    - Ofrece flexibilidad. La creación, aprobación y ejecución de un contrato de nube efectivo dentro de las políticas o regulaciones gubernamentales existentes requiere experimentación y una rápida capacidad de adaptación. Resulta mucho más beneficioso crear un acuerdo marco que permita al sector público y a los proveedores de nube trabajar juntos para mejorar el contrato, de forma contractual, mecánica y eficaz. Un contrato de

varios años que no funciona y no se puede adaptar se traduce en una mala experiencia para los usuarios finales del sector público, las organizaciones de adquisición y los proveedores de nube.

- Variedad:
    - Permite a los compradores elegir entre varios CISP cualificados y establece un alto nivel para todos los servicios en la nube y sus servicios asociados, como el marketplace de PaaS y SaaS en la nube y la consultoría de nube.
    - Facilita el control de los distintos proveedores dentro de un marco asegurándose de que se revisa adecuadamente el estándar de cada adjudicatario.

El acuerdo marco para la compra de servicios en la nube funciona mejor cuando incluye las principales tecnologías de IaaS o PaaS que proporciona el CISP, junto con el marketplace de IaaS o PaaS, y los servicios de consultoría a los que pueden acceder los usuarios finales del sector público, cuando sea necesario, para ayudarles a planificar, realizar la transición, utilizar y mantener la ejecución de una carga de trabajo en la nube. Por ello, aconsejamos que la licitación de servicios en la nube para establecer un Acuerdo marco de nube se divida en tres lotes, como se describe a continuación:

- LOTE 1: TECNOLOGÍAS DE LA NUBE
  Tecnologías de nube que se compran directamente del CISP o a través de un distribuidor del CISP.

- LOTE 2: MARKETPLACE
  Acceso a un marketplace de servicios de PaaS y SaaS

- LOTE 3: CONSULTORÍA DE NUBE
  Servicios de consultoría relacionados con la nube (formación, servicios profesionales, servicios administrados, etc.) y soporte técnico.

*Como se ha señalado anteriormente, este documento se centra en la compra de las tecnologías de nube IaaS y PaaS (**LOTE 1**) tal y como las proporciona el CISP (adquiridas directamente de un CISP o a través de un distribuidor del CISP). Se exigirían requisitos de cualificación distintos para los distribuidores de los LOTES 2 y 3 en una licitación de servicios en la nube.*

La **Figura 1** siguiente proporciona una vista de alto nivel de cómo una licitación de servicios en la nube bien estructurada, dividida en estos tres lotes, puede dar lugar a un Acuerdo marco de nube que dote a las entidades del sector público de agilidad (tanto técnica como contractual), visibilidad y control del gasto y uso de la nube, además de la capacidad de disponer de todos los servicios en la nube necesarios para crear y mantener las soluciones que precisen.

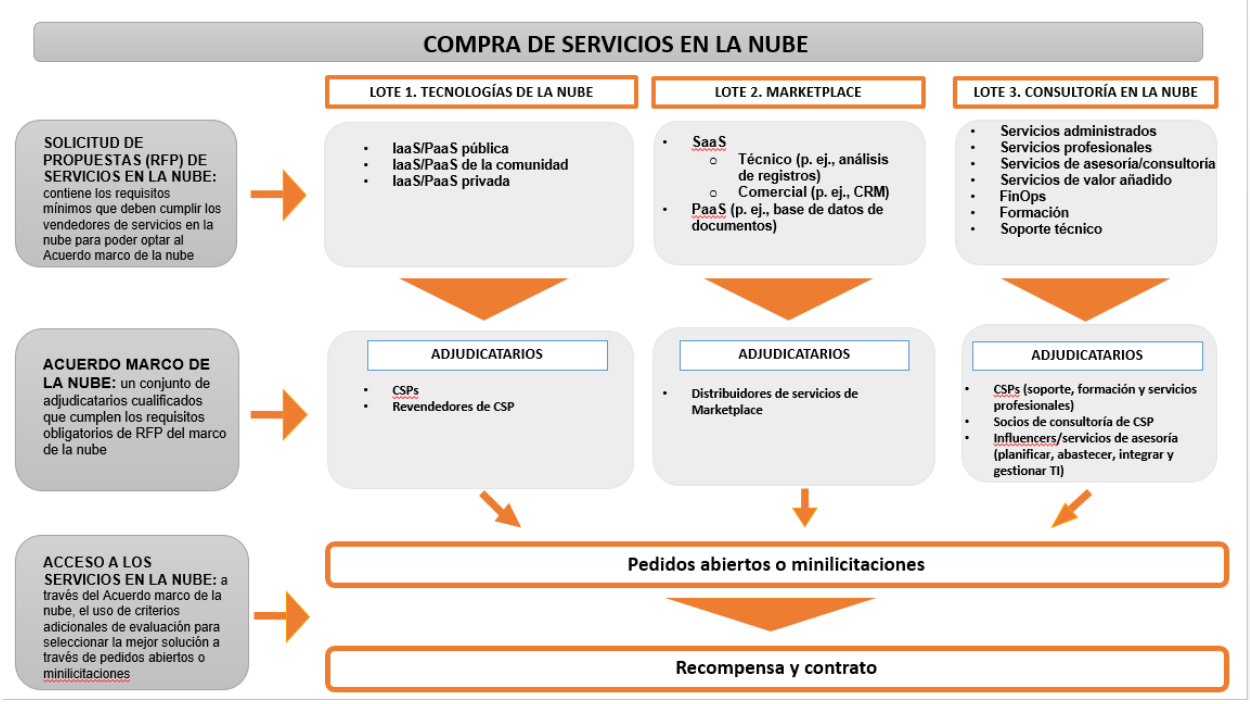

Figura 1: una licitación de servicios en la nube correcta se divide en tres lotes. Cada lote presenta categorías o "tipos de oferta" debajo del lote correspondiente, lo cual garantiza la adecuación técnica y contractual para satisfacer los requisitos del usuario final cuando se realiza la compra a partir del Acuerdo marco de nube.

Observe que:

- Cada lote consta de varias adjudicaciones.
- El LOTE 3 se puede adjudicar mediante otra licitación o posiblemente a través de un contrato existente para los servicios de consultoría.

Categorías del LOTE 1

Un acuerdo marco de nube satisfactorio solicita a los CISP que describan el modelo de nube que ofrecen dividido en categorías debajo de cada lote. Recomendamos que se utilice el estándar del sector de informática en la nube (las características esenciales de la nube según el National Institute of Standards and Technology [NIST, Instituto nacional de estándares y tecnología]) para las definiciones de nube **pública**, nube **comunitaria** y nube **privada**. La estructuración del acuerdo marco de nube de este modo permite a la agencia de compras y a los organismos públicos utilizar el marco para seleccionar una serie de modelos de nube que se ajusten a sus necesidades.

Remítase a la *Sección 2.1.3 Definiciones* para consultar la definición del NIST para cada modelo de nube del LOTE 1 (IaaS o PaaS pública, IaaS o PaaS comunitaria, y IaaS o PaaS privada).

Cómo competir: ¿pedidos abiertos o minilicitaciones?

Los criterios de cualificación de una licitación de servicios en la nube deben cubrir los elementos críticos y los estándares mínimos, y deben excluir estándares "deseables". La inclusión de estándares adicionales sobre la líneabase para los distribuidores aptos para el marco puede ocasionar que algunos no puedan concursar y que en última instancia se reduzcan las opciones para los compradores.

Después de la licitación y del establecimiento posterior de un Acuerdo marco de nube, los organismos del sector público que sean parte del marco pueden realizar un pedido o un "pedido abierto" de los servicios en la nube que precisen cuando sea necesario. Otorgar un contrato de entrega sucesiva bajo un acuerdo marco permite a los compradores ajustar los requisitos con especificaciones funcionales adicionales para un pedido abierto, a la vez que conservan los beneficios de dicho acuerdo marco.

Si se considera necesario, se puede convocar una minilicitación para identificar al mejor proveedor de una carga de trabajo o de un proyecto en particular. Mediante una minilicitación, el cliente convoca un nuevo concurso bajo el acuerdo marco invitando a todos los proveedores de un lote a dar respuesta a una serie de requisitos. El cliente invitará a todos los proveedores capacitados del lote a realizar una propuesta, de ahí la importancia de los requisitos mínimos para los adjudicatarios de una licitación de servicios en la nube, ya que garantiza que haya opciones de alto nivel bajo cada lote.

Tenga en cuenta que es importante que haya varios ***conjuntos de términos y condiciones diferentes*** *del contrato para cada uno de los lotes, como se muestra en la Figura 1 anterior. Un "planteamiento uniforme" de la contratación para todos los lotes causará problemas de viabilidad y compatibilidad técnica.*

2.0 Descripción general de la licitación de servicios en la nube

En esta sección se describe el modelo y el alcance de la licitación de servicios en la nube, incluyendo: objetivos estratégicos, participantes, definiciones, calendario y requisitos administrativos mínimos. Debemos destacar nuevamente que este manual se centra en el LOTE 1: TECNOLOGÍAS DE LA NUBE.

2.1 Configuración de una licitación de servicios en la nube

Recomendamos encarecidamente que las entidades del sector público describan con claridad sus requisitos y objetivos de alto nivel en la introducción de la licitación de servicios en la nube.

2.1.1 Introducción y objetivos estratégicos

En aras de la claridad en lo referente a objetivos estratégicos, se recomienda articular en la introducción de la licitación de los servicios en la nube: **(1)** los objetivos empresariales y los beneficios que espera obtener la organización con el uso de la nube; **(2)** la estructura del acuerdo marco: quién compra, quién opera, quién realiza el presupuesto, etc.; **(3)** una clara comprensión del modelo de responsabilidad compartida entre el sector público y los proveedores de nube, que es la base de una compra y un uso de la nube satisfactorios; y **(4)** el tipo de relación establecida entre los Cloud Service Providers (CISP, Proveedores de servicios de nube), los distribuidores de servicios de marketplace, los socios consultores, las agencias de adquisición o contratación gubernamentales y los usuarios finales gubernamentales. La articulación de estos cuatro puntos ayuda a las organizaciones a desarrollar la licitación que mejor satisface sus necesidades y garantiza asimismo que tanto los clientes como los proveedores describan con claridad los productos que se entregan.

La licitación de nube difiere de forma intencionada de las licitaciones de TI tradicionales. La tecnología basada en la nube no se limita a sustituir los métodos informáticos tradicionales por unos equiparables, ya que introduce una manera completamente novedosa de consumir la tecnología. Las licitaciones de servicios en la nube bien diseñadas pueden ayudar a las entidades del sector público a actuar rápidamente para beneficiarse de la nube.

Entre todos los aspectos de la compra de la nube que hemos citado como práctica recomendada, probablemente el mejor punto de partida sea una perfecta comprensión del modelo de responsabilidad compartida. El modelo de responsabilidad compartida[1] se emplea principalmente a la hora de analizar la seguridad y el cumplimiento de la normativa en la nube, pero esta delimitación de responsabilidades se aplica a todos los aspectos de las tecnologías de la nube. La licitación de servicios en la nube debe ser clara en cuanto a cuál debe ser la responsabilidad del CISP en el entorno de nube y cuál será la responsabilidad del cliente. Por ejemplo, un CISP proporciona capacidades para monitorizar recursos y aplicaciones que se ejecutan en la nube. ***Sin embargo***, es responsabilidad del cliente utilizar dichas capacidades proporcionadas por el CISP, dado que un CISP que opera a gran escala no está diseñado para hacerlo para millones de clientes.

Además, los clientes de la nube deben conocer cómo puede ayudar la red de socios del CISP al cliente a utilizar la nube y a gestionar sus responsabilidades. Por ejemplo, un Managed Service Provider (MSP, Proveedor de servicios administrados) puede ayudar a un cliente a configurar y utilizar las capacidades de

[1] Consulte la Sección 5 del Código de conducta de CISPE para proveedores de servicios de infraestructura de nube de Europa: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

monitorización proporcionadas por el CISP para satisfacer sus requisitos únicos de cumplimiento de la normativa y auditoría.

En resumen, las responsabilidades en el modelo de nube son las siguientes:

Un CISP proporciona la tecnología de nube.

Un cliente utiliza la tecnología de nube.

Las empresas consultoras (si es aplicable) ayudan al cliente a acceder a la tecnología de nube y a utilizarla.

*Las **"empresas consultoras"** son empresas de servicios administrados o profesionales y de consultoría que ayudan a los clientes a diseñar, crear, migrar y gestionar sus cargas de trabajo y aplicaciones en la nube. Entre estas empresas se incluyen integradores de sistemas, consultorías estratégicas, agencias, proveedores de servicios administrados y distribuidores de valor añadido.*

Considere la "compra" de servicios en la nube como algo similar a la compra en una ferretería. En una ferretería dispone de una amplia gama de materiales y herramientas para construir lo que necesite. Puede construir un armario o una piscina, o incluso toda una casa, si lo desea. Cuando compra los materiales y las herramientas, el personal de la ferretería puede ofrecerle orientación y conocimientos, pero no irá a su casa para hacer el trabajo por usted. De ese modo, dispone de una serie de opciones:

1. Comprar los materiales y las herramientas personalmente para construir algo usted mismo.
2. Comprar los materiales y las herramientas personalmente y contratar a alguien para construir u operar algo en su lugar.
3. Contratar a alguien para construir u operar algo en su lugar y pedirle que proporcione los materiales y las herramientas como parte de su oferta global.

Si una organización dispone internamente de las capacidades necesarias para crear y gestionar su entorno y soluciones de nube por sí misma, solo precisará acceder a las tecnologías y herramientas de nube estandarizadas del CISP (directamente de un CISP o a través de un distribuidor del CISP; consulte el LOTE 1). El software de SaaS y PaaS necesario debe estar disponible en el marketplace de la nube (LOTE 2). En el caso de que se necesite ayuda adicional con el asesoramiento, la migración, la implementación o la gestión, es cuando entra en acción la red de socios del CISP (LOTE 3).

Texto de licitación de ejemplo: introducción y objetivos estratégicos

La informática en la nube proporciona a las organizaciones del sector público acceso rápido a una amplia gama de recursos de TI de pago por uso y bajo coste. Las organizaciones pueden aprovisionarse de recursos del tipo y tamaño adecuados necesarios para impulsar sus grandes ideas y mantener en funcionamiento sus departamentos de TI, así como eliminar la necesidad de grandes inversiones en hardware o en contratos de licencias de software a largo plazo.

*La **<ORGANIZACIÓN>** necesita acceder a estos tipos de tecnologías de la nube y disponibles comercialmente para hacer frente a sus necesidades empresariales en un amplio espectro de organizaciones afiliadas.*

*El principal objetivo de esta licitción es adjudicar un **<ACUERDO MARCO>** paralelo no exclusivo con un máximo de **<x>** proveedores que representen diferentes tecnologías de nube y servicios relacionados con la nube.*

1. ***LOTE 1**. Cloud Service Providers (CISP, Proveedores de servicios en la nube) o distribuidores del CISP para la compra de tecnologías de la nube*

2. ***LOTE 2.** Proveedores de servicios de marketplace.*

3. ***LOTE 3.** Proveedores de servicios de consultoría que proporcionan conocimientos adicionales para migrar a estas ofertas del CISP y utilizarlas.*

*En cuanto al **LOTE 1**, las organizaciones que realizan la oferta (los CISP o los distribuidores del CISP) deben demostrar que sus ofertas cumplen los siguientes objetivos:*

- ***Agilidad:** poner los recursos de TI a disposición de los usuarios finales en cuestión de minutos en lugar de los plazos tradicionales de semanas o meses.*
- ***Innovación:** disponer de acceso instantáneo a la tecnología más reciente e innovadora del mercado.*
- ***Coste:*** cambiar los gastos de capital por gastos variables *(por ejemplo, de gastos de capital a gastos operativos). Solo se paga por la cantidad que se consume.*
- ***Elaboración del presupuesto:** presentar la información de facturación y uso tanto a nivel detallado como de resumen, mostrando los patrones de gasto a lo largo del tiempo, además de la previsión del gasto en el futuro.*
- ***Elasticidad:** obtener costes variables más bajos a partir de economías de escala más altas proporcionadas por la nube.*
- ***Capacidad:** eliminar las suposiciones en lo que se refiere a las necesidades de capacidad de infraestructura.*
- ***Eliminar la dependencia de los centros de datos:** centrarse en los ciudadanos en lugar de dedicarse a la ardua tarea de montar y apilar servidores y ponerlos en funcionamiento.*
- ***Seguridad:** formalizar el diseño de la cuenta con una mayor visibilidad y auditabilidad de los recursos y eliminar el coste derivado de la protección de las instalaciones y el hardware físico.*
- ***Responsabilidad compartida:** aliviar la carga operativa cuando el CISP opera, administra y controla los componentes desde el sistema operativo de alojamiento y la capa de virtualización hasta la seguridad física de las instalaciones en las que funciona el servicio.*
- ***Automatización:** integrar la automatización en la arquitectura de la nube para mejorar la capacidad de realizar un escalado seguro de manera más rápida y rentable.*
- ***Gestión de la nube:** (1) comenzar por un inventario completo de todos los activos de TI; (2) administrar todos estos activos de forma centralizada; y (3) crear alertas relativas al uso, la facturación, la seguridad, etc, todo ello con capacidad para realizar el seguimiento de los activos, la administración del inventario, la administración de los cambios, la administración y el análisis del registro, y la gobernanza integral de la visibilidad y la nube.*
- ***Control:** obtener visibilidad completa sobre cómo se consumen los servicios de TI y dónde se pueden ajustar en cuanto a seguridad, fiabilidad, rendimiento y costes.*
- ***Carácter reversible:** herramientas y servicios de portabilidad para ayudar a migrar a y desde la infraestructura del CISP, reduciendo de este modo la dependencia del proveedor, así como a respetar los códigos de conducta del sector.*

- ***Protección de datos:*** *capacidad para demostrar el cumplimiento del Reglamento general de protección de datos (*RGPD*) mediante un código de conducta del sector exclusivo para los servicios de infraestructura de nube: el Código de conducta de protección de datos de CISPE.*
- ***Transparencia:*** *los clientes deben tener la posibilidad de conocer la ubicación de las infraestructuras utilizadas para procesar y almacenar sus datos (el área de la ciudad).*

2.1.2 Calendario de respuesta a la licitación

Se recomienda proporcionar a los licitantes un calendario de la actividad de licitación anticipada al crear el acuerdo marco de nube, así como la licitación de servicios en la nube asociada. Cuanto mayor sea la interacción con el sector, tanto mejor, ya que contribuirá a garantizar que todas las partes comprenden perfectamente los requisitos de la licitación y que en efecto todos los servicios de los proveedores se ajustan al modelo de servicios en la nube.

Tenga en cuenta que el calendario de la licitación está sujeto a las leyes y obligaciones legales locales, y que la lista que se proporciona a continuación se ha concebido como una guía de buenas prácticas en lugar de una lista obligatoria de actividades y plazos.

Texto de la licitación de ejemplo: calendario de respuesta

Consulte a continuación el calendario de la licitación de servicios en la nube:

Calendario de la licitación de servicios en la nube
• *Publicación de la solicitud de información (consulta la mercardo):* • *Respuesta a la consulta al mercado:* • *Publicación del borrador de solicitud de propuesta (licitación):* • *Fecha límite de respuesta al borrador de licitación:* • *Fase de consulta del sector: <plazos>* • *Publicación de la licitación de precalificación:* • *Respuesta a la licitación de precalificación:* • *Publicación de la licitación:* • *Fecha límite de las preguntas de la ronda 1:* • *Respuestas de la ronda 1:* • *Fecha límite de las preguntas de la ronda 2:* • *Respuestas de la ronda 2:* • *Fecha límite de respuesta a la licitación:* • *Periodo de clarificación de la propuesta:* • *Periodo de negociación:* • *Fecha de intento de adjudicación:* • *Adjudicación del contrato:* • *Duración del contrato (opciones de ampliación):*

Tenga en cuenta que el calendario de la licitación está sujeto a las leyes y obligaciones legales locales, y que la lista que se proporciona a continuación se ha concebido como una guía de buenas prácticas en lugar de una lista obligatoria de actividades y plazos.

2.1.3 Definiciones

Una licitación de servicios en la nube debe incluir una lista detallada de definiciones. Esta lista incluye las funciones del proveedor (por ejemplo, proveedor de nube, distribuidor de nube, socio proveedor), conceptos tecnológicos generales (computación, almacenamiento, IaaS o PaaS, SaaS) y otras partes fundamentales del acuerdo. A continuación, se muestra una lista de definiciones de ejemplo:

Texto de licitación de ejemplo: definiciones

Las siguientes definiciones son definiciones de informática en la nube del National Institute of Standards and Technology (NIST).[2]

- ***Infraestructura como servicio (IaaS).*** *Se proporciona al consumidor la capacidad de aprovisionar el procesamiento, el almacenamiento, las redes y otros recursos informáticos fundamentales en los que puede implementar y ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones. El consumidor no administra ni controla la infraestructura de nube subyacente, pero tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones implementadas, y posiblemente un control limitado de determinados componentes de red (por ejemplo, firewalls del anfitrión).*

- ***Plataforma como servicio (PaaS).*** *Se proporciona al consumidor la capacidad de realizar implementaciones sobre la infraestructura de nube que ha creado o las aplicaciones adquiridas creadas empleando lenguajes de programación, bibliotecas, servicios y herramientas admitidas por el proveedor. El consumidor no administra ni controla la infraestructura de nube subyacente, que incluye la red, los servidores, los sistemas operativos o el almacenamiento, pero tiene el control de las aplicaciones implementadas y posiblemente de los ajustes de configuración del entorno de alojamiento de las aplicaciones.*

- ***Software como servicio (SaaS).*** *Se proporciona al consumidor la capacidad de utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura de nube. Se puede acceder a estas aplicaciones desde diversos dispositivos del cliente, ya sea mediante una interfaz de cliente ligero, un navegador web (por ejemplo, correo electrónico basado en web) o una interfaz de programa. El consumidor no administra ni controla la infraestructura de nube subyacente, que incluye la red, los servidores, los sistemas operativos, el almacenamiento o incluso funcionalidades individuales de las aplicaciones, con la posible excepción de determinados ajustes de configuración de aplicaciones específicos del usuario.*

- ***Nube pública.*** *Se aprovisiona la infraestructura de nube de modo que pueda usarla abiertamente el público general. Puede ser propiedad de una organización empresarial, académica o gubernamental, o de cualquier combinación de estas, encargándose de su administración y funcionamiento. Se encuentra ubicada en las instalaciones del proveedor de nube.*

- ***Nube comunitaria.*** *Se aprovisiona la infraestructura de nube para uso exclusivo de una comunidad específica de consumidores de organizaciones con inquietudes comunes (por ejemplo, consideraciones relativas al objetivo, los requisitos de seguridad, la política y el cumplimiento de la normativa). Puede ser propiedad de una o varias organizaciones de la comunidad, de una tercera parte o de cualquier combinación de estas, encargándose de su administración y funcionamiento, y puede estar ubicada en las instalaciones o fuera de ellas.*

- ***Nube híbrida.*** *La infraestructura de nube está formada por dos o más infraestructuras de nube distintas (privada, pública o comunitaria) que mantienen sus entidades únicas pero que están vinculadas por una tecnología estandarizada o propietaria que hace posible la portabilidad de los datos y las aplicaciones (por ejemplo, el desbordamiento de nube para equilibrar la carga entre nubes).*

[2] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

- ***Nube privada.*** *Se aprovisiona la infraestructura de nube para uso exclusivo de una sola organización formada por múltiples consumidores (por ejemplo, las unidades empresariales). Puede ser propiedad de la organización, de una tercera parte o de cualquier combinación de estas, encargándose de su administración y funcionamiento, y puede estar ubicada en las instalaciones o fuera de ellas.*

2.1.4 Descripción detallada del modelo de compra y competición dentro del acuerdo marco

Como se ha señalado anteriormente, las organizaciones del sector público deben identificar el modelo que determine cómo debe funcionar el acuerdo marco como mecanismo de compra de tecnologías de la nube y de los servicios de implementación y administración relacionados. Esto se debe exponer con claridad en la licitación de servicios en la nube de modo que los proveedores de tecnología, las organizaciones de servicios de consultoría relacionadas, los distribuidores de marketplace y las entidades compradoras conozcan sus respectivas funciones.

En cuanto al alcance del acuerdo marco, y los pedidos abiertos o las minilicitaciones subsiguientes, las organizaciones deben tener en cuenta lo siguiente:

- Quién será responsable de la integración y los servicios administrados relacionados con el uso de tecnologías de la nube bajo el contrato.
- ¿Se exige algún requisito para que un distribuidor o un socio de un CISP proporcione servicios de valor añadido además de mantener una relación contractual con el CISP, prestar servicios de facturación consolidados, y acceso directo y a los datos de uso y facturación asociados al uso de los servicios del proveedor de nube?
- ¿Se exige algún requisito al distribuidor de valor añadido de servicios globales, al integrador de sistemas, al proveedor de servicios administrados o para cualquier tipo de prestación laboral de TI?

Es importante tener en cuenta que un CISP no es un integrador de sistemas (SI) ni un proveedor de servicios administrados (MSP). Muchos clientes del sector público requerirán un CISP para su IaaS o PaaS y subcontratarán los servicios de consultoría y el trabajo práctico de planificación, migración y administración a un integrador de sistemas o un proveedor de servicios administrados. En la **Figura 2** que se muestra a continuación se representa la delimitación de las funciones y las responsabilidades en un modelo de servicios en la nube.

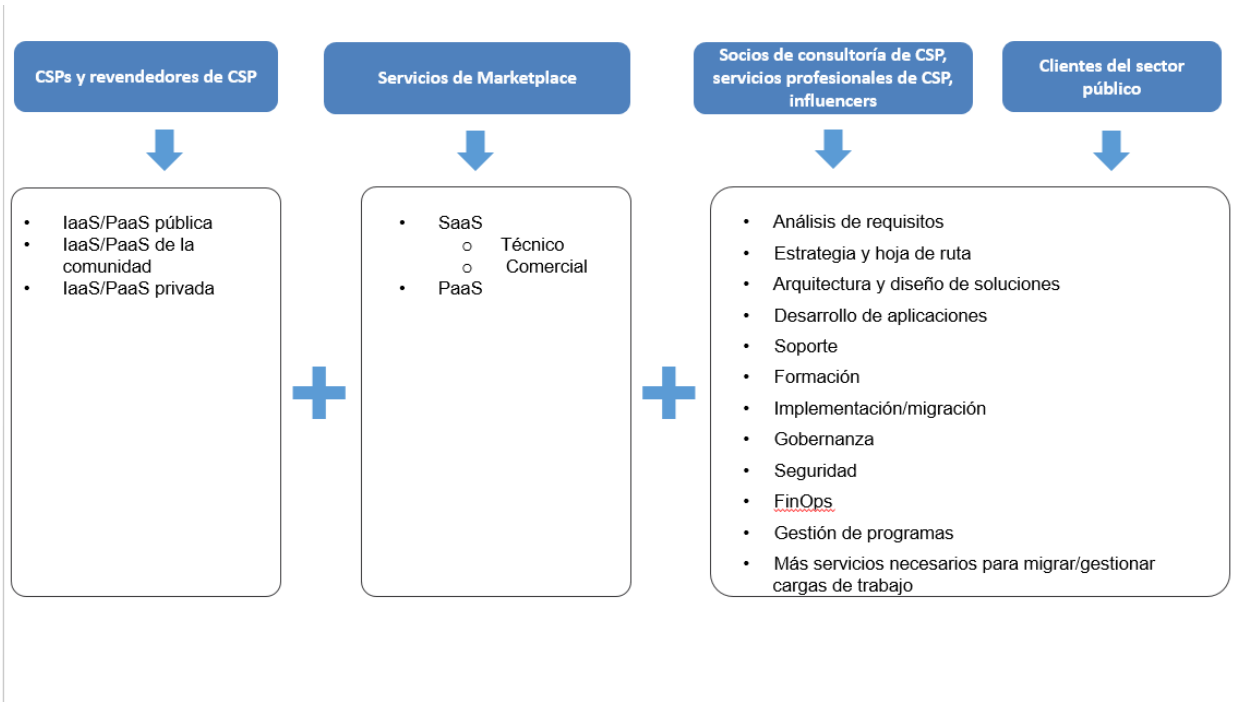

Figura 2: una licitación de servicios en la nube debe proporcionar a los usuarios finales un listado con todos los servicios en la nube que necesitan. Los clientes del sector público precisarán un CISP para las tecnologías de la nube, un marketplace para los productos de PaaS y SaaS si es necesario, y seguidamente podrán determinar el alcance de la función que desean asumir en la prestación de servicios en la nube y hasta qué punto desean subcontratar una empresa consultora, un integrador de sistemas, un proveedor de servicios administrados, etc.

El siguiente texto de ejemplo plasma las funciones y las responsabilidades, como se muestra en la Figura 2 anterior. Un acuerdo marco de nube, y la licitación de servicios en la nube asociada, debe asegurarse de que a los compradores se les ofrece la capacidad de evaluar adecuadamente las ofertas de cada proveedor, lo que les permite elegir y seleccionar entre los servicios necesarios para la carga de trabajo o el proyecto. Esto se consigue separando los servicios en lotes, como ya se ha comentado, y exponiendo claramente cómo se realizan los pedidos abiertos y las minilicitaciones bajo el acuerdo marco.

Texto de la licitación de ejemplo: modelo de compra

*Este contrato se utilizará como medio de compra **Marco**. Este acuerdo marco de nube incluirá múltiples **lotes**, según lo defina la <**ORGANIZACIÓN**>, de tecnologías de nube y servicios o productos de marketplace relacionados; servicios de consultoría; servicios profesionales, integración de sistemas, servicios administrados o servicios profesionales de migración; y formación y soporte, según lo defina la <**ORGANIZACIÓN**>, que utilizarán varios compradores cualificados afiliados a la <**ORGANIZACIÓN**>. De este modo se simplificará el proceso de adquisición al tiempo que se optimizan las economías de escala.*

Una vez establecido, este acuerdo marco permitirá a la organización comprar las tecnologías de nube y los servicios relacionados con la nube específicos que desee cuando los necesite, en lugar de realizar la compra mediante adquisiciones por separado. Mediante este enfoque se reducen los requisitos administrativos y se minimiza la complejidad de la adquisición y la duración del ciclo.

*El acuerdo marco tendrá una duración máxima de **<X>** años que incluye las posibles renovaciones. La duración máxima de un contrato marco de pedido abierto es de **<x>** meses normalmente; este se puede ampliar en **<x>** meses y,*

*posteriormente, en **<x>** meses adicionales con las correspondientes aprobaciones internas de ampliación de contrato si fuera necesario. Esto se especificará en cada **Pedido abierto** específico.*

*El MARCO se divide en **3 (tres) lotes**.*

1. ***LOTE 1: TECNOLOGÍAS DE LA NUBE:** gama completa de tecnologías del proveedor de nube (directamente del CISP, del distribuidor o de un distribuidor con servicio o soporte de valor añadido):*
    i. ***Servicios de IaaS y PaaS:** listado de tecnologías de la nube; por ejemplo, computación, almacenamiento, redes, base de datos, análisis, servicios de aplicaciones, implementación, administración, desarrollador, Internet de las cosas (IoT), etc. Incluye soluciones tecnológicas empaquetadas para la nube, como DR/COOP, Archive, Big Data & Analytics, DevOps, etc.*
2. ***LOTE 2: MARKETPLACE:** gama completa de productos y servicios de PaaS y SaaS, como contabilidad, CRM, diseño, recursos humanos, sistema de información geográfica (GIS) y mapeo, HPC, inteligencia empresarial (BI), gestión de contenido, análisis de registro, etc.*
3. ***LOTE 3: CONSULTORÍA DE NUBE:** gama completa de servicios de consultoría (servicios administrados, servicios profesionales, servicios de asesoramiento y consultoría, servicios de valor añadido, operaciones financieras, soporte técnico) relacionados con la migración a la nube y su uso. Estos servicios pueden incluir: planificación, diseño, migración, administración, soporte, control de calidad, seguridad, formación, etc.*

Los proveedores pueden presentar sus ofertas en varios lotes.

Los proveedores pueden presentar sus ofertas y los precios correspondientes en el formato que elijan.

PRESENTACIÓN A CONCURSO DENTRO DEL MARCO Y ADJUDICACIÓN DE CONTRATOS

PEDIDOS ABIERTOS

Los organismos del sector público que forman parte del acuerdo marco pueden realizar un pedido o un "pedido abierto" de los servicios que precisen cuando sea necesario. Otorgar un contrato de entrega sucesiva bajo un acuerdo marco permite a los compradores ajustar los requisitos con especificaciones funcionales adicionales para un pedido abierto, a la vez que conservan los beneficios que se ofrecen bajo dicho acuerdo marco.

Los contratos adjudicados mediante un acuerdo marco podrán demostrar un registro de auditoría claro en relación con los requisitos utilizados para seleccionar al proveedor dentro de cada lote. Los compradores finales guardarán un registro de comunicaciones con los proveedores, que incluirá todas las actividades iniciales de participación en el mercado, las preguntas aclaratorias, los correos electrónicos y las conversaciones cara a cara mantenidas.

1. REDACCIÓN DE LOS REQUISITOS DEL PEDIDO ABIERTO Y SOLICITUD DE APROBACIÓN INTERNA PARA REALIZAR LA COMPRA

Todos los compradores finales aptos para utilizar el acuerdo marco crearán equipos conjuntos de usuarios finales empresariales, especialistas en compras y expertos técnicos para elaborar una lista de requisitos indispensables y deseables. Estos requisitos servirán para decidir los lotes que son aplicables, así como el vendedor que está más cualificado para cumplir los requisitos. A la hora de redactar el borrador de los requisitos, los compradores deben tener en cuenta lo siguiente:

- *los fondos disponibles para utilizar el servicio*
- *los requisitos técnicos y de adquisiciones del proyecto*

- *los criterios en los que se basará la selección*

2. BÚSQUEDA DE SERVICIOS

Con arreglo al acuerdo marco, los compradores utilizarán un catálogo marco online (un portal donde figurarán los adjudicatarios cualificados del acuerdo marco y sus servicios) para buscar productos o servicios que cubran las necesidades que han identificado. Seleccionarán los lotes adecuados y seguidamente buscarán los servicios.

3. REVISIÓN Y EVALUACIÓN DE LOS SERVICIOS

Con arreglo al acuerdo marco, los compradores revisarán las descripciones de los servicios para buscar aquellos que cubran mejor sus necesidades teniendo en cuenta tanto los requisitos como el presupuesto. Cada descripción de servicio incluirá un:

- *Documento de definición de servicio o enlaces a definiciones de servicio*
- *Documento de términos y condiciones*
- *Documento de precios (se aceptarán enlaces a los precios públicos siempre que haya una lista de precios o un documento de precios completo disponible previa solicitud)*

El precio corresponderá al coste de la configuración más común del servicio. Sin embargo, el precio normalmente se basa en el volumen, por lo que los compradores deben consultar el documento de precios o los precios públicos del proveedor y utilizar las herramientas de cálculo de precios para calcular el precio real de lo que se compra, así como el valor total que se ofrece al comprador (por ejemplo, servicios de optimización y la reducción de costes resultante).

Con arreglo al acuerdo marco, los compradores pueden hablar con los proveedores para pedirles que expliquen la descripción del servicio, las condiciones, los precios, o los documentos o el modelo de definición de servicio. Se guardará un registro de todas las conversaciones mantenidas con los proveedores.

4. SELECCIÓN DE UN SERVICIO Y ADJUDICACIÓN DE UN CONTRATO

Único proveedor

Si solo uno de los proveedores cumple los requisitos, se le podrá adjudicar el contrato.

Varios proveedores

Si hay varios servicios en una preselección, el comprador elegirá el servicio con la oferta económicamente más ventajosa (MEAT, Most Economically Advantageous Tender). Consulte en la siguiente tabla los criterios de la evaluación basada en MEAT. Los compradores pueden decidir las características detalladas que desean usar y cómo ponderarlas.

Tenga en cuenta que el comprador puede precisar:

- *consultar las combinaciones de diferentes proveedores*
- *obtener información específica sobre el volumen o los descuentos empresariales, y sobre los servicios de optimización de costes del proveedor*

La evaluación de los proveedores debe ser siempre imparcial y transparente. La selección se basará en la opción más adecuada, y los proveedores o los servicios no se excluirán sin consultar los requisitos del proyecto.

Tabla 2: evaluación basada en MEAT

Criterios de adjudicación

Coste de la vida completo: *relación coste-eficacia, precio y costes de funcionamiento*
Mérito técnico y ajuste funcional: *cobertura, capacidad de red y rendimiento especificados en los niveles de servicio pertinentes*
Gestión de servicios posventa: *servicio de asistencia, documentación, función de administración de cuentas y garantía de suministro de una gama de servicios*
Características no funcionales

MINILICITACIONES

Si se considera necesario, se puede convocar una minilicitación para identificar al mejor proveedor de una carga de trabajo o de un proyecto en particular. Mediante una minilicitación, el cliente convoca un nuevo concurso bajo el acuerdo marco invitando a todos los proveedores de un lote a dar respuesta a una serie de requisitos. El cliente invitará a todos los proveedores capacitados del lote a realizar una oferta. Consulte información de comparación adicional en las secciones siguientes sobre aspectos técnicos, seguridad y precios o valor.

CONTRATO

Tanto el comprador como el vendedor firmarán una copia del contrato para que se pueda utilizar el servicio. La duración máxima de un contrato marco es de ***<x>*** *meses normalmente; este se puede ampliar en* ***<x>*** *meses y, posteriormente, en* ***<x>*** *meses adicionales, con las correspondientes aprobaciones internas de ampliación de contrato si fuera necesario.*

Todas las partes interesadas (el comprador y el proveedor) deben firmar una copia del contrato para que se pueda utilizar el servicio.

2.1.5 Requisitos mínimos del licitante: administrativos

Una redacción clara y sencilla para establecer los criterios de cualificación del acuerdo marco contribuirán a garantizar que no haya ninguna propuesta de centros de datos tradicionales o proveedores de hardware que empaqueten una solución tradicional como una "nube". Los participantes en la licitación deben demostrar que cumplen los requisitos administrativos mínimos del licitante.

Nuevamente, debe tener en cuenta que este documento se centra en el LOTE 1: TECNOLOGÍAS DE LA NUBE. Sin embargo, hemos añadido información adicional sobre el LOTE 2: MARKETPLACE y el LOTE 3: CONSULTORÍA DE NUBE cuando contribuye a ofrecer un contexto global en cuanto a los requisitos y el alcance de la licitación. Por ejemplo, es importante incluir los criterios mínimos de cualificación del distribuidor el CISP, un MSP, el SI o la empresa consultora, entre otros. Esto contribuye a garantizar que (1) están afiliados directamente al CISP como distribuidor o socio de canal, (2) que están certificados por un CISP para revender el acceso directo a las ofertas del CISP a entidades terceras y (3) que cuentan con certificaciones de estos CISP que acreditan sus capacidades y conocimientos

Texto de licitación de ejemplo: requisitos mínimos del licitante: administrativos

Este acuerdo marco adjudicará contratos a varios proveedores en las siguientes categorías. Los proveedores deben ser un CISP comercial, un distribuidor externo de un CISP, un distribuidor de servicios de marketplace o un proveedor de servicios para emplear un CISP (por ejemplo, consultoría, servicios de migración, servicios administrados, operaciones financieras, etc.). Identifique los roles para los que se ofrece:

LOTE 1

____ - Proveedor directo (CISP) de servicio de nube pública (IaaS Y PaaS)

____ - Proveedor directo (CISP) de servicio de nube comunitaria (IaaS Y PaaS)

____ - Proveedor directo (CISP) de servicio de nube privada (IaaS Y PaaS)

____ - Distribuidor externo del CISP (capacidad para proporcionar acceso directo a las ofertas de nube online de un CISP).

- *Identifique la oferta del CISP para cuyo servicio puede revender el acceso directo: _____*
- *Proporcione una carta del CISP en la que se declare que es usted un revendedor autorizado de sus ofertas: _____*

LOTE 2

____ - Proveedor directo de servicios de marketplace que se ejecutan en un CISP (PaaS y/o SaaS)

____ - Distribuidor de servicios de marketplace que se ejecutan en un CISP (PaaS o SaaS)

LOTE 3

____ - CISP que proporciona servicios profesionales

____ - Proveedor de soporte técnico del CISP

____- Socio del CISP que proporciona servicios que se utilizan u operan en un CISP

____- Persona con influencia o asesor que proporciona servicios que se utilizan u operan en un CISP

Identifique el tipo de oferta:

- *Servicios administrados de cargas de trabajo en un CISP (S/N): _____*
  - *Identifique las especialidades si es aplicable: _____*
- *Servicios profesionales: (S/N): _____*
- *Consultoría: formación (S/N): _____*
- *Consultoría: estrategia (S/N): _____*
- *Consultoría: migración (S/N): _____*
- *Consultoría: gobernanza de la nube (S/N): _____*
- *Consultoría: operaciones financieras (S/N): _____*
- *Consultoría: otro (identifíquelo): _____*

Identifique el CISP o los CISP para los que proporciona servicios: _____
Aporte una carta del CISP que confirme su nombramiento como socio bajo el modelo del CISP: _____

LOTE 1 REQUISITOS ADMINISTRATIVOS MÍNIMOS

Proveedores de servicios en la nube (CISP)
Para la cualificación del CISP, este debe demostrar que cumple los siguientes requisitos.

Criterios de cualificación propuestos para el CISP	*Motivo*
Detalles organizativos; por ejemplo: Nombre, Forma jurídica, Número de registro o DUNS, Número de identificación fiscal, etc.	

Tamaño de la empresa, situación económica y financiera[3]	*El cliente puede determinar si el CISP podrá cumplir el contrato.*
Motivos de exclusión; p. ej., actividades delictivas o fraudulentas, etc.	
Casos prácticos y referencias del cliente (especifique el número o el tipo de requisito)	*El cliente puede medir la experiencia del CISP para ofrecer los servicios solicitados.*
Responsabilidades sociales corporativas	*Deben ser versiones de acceso público proporcionadas por el CISP.*
Compromisos y prácticas de sostenibilidad disponibles públicamente.	*El cliente puede ver si un CISP está comprometido con dirigir su negocio de la forma más respetuosa con el medio ambiente.*
El CISP debe demostrar una trayectoria probada en innovación y lanzamiento de nuevos servicios y funciones útiles a lo largo de los últimos 5 años, especialmente en el ámbito de PAAS, aprendizaje automático y análisis, Big Data, servicios administrados y en las funciones de optimización de uso de la nube. Se pueden utilizar los registros de cambios o las fuentes de actualización de acceso público para demostrar este punto.	*Demuestra que el CISP trabaja para poner nuevos productos a disposición de los clientes con rapidez, y que a continuación itera rápidamente y mejora los productos. Ayuda a los clientes a mantener una infraestructura de TI de vanguardia sin tener que realizar inversiones de recapitalización.*

Relación del distribuidor o el socio con el CISP

*La **<ORGANIZACIÓN>** requiere que el contratista principal esté afiliado directamente al CISP como distribuidor o socio de canal, que esté certificado por el CISP para revender el acceso directo a ofertas del CISP a entidades terceras, y que cuente con certificaciones de dicho CISP que acrediten sus capacidades y conocimientos. Esto hace que no sea necesario que la **<ORGANIZACIÓN>** revise los Términos y servicios asociados a una capa adicional de la subcontratación entre el contratista principal del **Acuerdo marco** y el CISP. Este requisito reduce asimismo la complejidad que generan las capas adicionales de distribuidores cuando (1) la **<ORGANIZACIÓN>** actúa con la diligencia debida para garantizar una clara asignación de responsabilidades con respecto a los servicios que se van a proporcionar, y (2) la **<ORGANIZACIÓN>** ejecuta las actividades diarias que implican el consumo de servicios en la nube.*

2.2 Técnicos

Una licitación de servicios en la nube debe elevar el nivel de exigencia de los CISP solicitándoles que proporcionen las tecnologías de nube estandarizadas necesarias para que el cliente pueda crear su solución personalizada. Como se ha mencionado anteriormente, esta diferencia entre lo que está estandarizado y lo que está personalizado es muy importante cuando se plantea una licitación de servicios en la nube. Los CISP ofrecen servicios estandarizados a millones de clientes. Por ello, las personalizaciones de una licitación de servicios en la nube se centran en soluciones y resultados de nivel superior, frente a los métodos, la infraestructura o el hardware subyacentes empleados para ofrecer servicios en la nube que se utilizan para obtener resultados de solución.

[3] Tenga en cuenta que la licitación de servicios en la nube se centra en la información empresarial de alto nivel, en lugar del número de empleados de la empresa y la estructura de equipos de los empleados internos. Con la tecnología basada en la nube no existe ninguna correlación entre la garantía del rendimiento del servicio y el número de empleados. En su lugar, las licitaciones de nube se centran en el tamaño global de la empresa para satisfacer los requisitos (la escala adecuada) y en una experiencia y una eficiencia probadas.

2.2.1 Requisitos mínimos

Las adquisiciones de TI tradicionales suelen basarse en requisitos empresariales desarrollados mediante una serie de sesiones de trabajo que documentan cómo se está dirigiendo la actividad de negocio de la organización en ese momento. La obtención de estos requisitos de manera exacta es un proceso complejo en el mejor de los casos. Si se realizan correctamente, estas sesiones de requisitos documentan el proceso empresarial histórico que en sí podría estar anticuado y ser ineficaz. Si dichos requisitos pasan a formar parte de una licitación que será reproducida por el CISP, la única solución podría ser una solución personalizada. Este modelo es incompatible con las adquisiciones de nube.

Las organizaciones del sector público deben conocer sus objetivos empresariales y necesidades de rendimiento, pero estos no deben ser prescriptivos en una licitación en la que se dicte el diseño y la funcionalidad del sistema. En su lugar, la organización debe comprar la solución que mejor se adapte a su negocio. En vez de evaluar propuestas sobre cientos o incluso miles de requisitos prescriptivos que podrían no dar lugar a servicios satisfactorios, las organizaciones deben incluir criterios de evaluación basados en la capacidad de la tecnología y los servicios asociados de alcanzar o mejorar los objetivos empresariales, si cubren sus necesidades de rendimiento, así como de ajustar las reglas de negocio mediante la configuración.

Las licitaciones de nube deben formular las preguntas adecuadas para obtener las mejores soluciones. Dado que en un modelo de nube no se compran los activos físicos, se deduce que muchos de los requisitos de adquisición de los centros de datos tradicionales no son aplicables. ***El reciclado de las preguntas de los centros de datos conducirá inevitablemente a las respuestas de los centros de datos****. Esto ocasiona que los CISP no puedan presentar una oferta o que se generen contratos con un diseño deficiente que impidan a los clientes del sector público obtener todas las capacidades y los beneficios de la nube.*

La licitación de servicios en la nube se centra en los requisitos clave que se exigen de un CISP y de los servicios en la nube, y se asegura de que los proveedores que optan al LOTE 1 cumplen unos altos niveles de calidad. También se debe evitar que los requisitos sean demasiado prescriptivos para no limitar el acceso del sector público a una amplia variedad de CISP cualificados.

Texto de licitación de ejemplo: capacidades del proveedor de nube

Consulte también los requisitos administrativos mínimos del CISP para el LOTE 1

Criterios de cualificación propuestos para el CISP	*Motivo*
Infraestructura	
La infraestructura del CISP debe ofrecer al menos 2 clústeres de centros de datos. Cada clúster debe estar formado por al menos 2 centros de datos conectados mediante un enlace de baja latencia que permita realizar implementaciones en modo activo/activo de alta disponibilidad y de escenarios DR-BC. Los centros de datos que conforman cada clúster deben estar aislados físicamente y ser independientes en caso de fallo entre sí.	*El CISP debe poder ofrecer una infraestructura adecuada para crear aplicaciones de alta disponibilidad en las que se pueden evitar puntos únicos de error.*

El CISP debe proporcionar regiones aisladas de forma lógica y geográfica. El CISP no debe replicar los datos del cliente fuera de estas regiones.	*Los requisitos de residencia de datos exigen que el cliente tenga pleno control del lugar donde se ubican sus datos.*
El CISP debe tener la capacidad de ofrecer una conectividad directa, dedicada y privada entre los centros de datos del CISP.	*La conectividad privada es un requisito fundamental para poder crear una infraestructura híbrida y segura.*
El CISP debe proporcionar los mecanismos suficientes, que incluyen el cifrado de los datos en tránsito.	*El cliente puede exigir que haya una capacidad por la que ningún dato pueda transitar sin cifrar.*
Certificaciones mínimas del CISP	
El CISP debe contar con la certificación ISO 27001	*La realización de una auditoría y la obtención de una certificación y una acreditación de terceros garantiza que los clientes puedan realizar análisis comparativos de los servicios (y en concreto de la plataforma) en cuanto a calidad, seguridad y fiabilidad. Es imprescindible que se cumplan un mínimo de certificaciones.*
El CISP debe ofrecer servicios certificados del RGPD bajo el Código de conducta de protección de datos de CISPE para que el cliente pueda crear aplicaciones compatibles con el RGPD.	*El cliente debe poder crear o ejecutar aplicaciones compatibles con el RGPD, por lo que la oferta de servicios y herramientas compatibles con el RGPD debe ser un requisito previo.*
El CISP debe facilitar informes auditados de terceros, como los informes SOC 1 y 2 (que cubren las ubicaciones y los servicios que utiliza la Comisión Europea) que permitan conocer sus controles y procedimientos.	*El CISP debe ser transparente en lo referente al funcionamiento y la administración de la aplicación. Los informes SOC son un medio para garantizar la confianza y la transparencia.*
Características del servicio	
La infraestructura del CISP debe estar accesible a través de las interfaces programáticas (las API) y la consola de administración basada en Web.	*El acceso de autoservicio y las interfaces programáticas son un estándar necesario de los proveedores del CISP para dejar de mediar tanto como sea posible en el acceso de usuario y del propio proveedor.*
El CISP debe ofrecer un conjunto de servicios de base que incluyan: almacenamiento de objetos, base de datos relacional administrada, base de datos no relacional administrada, balanceadores de carga administrados, monitorización y escalado automático integrado.	*Una simple oferta de máquinas virtuales no es suficiente para que un proveedor pueda cualificarse como proveedor de nube. Los proveedores de nube deben ofrecer un conjunto de servicios PAAS e IAAS para acelerar y mejorar las aplicaciones del cliente.*
El CISP debe permitir al cliente cambiar libremente el uso y la configuración de sus servicios o mover los datos dentro y fuera del CISP (oferta de autoservicio).	*El acceso de autoservicio a los servicios y los datos es un requisito estricto que permite al consumidor ser completamente independiente.*
El CISP debe permitir una facturación de "pago según el uso" de sus servicios.	*El pago según el uso permite al cliente optimizar los costes de sus cargas de trabajo, minimizar los riesgos y utilizar el CISP para aplicaciones y pruebas de concepto (PdC) de corta duración.*
Seguridad de los datos y el sistema	
El CISP debe permitir al cliente mantener el control absoluto de sus datos, dar al cliente libertar para elegir dónde se almacenan los datos (área urbana de la ciudad) y garantizar	*El cliente debe tener el control sobre dónde se almacenan los datos, cómo administrar el acceso al contenido y disponer de acceso de usuario a los servicios y los recursos.*

que no se trasladará ninguno de los datos del cliente a menos que dicho traslado lo inicie el propio cliente.	
Las características del CISP deben proporcionar al cliente un control absoluto de sus políticas de seguridad, que incluyen la confidencialidad, la integridad y la disponibilidad de los datos y el sistema del cliente.	*El cliente debe estar habilitado para definir e implementar sus estándares de seguridad en sus cargas de trabajo. Confiar en que el proveedor "hará lo correcto" con los datos del cliente no es suficiente.*
Control de costes	
El CISP debe contar con mecanismos y herramientas que permitan al cliente monitorizar el gasto a lo largo del tiempo. Las herramientas deben hacer posible la segmentación básica de los costes según la carga de trabajo, el servicio y la cuenta.	
El CISP debe ofrecer herramientas para alertar al cliente siempre que se supere el umbral de coste.	
El CISP debe entregar facturas detalladas al cliente. Debe existir la posibilidad de estructurar la factura para dividir los costes por carga de trabajo, entorno y cuenta.	

Los CISP también deben responder las preguntas sobres requisitos técnicos que se muestran a continuación.

SOLUCIONES

El CISP debe demostrar que puede proporcionar plantillas prediseñadas y soluciones de software que, o bien estén alojadas en el CISP o integradas en él, para las siguientes soluciones:

- *Almacenamiento*
- *DevOps*
- *Seguridad o conformidad*
- *Big Data o análisis*
- *Aplicaciones empresariales*
- Telecomunicaciones y redes
- *Geoespacial*
- *IoT*
- *[Otro]*

Proporcione información general sobre cómo se ha utilizado el CISP para las cargas de trabajo siguientes:

- *Recuperación ante desastres*
- *Desarrollo y prueba*
- *Archivado*
- *Copia de seguridad y recuperación*
- *Big Data*
- *Computación de alto rendimiento (HPC)*
- *Internet de las cosas (IoT)*
- *Sitios web*
- *Computación sin servidor*
- *DevOps*
- *Entrega de contenido*
- *[Otro]*

2.2.2 Comparación entre proveedores

Además de los requisitos mínimos de una licitación de servicios en la nube, es importante proporcionar criterios con los que se puedan comparar las tecnologías del CISP durante una evaluación competitiva.

Las licitaciones de servicios en la nube deben preguntar por aquellas capacidades de nube que necesita una organización, con el conocimiento de que el cliente posee el uso dichas capacidades para crear su solución. Las funcionalidades que vayan más allá de los estándares que puede proporcionar un CISP (como las soluciones pre generadas a través del CISP o las funciones de automatización) se pueden utilizar para hacer un análisis más significativo de las "opciones de valor añadido" o el "mejor valor" de una licitación de servicios en la nube.

El sector público suele exigir que en la competición entre los licitantes se utilicen criterios de evaluación como el mejor valor, la oferta económicamente más ventajosa (MEAT) o el precio más bajo. Debido a que las entidades del sector público planifican esta parte de la licitación de servicios en la nube, es importante crear un enfoque que tenga en cuenta las características únicas de la nube. Por ejemplo, deben ser conscientes de que la simple comparación de las partidas presupuestarias entre las ofertas de los proveedores de nube (p. ej.: computación o almacenamiento) no es una forma efectiva de comparar las ofertas. En su lugar, recomendamos encarecidamente un enfoque en soluciones de alto nivel, como las mencionadas previamente en la sección *2.2.1*. Las entidades del sector público pueden por tanto buscar los requisitos específicos de la nube, como los que se muestran en *Apéndice A: Requisitos técnicos para la comparación entre* licitantes**.**

Las licitaciones deben establecer las características esenciales de la nube necesarias para crear su solución en la nube. Para ello, las organizaciones del sector público pueden utilizar las características esenciales de la nube según el National Institute of Standards and Technology (NIST, Instituto nacional de estándares y tecnología), además de informes de analistas de terceros para garantizar que el CISP cuente con la oferta de "nube verdadera" más adecuada, que opere a escala masiva.

Texto de ejemplo: comparación entre proveedores

Los CISP deben responder TODAS las preguntas sobres requisitos técnicos del ***Apéndice A****.*

Los proponentes deben tener los siguientes atributos y describir de qué manera sus ofertas de servicios en la nube cumplen las cinco características esenciales de la computación en la nube[4]*.*

1) ***Autoservicio bajo demanda:*** los proponentes deben proporcionar la capacidad de aprovisionar capacidades de computación, como el tiempo del servidor y el almacenamiento de red, de forma unilateral cuando sea necesario y de forma automática sin necesidad de interacción humana con cada proveedor de servicios. *Los proponentes deben proporcionar la capacidad por la cual la actividad de pedido dé lugar a la provisión de los servicios de forma unilateral (es decir, sin la revisión ni la aprobación del proveedor). Explique cómo funciona con la propuesta o la oferta que representa.*

2) ***Acceso universal a la red:*** *los proponentes deben ofrecer varias opciones de conectividad de red, una de las cuales debe basarse en Internet. Explique cómo funciona con su oferta o la oferta que representa.*

3) ***Agrupación de recursos:*** *el CISP del proponente debe ofrecer recursos de computación agrupados que presten servicio a múltiples consumidores utilizando un modelo multiinquilino con diferentes recursos virtuales asignados y reasignados de forma dinámica en función de la demanda del consumidor. El usuario puede*

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

especificar la ubicación con un nivel superior de abstracción (p. ej.: el condado, la región o la ubicación del centro de datos) El proponente debe admitir el escalado de estos recursos en cuestión de minutos u horas desde la solicitud de aprovisionamiento. Explique cómo funciona con su oferta o la oferta que representa.

4) ***Rápida elasticidad:*** *el CISP del proponente debe admitir capacidades de aprovisionamiento y desaprovisionamiento de servicios (escalado ascendente y descendente) y hacer que el servicio esté disponible en los plazos mínimos designados (un máximo de "x" horas) desde la solicitud de aprovisionamiento. El proponente debe admitir los ajustes de facturación que se deriven de estas solicitudes de aprovisionamiento por días o por horas.*

5) ***Servicio medido:*** *el proponente debe ofrecer visibilidad del uso del servicio mediante un panel o un medio electrónico similar.*

Además, el CISP debe:

- *Ser un líder reconocido como proveedor de servicios en la nube según se demuestra en el Cuadrante mágico de Gartner para IaaS*[5]*.*
- *Proporcionar informes de analistas de terceros reconocidos por el sector que demuestren las capacidades y la fiabilidad probadas del CISP.*

Finalmente, se compararán los CISP empleando los escenarios proporcionados en el Apéndice B.

2.2.2.1 Contratos de nivel de servicio (SLA)

Los CISP proporcionan contratos de nivel de servicio comerciales estandarizados a millones de clientes, por lo que no pueden ofrecer estos contratos personalizados, como ocurre en el modelo de centro de datos en las instalaciones. No obstante, los clientes del CISP (a menudo con la asistencia de los socios del CISP) pueden diseñar el uso de su nube para aprovechar los contratos de nivel de servicio comerciales del CISP de modo que cumplan y superen los requisitos y los contratos de nivel de servicio únicos específicos del cliente.

Las licitaciones de servicios en la nube deben garantizar que la oferta de los CISP ofrecen las capacidades y la orientación necesarias para aprovechar sus servicios y contratos de nivel de servicio comerciales, de manera que los usuarios finales individuales puedan cumplir los requisitos de rendimiento y disponibilidad.

Texto de licitación de ejemplo: contratos de nivel de servicio

Proporcione información y enlaces al planteamiento del CISP sobre los contratos de nivel de servicio.

La ***<ORGANIZACIÓN>*** *estará al tanto de los contratos de nivel de servicio del CISP e implementará aplicaciones y cargas de trabajo importantes de modo que sigan funcionando en el caso de que no se cumpla un contrato de nivel de servicio.*

<ORGANIZACIÓN> *será responsable del mantenimiento adecuado de los contratos de nivel de servicio adecuados asociados a todos los equipos propiedad de* ***<ORGANIZACIÓN>*** *o a los servicios que opera* ***<ORGANIZACIÓN>*** *que se utilizan con el CISP.*

El CISP debe proporcionar a ***<ORGANIZACIÓN>*** *las capacidades necesarias para disponer de visibilidad continua e informes de rendimiento de su contrato de nivel de servicio operativo, así como de prácticas recomendadas documentadas que permitan utilizar la infraestructura del CISP para diseñar servicios para un mayor rendimiento, durabilidad y fiabilidad.*

[5] https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb

2.2.3 Contratación

Las condiciones del CISP se han diseñado de modo que reflejen cómo funciona un modelo de servicios en la nube (no se compran los activos físicos y los CISP operan a escala masiva ofreciendo servicios estandarizados); por este motivo, es fundamental que se incorporen estas condiciones del CISP y que se utilicen en la mayor medida posible. Consulte la sección *2.5* a continuación para obtener más información sobre las condiciones y la contratación.

2.2.3.1 Servicios nuevos y modificados

Los CISP proporcionan rendimiento a través de un servicio. A diferencia de las soluciones locales, que precisan actualizaciones y contratos de mantenimiento de servicios que caducan, los proveedores de nube únicamente ofrecen un servicio estandarizado. Para que el modelo de nube alcance economías de escala, se implementan actualizaciones y cambios en la infraestructura subyacente para todos, no solo para usuarios individuales, y seguidamente los clientes seleccionan los servicios que utilizan. El servicio es más fluido que los sistemas locales del pasado y los proveedores de nube agregan constantemente servicios nuevos y mejorados para que los clientes los utilicen como deseen.

Si no se pueden agregar servicios del CISP nuevos o mejorados después de la fecha límite de presentación de la licitación, las organizaciones del sector público no podrán utilizar servicios nuevos ni funciones mejoradas hasta que se emita la siguiente versión del acuerdo marco. Por ello, recomendamos encarecidamente que la provisión de servicios descrita en el acuerdo marco sea amplia de modo que permita la adición de nuevos servicios del CISP tras la fecha límite de presentación. La ley sobre adquisiciones de la Unión Europea puede limitar la incorporación al acuerdo marco de nuevos servicios del CISP sustancialmente diferentes, pero se pueden agregar actualizaciones y nuevas versiones de los servicios que no se consideren cambios sustanciales sin que se impugnen las adquisiciones.

Texto de licitación de ejemplo: servicios nuevos y modificados

El CISP ofrecerá una solución rentable que utilice tanto las tecnologías de virtualización probadas y estables como las tecnologías de vanguardia en continua evolución. ***<ORGANIZACIÓN>*** *reconoce y acuerda que las tecnologías de la nube se pueden proporcionar como servicio compartido a* ***<ORGANIZACIÓN>*** *y a otros clientes del CISP desde un código base y/o un entorno común, y que el CISP puede ocasionalmente: cambiar, agregar o suprimir las funciones, las características, el rendimiento u otras características de los servicios en la nube, y en el caso de que se realice dicho cambio, adición o supresión, se deben modificar en consecuencia las especificaciones del servicio en la nube.*

El alcance de esta orden de entrega incluye todos los servicios del CISP existentes actualmente, así como los nuevos o mejorados ***DENTRO DEL ÁMBITO DEL MARCO****. Los servicios en la nube proporcionados por el CISP y disponibles para los clientes comerciales deben estar disponibles para* ***<ORGANIZACIÓN>****.*

2.2.3.2 Dependencia del proveedor y reversibilidad

La tecnología basada en la nube reduce la dependencia del proveedor dado que no se compran los activos físicos, lo que permite a los clientes mover sus datos de un proveedor de nube a otro en cualquier momento.

Sin embargo, es inevitable que exista cierto grado de dependencia del proveedor cuando se compran servicios en la nube debido a que no todas las nubes son iguales y, por tanto, un CISP puede ofrecer servicios y capacidades que otro simplemente no puede proporcionar. De este modo, se reduce la posibilidad de utilizar dichos servicios con otro proveedor. Un enfoque prudente consiste en solicitar a los CISP que proporcionen las funciones y los servicios necesarios para salir de su nube, junto con

documentación sobre el uso de estos servicios que sirva como "estrategia de salida" razonable, dado que es imposible que un CISP conozca la configuración única del uso de un cliente de sus servicios estandarizados y, por lo tanto, que proporcione un plan de salida personalizado.

Se están desarrollando códigos de conducta del sector relativos a la "portabilidad de los datos" y al "cambio de proveedor de nube" para cumplir los requisitos del artículo 6 de la normativa "Free Flow of non-personal Data Regulation" (Reglamento de libre circulación de datos no personales), que se podrán emplear como herramientas para demostrar dicha reversibilidad una vez que estén disponibles públicamente. Esta referencia estará disponible en el sitio web de CISPE.

Texto de licitación de ejemplo: incorporación y baja

*La **<ORGANIZACIÓN>** está estudiando propuestas que ofrezcan una estrategia de salida razonable para evitar la dependencia. La **<ORGANIZACIÓN>** no compra los activos físicos, y el CISP ofrecerá la posibilidad de incorporarse a la estructura de TI y de darse de baja nuevamente. El CISP proporcionará las herramientas y los servicios de portabilidad necesarios para ayudar a realizar la migración hacia y desde la plataforma del CISP, reduciendo la dependencia. Se utilizará documentación detallada sobre cómo utilizar las herramientas y los servicios de portabilidad proporcionados por el CISP como plan de salida razonable.*

*El CISP no **exigirá** compromisos mínimos ni contratos a largo plazo.*

*El cliente podrá exportar los datos almacenados con un proveedor de servicios en cualquier momento. El CISP permitirá a **<ORGANIZACIÓN>** mover los datos cuando sea necesario dentro y fuera del almacenamiento del CISP. El CISP también permitirá que se descarguen imágenes de la máquina virtual y que se migren a un nuevo proveedor de nube. **<ORGANIZACIÓN>** puede exportar sus imágenes de la máquina y utilizarlas en las instalaciones o en otro proveedor (sujeto a las restricciones de la licencia de software).*

2.3 Seguridad

El CISP y los clientes de la nube comparten responsabilidades en lo relativo a seguridad y conformidad. En este modelo, los clientes de la nube pueden controlar el diseño y la protección de sus aplicaciones y de los datos que se almacenan en la infraestructura, mientras que el CISP es responsable de prestar servicios en una plataforma controlada de alta seguridad y de proporcionar una amplia gama de funciones de seguridad adicionales. El nivel de responsabilidad el CISP y del cliente en este modelo depende del modelo de implementación de la nube (IaaS, PaaS o SaaS); los clientes deben tener claras sus responsabilidades en cada modelo.

El conocimiento de este modelo de responsabilidad compartida es crucial para la elaboración de una licitación de servicios en la nube. Las organizaciones del sector público deben asegurarse de conocer las responsabilidades del CISP, sus propias responsabilidades y cómo pueden servir de ayuda los socios consultores o los proveedores de software independientes.

2.3.1 Requisitos mínimos

La palabra clave en lo que respecta a seguridad en la nube es **capacidad**. Las organizaciones del sector público deben exigir a los CISP que proporcionen las capacidades de seguridad necesarias para garantizar que los clientes puedan asumir sus responsabilidades en el modelo de responsabilidades compartidas. Como se puede ver en la lista de requisitos representativa que se muestra a continuación, se solicita al CISP que proporcione capacidades estandarizadas que pueda utilizar el cliente para hacer que su entorno de nube único sea seguro.

- ***Proporcionar*** *firewalls de red y* ***capacidades*** *de firewall de aplicaciones web para crear redes privadas y controlar el acceso a las instancias y las aplicaciones.*
- ***Proporcionar opciones*** *de conectividad que permitan las conexiones privadas o dedicadas desde su oficina o en un entorno local.*
- ***Proporcionar*** *la* ***capacidad*** *de implementar una estrategia de defensa en profundidad y frustrar los ataques DDoS.*
- ***Capacidades*** *de cifrado de datos disponibles en los servicios de almacenamiento y base de datos.*
- ***Proporcionar opciones*** *de administración de claves flexibles, lo cual le permite optar por que el CISP administre las claves de cifrado o permitir que el cliente tenga el control absoluto de las claves.*
- ***Proporcionar las API*** *para que los clientes integren el cifrado y la protección de los datos con cualquiera de los servicios desarrollados e implementados en el entorno de un CISP.*
- ***Proporcionar herramientas*** *de implementación para administrar la creación y la retirada de los recursos del CISP de acuerdo con los estándares de la organización.*
- ***Proporcionar herramientas*** *de administración de inventario y configuración que identifiquen los recursos del CISP y que, seguidamente, realicen un seguimiento de los cambios de dichos recursos y los administren a lo largo del tiempo.*
- ***Proporcionar herramientas y funciones*** *que permitan a los clientes ver exactamente lo que está ocurriendo en el entorno de su CISP.*
- ***Posibilitar*** *una* ***visibilidad*** *en profundidad de las llamadas a API, que incluya quién, qué y desde dónde se han realizado las llamadas.*
- ***Proporciones opciones*** *de agregación de registros, investigaciones de optimización y generación de informes de conformidad.*
- *Proporcionar la capacidad para configurar notificaciones de alerta cuando se producen eventos específicos o se superan umbrales.*
- ***Proporcionar capacidades*** *para definir, aplicar y administrar políticas de acceso de usuario en todos los servicios del CISP.*
- ***Proporcionar*** *la* ***capacidad*** *de definir cuentas de usuario individuales con permisos en todos los recursos del CISP.*
- ***Proporcionar*** *la* ***capacidad*** *de integrar directorios corporativos y federarse con ellos para reducir la sobrecarga administrativa y mejorar la experiencia del usuario.*

Puede consultar más requisitos en *Apéndice A: Requisitos técnicos para la comparación entre* licitantes**.**

Se pueden utilizar las funciones que superen los estándares mínimos de seguridad para obtener análisis relevantes de las "opciones de valor añadido" o del "mejor valor" en una licitación. Y cuanto mayor sea el número de funciones que se integren o automaticen en lo que respecta a la seguridad, tanto mejor. Nuevamente, consulte en *Apéndice A: Requisitos técnicos para la comparación entre* licitantes los requisitos para la comparación entre los licitantes.

Las organizaciones del sector público deben buscar las certificaciones y evaluaciones de acreditación de la nube para asegurarse de que están implantados los controles de seguridad del CISP necesarios. Por ejemplo, supongamos que un CISP ha sido validado y certificado por un auditor independiente para confirmar que cumple con el estándar de certificación ISO 27001. En el anexo A de ISO 27001, el dominio 14 profundiza en los controles específicos a los que debe ceñirse el CISP de acuerdo con los requisitos ISO en torno a la adquisición, el desarrollo y el mantenimiento del sistema. Es probable que estos controles cubran la mayoría de los controles, si no todos, en torno a la adquisición, el desarrollo y el mantenimiento del sistema que solicitaría normalmente una organización en una licitación relacionada con la TI. Por ello, tiene sentido que una organización solicite únicamente que el CISP cuente con la certificación ISO 27001, en lugar de duplicar esfuerzos y elaborar una lista de requisitos de control en torno a la adquisición, el desarrollo y el mantenimiento del sistema en una licitaciónde servicios en la nube.

Este enfoque basado en utilizar informes de conformidad de terceros se puede aplicar a la mayoría de los controles de seguridad y conformidad; por ejemplo: RGPD, ISO, SOC, etc.

Texto de licitación de ejemplo: seguridad

El CISP debe comunicar los procesos de seguridad no propietarios y las limitaciones técnicas a **<ORGANIZACIÓN>** *para que se pueda lograr una protección y una flexibilidad adecuadas entre* **<ORGANIZACIÓN>** *y el proveedor de servicios.*

El CISP debe establecer sus funciones y responsabilidades en lo que respecta a la seguridad y el cumplimiento de la normativa:

- *Describa las funciones y las responsabilidades del CISP y* **<ORGANIZACIÓN>** *relacionadas con la seguridad en la oferta propuesta. Describa con claridad la delimitación de las responsabilidades y resuma los servicios del CISP para ayudar a* **<ORGANIZACIÓN>** *a crear y automatizar las funciones de seguridad en su entorno de nube.*
- *Proporcione las respuestas a las especificaciones técnicas del* **APPÉNDICE A** *relacionadas con los requisitos de seguridad de* **<ORGANIZACIÓN>**.

PROPIEDAD Y CONTROL DEL CONTENIDO DE <ORGANIZACIÓN>

Describa cómo pueden las capacidades del CISP proteger la privacidad de los datos de **<ORGANIZACIÓN>**. *Incluya los controles implantados para abordar la protección del contenido de* **<ORGANIZACIÓN>**. *El CISP debe proporcionar un sólido aislamiento regional, de modo que los objetos almacenados en una región nunca salgan de ella a menos que* **<ORGANIZACIÓN>** *los transfiera explícitamente a otra región.*

- **<ORGANIZACIÓN>** *administrará el acceso a sus contenidos, servicios y recursos. El CISP debe proporcionar un conjunto avanzado de funciones de acceso, cifrado y registro para ayudar a* **<ORGANIZACIÓN>** a llevarlo a cabo de forma eficaz. *El CISP no accederá al contenido de* **<ORGANIZACIÓN>** *ni utilizará dicho contenido para ningún propósito distinto del exigido legalmente, así como para realizar el mantenimiento de los servicios del CISP y para proporcionarlos a* **<ORGANIZACIÓN>** *y a sus usuarios finales.*

- *La* **<ORGANIZACIÓN>** *seleccionará la región o las regiones en las que se almacenará el contenido. El CISP no trasladará ni replicará el contenido de* **<ORGANIZACIÓN>** *fuera de la región o las regiones elegidas, salvo que sea legalmente requerido y según sea necesario para el mantenimiento de los servicios del CISP y para proporcionarlos a* **<ORGANIZACIÓN>** *y a sus usuarios finales.*

- **<ORGANIZATION>** *elegirá cómo se protegerá su contenido. El CISP debe proporcionar un cifrado de alta seguridad para el contenido de* **<ORGANIZACIÓN>** *en tránsito o en reposo, y ofrecer la posibilidad de que* **<ORGANIZACIÓN>** *administre sus propias claves de cifrado.*

- *El CISP debe disponer de un programa de garantía de seguridad que utilice las prácticas recomendadas globales de protección de privacidad y protección de datos para que* **<ORGANIZATION>** *establezca, opere y utilice el entorno de control de seguridad del CISP. Estos procesos de control y medidas de seguridad se deben validar mediante múltiples evaluaciones independientes externas.*

Las evaluaciones y las certificaciones de acreditación de la nube proporcionan a las organizaciones del sector público la certeza de que los CISP tienen implantados controles de seguridad físicos y lógicos eficaces. El uso de estas acreditaciones en las licitación optimiza el proceso de adquisición y contribuye a evitar procesos duplicados y excesivamente laboriosos o flujos de trabajo de aprobación que podrían no ser necesarios para el entorno de la nube.

Las licitaciones de nube deben ofrecen a los CISP la posibilidad de demostrar que cumplen con las acreditaciones y las evaluaciones de conformidad. Como se ha mencionado anteriormente, existe un

solapamiento considerable entre los escenarios de riesgo y las prácticas de administración de riesgos en todos estos esquemas de acreditación, y debido a que los controles y los requisitos están agrupados en dichas acreditaciones, solicitar que los CISP cumplan con ellas es una forma más rápida de abordar la conformidad en una licitación en lugar de doblar esfuerzos en elaborar la lista de dichos controles individuales (**muchos de los cuales se pueden tomar de las licitaciones anteriores situados directamente en los centros de datos de las instalaciones, por lo que podrían no ser aplicables a la computación en la nube**).

NOTA: también es de gran importancia conocer cómo se accede a los informes que se muestran a continuación. Por ejemplo, los informes SOC 1 y SOC 2 suelen ser documentos confidenciales. Comprenda los acuerdos necesarios para acceder a ellos (p. ej.: el acuerdo de confidencialidad, ADC) en lugar de pedir simplemente que se le envíen dichos documentos como parte de la respuesta a una licitación (estos documentos se podrían hacer públicos mediante leyes de registros abiertos o similares que comprometen la seguridad de la nube).

Texto de licitación de ejemplo: cumplimiento de la normativa

El empleo de estándares de seguridad, conformidad y operativos reconocidos, derivados de prácticas recomendadas en operaciones de servicios en la nube (como el control de datos, la seguridad de los datos, la confidencialidad, la disponibilidad, etc.), optimizan la adquisición de tecnología basada en la nube.

La ***<ORGANIZACIÓN>*** *evaluará las ofertas de propuesta únicas con respecto a los estándares de seguridad, conformidad y operativos aceptados, como se describe a continuación y en el* ***Apéndice A****. Al confiar en la certificación de conformidad del proveedor para cada estándar,* ***<ORGANIZATION>*** *puede utilizar como referencia el cumplimiento mínimo de la normativa con respecto a cada estándar para evaluar la propuesta.*

La exigencia de que el CISP mantenga el estándar mínimo de cumplimiento de la normativa durante el tiempo de vigencia del contrato ofrece el beneficio de que la conformidad del contrato se mantiene actualizada.

El CISP que realiza la propuesta (directamente o a través de un distribuidor) debe ser capaz de demostrar que cumple con las siguientes atestaciones, informes y certificaciones de terceros. (Nota: Si alguna de estas atestaciones, informes y certificaciones tiene restricciones de divulgación por problemas de seguridad, ***<Organización>*** *trabajará con el CISP para obtener acceso de común acuerdo):*

Certificaciones y atestaciones	*Leyes, normativas y privacidad*	*Conformidad y marcos*
☐ *C5 (Alemania)*		☐ *CDSA*
☐ *Código de conducta de protección de datos de CISPE (*RGPD*)*		
☐ *DIACAP*	☐ *Directiva de protección de datos de la UE*	☐ *CIS*
☐ *DoD SRG Niveles 2 y 4*	☐ *Cláusulas modelo de la UE*	☐ *Información de justicia criminal Servicio (CJIS)*
☐ *HDS (Francia, atención sanitaria)*		
☐ *FedRAMP*	☐ *FERPA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *RGPD*	☐ *Escudo de privacidad entre la UE y los EE. UU.*
☐ *ISO 9001*	☐ *GLBA*	☐ *Puerto seguro de la UE*

☐ *ISO 27001*	☐ *HIPAA*	☐ *FISC*
☐ *ISO 27017*	☐ *HITECH*	☐ *FISMA*
☐ *ISO 27018*	☐ *IRS 1075*	☐ *G-Cloud [Reino Unido]*
☐ *IRAP [Australia]*	☐ *ITAR*	☐ *GxP (FDA CFR 21 Parte 11)*
☐ *MTCS Nivel 3 [Singapur]*	☐ *PDPA – 2010 [Malasia]*	☐ *ICREA*
☐ *PCI DSS Nivel 1*	☐ *PDPA – 2012 [Singapur]*	☐ *IT Grundschutz [Alemania]*
☐ *SEC Rule 17-a-4(f)*	☐ *PIPEDA [Canadá]*	☐ *MARS – E*
☐ *SecNumCloud (Francia)*		
☐ *SOC1 / ISAE 3402*	☐ *Ley de privacidad [Australia]*	☐ *MITA 3.0*
☐ *SOC2 / SOC3*	☐ *Ley de privacidad [Nueva Zelanda]*	☐ *MPAA*
	☐ *Autorización del DPA español*	☐ *NIST*
	☐ *DPA del Reino Unido - 1988*	☐ *Niveles de Uptime Institute*
	☐ *VPAT/Sección 508*	☐ *Principios de seguridad de la nube del Reino Unido*

La lista anterior tiene un fin meramente ilustrativo y no aspira a ser una lista exhaustiva de las certificaciones y los estándares que pueden aplicarse a los servicios en la nube.

2.3.2 Comparación entre proveedores

Como ocurría con los criterios técnicos de las secciones anteriores, además de los requisitos mínimos de seguridad de la licitación de servicios en la nube, es importante indicar los criterios que permiten comparar las capacidades y los servicios de seguridad del CISP en una evaluación competitiva.

Consulte en *Apéndice A: Requisitos técnicos para la comparación entre* licitantes ejemplos de requisitos de seguridad del CISP. Recomendamos encarecidamente que las capacidades siguientes sean consideraciones clave de seguridad para las entidades del sector público que evalúan a los CISP:

Texto de licitación de ejemplo: consideraciones clave de seguridad

- *La comprensión del CISP del modelo de responsabilidad compartida y la documentación para ayudar a los clientes a comprender la delimitación de las responsabilidades de seguridad para las funciones y los servicios del CISP (por ejemplo, en el contexto del RGPD)*
- *Historial demostrado de la seguridad de la infraestructura del CISP, con documentación de propiedad no exclusiva y disponible públicamente sobre los controles físicos y lógicos y la posición de seguridad del CISP.*
- *Soporte del CISP específico para la seguridad de la nube*
- *Servicios que permiten a los clientes formalizar el diseño de cuenta, automatizar la seguridad y los controles de gobernanza de la nube, y optimizar la auditoría*
- *Capacidad para crear, aprovisionar y administrar un conjunto de recursos en una plantilla (incluye plantillas de seguridad con estándar referencial creadas por el CISP o por el socio del CISP)*
- *Capacidad de establecer un funcionamiento fiable y repetible de los controles*
- *Funciones para una auditoría continua y en tiempo real*

- *Capacidad para crear scripts técnicos de políticas de gobernanza de la nube*
- *Capacidad para crear funciones de forzado que no puedan anular los usuarios que no tengan permiso para modificar dichas funciones*
- *Capacidad de ejecución de una implementación fiable de lo que se ha descrito previamente en las políticas, los estándares y las regulaciones, además de crear unas normas de seguridad y conformidad que sean aplicables, lo que a su vez genera un modelo funcional de gobernanza de la nube fiable para los entornos de TI.*
- *Servicios para protegerse de los ataques (DDoS) comunes más frecuentes de denegación distribuida de servicio que se producen en la red y en la capa de transporte, además de la capacidad de escribir reglas personalizadas para mitigar ataques sofisticados en la capa de aplicación*
- *Servicio administrado de detección de amenazas*

2.3.3 Contratación

Como se ha indicado anteriormente, las condiciones del CISP se han diseñado de modo que reflejen cómo funciona un modelo de servicios en la nube (no se compran los activos físicos y los CISP operan a escala masiva ofreciendo servicios estandarizados); por este motivo, es fundamental que se incorporen estas condiciones del CISP y que se utilicen en la mayor medida posible. Consulte la sección *2.5* a continuación para obtener más información sobre las condiciones y la contratación.

En materia de seguridad, volvemos a recomendar encarecidamente que se permita a los CISP actualizar continuamente sus ofertas, o que se permita a los proveedores agregar productos después de la fecha límite de presentación, siempre y cuando se ajusten a los parámetros originales de la licitación. Esto refleja el hecho de que las funciones y los servicios de seguridad evolucionan con rapidez y que los CISP lanzan a menudo nuevos servicios centrados en la seguridad, que en muchos casos se pueden utilizar libremente. Tenga en cuenta que es importante contar con un nivel de seguridad de referencia (consulte los requisitos mínimos anteriores) para garantizar que los cambios en las ofertas de seguridad no sean perjudiciales.

Lógicamente, el modelo de responsabilidad compartida es el fundamento de la seguridad en una licitación de servicios en la nube. Cada parte debe exponer con claridad sus responsabilidades de seguridad y los CISP deben documentar las responsabilidades de seguridad tanto del CISP como del cliente con respecto a las tecnologías de la nube proporcionadas por el CISP, junto con documentación para ayudar a los clientes a integrar y automatizar las prácticas de seguridad recomendadas.

El acuerdo marco de nube debe ofrecer flexibilidad para eliminar a un proveedor que ya no cumpla con los requisitos mínimos de seguridad y conformidad establecidos en la licitación de servicios en la nube.

2.4 Precios

Para contratar una tecnología basada en la nube de manera que refleje la demanda fluctuante, las organizaciones del sector público precisan un contrato que les permita pagar los servicios a medida que los consumen, con la gobernanza y la visibilidad de nube necesarias con respecto al uso y al gasto.

Es importante que las licitaciones de servicios en la nube consideren el valor y el coste total de propiedad (TCO), en lugar de realizar sencillas comparaciones de igual a igual de precios unitarios. Esta práctica tradicional de considerar el precio unitario más bajo no es aplicable al modelo de nube y, como tal, no suele dar lugar a la oferta económicamente más ventajosa ni al precio global más bajo.

Como ayuda para la evaluación del precio del CISP, resulta útil contar en primer lugar con una cualificación previa o una preselección con los ***requisitos mínimos en cuanto a precios*** *de modo que los CISP con capacidades similares puedan ser candidatos para el acuerdo marco. El proceso de evaluación de los pedidos abiertos o las minilicitaciones puede entonces buscar una selección de arquitecturas de nube y* ***escenarios de precios*** *típicos de ejemplo que coincidan con cargas de trabajo típicas del sector público y pedir a los CISP que fijen los precios. También se recomienda realizar demostraciones de prueba en directo para comparar el rendimiento y la elasticidad de los servicios de tecnologías de la nube que proporcionan los CISP. Consulte en el Apéndice B un ejemplo de script de prueba de demostración de tecnologías de la nube.*

2.4.1 Requisitos mínimos

La sección de precios de la licitación de servicios en la nube tiene cuatro elementos clave:

1. **Precios de los servicios:** los clientes de la nube están incorporando un modelo de servicios de pago por uso por el cual al final de cada mes solo tienen que pagar por el uso realizado, lo cual es idóneo para las métricas de uso y de recursos.
2. **Precios transparentes:** los precios del CISP deben ser transparentes y estar disponibles públicamente.
3. **Precios dinámicos:** los precios de la nube son flexibles y fluctúan en función de los precios del mercado. Este enfoque aprovecha el carácter dinámico y competitivo de los precios de la nube y apoya la innovación y las reducciones de precios.
4. **Control de gastos:** los CISP deben suministrar herramientas de generación de informes, monitorización y previsión que permitan a los clientes (1) monitorizar el uso y el gasto tanto a nivel de resumen como detallado, (2) recibir alertas cuando el uso y el gasto alcancen umbrales personalizados y (3) calcular el uso y el gasto con el fin de planificar los presupuestos de nube futuros.

Texto de la licitación de ejemplo: precios

<ORGANIZATION> solicita a los CISP interesados en responder que incluyan el método y el modelo de precios que proponen para ofrecer cada uno de sus servicios como una capacidad de nube comercial a los usuarios finales.

El CISP debe proporcionar:

- *Documento de definición de servicio o enlaces a definiciones de servicio*
- *Documento de términos y condiciones*
- *Documento de precios (se aceptarán enlaces a los precios públicos siempre que haya una lista de precios o un documento de precios completo disponible previa solicitud)*

El precio corresponderá al coste de la configuración más común del servicio. Los CISP deben ofrecer opciones de descuento por volumen y herramientas de cálculo de precios para calcular el precio real de lo que se compra, así como el valor total que se ofrece al comprador (por ejemplo, servicios de optimización y la reducción de costes resultante).

Con arreglo al acuerdo marco, los compradores pueden hablar con los proveedores para pedirles que expliquen la descripción del servicio, las condiciones, los precios, o los documentos o el modelo de definición de servicio. Se guardará un registro de todas las conversaciones mantenidas con los proveedores.

Requisitos de precios adicionales

- *Proporcionar tecnologías de la nube con un modelo de precios dinámico que ofrezca la máxima flexibilidad empresarial y permita la escalabilidad y el crecimiento.*
- *Los atributos de precios deben incluir lo siguiente:*
  - *¿Se ofrecen los precios mediante el pago por uso bajo demanda de un servicio público? Explique su modelo de precios.*
  - *¿Puede ofrecer descuentos adicionales si existe un compromiso de uso o se realiza una compra de gran volumen? Describa cómo con detalle.*
  - *¿Son los precios transparentes y están disponibles públicamente? Incluya enlaces a los precios disponibles públicamente.*
  - *¿Son los precios dinámicos y responden de forma rápida y eficiente a la competición del mercado?*
  - *¿Proporciona prácticas recomendadas y recursos para hacer un seguimiento de los gastos?*
  - *¿Proporciona prácticas recomendadas y recursos para optimizar los costes?*

Transparencia de precios
Debido a la tendencia constante de reducción de precios en las tecnologías de nube comerciales como consecuencia de la innovación y la competencia, el coste de la unidad de servicio medida del CISP que paga ***<ORGANIZACIÓN>*** *bajo el Acuerdo marco no debe superar el precio unitario publicado en el sitio web del proveedor de nube aplicable cuando el consumidor consume la unidad de servicio.*

Presupuestos e informes y alertas de facturación
Para demostrar la entrega y el uso de las tecnologías de nube, los CISP deben suministrar a ***<ORGANIZACIÓN>*** *las herramientas necesarias para generar informes de facturación detallados que desglosen los costes por hora, día o mes; por cada una de las cuentas de la organización; o por las etiquetas definidas por el cliente.* ***<ORGANIZACIÓN>*** *reconoce que como parte del modelo de nube de responsabilidad compartida,* ***<ORGANIZACIÓN>*** *será responsable de utilizar las funciones de facturación y elaboración de presupuestos, así como las herramientas para hacer frente a los requisitos únicos de previsión y generación de informes proporcionadas por el CISP.*

- *Proporcione información sobre cómo puede* ***<ORGANIZACIÓN>*** *visualizar la información de facturación y uso tanto a nivel detallado como de resumen, mostrando los patrones de gasto de los recursos del CISP a lo largo del tiempo, además de la previsión del gasto en el futuro.*
- *Proporcione información sobre cómo puede* ***<ORGANIZACIÓN>*** *filtrar la vista de uso o facturación por servicio, por cuenta vinculada o por las etiquetas personalizadas aplicadas a los recursos, y crear alertas de facturación que envíen notificaciones cuando el uso de los servicios alcance o supere los umbrales o los presupuestos definidos por <****ORGANIZACIÓN****>.*
- *Proporcione información sobre cómo puede* ***<ORGANIZACIÓN>*** *prever cuántos servicios de nube utilizará a lo largo de un periodo de tiempo definido basándose en el uso en el pasado. Los CISP deben ofrecer una* ***estimación*** *de cuál será la factura del CISP de* ***<ORGANIZACIÓN>****, lo cual permite a* ***<ORGANIZATION>*** *utilizar alarmas y presupuestos para cantidades que se prevé que utilizará con objeto de tener un mayor control de los costes y los gastos.*

2.4.2 Comparación entre proveedores

Las organizaciones del sector público suelen exigir que en la competición entre los licitantes se utilicen criterios de evaluación como el mejor valor, la oferta económicamente más ventajosa (MEAT) o el precio más bajo. Cuando se planifican los precios de los pedidos abiertos o las minilicitaciones del acuerdo marco, es importante crear un enfoque que tenga en cuenta las características únicas de la nube. Por ejemplo, comprender que la simple comparación de las partidas presupuestarias entre las ofertas de los proveedores de nube (p. ej., computación o almacenamiento) no es un modo eficaz de realizar la comparación, ya que no se tienen en cuenta funciones como el rendimiento, la optimización de costes que utiliza servicios nativos de la nube y herramientas de monitorización del CISP, ni los servicios de diferenciación que los CISP pueden ofrecer de forma gratuita. Además, el precio de catálogo de un CISP puede constar de decenas de miles de partidas y los modelos de precios pueden diferir de un servicio a otro y de un proveedor a otro.

Análisis del coste total de propiedad

Recomendamos adoptar un enfoque en el coste total de propiedad (TCO) de los casos de uso definidos, que tenga en cuenta todos los aspectos de una solución en la nube (incluyendo servicios de los socios, descuentos estandarizados del CISP, características técnicas que puedan mejorar el rendimiento, y costes de optimización o reducción, entre otros).

Comparación por escenarios

El proceso de evaluación también puede considerar los escenarios típicos que corresponden a los sistemas o las aplicaciones. Dichos escenarios (como el alojamiento web o la implementación de un sistema de recursos humanos con un número x de usuarios, etc.) pueden incluir variables como la velocidad y la escala de los recursos, el rendimiento de la aplicación o la solución, los tiempos de acceso al almacenamiento, datos complejos de bajo volumen comparados con tareas de computación simples de gran volumen, etc. Las aplicaciones o los sistemas también pueden tener escenarios típicos como el procesamiento de un gran volumen para la declaración de impuestos, y notificaciones de emergencia como las advertencias de inundación. Los escenarios deben ser generales de modo que incluya el ámbito de la tecnología y los servicios que puede utilizar el cliente durante el proyecto. De este modo, el cliente puede comparar el coste global estimado del proyecto.

Comparación financiera y técnica de escenarios

También es importante tener en cuenta los beneficios técnicos al comparar los precios de las ofertas de los CISP. Por ejemplo, un CISP podría permitir a los clientes crear una topología de Disaster Recovery (DR, Recuperación ante desastres) activa/activa gracias a su modelo de centros de datos en clústeres dentro de una región geográfica. Un CISP que no tenga este tipo de configuración de redundancia y centro de datos podría ser x % más caro dado el coste de tener en cuenta las necesidades de recuperación ante desastres. Como ejemplo de por qué un enfoque holístico de los precios que incluya funciones técnicas adicionales es crucial para evaluar a los CISP, supongamos la siguiente alternativa de comparación directa de igual a igual.

Ejemplo: un cliente desea comparar el precio del almacenamiento de objetos ofrecido por CISP cualificados en un acuerdo marco. El precio del artículo de la "unidad" de almacenamiento del CISP 1 es de 0,023 € por GB. El precio de la misma "unidad" del CISP 2 es de 0,01 € por GB. En una comparación sencilla de unidad a unidad, el cliente no formularía preguntas clave como:

1. ¿Cuántas copias de redundancia hay disponibles del objeto en caso de fallo? En el ejemplo anterior, el CISP 1 se ha concebido para soportar una pérdida de datos simultánea en dos instalaciones diferentes, y mantiene varias copias de datos. En el caso del CISP 2, no se realizan copias de redundancia.

2. ¿Cuál es el nivel de sostenibilidad de objetos almacenados? El del CISP 1 es del 99,999999999 %; el del CISP 2, del 99 %.
3. Tenga en cuenta el coste a lo largo de la vida de la propiedad del proyecto o de la carga de trabajo global, y cómo pueden las funciones de optimización de costes reducir los costes en lo referente al modo de almacenar y utilizar los datos (por ejemplo, incrementar el uso de las funciones sin servidor de un CISP puede reducir los costes en un x %).

Estas son solo algunas de las muchas consideraciones técnicas que deben tenerse en cuenta en los precios, especialmente las relacionadas con la seguridad y la conformidad.

Las consideraciones de escenarios de precios incluyen:

Tarifas base: se trata básicamente de los precios públicos de los CISP. Los CISP deben ofrecer estos precios públicamente; sin embargo, como se ha indicado anteriormente, para comparar los CISP de formar eficaz, los clientes pueden pedir los precios de, por ejemplo, 3 a 5 escenarios específicos (o de tantos como considere oportuno el cliente) a todos los proveedores. Los escenarios deben ser integrales e incluir todo el abanico de servicios y tecnologías que es probable que utilice el cliente durante el transcurso del proyecto. De este modo, el cliente puede comparar el coste global estimado del proyecto. Las comparaciones realizadas en el nivel de partida o de unidad de almacenaje suelen ser más problemáticas que útiles para los clientes y los proveedores (los clientes tendrían que comparar decenas de miles de partidas de todos los CISP, y los proveedores tendrían que proporcionar este nivel de detalle y administrarlo cuando el precio real se determine únicamente en función del consumo del servicio).

La evaluación del conjunto de capacidades globales del CISP es una necesidad para los clientes de la nube que deseen obtener el mejor valor. Por ejemplo, los CISP deben contar con un número de servicios que sean gratuitos o esencialmente gratuitos, y una evaluación de precios debe tener en cuenta dichos servicios, así como que otros CISP podrían cobrar por funciones similares.

Los criterios de evaluación se pueden redactar de manera que los CISP puedan anunciar sus funciones "predeterminadas x incluidas" y de qué modo dichos servicios tienen un impacto en el coste global. Los criterios de evaluación también pueden considerar los precios por volumen o escalonados del CISP y los descuentos disponibles comercialmente, como las instancias reservadas o las instancias de spot. Por ejemplo:

- x % de ahorro si los clientes compran una capacidad de computación reservada (por 1 año, 3 años, etc.)
- x % de descuento en precios por volumen o escalonados
- x % de ahorro basado en las revisiones de arquitectura y la optimización de la infraestructura, como cambiar a la opción de computación más adecuada
- Como se ha mencionado anteriormente, debe tenerse en cuenta el coste de la vida completa y cómo pueden reducirlos las funciones de optimización de costes

ESCENARIO DE PRECIOS
Los licitantes deben ofrecer sus precios para el siguiente escenario únicamente para fines de evaluación. El precio real se basará en el consumo de servicios en un modelo de pago por uso bajo demanda.

A continuación se muestran los requisitos representativos para la determinación de precios, los cuales se proporcionan con el conocimiento explícito de que durante el periodo de vigencia del contrato cambiarán estos requisitos nominales. Indique los precios para una capacidad de 12 y 36 meses bajo demanda, y de 12 y 36 meses reservada.

Indique:

- *Nombre de la solución o soluciones propuestas:*
- *Mejor precio del licitante:*
- *Horas de servicio: 24x7x365*
- *Disponibilidad del servicio: 99,95 %*

Los escenarios de precios pueden incluir asimismo ejemplos de clientes existentes con cargas de trabajo similares que hayan optimizado sus gastos a lo largo de 1, 2 o 3 años (mediante el uso de herramientas de monitorización y optimización del CISP, la adopción de soluciones nativas de la nube optimizadas y la reducción de los precios del CISP:

2.5 Configuración y condiciones de ejecución del contrato

Las tecnologías y operaciones basadas en la nube que ofrece el CISP tienen un diseño estandarizado, por lo que también están estandarizadas las condiciones contractuales No obstante, existe la posibilidad de ajustar ligeramente estos contratos para adaptarlos a los contextos legislativos y normativos locales.

Con frecuencia, los métodos de adquisición de TI tradicionales incluyen reglas estrictas que exigen que los solicitantes cumplan muchos o todos los requisitos de la adquisición o que sean rechazados. O quizás incluyen un subconjunto estricto de requisitos obligatorios. Cuando se utiliza este método de abastecimiento con las tecnologías de la nube, que son en realidad un conjunto de componentes y herramientas estandarizados que le ayudan a diseñar una solución personalizada, las adquisiciones suelen fracasar.

2.5.1 Términos y condiciones

El primer paso de la contratación en una licitación de servicios en la nube es revisar y comprender las condiciones comerciales existentes del CISP que, en muchos casos, están disponibles públicamente en los sitios web del CISP. Las entidades del sector público se encuentran cada vez más cómodas aceptando las condiciones comerciales de los CISP. Parte de este esfuerzo para comprender las condiciones consiste en reunirse con los CISP y sus socios para profundizar en sus enfoques. La pregunta clave que cabe formularse es “por qué” operan los CISP con condiciones específicas. Algunas de estas condiciones podrían parecer diferentes de las condiciones de TI tradicionales, pero hay motivos específicos que “explican” que formen parte de un contrato de nube. Si las condiciones disponibles públicamente no son aceptables, los CISP suelen tener acuerdos ligeramente modificables para los clientes empresariales que se pueden explorar.

Además de revisar los términos y las condiciones del CISP, es importante conocer las políticas existentes, la normativa o las leyes (por ejemplo, las relacionadas con la tecnología, la clasificación de los datos, la privacidad, el personal, etc.). A menudo, existen políticas, regulaciones o leyes diseñadas para comprar y utilizar ofertas de TI tradicionales que pueden entrar en conflicto con el modelo del CISP. Por ejemplo, permitiendo únicamente el uso de las tecnologías de la nube que se incluían en la oferta de acuerdo marco a través de la licitación de servicios en la nube. Los CISP agregan constantemente nuevos servicios y funciones. El hecho de que se impida el acceso a estos nuevos servicios simplemente porque se siga un enfoque tradicional de actualización de productos de TI no tiene sentido para el cliente final. Si es este el caso, es importante mantener una discusión en profundidad con los CISP en la que se traten estas políticas, regulaciones o leyes.

Aprovechar las discusiones previas a la licitación

Como se ha indicado anteriormente, antes de elaborar un borrador de licitación, debe tomarse tiempo para reunirse con los CISP y los proveedores relacionados para conocer sus términos y condiciones e informarles del enfoque, las políticas, las regulaciones y las leyes de su entidad. Lo más importante de estas conversaciones es que ambas partes descubran "por qué" las condiciones relevantes funcionan de la manera que lo hacen. Por ejemplo, los términos y condiciones de la nube difieren de las condiciones de los centros de datos, los servicios administrados, el hardware, el software listo para usar y la integración de sistemas tradicionales. Dado que son modelos individuales que requieren una innovación constante, estos modelos de negocio precisan de un proceso de licitación lo suficientemente flexible como para mantener negociaciones o conversaciones que permitan obtener aclaraciones.

Al incluir la posibilidad de aclarar los términos y las condiciones mediante discusiones o negociaciones, las organizaciones del sector público pueden conocer mejor los modelos de nube y evitan rechazar proveedores que en realidad podrían satisfacer las necesidades de la organización. Un proceso típico sería que la organización identificase determinadas condiciones por adelantado que desee discutir y negociar antes de la adjudicación. Con la negociación por adelantado con los licitantes de las condiciones aceptables, la organización se asegura de obtener la adjudicación más adecuada y resuelve las diferencias que de otra manera podrían dar lugar al rechazo de una propuesta efectiva. Las entidades del sector público también pueden revisar sus políticas, regulaciones y leyes, y ambas partes pueden descubrir cómo se ajusta el uso de la nube a dichos modelos. A menudo ocurre que hay posibilidades de trabajar con las cláusulas existentes. Sin embargo, si un área es problemática, ambos equipos pueden trabajar juntos para buscar una solución (es mejor mantener estas conversaciones mucho antes de la licitación y de cualquier negociación contractual posterior).

Flexibilidad de la negociación

Para poder firmar los contratos con arreglo a la legislación local, basados a su vez en los términos contractuales estandarizados del CISP, se recomienda (1) pedir a los solicitantes su contrato estandarizado, (2) no establecer condiciones contractuales inadecuadas al elaborar el acuerdo marco para la licitación de servicios en la nube, y (3) ofrecer una opción de negociación sobre todas las disposiciones de la consulta y las propuestas que darán lugar al acuerdo marco (excepto, lógicamente, las cláusulas obligatorias exigidas por la ley).

Nota: El alcance de la responsabilidad compartida es inherente en el modelo de nube y se debe reflejar en los términos del contrato (p. ej.: el CISP confirma que los clientes son propietarios de sus datos y del lugar donde residen, y proporcionan herramientas para garantizar que la elección de ubicaciones de datos sea limitada, **PERO** es responsabilidad del cliente o del socio utilizar estas herramientas).

Tenga en cuenta que es importante que haya varios ***conjuntos de términos y condiciones diferentes*** *del contrato para cada uno de los LOTES en un acuerdo marco de nube. Un "planteamiento uniforme" de la contratación para todos los LOTES causará problemas de viabilidad y compatibilidad técnica.*

Como se ha indicado anteriormente, las licitaciones que incluyen términos obligatorios que no son negociables son básicamente una propuesta del tipo "tómelo o déjelo" a los proveedores, que pueden causar que una propuesta que de otro modo sería aceptada sea rechazada. Las organizaciones del sector

público deberían considerar cuidadosamente las consecuencias de utilizar términos obligatorios **a menos que sea un requisito legal**. Las organizaciones deben estar convencidas de la necesidad de un requisito o una condición obligatoria, dado que las futuras negociaciones vienen determinadas por su clasificación como obligatoria. El uso de requisitos o de términos obligatorios debe mantenerse en el mínimo absoluto para dotar a la organización de la flexibilidad necesaria para adquirir la mejor tecnología y solución.

Tenga en cuenta que las tecnologías de nube del CISP están completamente estandarizadas y se entregan de manera completamente automática. Por lo tanto, el CISP no puede realizar ningún tipo de cambio en los términos ni en las condiciones que pudiera requerir la personalización de un servicio subyacente. Además, los precios de los servicios son normalmente públicos y están estandarizados para todos los usuarios, lo que significa que el CISP no puede ajustar los precios para asumir mayores riesgos en representación de un cliente en particular.

Compras indirectas

Una alternativa a la compra de tecnologías de la nube directamente de un CISP es comprarlas de un distribuidor del CISP en su lugar. Puede obtener más información sobre los distribuidores de CISP en la sección *2.1.3* anterior.

Texto de licitación de ejemplo: términos y condiciones

*Los CISP o los proveedores representativos deben proporcionar sus términos y condiciones disponibles públicamente y ofrecer información sobre los términos y las condiciones clave proporcionados por <**ORGANIZACIÓN**>.*

*<**ORGANIZACIÓN**> pretende celebrar un contrato por escrito con el licitante elegido basado en los términos contractuales del licitante. El licitante debe proporcionar una serie de términos contractuales propuestos para que los revise <**ORGANIZACIÓN**>, que representa su mejor propuesta comercial y legal. Los oferentes y <ORGANIZACIÓN> pueden discutir las dos series de términos y condiciones durante la fase <DISCUSIÓN/NEGOCIACIÓN>.*

- *La carta de intenciones del marco de alto nivel constaría principalmente de los siguientes componentes:*
  - *Duración del marco*
  - *Gestión del marco*
  - *Desempeño del marco*
  - *Finalización del marco*
  - *Alcance del marco*
  - *Proceso de pedido*
  - *Disposiciones de confidencialidad*
  - *IP e información específicos de la categoría*
  - *Requisitos técnicos mínimos que deben cumplir los CISP (p. ej., estándares de calidad, acreditación, seguridad y protección de los datos)*
- ***Se incluirán diferentes términos para cada uno de los lotes del acuerdo marco***
- *Se pueden considerar los pormenores del servicio del CISP, los cuales se tratarán en el pedido abierto.*
- *Permita cambios en el contrato. Los términos no deben limitar que los clientes ni los proveedores puedan acordar cambios en el contrato para agregar nuevos servicios o mejoras. El carácter evolutivo de los servicios en la nube es tal que las mejoras de servicios estarán disponibles de forma continua, lo cual puede contribuir a brindar una mayor eficiencia a los clientes.*
- *Los Acuerdos de nivel de servicio (ANS) no debe especificarlos el cliente. Los términos del cliente no deben definir los ANS personalizados específicos de la comisión, que difieren de los modelos estándar de prestación de servicios del CISP. Permitiendo los ANS estándar de los CISP, estos podrán mantener los costes bajos y trasladarlos a los clientes, lo que a su vez hace que los clientes confíen en que el CISP puede cumplir el ANS.*

- *Los límites de responsabilidad deben ser proporcionados. La responsabilidad debe ser proporcional a los servicios que se compran, por lo que no deben establecerse límites de responsabilidad desproporcionadamente altos. Unos límites desproporcionadamente altos pueden disuadir a los CISP de aceptar proyectos de bajo valor. Con frecuencia, estos proyectos son una introducción útil y un caso de "prueba" que permite a los clientes determinar si determinadas soluciones en la nube son eficaces para su organización.*
- *Los clientes deben ser los propietarios de sus datos. Los clientes deben controlar sus datos y ser sus propietarios, así como tener la capacidad de determinar la ubicación geográfica en la que se hospedan. De este modo los clientes podrán evitar depender del proveedor y podrán mover los datos libremente hacia nuevos proveedores.*

2.5.2 Cómo seleccionar entre los adjudicatarios por proyecto

Los organismos del sector público que forman parte del marco pueden realizar un pedido o un "pedido abierto" de los servicios que precisen cuando sea necesario. Otorgar un contrato de entrega sucesiva bajo un acuerdo marco permite a los compradores ajustar los requisitos con especificaciones funcionales adicionales para un pedido abierto, a la vez que conservan los beneficios de dicho acuerdo marco.

Si se considera necesario, se puede convocar una minilicitación para identificar al mejor proveedor de una carga de trabajo o de un proyecto en particular. Mediante una minilicitación, el cliente convoca un nuevo concurso bajo el marco invitando a todos los proveedores de un lote a dar respuesta a una serie de requisitos. El cliente invitará a todos los proveedores capacitados del lote a realizar una propuesta, de ahí la importancia de los requisitos mínimos para los adjudicatarios de una licitación de servicios en la nube, ya que garantiza que haya opciones de alto nivel bajo cada lote.

Tenga en cuenta que es importante que haya varios conjuntos de términos y condiciones diferentes del contrato para cada una de las categorías de lote del tipo de oferta (p. ej., IaaS o PaaS pública, IaaS o PaaS comunitaria, y IaaS o PaaS privada), ya que un "planteamiento uniforme" de la contratación para todos los lotes causará problemas de viabilidad y compatibilidad técnica.

Consulte en la sección *2.1.4* un texto de la licitación de ejemplo relativo a la selección entre adjudicatarios.

2.5.3 Incorporación y baja

Una consideración que debe tenerse en cuenta al definir un acuerdo marco de nube es la opción de un Sistema dinámico de adquisición (SDA). Con un modelo de SDA, se admitirán en el marco todos los proveedores que cumplan los requisitos mínimos del acuerdo marco. No existe ningún límite máximo en cuanto al número de proveedores que pueden unirse al marco, y a diferencia del modelo tradicional, los proveedores también pueden solicitar unirse al "Marco SDA" en cualquier momento durante su vigencia.

Recomendamos encarecidamente que las entidades del sector público definan altos estándares para garantizar la calidad y la fiabilidad del servicio prestado por los proveedores cualificados, pero a su vez que no sean demasiados específicos como para descalificar a los CISP de modo que no se garantice una competición justa. El fin último es evitar saturar al usuario final con un gran número de opciones, a la vez que se mantiene un estándar alto de tecnologías de la nube disponibles.

3.0 Prácticas recomendadas y lecciones aprendidas

A continuación destacamos algunas lecciones aprendidas sobre cómo concretar un acuerdo marco de nube adecuado con una licitación de servicios en la nube bien redactada.

3.1 Gestión de la nube

La gestión de la nube es una responsabilidad compartida. Los CISP proporcionan funciones y servicios para integrar la gestión de la nube en cada aspecto de un entorno de nube, mientras que los clientes aportan sus estándares existentes de gestión de la nube y descubren de qué manera la nube propicia la gestión de la nube.

En la nube, los clientes tienen la oportunidad de crear el entorno de TI que deseen, en lugar de limitarse a administrar el que ya tienen. La nube permite a los clientes: (1) comenzar por un inventario completo de todos los recursos de TI; (2) administrar centralmente todos estos recursos; y (3) crear alertas relacionadas con el uso, la facturación, la seguridad, etc. Todos estos beneficios vitales de la nube ayudan a los clientes a disponer de una arquitectura optimizada y automatizada al máximo sin necesidad de adquirir e instalar continuamente nuevo hardware. Eso lo hace el CISP, lo que permite que los clientes pasen de realizar tareas de administración generales de la infraestructura a centrarse en el nivel operativo fundamental.

Una forma útil de ver la nube del CISP es considerarla en realidad una API de grandes dimensiones. Cuando lanza un nuevo servidor o cambia la configuración de seguridad, lo que está haciendo es llamar a una API. Se registra y se graba cada cambio realizado en el entorno (quién hizo el cambio, qué cambios introdujo, dónde hizo el cambio y cuándo). Esto proporciona un nivel de gestión, control y visibilidad que solo es posible en un entorno de nube. Esto permite a los clientes reconsiderar sus modelos de gestión de TI existentes, así como determinar de qué manera se pueden optimizar y mejorar, dados los beneficios que comporta la nube.

La gestión de la nube también puede implicar comunicar e incorporar los cambios positivos en el proceso y los nuevos conjuntos de capacidades que se suministren con la nube. Por ejemplo, los administradores de proyectos están familiarizados con plazos de meses de duración para la creación de un entorno de TI, y como tales podrían excederse en la estimación de los calendarios para crear un entorno de desarrollo o prueba en la nube (que con la nube apenas tarda unos minutos). La adaptación a esta nueva agilidad será un periodo de evolución y se produce programa a programa: Estas lecciones aprendidas se deben compartir para que el acuerdo marco de nube pueda seguir evolucionando de modo que los requisitos sean perfectos para los nuevos procesos y la agilidad.

3.2 Elaboración de un presupuesto para la nube

Cuando se trata de cómo estructurar los precios de la nube de pago por uso para ajustarlos a los requisitos de adquisición y presupuesto del sector público, hemos comprobado que es de gran ayuda agrupar los servicios del CISP en una única partida (computación, almacenamiento, redes, base de datos, IoT, etc.), todos ellos bajo la partida **Tecnologías de la nube**. Este enfoque brinda flexibilidad para ofrecer todas las tecnologías actuales y nuevas del CISP a los usuarios en tiempo real, y proporciona a los usuarios un rápido acceso a los recursos que precisen cuando sea necesario. También se adapta a la fluctuación de la demanda, lo que se traduce en un uso optimizado y bajos costes.

Las organizaciones del sector público pueden agregar más partidas para pedidos desde otros lotes en un marco de nube, en el caso de que necesiten servicios de consultoría, profesionales o administrados, software de un marketplace, servicios de soporte en la nube y formación sobre las ofertas del CISP.

Se puede dotar de una flexibilidad contractual adicional utilizando partidas contractuales opcionales dentro de las categorías de recursos adecuadas para dejar las puertas abiertas a un crecimiento en el futuro. Opcionalmente, si una organización desea agrupar tecnologías de la nube con servicios de consultoría,

profesionales o administrados en una misma partida, se puede hacer con una partida como "Tecnologías de la nube y trabajos auxiliares".

A continuación se muestra un ejemplo representativo de este enfoque. En el ejemplo siguiente, cada unidad de la partida número 1001 de Tecnologías de la nube equivale a 1 € de las "Tecnologías de la nube" utilizadas. Cada mes, los incrementos de pedidos se pueden basar en las estimaciones de uso actuales y previstas.

Tabla 3: Ejemplo de estructura de precios de partidas individuales.

Nº DE ARTÍCULO	SUMINISTROS/SERVICIOS	CANTIDAD	UNIDAD	PRECIO UNITARIO	TOTAL
1001	Tecnologías de la nube	1000	Por unidad	1 €	1000 €
1002	Servicios de consultoría	1	Por semana	3000 €	3000 €
1003	Asistencia en la nube	1	Por mes	1000 €	1000 €
1004	Formación en la nube	1	Por día	3,00 €	3000 €
1005	Marketplace de la nube	10	Por unidad	10 €	100 €

Ejemplo del funcionamiento de esta estructura: una organización del sector público se pone en contacto con un CISP para calcular cuántos servicios de tecnologías de la nube necesitará utilizar la organización. La organización acepta los términos del proveedor de 10 millones de euros en un plazo de 5 años, lo que equivale a 2 millones de euros por año. La organización asigna un importe anual inicial de 2 millones de euros. Cada mes se emite una factura y el dinero se retira del fondo para pagarla. Se realiza una retirada de fondos de esa cuenta. En los fondos restantes se monitoriza la tasa de gasto mediante las herramientas de monitorización y previsión del CISP. Si los fondos restantes son bajos, la organización solicita fondos adicionales al director financiero que pueden asignarse al mantenimiento de los servicios.

Texto de la licitación de ejemplo: precios - contratación

CONDICIONES DE PAGO

Las condiciones de pago deben estructurarse según corresponda de manera que se paguen únicamente los recursos utilizados por ***<ORGANIZACIÓN>,*** *como se indica a continuación:*

1. *El pago mensual se debe basar en el uso o consumo real de los servicios y según el precio públicamente disponible del CISP.*

GARANTÍA MÍNIMA Y GASTO MÁXIMO

Dado que le resultará imposible a ***<ORGANIZACIÓN>*** *determinar con exactitud el volumen de recursos que se consumirá de un proveedor de servicios en la nube específico a lo largo de un periodo de tiempo, los pedidos se especificarán como cantidades de unidad de precio fijo de una partida de pedido individual de "Tecnologías de la nube".*

Cada unidad de la partida pedida equivaldrá a ***<1,00 €>*** *de las Tecnologías de la nube pedidas. Periódicamente se realizarán pedidos incrementales mediante una modificación de este pedido con diferentes cantidades para dotar a* ***<ORGANIZACIÓN>*** *de flexibilidad para realizar pedidos anticipados de diversas cantidades en "euros" de tecnologías de la nube del CISP según el uso estimado para necesidades de duración variable.* ***<ORGANIZACIÓN>*** *realizará pedidos anticipados de cantidades de forma periódica en cantidad suficiente para cubrir el coste estimado de las tecnologías de nube que se utilizarán para cubrir una serie de necesidades.*

Nº de artículo	Descripción	Cantidad	Unidad	Precio
01	Tecnologías de la nube del CISP	1000	Por unidad	1000,00 €

PEDIDO MÍNIMO Y PEDIDO INCREMENTAL

Se realizarán pedidos de forma periódica por diversas cantidades de <10 000> unidades de la partida en función del uso de tecnologías de nube estimado por <ORGANIZACIÓN>. Este acuerdo dotará a <ORGANIZACIÓN> de flexibilidad para realizar pedidos anticipados de <10 000> unidades de "Tecnologías de la nube" según sea necesario para respaldar las operaciones y mantener una coherencia con las prácticas comerciales de "pago por uso".

Se solicitará un incremento inicial de <100 000> unidades con un coste de <100 000 €> cuando se realice el pedido abierto. El número mínimo de unidades de partidas totales que se puede solicitar en un pedido incremental utilizando una o varias partidas es <x>. El número máximo de unidades que se pueden solicitar en el pedido no puede superar las <x>, pero a su vez no se debe exceder nunca el valor del pedido abierto cuando se combina con todas las unidades pedidas previamente.<ORGANIZACIÓN> será responsable de garantizar que todos los pedidos estén dentro de los límites especificados en esta sección.

MÁXIMO DEL PEDIDO

El valor máximo total del pedido es de <x> y debe constar de un máximo de < x> unidades de una única partida con un precio de <x> por unidad. Este valor se basa es una estimación de las necesidades de <ORGANIZACIÓN> durante el periodo de ejecución, pero no está garantizado.

3.3 Conocimiento del modelo empresarial basado en socios

Las entidades del sector público deben intentar comprender los modelos bajo los cuales los CISP realizan sus ofertas, así como reconocer que los socios que ofrecen servicios de consultoría, servicios administrados o de distribución, entre muchos otros, son fundamentales en el proceso. Muchos clientes requieren un proveedor de nube por su infraestructura y subcontratan el "trabajo práctico" de planificación, migración y administración a un integrador de sistemas o a un proveedor de servicios administrados. Debido a esta mezcla de "servicios", es posible que algunos requisitos no sean aplicables a los proveedores de nube, como las cláusulas de responsabilidad solidaria con los subcontratistas.

Tomando estas cláusulas de responsabilidad solidaria para ilustrar por qué es importante conocer cómo operan los socios y los distribuidores en relación con los CISP, en algunos tipos de adquisiciones existen cláusulas que exigen que el primer contratista aplique determinadas cláusulas obligatorias a todos sus socios o subcontratistas. Normalmente, los CISP no proporcionarán ni ofrecerán como socios subcontratistas formales un servicio estandarizado a gran escala que no esté adaptado a los requisitos únicos de un cliente final en particular (incluyendo las necesidades de un cliente del sector público bajo un contrato del sector público). En un modelo de adquisición indirecto (de adquisición de servicios en la nube a través de un distribuidor del CISP), el CISP puede rechazar dichas cláusulas de su distribuidor como no aplicables a un proveedor de "segundo nivel" de servicios comerciales. En este caso, el CISP no realiza el volumen de trabajo por sí mismo bajo contrato; en lugar de ello, un socio del CISP utiliza la infraestructura del CISP para realizarlo. Por lo tanto, el CISP es un proveedor comercial (no un subcontratista) de las operaciones de un socio. En un modelo de adquisición directo (compra de servicios en la nube directamente del CISP), el CISP rechazaría normalmente estas cláusulas "obligatorias" adecuadas para un subcontratista de productos de consumo normal debido al carácter comercial de los servicios contratados y al hecho de que la mayoría de los CISP no requieren subcontratistas para suministrar sus servicios comerciales.

3.4 Intermediarios en la nube

El concepto de "intermediario en la nube" como modo de reducir la posibilidad de dependencia de un proveedor puede ser problemático. Aunque un intermediario en la nube puede ser una idea acertada en teoría, en la práctica aportaría más complejidad y confusión que valor tangible.

Intentar diseñar aplicaciones para que funcionen en varias nubes de forma simultánea o intercambiable da lugar inevitablemente a concesiones en capacidad (no existe una piedra Rosetta para la nube). Este enfoque puede sumar en definitiva una capa innecesaria de complejidad entre los clientes del sector público y sus servicios en la nube, lo cual podría comprometer las eficiencias y las mejoras en seguridad que espera obtener (dando lugar a una reducción de la escalabilidad y la agilidad, un aumento de los costes y la desaceleración de la innovación).

3.5 Recursos y estudio de mercado previo a la licitación

Cuando una entidad del sector público planifica una licitación de recursos en la nube, debe incluir las partes interesadas de todos los aspectos de la organización: el personal directivo, los involucrados en el negocio, la tecnología, las finanzas, las adquisiciones, los aspectos legales y los contratos del proceso. Este enfoque garantiza que todas las partes interesadas comprenden el modelo de nube y que, por tanto, tienen una visión formada que les permita replantear los métodos de adquisición de TI tradicionales.

En cuanto al diálogo con el sector, recomendamos encarecidamente que las entidades del sector público dediquen tiempo a mantener conversaciones para recabar información del sector: los CISP, los socios del CISP, los proveedores de marketplace de PaaS o SaaS y los expertos del sector. Por ejemplo, dicho diálogo puede adoptar la forma de jornadas del sector o seminarios de seguridad y adquisiciones. Otra forma eficaz de adquirir un profundo conocimiento sobre la adquisición de la nube es realizar una licitación o elaborar un documento borrador de licitación. A menudo incluyen problemas potenciales que se pueden identificar, discutir y ajustar antes de que se emita la licitación finalizada de servicios en la nube.

Apéndice A: Requisitos técnicos para la comparación entre licitantes

A continuación se muestra una lista de los requisitos de tecnología de nube genéricos que se podrían utilizar para comparar a los CISP durante los pedidos abiertos o las minilicitaciones en un acuerdo marco de nube.

1. Perfil del proveedor de nube

	Requisito
1.	***EXPERIENCIA EN EL MERCADO:*** *¿Cuántos años ha estado operando el proveedor de nube en el segmento de mercado de la nube?*
2.	***APERTURA Y PROTECCIÓN DE DATOS:*** *¿Se ciñe el proveedor de nube a los códigos de conducta del sector sobre protección de datos o reversibilidad? ¿Se ciñe el proveedor de nube a los principios de desarrollo de código abierto y API abierta?*

2. Infraestructura global

	Requisito
1.	***ALCANCE GLOBAL:*** *¿Ofrece el proveedor de nube una infraestructura global para ayudar a los usuarios a lograr una baja latencia y un alto rendimiento?*
2.	***REGIONES:*** *¿Tiene el proveedor de nube presencia regional en las regiones geográficas necesarias?*
3.	***DOMINIOS O ZONAS:*** *¿Implementa el proveedor de nube el concepto de dominios o zonas en las que se agrupan varios centros de datos mediante una red de baja latencia para ofrecer un mayor grado de alta disponibilidad y tolerancia a errores?* • *En caso afirmativo, indique el número de dominios o zonas y el número de centros de datos dentro de la región geográfica necesaria.*
4.	***DISTANCIA DE LOS DOMINIOS O ZONAS:*** *¿Ha creado el proveedor de nube sus dominios o zonas con centros de datos separados físicamente para ofrecer redundancia, una alta disponibilidad y una baja latencia?*
5.	***CENTROS DE DATOS CREADOS:*** *¿Ofrece el proveedor de nube centros de datos diseñados para que queden aislados de los errores en otros centros de datos con alimentación redundante, refrigeración y redes?*
6.	***REPLICACIÓN EN CENTROS DE DATOS:*** *¿Ofrece el proveedor de servicios replicación de datos en todos los centros de datos dentro de un domino o una zona con conmutación automática por error?*
7.	***REPLICACIÓN EN DOMINIOS O ZONAS:*** *¿Ofrece el proveedor de nube replicación de datos en todos los dominios o las zonas dentro de una región?*

3. Infraestructura

3.1 Computación

	Requisito
1.	***COMPUTACIÓN – INSTANCIA NORMAL – USO GENERAL:*** *¿Ofrece el proveedor de nube los siguientes tipos de instancia?* • *Uso general: optimizada para las aplicaciones genéricas; proporciona un equilibrio de recursos de computación, memoria y redes.* ○ *En caso afirmativo, ¿cuál es la instancia de mayor tamaño?*
2.	***COMPUTACIÓN – INSTANCIA NORMAL – OPTIMIZADA PARA LA MEMORIA:*** *¿Ofrece el proveedor de nube los siguientes tipos de instancia?* • *Optimizada para la memoria: optimizada para aplicaciones con un uso intensivo de la memoria.* ○ *En caso afirmativo, ¿cuál es la instancia de mayor tamaño?*
3.	***COMPUTACIÓN – INSTANCIA NORMAL – OPTIMIZADA PARA COMPUTACIÓN:*** *¿Ofrece el proveedor de nube los siguientes tipos de instancia?* • *Optimizada para computación: optimizada para aplicaciones de proceso intensivo.* ○ *En caso afirmativo, ¿cuál es la instancia de mayor tamaño?*
4.	***COMPUTACIÓN – INSTANCIA NORMAL – ALMACENAMIENTO OPTIMIZADO:*** *¿Ofrece el proveedor de nube los siguientes tipos de instancia?* • *Almacenamiento optimizado: ofrece una gran capacidad de almacenamiento local.* ○ *En caso afirmativo, ¿cuál es la capacidad de almacenamiento máxima (p. ej., 5, 10, 20, 50 TB) y el número máximo de discos (HDD o SSD) que pueden aprovisionarse y asociarse a una instancia?*
5.	***COMPUTACIÓN – INSTANCIA NORMAL – OPTIMIZADA PARA GRÁFICOS:*** *¿Ofrece el proveedor de nube los siguientes tipos de instancia?* • *Gráficos de bajo coste: ofrece aceleración de gráficos de bajo coste en las instancias de computación.* ○ *En caso afirmativo, ¿cuál es la instancia de mayor tamaño?*
6.	***COMPUTACIÓN – INSTANCIA NORMAL – OPTIMIZADA PARA GPU:*** *¿Ofrece el proveedor de nube los siguientes tipos de instancia?* • *GPU: ofrece unidades de procesamiento de gráficos (GPU) de hardware para aplicaciones con un uso intensivo de gráficos.* ○ *En caso afirmativo, ¿cuántas GPU y qué modelos de GPU puede ofrecer el proveedor de nube por instancia?*
7.	***COMPUTACIÓN – INSTANCIA NORMAL – OPTIMIZADA PARA FPGA:*** *¿Ofrece el proveedor de nube los siguientes tipos de instancia?* • *FPGA: ofrece matrices de puerta programables de campos (FPGA, Field Programmable Gate Arrays) para el desarrollo y la implementación de aceleración de hardware personalizado para las aplicaciones.* ○ *En caso afirmativo, ¿cuántas FPGA puede ofrecer el proveedor de nube por instancia?*
8.	***COMPUTACIÓN – INSTANCIA FLEXIBLE:***

	¿Ofrece el proveedor de nube instancias flexibles que proporcionen un nivel de línea base de rendimiento de Central Processing Unit (CPU, Unidad central de procesamiento) con capacidad para irrumpir sobre la línea base? • *En caso afirmativo, ¿cuál es la instancia con mayor capacidad de irrupción?*
9.	*COMPUTACIÓN – INSTANCIA DE E/S INTENSIVA:* *¿Ofrece el proveedor de nube instancias que utilicen Solid State Drives (SSD, Unidades de estado sólido) de Non-volatile Memory Express (NVMe, Memoria no volátil Express optimizada para baja latencia), un rendimiento de E/S aleatorio muy alto y un rendimiento de lectura secuencial alto?* • *En caso afirmativo, ¿cuál es la capacidad máxima de Input/Output Operations per Second* (IOPS, Operaciones de entrada o salida por segundo) de la instancia de mayor tamaño?
10.	*COMPUTACIÓN – ALMACENAMIENTO LOCAL TEMPORAL:* *¿Ofrece el proveedor de nube almacenamiento local para que las instancias de computación se puedan utilizar como almacenamiento temporal de la información que cambia con frecuencia?*
11.	*COMPUTACIÓN – COMPATIBILIDAD CON VARIAS NIC:* *¿Admite el proveedor de nube varias tarjetas Network Interface Card (NIC, Tarjeta de interfaz de red), primaria y adicional, que se puedan asignar a una instancia determinada?* • *En caso afirmativo, ¿cuál es el número máximo de tarjetas NIC por instancia?*
12.	*COMPUTACIÓN – AFINIDAD DE INSTANCIAS:* *¿Ofrece el proveedor de nube a los usuarios la capacidad de agrupar instancias de forma lógica dentro del mismo centro de datos?*
13.	*COMPUTACIÓN – ANTIAFINIDAD DE INSTANCIAS:* *¿Ofrece el proveedor de nube a los usuarios la capacidad de agrupar instancias de forma lógica y situarlas en diferentes centros de datos dentro de una región?*
14.	*COMPUTACIÓN – APROVISIONAMIENTO DE AUTOSERVICIO:* *¿Ofrece el proveedor de nube un aprovisionamiento de autoservicio de múltiples instancias de forma simultánea a través de una interfaz programática, una consola de administración o un portal web?*
15.	*COMPUTACIÓN – PERSONALIZACIÓN:* *¿Ofrece el proveedor de nube instancias personalizables; por ejemplo, la capacidad de modificar ajustes de configuración como Virtual Central Processing Units (vCPU, Unidades centrales de procesamiento virtual) y Random Access Memory (RAM, Memoria de acceso aleatorio)?*
16.	*COMPUTACIÓN – TENENCIA:* *¿Ofrece el proveedor de nube instancias de un solo inquilino que se ejecuten en hardware dedicado a un solo usuario?* • *En caso afirmativo, ¿cuál es la instancia de un solo inquilino de mayor tamaño disponible?*
17.	*COMPUTACIÓN – AFINIDAD DEL ANFITRIÓN:* *¿Ofrece el proveedor de nube la capacidad de ejecutar una instancia y de especificar que dicha instancia siempre se reinicie en el mismo anfitrión físico?*
18.	*COMPUTACIÓN – ANTIAFINIDAD DEL ANFITRIÓN:* *¿Ofrece el proveedor de nube la capacidad de dividir y hospedar instancias específicas en los diferentes anfitriones físicos?*
19.	*COMPUTACIÓN – ESCALADO AUTOMÁTICO:* *¿Ofrece el proveedor de nube la capacidad de aumentar automáticamente el número de instancias durante los picos de demanda para mantener el rendimiento (p. ej., "escalar horizontalmente").*
20.	*COMPUTACIÓN – MECANISMO DE IMPORTACIÓN DE IMÁGENES:*

	¿Ofrece el proveedor de nube a los usuarios la capacidad de importar sus imágenes existentes y de guardarlas como imágenes nuevas de forma privada que pueden utilizarse para aprovisionar instancias en el futuro? • *En caso afirmativo, ¿cuáles son los formatos admitidos?*
21.	*COMPUTACIÓN – MECANISMO DE EXPORTACIÓN DE IMÁGENES:* *¿Ofrece el proveedor de nube la capacidad de tomar una instancia de ejecución existente o una copia de una instancia y exportarla a un formato de máquina virtual?* • *En caso afirmativo, ¿cuáles son los formatos admitidos?*
22.	*COMPUTACIÓN – INTERRUPCIÓN DEL SERVICIO:* *¿Ofrece el proveedor de nube la capacidad de programar eventos para las instancias del usuario, como el reinicio, la parada, el inicio o la retirada de la instancia?*
23.	*COMPUTACIÓN – REINICIO DE INSTANCIAS:* *¿Ofrece el proveedor de nube mecanismos para reiniciar las instancias de forma automática en un anfitrión en buen estado si falla el anfitrión físico original?*
24.	*COMPUTACIÓN – NOTIFICACIONES:* *Si se produce un evento de computación resistente, ¿tiene el proveedor de nube la capacidad de notificar al usuario que se ha producido dicho evento? Además, ¿puede el usuario participar en esta comunicación o salir de ella mediante opciones de autoservicio?*
25.	*COMPUTACIÓN – PROGRAMACIÓN DE EVENTOS:* *¿Ofrece el proveedor de nube la capacidad de programar de programar eventos para las instancias del usuario, como el reinicio, la parada, el inicio o la retirada de la instancia?*
26.	*COMPUTACIÓN – MECANISMO DE COPIA DE SEGURIDAD Y RESTAURACIÓN:* *¿Ofrece el proveedor de nube un mecanismo integrado de copia de seguridad y recuperación?*
27.	*COMPUTACIÓN – MECANISMO DE CAPTURA:* *¿Ofrece el proveedor de nube un mecanismo manual de captura bajo demanda?*
28.	*COMPUTACIÓN – METADATOS:* *¿Ofrece el proveedor de nube un servicio de metadatos de instancia que permita a los usuarios definir pares clave-valor arbitrarios para la instancia?*
29.	*COMPUTACIÓN – LLAMADA DE METADATOS:* *¿Ofrece el proveedor de nube un servicio de metadatos de instancia que proporcione una interfaz de programación de aplicaciones (API) que pueda llamar la instancia para buscar información sobre sí misma?*
30.	*COMPUTACIÓN – MECANISMO DE OFERTA:* *¿Ofrece el proveedor de nube un mecanismo de oferta para ofertar instancias de coste más bajo que se puedan instanciar de forma inmediata para cargas de trabajo no esenciales del anfitrión?*
31.	*COMPUTACIÓN – MECANISMO DE PROGRAMACIÓN:* *¿Ofrece el proveedor de nube algún modo de programar y reservar capacidad de computación adicional de manera periódica (p. ej., una programación diaria, semanal o mensual)?*
32.	*COMPUTACIÓN – MECANISMO DE RESERVA:* *¿Ofrece el proveedor de nube algún modo de reservar capacidad de computación adicional para el futuro (p. ej., 1 año, 2 años, 3 años, etc.)?*
33.	*COMPUTACIÓN – SISTEMA OPERATIVO LINUX:*

	¿Es compatible el proveedor de nube con las dos últimas versiones admitidas a largo plazo de al menos una distribución de Linux empresarial (como Red Hat y SUSE) y una distribución gratuita de Linux de uso generalizado (como Ubuntu, CentOS y Debian)?
34.	***COMPUTACIÓN – SISTEMA OPERATIVO WINDOWS:*** *¿Es compatible el proveedor de nube con las dos principales versiones más recientes de Windows Server (Windows Server 2017 y Windows Server 2016)?*
35.	***COMPUTACIÓN – PORTABILIDAD DE LICENCIA:*** *¿Ofrece el proveedor de nube portabilidad y soporte para licencias?* • *En caso afirmativo, indique el proveedor de software, los nombres del software, las ediciones y sus versiones.*
36.	***COMPUTACIÓN – LÍMITES DEL SERVICIO:*** *¿Establece el proveedor de nube alguna restricción (p. ej., límites del servicio) en cuanto a la sección de computación anterior?* *Ejemplo:* *Número máximo de instancias por cuenta* *Número máximo de anfitriones dedicados por hora* *Número máximo de direcciones de protocolo de Internet (IP)*

3.2 Redes

	Requisito
1.	***REDES – REDES VIRTUALES:*** *¿Ofrece el proveedor de nube la capacidad de crear una red virtual lógica aislada que represente a la propia red de la empresa en la nube?*
2.	***REDES – CONECTIVIDAD EN LA MISMA REGIÓN:*** *¿Admite el proveedor de nube la conexión de dos redes virtuales dentro de la misma región para enrutar el tráfico entre ellas mediante direcciones de protocolo de Internet (IP)?*
3.	***REDES – CONECTIVIDAD ENTRE DIFERENTES REGIONES:*** *¿Admite el proveedor de nube la conexión de dos redes virtuales de diferentes regiones para enrutar el tráfico entre ellas mediante direcciones de protocolo de Internet (IP)?*
4.	***REDES – SUBRED PRIVADA:*** *¿Ofrece el proveedor de nube la capacidad de crear redes y subredes virtuales completamente aisladas (privadas) en las que se puedan aprovisionar las instancias sin utilizar ninguna dirección pública de protocolo de Internet (IP) ni enrutamiento de Internet?*
5.	***REDES – RANGO DE DIRECCIONES DE RED VIRTUAL:*** *¿Admite el proveedor de nube los rangos de direcciones de protocolo de Internet (IP) especificados en la Solicitud de comentarios (RFC) 1918 así como bloques de enrutamiento entre dominios sin clases (CIDR) que se pueden enrutar públicamente?*
6.	***REDES – VARIOS PROTOCOLOS:*** *¿Admite el proveedor de nube varios protocolos como Transmission Control Protocol (TCP, Protocolo de control de transmisión), User Datagram Protocol (UDP, Protocolo de datagramas de usuario) e Internet Control Message Protocol (ICMP, Protocolo de mensajes de control de Internet)?*

7.	***REDES – ASIGNACIÓN AUTOMÁTICA DE DIRECCIONES IP:*** *¿Ofrece el proveedor de nube la capacidad de asignar automáticamente direcciones públicas de protocolo de Internet (IP) a las instancias?*
8.	***REDES – DIRECCIONES IP ESTÁTICAS RESERVADAS*** *¿Admite el proveedor de nube direcciones del protocolo de Internet (IP) asociadas a la cuenta de usuario, y no a una instancia determinada? La dirección IP debe permanecer asociada a la cuenta hasta que se emita de forma explícita.*
9.	***REDES – COMPATIBILIDAD CON IPV6:*** *¿Admite el proveedor de nube Internet Protocol version 6 (IPv6, Protocolo de Internet versión 6) con respecto a gateway o a instancia y expone esta funcionalidad a los usuarios?*
10.	***REDES – VARIAS DIRECCIONES IP POR NIC:*** *¿Ofrece el proveedor de nube la capacidad de asignar una dirección de protocolo de Internet (IP) primaria y secundaria a una tarjeta de interfaz de red (NIC) asociada a una instancia determinada?*
11.	***REDES – VARIAS NIC:*** *¿Ofrece el proveedor de nube la capacidad de asignar varias tarjetas de interfaz de red (NIC) a una instancia determinada?*
12.	***REDES – MOVILIDAD DE NIC E IP:*** *¿Ofrece el proveedor de nube la capacidad de mover las tarjetas de interfaz de red (NIC) así como las direcciones de protocolo de Internet (IP) entre instancias?*
13.	***REDES – COMPATIBILIDAD CON SR-IOV:*** *¿Ofrece el proveedor de nube capacidades como la virtualización de entrada/salida de raíz única (SR-IOV) para un mayor rendimiento (p. ej., paquetes por segundo [PPS]), una latencia más baja y menor vibración?*
14.	***REDES – FILTRADO DE ENTRADA:*** *¿Permite el proveedor de nube agregar o eliminar reglas aplicables al tráfico de entrada a las instancias?*
15.	***REDES – FILTRADO DE SALIDA:*** *¿Permite el proveedor de nube agregar o eliminar reglas aplicables al tráfico de salida que se origina en las instancias?*
16.	***REDES – ACL:*** *¿Ofrece el proveedor de nube acceso a las listas de control de acceso (ACL) para controlar el tráfico entrante y saliente a las subredes?*
17.	***REDES – COMPATIBILIDAD CON REGISTRO DE FLUJO:*** *¿Ofrece el proveedor de nube la capacidad de capturar los registros de flujo de tráfico de red?*
18.	***REDES – NAT:*** *¿Proporciona el proveedor de red un servicio administrado de gateway de traducción de direcciones de red (NAT) en una red privada para conectarse a Internet o a otros servicios en la nube, pero que evite que Internet inicie una conexión con dichas instancias?*
19.	***REDES – COMPROBACIÓN DE ORIGEN O DESTINO:*** *¿Tiene el proveedor de nube la capacidad de desactivar la comprobación de origen o destino en las tarjetas de interfaz de red (NIC)?*
20.	***REDES – COMPATIBILIDAD CON VPN:*** *¿Ofrece el proveedor de nube conectividad Virtual Private Network (VPN, Red privada virtual) entre el proveedor de nube y el centro de datos del usuario?*
21.	***REDES – TÚNELES DE VPN:***

	¿Admite el proveedor de nube varias conexiones de redes privadas virtuales (VPN) por red virtual?
22.	*REDES – COMPATIBILIDAD CON VPN IPSEC:* *¿Permite el proveedor de nube a los usuarios acceder a los servicios en la nube a través de un túnel de red privada virtual (VPN) con protocolo de seguridad de Internet (IPsec) o un túnel de red privada virtual (VPN) con Secure Sockets Layer (SSL, Capa de sockets seguros)?*
23.	*REDES – COMPATIBILIDAD CON BGP:* *¿Utiliza el proveedor de nube el protocolo de gateway fronteriza (BGP) para mejorar la conmutación por error en los túneles de red privada virtual (VPN) con protocolo de seguridad de Internet (IPsec)?*
24.	*REDES – CONECTIVIDAD PRIVADA DEDICADA:* *¿Ofrece el proveedor de nube un servicio de conectividad privada directa entre las ubicaciones del proveedor de nube y el centro de datos, la oficina o el entorno de ubicación de un usuario que permita transferencias de datos rápidas y de gran volumen?*
25.	*REDES – BALANCEADOR DE CARGA FRONT-END:* *¿Ofrece el proveedor de nube un servicio de balanceador de carga de front-end (con conexión a Internet) que tome las solicitudes de los clientes a través de Internet y las distribuya entre las instancias que están registradas con el balanceador de carga?*
26.	*REDES – BALANCEADOR DE CARGA BACK-END:* *¿Ofrece el proveedor de nube un servicio de balanceador de carga back-end (privado) que enrute el tráfico hacia instancias alojadas en subredes privadas?*
27.	*REDES – BALANCEADOR DE CARGA DE 7 CAPAS:* *¿Ofrece el proveedor de nube un servicio de balanceador de carga de 7 capas (Hypertext Transfer Protocol [HTTP, Protocolo de transferencia de hipertexto]) que pueda balancear la carga del tráfico de red en varias instancias?*
28.	*REDES – BALANCEADOR DE CARGA DE 4 CAPAS:* *¿Ofrece el proveedor de nube un servicio de balanceador de carga de 4 capas (transmission control protocol [TCP, protocolo de control de transmisión]) que pueda balancear la carga del tráfico de red en varias instancias?*
29.	*REDES – AFINIDAD DE SESIÓN DE BALANCEADORES DE CARGA:* *¿Ofrece el proveedor de nube un servicio de balanceo de carga que admita la afinidad de sesión?*
30.	*REDES – BALANCEO DE CARGA BASADO EN DNS:* *¿Ofrece el proveedor de nube un servicio de balanceo de carga que pueda balancear la carga del tráfico a las instancias alojadas en varios anfitriones que pertenecen a un único dominio?*
31.	*REDES – REGISTROS DE BALANCEADOR DE CARGA:* *¿Proporciona el proveedor de nube registros que capturen información detallada sobre todas las solicitudes enviadas a un balanceador de carga?*
32.	*REDES – DNS:* *¿Ofrece el proveedor de nube un servicio Domain Name System (DNS, Sistema de nombres de dominio)?*
33.	*REDES – ENRUTAMIENTO DE DNS BASADO EN LA LATENCIA:* *¿Ofrece el proveedor de nube un servicio de sistema de nombres de dominio (DNS) que admita un enrutamiento basado en la latencia (p. ej., el servicio DNS responde las consultas de DNS con los recursos que proporcionan la mejor latencia)?*
34.	*REDES – ENRUTAMIENTO DE DNS BASADO EN EL ÁREA GEOGRÁFICA:* *¿Ofrece el proveedor de nube un servicio de sistema de nombres de dominio (DNS) que admita un enrutamiento*

	basado en el área geográfica (p. ej., el servicio DNS responde las consultas de DNS según la ubicación geográfica de los usuarios)?
35.	*REDES – ENRUTAMIENTO DE DNS BASADO EN LA CONMUTACIÓN POR ERROR:* *¿Ofrece el proveedor de nube un servicio de sistema de nombres de dominio (DNS) que admita un enrutamiento basado en la conmutación por error (p. ej., el servicio DNS enruta las consultas de DNS hacia el recurso actualmente activo, mientras que un segundo recurso espera y solo se activa si se produce un error en el recurso principal)?*
36.	*REDES – SERVICIO DE REGISTRO DE DOMINIOS:* *¿Ofrece el proveedor de nube servicios de registro de nombres de dominio (p. ej., que permitan a los usuarios buscar y registrar nombres de dominio disponibles)?*
37.	*REDES – COMPROBACIONES DE ESTADO DE DNS:* *¿Ofrece el proveedor de nube un servicio de sistema de nombres de dominio (DNS) que utilice comprobaciones de estado para monitorizar el estado y el rendimiento de los recursos?*
38.	*REDES – INTEGRACIÓN DEL DNS Y EL BALANCEADOR DE CARGA:* *¿Ofrece el proveedor de nube un servicio de sistema de nombres de dominio (DNS) que se integre con el balanceador de carga del proveedor de nube?*
39.	*REDES – EDITOR VISUAL:* *¿Ofrece el proveedor de nube una herramienta que permita a los usuarios crear políticas de administración del trafico?*
40.	*RED DE ENTREGA DE CONTENIDO (CDN):* *¿Ofrece el proveedor de nube un servicio Content Delivery Network (CDN, Red de entrega de contenido) para distribuir contenido con baja latencia y altas velocidades de transferencia de datos?*
41.	*REDES – VENCIMIENTO DE LA CACHÉ DE CDN:* *¿Ofrece el proveedor de nube un servicio de red de entrega de contenido (CDN) que permita eliminar un objeto de las cachés perimetrales antes de que caduque, y con funciones como la invalidación de objetos y el control de versiones de objetos?*
42.	*REDES – ORÍGENES EXTERNOS DE CDN:* *¿Ofrece el proveedor de nube un servicio de red de entrega de contenido (CDN) que admita un origen personalizado; p. ej., un servidor de protocolo de transferencia de hipertexto (HTTP)?*
43.	*REDES – OPTIMIZACIÓN DE CDN:* *¿Ofrece el proveedor de nube un servicio de red de entrega de contenido (CDN) con control detallado para configurar varios servidores de origen y almacenar en caché las propiedades de diferentes Uniform Resource Locator (URL, Localizador Uniforme de Recursos)?*
44.	*REDES – CDN CON RESTRICCIÓN GEOGRÁFICA:* *¿Ofrece el proveedor de nube un servicio de red de entrega de contenido (CDN) que admita la restricción geográfica; p. ej., para impedir que los usuarios de determinadas regiones geográficas accedan al contenido?*
45.	*REDES – TOKENS DE CDN:* *¿Ofrece el proveedor de nube un servicio de red de entrega de contenido (CDN) que admita localizadores uniformes de recursos (URL) firmados que incluyan normalmente información adicional, como la fecha y hora de vencimiento, para dotar a los usuarios de mayor control sobre el acceso a su contenido?*

46.	***REDES – CERTIFICADOS DE CDN:*** *¿Ofrece el proveedor de nube un servicio de red de entrega de contenido (CDN) que admita certificados de capa de sockets seguros (SSL) para entregar el contenido de forma segura mediante un protocolo de transferencia de hipertexto (HTTPS) seguro desde ubicaciones de borde?*
47.	***REDES – CACHÉ MULTICAPA DE CDN:*** *¿Ofrece el proveedor de nube un servicio de red de entrega de contenido (CDN) que utilice un enfoque de caché de varias capas con el uso de cachés de borde regional para reducir la latencia?*
48.	***REDES – COMPRESIÓN DE CDN:*** *¿Ofrece el proveedor de nube un servicio de red de entrega de contenido (CDN) que admita la compresión de archivos?*
49.	***REDES – CARGAS CIFRADAS DE CDN:*** *¿Ofrece el proveedor de nube un servicio de red de entrega de contenido (CDN) que permita a los usuarios cargar su información confidencial de forma segura de manera que dicha información solo puedan verla determinados componentes y servicios en la infraestructura original del usuario?*
50.	***REDES – PUNTOS DE ENLACE:*** *¿Ofrece el servicio de red del proveedor de nube a los usuarios puntos de enlace que puedan enrutar el tráfico a través de la conectividad de red interna del proveedor (p. ej., conectividad privada) para reducir los costes de las comunicaciones y mejorar la seguridad del tráfico?*
51.	***REDES – LÍMITES DEL SERVICIO:*** *¿Establece el proveedor de nube alguna restricción (p. ej., límites del servicio) en cuanto a la sección de redes anterior?* *Ejemplo:* *Número máximo de redes virtuales por cuenta* *Tamaño máximo de la red virtual* *Número máximo de subredes por cuenta* *Número máximo de balanceadores de carga por cuenta* *Número máximo de entradas de la lista de control de acceso (ACL)* *Número máximo de túneles de red privada virtual (VPN)* *Número máximo de orígenes por distribución* *Número máximo de certificados por balanceador de carga*

3.3 Almacenamiento

	Requisito
1.	***SERVICIO DE ALMACENAMIENTO EN BLOQUES:*** *¿Ofrece el proveedor de nube volúmenes de almacenamiento con respecto a bloques para utilizarlos con las instancias de computación?*
2.	***ALMACENAMIENTO EN BLOQUES – IOPS:*** *¿Ofrece el proveedor de nube la opción de comprar un objetivo de rendimiento explícito o un nivel de rendimiento en volúmenes de almacenamiento en bloques, como un determinado número de operaciones de entrada y salida por segundo (IOPS) o de megabites por segundo (MB/S) de rendimiento?*
3.	***ALMACENAMIENTO EN BLOQUES – UNIDADES DE ESTADO SÓLIDO:***

	¿Admite el proveedor de nube medios de almacenamiento de copia de seguridad en unidades de estado sólido (SSD) que ofrezcan latencias en milisegundos de un solo dígito? • *En caso afirmativo, ¿cuál es el número máximo de SSD que se puede asociar por instancia?*
4.	*ALMACENAMIENTO EN BLOQUES – ESCALADO:* *¿Ofrece el proveedor de nube a los usuarios la capacidad de aumentar el tamaño de un volumen de almacenamiento en bloques existente sin tener que aprovisionar un nuevo volumen ni copiar o mover los datos?*
5.	*ALMACENAMIENTO EN BLOQUES – INSTANTÁNEAS:* *¿Dispone el proveedor de nube de capacidad de instantáneas para su servicio de almacenamiento en bloques?*
6.	*ALMACENAMIENTO EN BLOQUES – ERRADICACIÓN DE DATOS:* *¿Ofrece el proveedor de nube la erradicación completa de datos de manera que los usuarios no autorizados o terceras partes ya no puedan leer estos datos ni acceder a ellos?*
7.	*ALMACENAMIENTO DE DATOS – CIFRADO EN REPOSO:* *¿Ofrece el proveedor de nube cifrado de datos en reposo del lado del servidor para datos almacenados en volúmenes y sus instantáneas?* • *En caso afirmativo, ¿cuál es el algoritmo de cifrado empleado?*
8.	*SERVICIO DE ALMACENAMIENTO DE OBJETOS:* *¿Ofrece el proveedor de nube un almacenamiento de objetos altamente escalable, duradero y seguro para almacenar y recuperar cualquier cantidad de datos desde la web?*
9.	*ALMACENAMIENTO DE OBJETOS – ACCESO POCO FRECUENTE:* *¿Ofrece el proveedor de nube un nivel de servicio de almacenamiento a un coste más bajo destinado al almacenamiento de objetos y archivos a los que se accede con menor frecuencia?*
10.	*ALMACENAMIENTO DE OBJETOS – MENOR DURABILIDAD:* *¿Ofrece el proveedor de nube un nivel de redundancia reducido en el que el usuario puede almacenar objetos no esenciales fácilmente reproducibles a un precio más bajo?*
11.	*ALMACENAMIENTO DE OBJETOS – ACCESO MENOS FRECUENTE:* *¿Ofrece el proveedor de nube un nivel para datos a los que se accede con una frecuencia menor pero que siguen precisando un acceso rápido?*
12.	*ALMACENAMIENTO DE OBJETOS – NIVELES DE OBJETOS:* *¿Ofrece el proveedor de nube la capacidad de organización en niveles para el almacenamiento de objetos; p. ej.: la capacidad de recomendar la transición de un objeto entre clases o niveles de almacenamiento de objetos en función de su frecuencia de acceso?*
13.	*ALMACENAMIENTO DE OBJETOS – ADMINISTRACIÓN DEL CICLO DE VIDA:* *¿Ofrece el proveedor de nube la administración del ciclo de vida de un objeto mediante el uso de una configuración de ciclo de vida que define cómo se administran los objetos durante su ciclo de vida, desde la creación hasta la eliminación?*
14.	*ALMACENAMIENTO DE OBJETOS – ADMINISTRACIÓN CONTROLADA POR POLÍTICAS:* *¿Ofrece el proveedor de nube la capacidad de crear y usar políticas para administrar los datos almacenados, su ciclo de vida y la configuración de sus niveles?*
15.	*ALMACENAMIENTO DE OBJETOS – POLÍTICAS BASADAS EN LA UBICACIÓN Y LA HORA:* *¿Ofrece el proveedor de nube a los usuarios la capacidad de crear políticas que puedan restringir el acceso a los datos en función de la ubicación y la hora de solicitud del usuario?*
16.	*ALMACENAMIENTO DE OBJETOS – ALOJAMIENTO DE SITIOS WEB:*

	¿Permite el proveedor de nube el alojamiento de sitios web estáticos fuera de su servicio de almacenamiento de objetos?
17.	*ALMACENAMIENTO DE OBJETOS – CIFRADO EN REPOSO:* *¿Admite el proveedor de nube cifrado del lado del servidor (SSE) de datos en reposo, en el que el proveedor de nube administra las claves de cifrado?* • *En caso afirmativo, ¿cuál es el algoritmo de cifrado empleado?*
18.	*ALMACENAMIENTO DE OBJETOS – CIFRADO CON CLVES DE USUARIO:* *¿Ofrece el proveedor de nube capacidades de cifrado del lado del servidor (SSE) utilizando las claves criptográficas suministradas por el cliente?*
19.	*ALMACENAMIENTO DE OBJETOS – SERVICIO ADMINISTRADO DE CLAVES:* *¿Admite el proveedor de nube cifrado del lado del servidor (SSE) utilizando un servicio de administración de claves que permita crear claves de cifrado, definir las políticas que controlan cómo se puede utilizar estas claves y auditar el uso de las claves para comprobar que se utilizan correctamente?*
20.	*ALMACENAMIENTO DE OBJETOS – CLAVE MAESTRA DEL LADO CLIENTE:* *¿Ofrece el proveedor de nube a los usuarios la opción de conservar el control de las claves de cifrado y completar el cifrado o descifrado de los objetos del lado cliente?*
21.	*ALMACENAMIENTO DE OBJETOS – ALTA COHERENCIA:* *¿Es compatible el proveedor de nube con la coherencia de lectura después de escritura para las operaciones PUT de nuevos objetos?*
22.	*ALMACENAMIENTO DE OBJETOS – LOCALIDAD DE LOS DATOS:* *¿Ofrece el proveedor de nube un sólido aislamiento regional, de modo que los objetos almacenados en una región nunca salgan de ella a menos que el usuario los transfiera explícitamente a otra región?*
23.	*ALMACENAMIENTO DE OBJETOS – REPLICACIÓN:* *¿Ofrece el proveedor de nube una función de replicación interregional que permita replicar automáticamente los objetos entre las regiones seleccionadas por el usuario?*
24.	*ALMACENAMIENTO DE OBJETOS – CONTROL DE VERSIONES:* *¿Admite el proveedor de nube el control de versiones (p. ej. la capacidad de almacenar y mantener varias versiones de un objeto)?*
25.	*ALMACENAMIENTO DE OBJETOS – MARCADOR DE RECUPERACIÓN:* *¿Permite el proveedor de nube al usuario marcar un elemento como recuperable?*
26.	*ALMACENAMIENTO DE OBJETOS – ELIMINACIÓN CON MFA:* *¿Admite el proveedor de nube la autenticación de factor múltiple (MFA) para las operaciones de eliminación como opción de seguridad adicional?*
27.	*ALMACENAMIENTO DE OBJETOS – CARGA EN VARIAS PARTES:* *¿Admite el proveedor de nube la carga de un objeto como un conjunto de partes en el que cada parte es una porción contigua de los datos del objeto y estas partes del objeto se pueden cargar de forma independiente y en cualquier orden?*
28.	*ALMACENAMIENTO DE OBJETOS – ETIQUETAS:* *¿Ofrece el proveedor de nube la capacidad de crear y asociar etiquetas dinámicas mutables en el nivel de objeto?*

29.	***ALMACENAMIENTO DE OBJETOS – NOTIFICACIONES:*** *¿Ofrece el proveedor de nube la capacidad de enviar notificaciones cuando se producen determinados eventos en el nivel de objeto (p. ej., operaciones de adición o eliminación)?*
30.	***ALMACENAMIENTO DE OBJETOS – REGISTROS:*** *¿Ofrece el proveedor de nube la capacidad de generar registros de auditoría que incluyan detalles sobre una solicitud de acceso individual, como el solicitante, la hora de solicitud, la acción de solicitud, el estado de la respuesta y el código de error?*
31.	***ALMACENAMIENTO DE OBJETOS – INVENTARIO DE OBJETOS:*** *¿Ofrece el proveedor de nube una capacidad de inventario de objetos que permita a los usuarios visualizar rápidamente los objetos y su estado de modo que puedan encontrar rápidamente los objetos con acceso público?*
32.	***ALMACENAMIENTO DE OBJETOS – INVENTARIO DE METADATOS:*** *¿Ofrece el proveedor de nube una capacidad de inventario de objetos que permita a los usuarios visualizar rápidamente los metadatos de los objetos?*
33.	***ALMACENAMIENTO DE OBJETOS – OPTIMIZACIÓN DE CARGAS:*** *¿Tiene el proveedor de nube la capacidad de enrutar los datos desde la ubicación de borde hasta el servicio de almacenamiento utilizando una ruta de red optimizada?*
34.	***ALMACENAMIENTO DE OBJETOS – CAPACIDAD DE CONSULTA:*** *¿Ofrece el proveedor de nube la capacidad de consultar su servicio de almacenamiento de objetos mediante instrucciones de lenguaje de consulta estructurado (SQL)?*
35.	***ALMACENAMIENTO DE OBJETOS – RECUPERACIÓN DE SUBCONJUNTOS:*** *¿Ofrece el proveedor de nube a los usuarios la capacidad de recuperar solo un subconjunto de datos desde un objeto mediante expresiones simples de lenguaje de consulta estructurado (SQL)?*
36.	***SERVICIO DE ALMACENAMIENTO DE ARCHIVOS:*** *¿Ofrece el proveedor de nube un servicio de almacenamiento de archivos sencillo y escalable para utilizarlo con las instancias de computación en la nube?*
37.	***ALMACENAMIENTO DE ARCHIVOS – REDUNDANCIA:*** *¿Almacena el proveedor de nube los objetos del sistema de archivos (p. ej., directorio, archivo y enlace) de forma redundante en varios centros de datos o instalaciones para lograr mayores niveles de disponibilidad y durabilidad?*
38.	***ALMACENAMIENTO DE ARCHIVOS – ERRADICACIÓN DE DATOS:*** *¿Admite el proveedor de nube la erradicación completa de datos de almacenamiento de archivos de manera que los usuarios no autorizados o terceras partes ya no puedan leer estos datos ni acceder a ellos?*
39.	***ALMACENAMIENTO DE ARCHIVOS – ALTA DISPONIBILIDAD:*** *¿Proporciona el sistema de archivos administrados del proveedor de nube un alto grado de alta disponibilidad?*
40.	***ALMACENAMIENTO DE ARCHIVOS – NFS:*** *¿Admite el proveedor de nube el protocolo Network File System (NFS, Sistema de archivos de red)?*
41.	***ALMACENAMIENTO DE ARCHIVOS – SMB:*** *¿Admite el proveedor de nube el protocolo server message block (SMB, bloque de mensajes del servidor)?*
42.	***ALMACENAMIENTO DE DATOS – CIFRADO EN REPOSO:*** *¿Es compatible el servicio de almacenamiento de archivos del proveedor de nube con el cifrado en reposo?*

43.	***ALMACENAMIENTO DE ARCHIVOS – CIFRADO EN TRÁNSITO:*** *¿Es compatible el servicio de almacenamiento de archivos del proveedor de nube con el cifrado de datos en tránsito?*
44.	***ALMACENAMIENTO DE ARCHIVOS – HERRAMIENTA DE MIGRACIÓN DE DATOS:*** *¿Ofrece el proveedor de nube alguna herramienta de migración de datos que permita a los usuarios mover datos desde sistemas locales al sistema de archivos basado en la nube?*
45.	***SERVICIO DE ALMACENAMIENTO DE ARCHIVOS:*** *¿Ofrece el proveedor de nube un nivel de servicio de almacenamiento a un coste muy bajo destinado al almacenamiento de objetos y archivos casi inmutables a los que se accede con menor frecuencia?*
46.	***ALMACENAMIENTO DE ARCHIVOS – TOLERANCIA A ERRORES:*** *¿Ofrece la arquitectura del proveedor de nube tolerancia a errores para su servicio de almacenamiento de archivado?*
47.	***ALMACENAMIENTO DE ARCHIVOS – INMUTABILIDAD:*** *¿Ofrece el proveedor de nube inmutabilidad para los objetos y los archivos archivados?*
48.	***ALMACENAMIENTO DE ARCHIVOS – WORM:*** *¿Ofrece el proveedor de nube la capacidad de una sola escritura y lectura múltiple (WORM)?*
49.	***ALMACENAMIENTO DE ARCHIVOS – RECUPERACIÓN DE SUBCONJUNTOS:*** *¿Ofrece el proveedor de nube a los usuarios la capacidad de recuperar solo un subconjunto de datos desde un objeto archivado mediante expresiones simples de lenguaje de consulta estructurado (SQL)?*
50.	***ALMACENAMIENTO DE ARCHIVOS – VELOCIDAD DE RECUPERACIÓN:*** *¿Ofrece el proveedor de nube a los usuarios varias opciones de recuperación de datos con diferentes costes y tiempos de recuperación?*
51.	***ALMACENAMIENTO DE ARCHIVOS – CIFRADO EN REPOSO:*** *¿Es compatible el servicio de almacenamiento de archivos del proveedor de nube con el cifrado en reposo?*
52.	***ALMACENAMIENTO – LÍMITES DEL SERVICIO:*** *¿Establece el proveedor de nube alguna restricción (p. ej., límites del servicio) en cuanto a la sección de almacenamiento anterior?* *Ejemplo:* *Tamaño de volumen máximo* *Número máximo de unidades de disco asociadas a una instancia* *Máximo de operaciones de entrada o salida por segundo (IOPS)* *Tamaño de objeto máximo* *Número máximo de objetos por cuenta de almacenamiento* *Número máximo de instantáneas*

4. Administración

	Requisito
1.	***ADMINISTRACIÓN – USUARIOS Y GRUPOS:*** *¿Ofrece el proveedor de nube un servicio para crear y administrar usuarios y grupos de su infraestructura y recursos?*

2.	***ADMINISTRACIÓN – RESTABLECIMIENTO DE CONTRASEÑA:*** *¿Permite el proveedor de nube a los usuarios restablecer su propia contraseña en modo de autoservicio?*
3.	***ADMINISTRACIÓN – PERMISOS:*** *¿Ofrece el proveedor de nube la capacidad de agregar permisos a usuarios y grupos en el nivel de recursos?*
4.	***ADMINISTRACIÓN – PERMISOS TEMPORALES:*** *¿Ofrece el proveedor de nube la capacidad de crear permisos que sean válidos para un intervalo de tiempo específico?*
5.	***ADMINISTRACIÓN – CRECENCIALES TEMPORALES:*** *¿Ofrece el proveedor de nube a los usuarios la capacidad de crear y proporcionar credenciales de seguridad temporales a los usuarios de confianza configuradas para una duración entre unos minutos y varias horas?*
6.	***ADMINISTRACIÓN – CONTROL DE ACCESO:*** *¿Ofrece el proveedor de nube controles de acceso específicos a los recursos de su infraestructura?* • *En caso afirmativo, ¿qué condiciones pueden utilizar estos controles (p. ej., hora del día, dirección IP de origen, etc.)?*
7.	***ADMINISTRACIÓN – POLÍTICAS INTEGRADAS:*** *¿Contiene la infraestructura del proveedor de nube políticas de acceso integradas que se pueden asociar a usuarios y grupos?*
8.	***ADMINISTRACIÓN – POLÍTICAS PERSONALIZADAS:*** *¿Permite la infraestructura del proveedor de nube crear y personalizar políticas de control de acceso que se puedan asociar a usuarios y grupos?*
9.	***ADMINISTRACIÓN – SIMULADOR DE POLÍTICAS:*** *¿Ofrece el proveedor de nube un mecanismo para probar los efectos de las políticas de control de acceso antes de remitir dichas políticas a producción?*
10.	***ADMINISTRACIÓN – MFA DE NUBE:*** *¿Admite el proveedor de nube el uso de autenticación multifactor (MFA) como capa adicional de control de acceso y autenticación para su infraestructura?*
11.	***ADMINISTRACIÓN – LÍMITES DEL SERVICIO:*** *¿Establece el proveedor de nube alguna restricción (p. ej., límites del servicio) en cuanto a la sección de administración anterior?* *Ejemplo:* *Número máximo de usuarios* *Número máximo de grupos* *Número máximo de políticas administradas*

5. Seguridad

	Requisito
1.	***SEGURIDAD – COMPROBACIONES DE ANTECEDENTES:*** *¿Están sujetos a comprobaciones de antecedentes todos los miembros del personal del proveedor de nube que tienen acceso al servicio de infraestructura (tanto físico como no físico)?*
2.	***SEGURIDAD – ACCESO FÍSICO:***

	¿Restringe el proveedor de nube que el personal acceda al servicio de infraestructura a menos que haya una notificación de avería, una solicitud de cambio o una autorización formal similar?
3.	*SEGURIDAD – REGISTROS DE ACCESO:* *¿Registra el proveedor de nube el acceso del personal a su infraestructura, donde dicho acceso siempre se registra y los registros se conservan por un mínimo de 90 días?*
4.	*SEGURIDAD – INICIOS DE SESIÓN EN EL ANFITRIÓN:* *¿Restringe el proveedor de nube que el personal inicie sesión en los anfitriones de computación, en lugar de automatizar todas las tareas realizadas en los anfitriones de computación donde se registran los contenidos de dichos trabajos automatizados y los registros se conservan un mínimo de 90 días?*
5.	*SEGURIDAD – CLAVES CRIPTOGRÁFICAS:* *¿Ofrece el proveedor de nube un servicio para crear y controlar las claves criptográficas que se utilizan para cifrar datos de usuarios?*
6.	*SEGURIDAD – ADMINISTRACIÓN DE CLAVES DE ACCESO:* *¿Ofrece el proveedor de nube la capacidad de identificar cuándo se ha utilizado por última vez una clave de acceso, rotar las claves antiguas y eliminar a los usuarios inactivos?*
7.	*SEGURIDAD – CLAVES PROPORCIONADAS POR EL CLIENTE:* *¿Permite el proveedor de nube a los usuarios importar claves de su propia infraestructura de administración de claves al servicio de administración de claves del proveedor de servicios en la nube?*
8.	*SEGURIDAD – INTEGRACIÓN DEL SERVICIO DE CLAVES CRIPTOGRÁFICAS:* *¿Se integra el servicio de administración de claves del proveedor de nube con otros servicios de nube para ofrecer la capacidad de cifrados de datos en reposo?*
9.	*SEGURIDAD – HSM:* *¿Ofrece el proveedor de nube módulos de seguridad de hardware (HSM) dedicados; por ejemplo, dispositivos de hardware que proporcionen almacenamiento de claves de seguridad y operaciones criptográficas dentro de un módulo de hardware resistente a prueba de manipulaciones?*
10.	*SEGURIDAD – DURABILIDAD DE LAS CLAVES CRIPTOGRÁFICAS:* *¿Ofrece el proveedor de nube durabilidad de claves, como el almacenamiento de varias copias de modo que las claves estén disponibles cuando sea necesario?*
11.	*SEGURIDAD – SSO:* *¿Ofrece el proveedor de nube un servicio administrado de inicio de sesión único (SSO) que permita a los usuarios administrar de manera centralizada el acceso a varias cuentas y aplicaciones empresariales?*
12.	*SEGURIDAD – CERTIFICADOS:* *¿Ofrece el proveedor de nube un servicio administrado para aprovisionar, administrar e implementar certificados de capa de sockets seguros (SSL) o de seguridad de la capa de transporte (TLS)?*
13.	*SEGURIDAD – RENOVACIÓN DE CERTIFICADOS:* *¿Facilita el servicio de administración de certificados del proveedor de nube la renovación de los certificados?*
14.	*SEGURIDAD – CERTIFICADOS DE COMODÍN:* *¿Admite el servicio de administración de certificados del proveedor de nube el uso de certificados comodín?*
15.	*SEGURIDAD – ENTIDAD DE CERTIFICACIÓN:* *¿Actúa el servicio de administración de certificados del proveedor de nube asimismo como entidad de certificación (CA)?*
16.	*SEGURIDAD – ACTIVE DIRECTORY:*

	¿Ofrece el proveedor de nube un servicio administrado de Active Directory (AD) de Microsoft en la nube?
17.	***SEGURIDAD – ACTIVE DIRECTORY LOCAL:*** *¿Admite el servicio administrado de Active Directory (AD) de Microsoft del proveedor de nube la integración con Active Directory (AD) de Microsoft local?*
18.	***SEGURIDAD – LADP:*** *¿Es compatible el servicio administrado de Active Directory (AD) de Microsoft del proveedor de nube con el protocolo ligero de acceso a directorios (LDAP)?*
19.	***SEGURIDAD – ACTIVE DIRECTORY:*** *¿Es compatible el servicio administrado de Active Directory (AD) de Microsoft del proveedor de nube con el lenguaje de marcado de aserción de seguridad (SAML)?*
20.	***SEGURIDAD – ADMINISTRACIÓN DE CREDENCIALES:*** *¿Ofrece el proveedor de nube un servicio administrado que ayude a los usuarios a rotar, administrar y recuperar credenciales fácilmente, como las claves de la interfaz de programación de aplicaciones (API), las credenciales de base de datos y otros secretos?*
21.	***SEGURIDAD – WAF:*** *¿Ofrece el proveedor de nube un cortafuegos de aplicación web (WAF) que ayude a proteger las aplicaciones web de ataques comunes de web que podrían afectar a la disponibilidad de la aplicación, comprometer la seguridad o consumir excesivos recursos?*
22.	***SEGURIDAD – DDOS:*** *¿Ofrece el proveedor de nube un servicio para protegerse de los ataques comunes más frecuentes de denegación distribuida de servicio (DDoS) que se producen en la red y en la capa de transporte, además de la capacidad de escribir reglas personalizadas para mitigar ataques sofisticados en la capa de aplicación?*
23.	***SEGURIDAD – RECOMENDACIONES DE SEGURIDAD:*** *¿Ofrece el proveedor de nube un servicio para evaluar de forma automática las vulnerabilidades potenciales en las aplicaciones y los recursos?*
24.	***SEGURIDAD – DETECCIÓN DE AMENAZAS:*** *¿Ofrece el proveedor de nube un servicio administrado de detección de amenazas?*
25.	***SEGURIDAD – LÍMITES DEL SERVICIO:*** *¿Establece el proveedor de nube alguna restricción (p. ej., límites del servicio) en cuanto a la sección de seguridad anterior?* *Ejemplo:* *Número máximo de claves maestras de cliente* *Número máximo de módulos de seguridad de hardware (HSM)*

6. Cumplimiento de normas

La lista siguiente tiene un fin meramente ilustrativo y no aspira a ser una lista exhaustiva de las certificaciones y los estándares que pueden aplicarse a los servicios en la nube.

Indique el conjunto de estándares de conformidad internacionales y específicos del sector que cumple el proveedor de nube.

Certificaciones y atestaciones	*Leyes, normativas y privacidad*	*Conformidad y marcos*
☐ *C5 [Alemania]*	☐ *Directiva de protección de datos de la UE*	☐ *CDSA*
☐ *Código de conducta de protección de datos de CISPE*	☐ *Cláusulas modelo de la UE*	
☐ *DIACAP*	☐ *FERPA*	☐ *CIS*
☐ *DoD SRG Niveles 2 y 4*	☐ *RGPD*	☐ *Información de justicia criminal Servicio (CJIS)*
☐ *FedRAMP*	☐ *GLBA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *HIPAA*	☐ *Escudo de privacidad entre la UE y los EE. UU.*
☐ *HDS (Francia, atención sanitaria)*	☐ *HITECH*	☐ *Puerto seguro de la UE*
☐ *ISO 9001*	☐ *IRS 1075*	☐ *FISC*
☐ *ISO 27001*	☐ *ITAR*	☐ *FISMA*
☐ *ISO 27017*	☐ *PDPA – 2010 [Malasia]*	☐ *G-Cloud [Reino Unido]*
☐ *ISO 27018*	☐ *PDPA – 2012 [Singapur]*	☐ *GxP (FDA CFR 21 Parte 11)*
☐ *IRAP [Australia]*	☐ *PIPEDA [Canadá]*	☐ *ICREA*
☐ *MTCS Nivel 3 [Singapur]*	☐ *Ley de privacidad [Australia]*	☐ *IT Grundschutz [Alemania]*
☐ *PCI DSS Nivel 1*	☐ *Ley de privacidad [Nueva Zelanda]*	☐ *MARS – E*
☐ *SEC Rule 17-a-4(f)*	☐ *Autorización del DPA español*	☐ *MITA 3.0*
☐ *SOC1 / ISAE 3402*	☐ *DPA del Reino Unido - 1988*	☐ *MPAA*
☐ *SOC2 / SOC3*	☐ *VPAT/Sección 508*	☐ *NIST*
		☐ *Niveles de Uptime Institute*
		☐ *Principios de seguridad de la nube del Reino Unido*

El uso de los informes de conformidad anteriores permite a las organizaciones del sector público evaluar las ofertas individuales con respecto a los estándares aceptados de seguridad, conformidad y operativos. Dichos informes pueden mostrar que el CISP, mediante

su conformidad con ellos, cumple los controles de funcionamiento del centro de datos siguientes que se exigen al proveedor de servicios en la nube pública. La exigencia de conformidad con dichos informes ayuda a las entidades del sector público a tener la seguridad de que se aplican los controles siguientes.

- ***Estricto control de acceso:*** *el CISP debe limitar el acceso físico a aquellas personas que necesiten estar en una ubicación por razones empresariales justificadas. Si se concede acceso, se debe revocar tan pronto como se haya completado el trabajo necesario.*

- ***Entrada controlada y monitorizada:*** *el acceso a la capa perimetral del centro de datos debe ser un proceso controlado. El CISP debe dotar las puertas de entrada de agentes de seguridad y supervisores de empleados que monitoricen a los agentes y visitantes mediante cámaras de seguridad. Cuando haya personas autorizadas en las instalaciones, se les debe entregar una credencial que requiera autenticación de factor múltiple y limite el acceso a las áreas previamente aprobadas.*

- ***Trabajadores de los centros de datos del CISP:*** *los empleados del CISP que necesiten acceder habitualmente a un centro de datos deben obtener permisos para las áreas relevantes de las instalaciones según el puesto de trabajo y bajo un estricto control de acceso de manera regular. Un responsable de acceso al área debe revisar de manera rutinaria las listas de empleados para asegurarse de que la autorización de cada empleado sigue siendo necesaria. Si un empleado no tiene una necesidad continua de estar en el centro de datos, se le debe pedir que siga el proceso para visitantes.*

- ***Monitorización de entrada no autorizada:*** *los CISP deben monitorizar de forma continua las entradas no autorizadas a la propiedad del centro de datos mediante videovigilancia, detección de intrusiones y los sistemas de monitorización de registros de acceso. Las entradas se deben asegurar con dispositivos que hagan sonar alarmas si se fuerza o se mantiene abierta una puerta.*

- ***Los centros de operaciones de seguridad del CISP monitorizan la seguridad global:*** *los centros de operaciones de seguridad del CISP deben estar situados en todo el mundo y ser responsables de monitorizar, clasificar y ejecutar programas de seguridad para los centros de datos del CISP. Deben supervisar la administración del acceso físico y la respuesta a la detección de intrusión al tiempo que proporcionan soporte global de forma ininterrumpida a los equipos de seguridad locales del centro de datos, así como actividades de monitorización continuas, como el seguimiento de actividades de acceso, la revocación de permisos de acceso y estar disponibles para responder a un incidente de seguridad potencial y analizarlo.*

- ***Revisión de acceso capa a capa:*** *se debe restringir el acceso a la capa de infraestructura en función de las necesidades empresariales. Mediante la implementación de una revisión de acceso capa a capa, el derecho de acceso en cada capa no se concede de forma predeterminada. El acceso a una determinada capa solo se debe conceder si hay una necesidad específica de acceder a dicha capa.*

- ***Mantenimiento del equipo como parte de las operaciones habituales:*** *los equipos del CISP deben ejecutar diagnósticos en las máquinas, las redes y el equipo de reserva para asegurarse de que funcionan correctamente en ese momento y en caso de emergencia. Las comprobaciones de mantenimiento rutinarias en el equipo y los servicios del centro de datos deben formar parte de las operaciones habituales de los centros de datos del CISP.*

- ***Equipo de reserva preparado para emergencias:*** *el abastecimiento de agua, el suministro eléctrico, las telecomunicaciones y la conectividad de Internet se deben diseñar con redundancia para que el CISP pueda mantener las operaciones continuas si se produce una emergencia. Los sistemas eléctricos se deben diseñar de modo que sean completamente redundantes para que, en caso de interrupción, se puedan conectar unidades con un sistema de alimentación ininterrumpida para determinadas funciones hasta que los generadores puedan suministrar alimentación de respaldo para las instalaciones completas. Las personas y los sistemas deben monitorizar y controlar la temperatura y la humedad para evitar sobrecalentamientos, para así reducir aún más la posibilidad de que se produzcan interrupciones de servicio.*

- ***La tecnología y las personas trabajan juntas para una mayor seguridad:*** *se deben establecer procedimientos obligatorios para obtener autorización de acceso a la capa de datos. Esto incluye la revisión y la aprobación de la aplicación de acceso de una persona por parte de los sujetos autorizados. Mientras tanto, los sistemas de detección de amenazas e intrusiones electrónicas deben monitorizar y activar automáticamente alertas de amenazas identificadas o actividad sospechosa. Por ejemplo, si una puerta se mantiene abierta o si se fuerza su apertura, se desencadena una alarma. Los CISP deben instalar cámaras de seguridad y guardar las grabaciones en cumplimiento de los requisitos legales y de conformidad.*

- ***Prevención de intrusiones físicas y tecnológicas:*** *los puntos de acceso a las salas de servidores se deben reforzar con dispositivos de control electrónico que precisen autorización de factor múltiple. El CISP también debe estar preparado*

para evitar las intrusiones tecnológicas. Los servidores del CISP deben ser capaces de avisar a los empleados de cualquier intento de eliminar datos. En el caso poco probable de que se produzca una infracción de seguridad, se debe desactivar el servidor de forma automática.

- ***Los servidores y los soportes físicos reciben una atención rigurosa:*** *el CISP debe clasificar como críticos los dispositivos de almacenamiento utilizados para guardar los datos de cliente y tratarlos como corresponda (de alto impacto) a lo largo de su ciclo de vida. El CISP debe aplicar estándares rigurosos relacionados con la instalación, el mantenimiento y, en última instancia, la destrucción de los dispositivos cuando dejen de ser útiles. Cuando un dispositivo de almacenamiento llega al final de su vida útil, el CISP retirará los soportes físicos empleando las técnicas detalladas en NIST 800-88. Los soportes físicos que almacenan datos del cliente no se eliminan de la unidad de control del CISP hasta que se hayan retirado de forma segura.*

- ***Auditores externos verifican los procedimientos y los sistemas del CISP:*** *unos auditores externos deben realizar una auditoría del CISP para inspeccionar los centros de datos, donde deben realizar un análisis detallado para confirmar que el CISP sigue las reglas establecidas necesarias para obtener sus certificaciones de seguridad. En función del programa de conformidad y sus requisitos, los auditores externos podrían entrevistar a los empleados del CISP sobre cómo manipulan y desechan los soportes físicos. Los auditores también podrían ver las transmisiones de la cámara de seguridad y observar las entradas y los pasillos del centro de datos. También podrían examinar equipos como los dispositivos de control de acceso electrónico y las cámaras de seguridad del CISP.*

- ***Preparado para lo inesperado:*** *el CISP debe prepararse de forma proactiva ante posibles amenazas ambientales, como pueden ser los desastres naturales y los incendios. La instalación de sensores automáticos y de equipos sensibles son dos modos de proteger los centros de datos que puede utilizar el CISP. Se deben instalar equipos de detección de agua para avisar a los empleados de la existencia de problemas mientras las bombas automáticas funcionan para retirar el líquido y evitar daños. De igual modo, el equipo de detección y extinción automática de incendios reduce los riesgos y puede informar a los empleados del CISP y a los bomberos de la existencia de un problema.*

- ***Alta disponibilidad mediante varias zonas de disponibilidad:*** *el CISP debe disponer de varias zonas de disponibilidad para ofrecer una mayor tolerancia a errores. Cada zona de disponibilidad debe estar formada por uno o más centros de datos, estar separada físicamente de las demás y contar con alimentación y redes redundantes. Las zonas de disponibilidad deben estar conectadas entre sí mediante redes privadas de fibra óptica rápidas para diseñar aplicaciones que conmuten por error de forma automática entre las zonas de disponibilidad sin interrupción.*

- ***Simulación de interrupciones y medición de la respuesta****: el CISP debe contar con un Plan de continuidad del negocio como guía de proceso de operaciones que describa cómo evitar y reducir las interrupciones causadas por desastres naturales con pasos detallados que se deben seguir antes, durante y después de un evento. Para mitigar y prepararse para lo inesperado, el CISP debe probar el Plan de continuidad del negocio de forma regular con simulacros que recreen diferentes escenarios. El CISP debe documentar cómo responden su personal y los procesos e informar a continuación sobre las lecciones aprendidas y las posibles acciones correctivas que puedan ser necesarias para mejorar la tasa de respuesta. Los empleados del CISP deben estar formados y preparados para recuperarse rápidamente de las interrupciones mediante un proceso de recuperación metódico que minimice el tiempo de inactividad debido a errores.*

- ***Ayudar a cumplir los objetivos de eficiencia energética:*** *además de abordar los riesgos medioambientales, el CISP también debe incorporar consideraciones relativas a la sostenibilidad en el diseño del centro de datos. El CISP debe proporcionar información detallada sobre su compromiso de utilizar energías renovables para sus centros de datos y proporcionar información sobre cómo pueden sus clientes reducir las emisiones de carbono con respecto a sus propios centros de datos.*

- ***Selección de sitio****: antes de seleccionar una ubicación, el CISP debe realiza evaluaciones geográficas y medioambientales iniciales. Las ubicaciones de los centros de datos se deben elegir cuidadosamente para mitigar riesgos medioambientales, como inundaciones, condiciones meteorológicas extremas y actividad sísmica. Las zonas de disponibilidad de los CISP se deben crear de modo que sean independientes y estén separadas físicamente entre ellas.*

- ***Redundancia:*** *se deben diseñar los centros de datos para anticipar y tolerar los errores a la vez que se mantienen los niveles de servicio. En caso de error, los procesos automatizados deben alejar el tráfico de la zona afectada. Las aplicaciones principales se deben implementar según el estándar N+1, de manera que en caso de que se produzca un fallo en el centro de datos, se disponga de capacidad suficiente para balancear la carga del tráfico en los sitios restantes.*

- ***Disponibilidad:*** *el CISP debe identificar los componentes críticos del sistema para mantener la disponibilidad del sistema y recuperar el servicio en caso de interrupción. Se debe realizar una copia de seguridad de los componentes críticos del sistema en varias ubicaciones aisladas. Cada ubicación o zona de disponibilidad se debe diseñar para funcionar de manera*

independiente con una alta fiabilidad. Las zonas de disponibilidad deben estar conectadas para que las aplicaciones puedan conmutar por error de forma automática entre las zonas de disponibilidad sin interrupción. Su alta resistencia y, por tanto, la disponibilidad del servicio, deben ser una característica del diseño del sistema. El diseño del centro de datos con zonas de disponibilidad y replicación de datos debe hacer posible que los clientes del CISP consigan un tiempo de recuperación extremadamente corto y objetivos de punto de recuperación, así como los niveles más altos de disponibilidad del servicio.

- ***Planificación de la capacidad**: el CISP debe monitorizar el uso del servicio de forma continua para implementar la estructura que permita cumplir los compromisos y los requisitos de disponibilidad. El CISP debe mantener un modelo de planificación de capacidad que evalúe el uso y las demandas de infraestructura del CISP al menos mensualmente. Este modelo debe fomentar la planificación de demandas futuras e incluir consideraciones como el procesamiento de la información, las telecomunicaciones y el almacenamiento del registro de auditoría.*

CONTINUIDAD DEL NEGOCIO y RECUPERACIÓN ANTE DESASTRES

- ***Plan de continuidad del negocio:** el Plan de continuidad del negocio del CISP debe describir las medidas para evitar y reducir las interrupciones medioambientales. Debe incluir detalles operativos sobre los pasos que hay que seguir antes, durante y después del evento. El Plan de continuidad del negocio debe estar respaldado por pruebas que incluyan simulaciones de diferentes escenarios. Durante y después de las pruebas, el CISP debe documentar el rendimiento de las personas y el proceso, las acciones correctivas y las lecciones aprendidas teniendo como objetivo la mejora continua.*

- ***Respuesta en caso de pandemia:** el CISP debe incorporar políticas y procedimientos de respuesta a pandemias en su planificación de recuperación ante desastres con el fin de prepararse para responder con rapidez ante amenazas de brotes de enfermedades infecciosas. Las estrategias de mitigación incluyen modelos de empleo de personal alternativos para transferir los procesos críticos a recursos fuera de región, y la activación de un plan de administración de crisis que respalde las operaciones empresariales críticas. Los planes de pandemias deben hacer referencia a los organismos de salud y las normas sanitarias internacionales, incluyendo los puntos de contacto de los organismos internacionales.*

MONITORIZACIÓN y REGISTRO

- ***Revisión del acceso a los centros de datos:** el acceso a los centros de datos se debe revisar de forma regular. Este acceso se revocará de forma automática cuando se dé por terminado el registro de un empleado en el sistema de recursos humanos del CISP. Además, cuando expira el acceso de un empleado o de un contratista de acuerdo con la solicitud de duración aprobada, se debe revocar su acceso incluso aunque siga siendo empleado del CISP.*

- ***Registros de acceso de los centros de datos:** es necesario registrar, monitorizar y conservar el acceso físico a los centros de datos del CISP. El CISP debe correlacionar la información obtenida de sistemas de monitorización lógicos y físicos para mejorar la seguridad según sea necesario.*

- ***Monitorización del acceso a los centros de datos:** el CISP debe monitorizar los centros de datos a través de centros de operaciones de seguridad globales responsables de monitorizar, clasificar y ejecutar programas de seguridad. Estos deben proporcionar soporte global de forma ininterrumpida en la administración y monitorización de las actividades de acceso a los centros de datos, equipando a los equipos locales y otros equipos de soporte para responder ante incidentes de seguridad mediante la clasificación, la consulta, el análisis y el envío de respuestas.*

VIDEOVIGILANCIA y DETECCIÓN

- ***CCTV:** una Closed Circuit Television Camera (CCTV, Cámara de circuito cerrado de televisión) debe grabar los puntos de acceso físico a las salas de servidores . Las imágenes se deben conservar de acuerdo con los requisitos legales y de conformidad.*

- ***Puntos de entrada a los centros de datos:** el acceso físico debe estar controlado en los puntos de entrada del edificio por personal de seguridad profesional que utilice videovigilancia, sistemas de detección y otros medios electrónicos. El personal autorizado debe utilizar mecanismos de autenticación de factor múltiple para acceder a los centros de datos. Las entradas a las salas de los servidores deben estar protegidas con dispositivos que generen alarmas sonoras para iniciar una respuesta a un incidente si se fuerza la puerta o se mantiene abierta.*

- ***Detección de intrusiones:** se deben instalar sistemas electrónicos de detección de intrusiones dentro de la capa de datos para monitorizar, detectar y alertar de forma automática al personal adecuado sobre incidentes de seguridad. Los puntos*

de entrada y salida a las salas de servidores se deben proteger con dispositivos que exijan que cada sujeto proporcione una autenticación de factor múltiple para que se le permita la entrada o la salida. Estos dispositivos generarán alarmas sonoras si se fuerza la apertura de la puerta sin autenticación o si esta se mantiene abierta. Los dispositivos de alarma de puerta se deben configurar para detectar instancias en las que un sujeto sale o entra en una capa de datos sin proporcionar una autenticación de factor múltiple. Las alarmas se deben enviar inmediatamente a los Centros de operaciones de seguridad del CISP, abiertos de forma ininterrumpida, para su registro, análisis y respuesta.

ADMINISTRACIÓN DE DISPOSITIVOS

- ***Administración de recursos:*** *los activos del CISP se deben administrar de forma centralizada mediante un sistema de administración de inventario que almacene y realice un seguimiento de la información sobre el propietario, la ubicación, el estado, el mantenimiento y la descripción de los activos que posee el CISP. Después de su adquisición, es necesario escanear y realizar un seguimiento de los activos, así como comprobar y monitorizar la propiedad, el estado y la resolución de los recursos en mantenimiento.*

- ***Destrucción de soportes físicos:*** *el CISP debe clasificar como críticos los dispositivos de almacenamiento físicos utilizados para guardar los datos de cliente y tratarlos como corresponda (de alto impacto) a lo largo de su ciclo de vida. El CISP debe aplicar estándares rigurosos relacionados con la instalación, el mantenimiento y, en última instancia, la destrucción de los dispositivos cuando dejen de ser útiles. Cuando un dispositivo de almacenamiento llega al final de su vida útil, el CISP debe desinstalar los soportes físicos empleando las técnicas detalladas en NIST 800-88. Los soportes físicos que almacenan datos del cliente no se deben retirar de la unidad de control del CISP hasta que se hayan desmantelado de forma segura.*

SISTEMAS DE SOPORTE OPERATIVO

- ***Suministro eléctrico:*** *los sistemas de suministro eléctrico de los centros de datos del CISP se deben diseñar de modo que sean completamente redundantes y se puedan mantener sin ningún impacto en las operaciones las 24 horas del día. El CISP debe asegurarse de que los centros de datos estén equipados con un suministro eléctrico de reserva con el fin de garantizar que el suministro esté disponible para mantener las operaciones en el caso de que se produzca un fallo eléctrico para cargas críticas y esenciales en las instalaciones.*

- ***Clima y temperatura:*** *los centros de datos del CISP deben utilizar mecanismos para controlar el clima y mantener la temperatura de funcionamiento adecuada para los servidores y otros dispositivos de hardware a fin de evitar sobrecalentamientos y reducir la posibilidad de que se produzcan interrupciones del servicio. El personal y los sistemas deben monitorizar y controlar que se mantienen los niveles adecuados de temperatura y humedad.*

- ***Detección y extinción de incendios****: los centros de datos del CISP deben estar equipados con equipos automáticos de detección y extinción de incendios. Los sistemas de detección de incendios deben utilizar sensores de detección de humo dentro en los espacios de redes, mecánicos y de infraestructura. Estas áreas también deben estar protegidas por sistemas de extinción.*

- ***Detección de fugas:*** *para detectar la presencia de fugas de agua, el CISP debe equipar los centros de datos con una funcionalidad para detectar la presencia de agua. Si se detecta la presencia de agua, se debe disponer de los mecanismos correspondientes para retirarla y evitar de ese modo que se produzcan más daños causados por el agua.*

MANTENIMIENTO DE LA INFRAESTRUCTURA

- ***Mantenimiento del equipo****: el CISP debe monitorizar y llevar a cabo un mantenimiento preventivo del equipo eléctrico y mecánico para mantener la capacidad operativa continua de los sistemas en los centros de datos del CISP. Los procedimientos de mantenimiento del equipo los deben llevar a cabo personas cualificadas y se deben completar de acuerdo con un programa de mantenimiento documentado.*

- ***Administración del entorno:*** *el CISP debe monitorizar los sistemas y los equipos eléctricos y mecánicos para poder identificar los problemas de forma inmediata. Esto se debe realizar mediante el uso de herramientas de auditoría continua y la información que se proporcionan mediante los sistemas de administración de edificios y monitorización eléctrica del CISP. Es necesario llevar a cabo un mantenimiento preventivo para mantener la capacidad operativa continua del equipo.*

GOBERNANZA Y RIESGOS

- ***Administración continua de riesgos de los centros de datos:*** *el Centro de operaciones de seguridad del CISP debe realizar revisiones frecuentes de las amenazas y las vulnerabilidades de los centros de datos. Es necesario realizar una evaluación y mitigación continua de las vulnerabilidades potenciales a través de las actividades de evaluación de riesgos de los centros de datos. Esta evaluación se debe realizar además del proceso de evaluación de riesgos en el nivel de empresa, que se utiliza para identificar y administrar riesgos que se presentan en la empresa en general. Este proceso también debe tener en cuenta los riesgos medioambientales y los relacionados con la normativa regional.*

- ***Certificación de seguridad externa:*** *la comprobación externa de los centros de datos del CISP, como se documenta en los informes de terceros, debe garantizar que el CISP ha implementado correctamente las medidas de seguridad de conformidad con las reglas establecidas necesarias para obtener las certificaciones de seguridad. En función del programa de conformidad y sus requisitos, los auditores externos pueden realizar pruebas de desecho de soportes físicos, revisar las grabaciones de la cámara de seguridad, observar las entradas y los pasillos de un centro de datos, probar los dispositivos de control de acceso electrónico y examinar el equipo del centro de datos.*

7. Migraciones

	Requisito
1.	***SERVICIO DE MIGRACIONES:*** *¿Cuántos servicios diferentes de migración de datos ofrece el proveedor de nube?*
2.	***MIGRACIONES – MONITORIZACIÓN CENTRALIZADA:*** *¿Ofrece el proveedor de nube a las organizaciones un servicio centralizado (p. ej., un único panel de vidrio), donde puedan monitorizar y realizar un seguimiento del estado del servidor y las migraciones de aplicaciones?*
3.	***MIGRACIONES – PANEL:*** *¿Ofrece la herramienta de migración del proveedor de nube un panel para visualizar rápidamente el estado de la migración, las métricas relacionadas y el historial de migraciones?*
4.	***MIGRACIONES – HERRAMIENTAS DEL PROVEEDOR DE NUBE:*** *¿Ofrece la herramienta de migración del proveedor de nube integración con otras herramientas de migración del proveedor de nube que puedan realizar migraciones de servidor y de aplicaciones?*
5.	***MIGRACIONES – HERRAMIENTAS DE TERCEROS:*** *¿Permite la herramienta de migración del proveedor de nube incorporar herramientas de migración de terceros?* • *En caso afirmativo, ¿cuáles son las herramientas de migración de terceros admitidas?*
6.	***MIGRACIONES – MIGRACIONES DE VARIAS REGIONES:*** *¿Ofrece la herramienta de migración del proveedor de nube una capacidad de seguimiento y monitorización de las migraciones de servidor y aplicaciones que se producen en diferentes regiones?*
7.	***MIGRACIONES – MIGRACIÓN DE SERVIDOR:*** *¿Ofrece la herramienta de migración del proveedor de nube un modo de migrar los servidores virtualizados de las instalaciones a la nube?* • *En caso afirmativo, ¿cuáles son los entornos virtualizados admitidos actualmente?*
8.	***MIGRACIONES – DETECCIÓN DE SERVIDORES:*** *¿Tiene la herramienta de migración del proveedor de nube la capacidad de detección que permita buscar automáticamente servidores virtuales de las instalaciones para migrarlos a la nube?*
9.	***MIGRACIONES – DATOS DE RENDIMIENTO DEL SERVIDOR:*** *¿Tiene la herramienta de migración del proveedor de nube la capacidad de recopilar y mostrar el rendimiento del servidor o la máquina virtual como uso de la unidad central de procesamiento (CPU) y la memoria de acceso aleatorio (RAM)?*
10.	***MIGRACIONES – BASE DE DATOS DE DETECCIÓN:***

	¿Tiene la herramienta de migración del proveedor de nube la capacidad de almacenar todos los datos recopilados en una base de datos centralizada? • *En caso afirmativo, ¿tienen las organizaciones la capacidad de exportar estos datos? ¿A qué formatos?*
11.	*MIGRACIONES – CIFRADO EN REPOSO:* *¿Realiza el proveedor de nube el cifrado en reposo de toda la información recopilada y almacenada en la base de datos de detección?*
12.	*MIGRACIONES – REPLICACIÓN INCREMENTAL DEL SERVIDOR:* *¿Ofrece la herramienta de migración del proveedor de nube replicaciones incrementales en directo y automatizadas del servidor durante la migración del servidor o la máquina virtual como modo de respaldar que todos los cambios realizados en el servidor o la máquina virtual se incluyan en la imagen final migrada?* • *En caso afirmativo, ¿durante cuánto tiempo se puede ejecutar este servicio?*
13.	*MIGRACIONES – VMWARE:* *¿Admite la herramienta de migración del proveedor de nube la realización de migraciones de la máquina virtual de VMWare de las instalaciones a la nube?*
14.	*MIGRACIONES – HYPER-V:* *¿Admite la herramienta de migración del proveedor de nube la realización de migraciones de la máquina virtual de Hyper-V de las instalaciones a la nube?*
15.	*MIGRACIONES – DETECCIÓN DE APLICACIONES:* *¿Tiene la herramienta de migración del proveedor de nube la capacidad de detectar y agrupar aplicaciones antes de su migración?*
16.	*MIGRACIONES – ASIGNACIÓN DE DEPENDENCIAS:* *¿Tiene la herramienta de migración del proveedor de nube la capacidad de detectar las dependencias entre los servidores y las aplicaciones antes de su migración?*
17.	*MIGRACIONES – MIGRACIÓN DE BASES DE DATOS:* *¿Tiene la herramienta de migración del proveedor de nube la capacidad de migrar bases de datos de las instalaciones a la nube?*
18.	*MIGRACIONES – TIEMPO DE INACTIVIDAD DE MIGRACIÓN DE BASES DE DATOS:* *¿Tiene la herramienta de migración del proveedor de nube la capacidad de realizar una migración de bases de datos a la nube con un mínimo de tiempo de inactividad (p. ej.: la base de datos de origen debe permanecer completamente operativa durante el proceso de migración)?*
19.	*MIGRACIONES – BASE DE DATOS DE ORIGEN:* *¿Admite la herramienta de migración del proveedor de nube la migración de orígenes de bases de datos diferentes como Oracle, SQL Server, etc.?* • *En caso afirmativo, indique las bases de datos de origen compatibles que se pueden migrar a la nube.*
20.	*MIGRACIONES – MIGRACIONES HETEROGÉNEAS:* *¿Tiene la herramienta de migración del proveedor de nube la capacidad de realizar migraciones de bases de datos heterogéneas (p. ej., de una base de datos de origen a una base de datos de destino diferente, como puede ser de Oracle a SQL Server)?* • *En caso afirmativo, indique todas las combinaciones posibles de migraciones de bases de datos heterogéneas.*
21.	*MIGRACIONES – MIGRACIÓN DE DATOS A ESCALA DE PETABYTES:* *¿Ofrece el proveedor de nube una solución de transporte de datos a escala de petabytes que utilice aplicaciones seguras para transferir grandes volúmenes de datos hacia la nube y desde esta?*

22.	***MIGRACIONES – MIGRACIÓN DE DATOS A ESCALA DE EXABYTES:*** *¿Ofrece el proveedor de nube una solución de transporte de datos a escala de exabytes para mover volúmenes extremadamente grandes de datos a la nube?*
23.	***MIGRACIONES – COPIAS DE SEGURIDAD EMPRESARIALES:*** *¿Ofrece el proveedor de nube un servicio para integrar perfectamente el centro de datos de un cliente con servicios de almacenamiento en la nube que permita transferir y almacenar datos en el servicio de almacenamiento del proveedor de nube?*
24.	***MIGRACIONES – COPIAS DE SEGURIDAD EMPRESARIALES – ALMACENAMIENTO DE OBJETOS:*** *¿Ofrece el servicio de copia de seguridad empresarial del proveedor de nube integración con el servicio de almacenamiento de objetos en la nube del proveedor?*
25.	***MIGRACIONES – COPIAS DE SEGURIDAD EMPRESARIALES – ACCESO A ARCHIVOS:*** *¿Permite el servicio de copia de seguridad empresarial del proveedor de nube a los usuarios almacenar y recuperar objetos utilizando protocolos de archivo como el protocolo de sistema de archivos de red (NFS)?*
26.	***MIGRACIONES – COPIAS DE SEGURIDAD EMPRESARIALES – ACCESO A BLOQUES:*** *¿Permite el servicio de copia de seguridad empresarial del proveedor de nube a los usuarios almacenar y recuperar objetos utilizando protocolos de bloques como el protocolo Internet Small Computer Systems Interface (iSCSI, Interfaz para pequeños sistemas informático de Internet)?*
27.	***MIGRACIONES – COPIAS DE SEGURIDAD EMPRESARIALES – ACCESO A CINTAS:*** *¿Permite el servicio de copia de seguridad empresarial del proveedor de nube a los usuarios realizar copias de seguridad de sus datos mediante una biblioteca de cintas virtuales y almacenar estas copias de seguridad en cintas en la nube del proveedor?*
28.	***MIGRACIONES – COPIAS DE SEGURIDAD EMPRESARIALES – CIFRADO:*** *¿Ofrece el servicio de copia de seguridad empresarial del proveedor de nube cifrado de datos en reposo y en tránsito?*
29.	***MIGRACIONES – COPIAS DE SEGURIDAD EMPRESARIALES – INTEGRACIÓN CON SOFTWARE DE TERCEROS:*** *¿Se integra el servicio de copia de seguridad empresarial del proveedor de nube con el software de copia de seguridad de terceros que se usa habitualmente?*
30.	***MIGRACIONES – LÍMITES DEL SERVICIO:*** *¿Establece el proveedor de nube alguna restricción (p. ej., límites del servicio) en cuanto a la sección de migraciones anterior?* *Ejemplo:* *Número máximo de migraciones simultáneas de máquinas virtuales* *Número máximo de soluciones de transporte de datos que se puede solicitar*

8. Facturación

	Requisito
1.	***FACTURACIÓN – SEGUIMIENTO E INFORMES:*** *¿Ofrece el proveedor de nube un servicio de seguimiento y facturación que ayude a los usuarios a administrar y monitorizar el uso que realizan de las ofertas de nube?*
2.	***FACTURACIÓN – ALARMAS Y NOTIFICACIONES:*** *¿Ofrece el proveedor de nube a los usuarios un mecanismo para configurar alarmas con notificaciones para alertar a los usuarios cuando su gasto ha superado un umbral específico?*

3.	***FACTURACIÓN – ADMINISTRACIÓN DE COSTOS:*** *¿Ofrece el proveedor de nube un mecanismo para crear y mostrar gráficos que resuman los costes y los gastos?*
4.	***FACTURACIÓN – PRESUPUESTOS:*** *¿Ofrece el proveedor de nube un mecanismo para mostrar y administrar presupuestos y hacer previsiones de costes estimados?*
5.	***FACTURACIÓN – VISTA CONSOLIDADA:*** *¿Ofrece el proveedor de nube un mecanismo para consolidar la facturación de varias cuentas en una sola cuenta de pago principal?*
6.	***FACTURACIÓN – LÍMITES DEL SERVICIO:*** *¿Establece el proveedor de nube alguna restricción (p. ej., límites del servicio) en cuanto a la sección de facturación anterior?* *Ejemplo:* *Número máximo de cuentas que se pueden agrupar* *Número máximo de alarmas que se pueden crear* *Número máximo de presupuestos que se pueden administrar*

9. Gestión

	Requisito
1.	***ADMINISTRACIÓN – SERVICIO DE MONITORIZACIÓN:*** *¿Ofrece el proveedor de nube un servicio de monitorización para administrar los recursos y las aplicaciones en la nube que recopila, monitoriza y para los que genera informes empleando métricas predefinidas?*
2.	***ADMINISTRACIÓN – ALARMAS:*** *¿Permite el servicio de monitorización del proveedor de nube a los usuarios configurar alarmas?*
3.	***ADMINISTRACIÓN – MÉTRICAS PERSONALIZADAS:*** *¿Permite el servicio de monitorización del proveedor de nube a los usuarios crear y monitorizar métricas personalizadas?*
4.	***ADMINISTRACIÓN – SERVICIO DE MONITORIZACIÓN:*** *¿Proporciona el servicio de monitorización del proveedor de nube varios niveles de detalle de monitorización hasta el nivel de 1 minuto?*
5.	***ADMINISTRACIÓN – SERVICIO DE SEGUIMIENTO DE API:*** *¿Ofrece el proveedor de nube un servicio que registre, monitorice y almacene la actividad de los recursos de nube tanto con respecto a la consola como a la interfaz de programación de aplicaciones (API) para una mejor visibilidad?* • *En caso afirmativo, ¿cuáles son los servicios del proveedor de nube que se integran con este servicio de seguimiento?*
6.	***ADMINISTRACIÓN – NOTIFICACIÓN:*** *¿Admite el proveedor de nube la capacidad de enviar notificaciones basadas en los niveles de actividad de la interfaz de programación de aplicaciones (API)?*
7.	***ADMINISTRACIÓN – COMPRESIÓN:***

	¿Ofrece el proveedor de nube un mecanismo para comprimir los registros generados por el sistema de seguimiento de la interfaz de programación de aplicaciones (API) para ayudar a los usuarios a reducir los costes de almacenamiento asociados a este servicio?
8.	***ADMINISTRACIÓN – AGREGACIÓN DE REGIONES:*** *¿Ofrece el proveedor de nube la capacidad de registrar la actividad de la interfaz de interfaz de programación de aplicaciones (API) de la cuenta y de presentar esta información de forma agregada para facilitar su uso?*
9.	***ADMINISTRACIÓN – INVENTARIO DE RECURSOS:*** *Ofrece el proveedor de nube un servicio para evaluar y auditar las configuraciones de los recursos implementados por un usuario?*
10.	***ADMINISTRACIÓN – CAMBIOS DE CONFIGURACIÓN:*** *¿Registra el proveedor de nube de forma automática un cambio de configuración de recurso cuando este se produce?*
11.	***ADMINISTRACIÓN – HISTORIAL DE CONFIGURACIÓN:*** *¿Ofrece el proveedor de nube la capacidad de examinar la configuración de recursos en cualquier punto del pasado?*
12.	***ADMINISTRACIÓN – REGLAS DE CONFIGURACIÓN:*** *¿Ofrece el proveedor de nube directrices y recomendaciones para el aprovisionamiento, la configuración y la monitorización continua del cumplimiento de la normativa?*
13.	***ADMINISTRACIÓN – PLANTILLAS DE RECURSOS:*** *¿Ofrece el proveedor de nube a los usuarios la capacidad de crear, aprovisionar y administrar una recopilación de recursos a modo de plantilla?*
14.	***ADMINISTRACIÓN – REPLICACIÓN DE PLANTILLAS DE RECURSOS:*** *¿Ofrece el proveedor de nube la capacidad de replicar rápidamente estas plantillas de recursos en diferentes regiones para su posible uso en situaciones de recuperación ante desastres (DR)?*
15.	***ADMINISTRACIÓN – DISEÑADOR DE PLANTILLAS:*** *¿Ofrece el proveedor de nube una herramienta de gráficos de uso sencillo con funcionalidad de arrastrar y colocar que acelere el proceso de creación de dichas plantillas de recursos?*
16.	***ADMINISTRACIÓN – CATÁLOGO DE SERVICIOS:*** *¿Ofrece el proveedor de nube un servicio para crear y administrar un catálogo de servicios (p. ej., servidores, máquinas virtuales, software, bases de datos, etc.)?*
17.	***ADMINISTRACIÓN – ACCESO DESDE LA CONSOLA:*** *¿Ofrece el proveedor de nube una interfaz de usuario basada en Web para facilitar la administración y monitorización de los servicios en la nube?*
18.	***ADMINISTRACIÓN – ACCESO DESDE CLI:*** *¿Ofrece el proveedor de servicio una herramienta unificada para administrar y configurar varios servicios en la nube desde la command line interface (CLI, interfaz de línea de comandos) que permita automatizar las tareas de administración mediante el uso de scripts?*
19.	***ADMINISTRACIÓN – ACCESO MÓVIL:*** *¿Ofrece el proveedor de nube una aplicación para smartphone que permita a los usuarios conectarse al servicio en la nube y administrar sus recursos?* • *En caso afirmativo, ¿está disponible esta aplicación para iOS y Android?*
20.	***ADMINISTRACIÓN – PRÁCTICAS RECOMENDADAS:*** *¿Tiene el proveedor de nube un servicio que ayude a los usuarios a comparar su uso de la nube en relación con las prácticas recomendadas?*

21.	***ADMINISTRACIÓN – LÍMITES DEL SERVICIO:*** *¿Establece el proveedor de nube alguna restricción (p. ej., límites del servicio) en cuanto a la sección de administración anterior?* *Ejemplo:* *Número máximo de reglas de configuración por cuenta* *Número máximo de alarmas que se pueden crear* *Número máximo de registros que se pueden almacenar*

10. Soporte

	Requisito
1.	***SOPORTE – SERVICIO:*** *¿Ofrece el proveedor de nube soporte en todo momento, las 24 horas al día, los 7 días de la semana y los 365 días del año a través de teléfono, chat y correo electrónico?*
2.	***SOPORTE – NIVELES DE SOPORTE:*** *¿Ofrece el proveedor de nube diferentes niveles de soporte?*
3.	***SOPORTE – ASIGNACIÓN DE NIVELES:*** *¿Permite el proveedor de nube a los usuarios autoasignarse los recursos o los servicios consumidos en diferentes niveles de soporte según una clasificación detallada, en lugar de obligar a los usuarios a mantener cuentas en la nube diferentes para lograr y obtener diferentes niveles de soporte?*
4.	***SOPORTE – FOROS:*** *¿Ofrece el proveedor de nube foros de soporte público donde los clientes pueden comentar problemas?*
5.	***SOPORTE – PANEL DE ESTADO DEL SERVICIO:*** *¿Ofrece el proveedor de nube un panel de estado del servicio que muestre información actualizada sobre la disponibilidad del servicio en varias regiones?*
6.	***SOPORTE – PANEL PERSONALIZADO:*** *¿Ofrece el proveedor de nube un panel que muestre una vista personalizada del rendimiento y la disponibilidad de los servicios subyacentes a los recursos específicos del usuario?*
7.	***SOPORTE – HISTORIAL DEL PANEL:*** *¿Ofrece el proveedor de nube un historial del panel de estado del servicio de 365 días?*
8.	***SOPORTE – ASESOR DE NUBE:*** *¿Ofrece el proveedor de servicio un servicio que actúe como un experto en la nube personalizado que ayude a comparar el uso de recursos en relación con las prácticas recomendadas?*
9.	***SOPORTE – TAM:*** *¿Ofrece el proveedor de nube un Technical account manager (TAM, Director de cuentas técnicas) que proporcione experiencia técnica para la gama completa de servicios en la nube?*
10.	***SOPORTE – SOPORTE PARA APLICACIONES DE TERCEROS:*** *¿Ofrece el proveedor de nube soporte para los sistemas operativos comunes y los componentes de conjuntos de aplicaciones comunes?*
11.	***SOPORTE – API PÚBLICA:***

	¿Ofrece el proveedor de nube una interfaz de programación de aplicaciones (API) que interactúe de forma programática con casos de soporte para crear, editar y cerrar dichos casos?
12.	*SOPORTE – DOCUMENTACIÓN DE LOS SERVICIOS:* *¿Ofrece el proveedor de nube documentación técnica de calidad disponible públicamente para todos sus servicios incluyendo, pero sin limitarse a ellos, guías de usuario, turoriales, preguntas frecuentes y notas de la versión?*
13.	*SOPORTE – DOCUMENTACIÓN DE CLI:* *¿Ofrece el proveedor de nube documentación técnica de calidad disponible públicamente para su Command Line Interface (CLI, Interfaz de línea de comandos)?*
14.	*SOPORTE – ARQUITECTURAS DE REFERENCIA:* *¿Ofrece el proveedor de nube una serie de documentos de arquitectura de referencia online gratuitos para ayudar a los clientes a crear soluciones específicas que combinen muchos de los servicios en la nube del proveedor de nube?*
15.	*SOPORTE – IMPLEMENTACIONES DE REFERENCIA:* *¿Ofrece el proveedor de nube una serie de documentos online gratuitos que contengan procedimientos paso a paso detallados, probados y validados, incluyendo las prácticas recomendadas, para implementar las soluciones comunes (p. ej., DevOps, Big Data, Data Warehouse, cargas de trabajo de Microsoft, cargas de trabajo de SAP, etc.) en sus ofertas de nube?*

Apéndice B: demostración

Con las demostraciones, los usuarios finales disponen de un modo eficaz de probar las ofertas de nube, y permiten a la decisión de adjudicación reflejar el ajuste perfecto para las necesidades empresariales de la organización. A continuación se muestra un ejemplo de guion de prueba de demostración de tecnologías de nube.

1. *Muestre, a grandes rasgos, la consola y las ofertas y recursos del CISP disponibles públicamente:*
    - *Capacidades de almacenamiento*
    - *Capacidades de computación*
    - *Capacidades y tipos de bases de datos*
    - *Redes*
    - *Herramientas de administración y análisis*
    - *Seguridad*
    - *Otras capacidades*
2. *Describa cómo opera las tecnologías de nube utilizadas en la demostración.*
3. *Muestre cómo lleva a cabo esta demostración, en tiempo real, utilizando la oferta de nube.*
4. *Cuentas:*
    - *Describa el sistema de claves de cuenta (raíz y usuario) utilizado en la demostración.*
    - *Muestre cómo administra y protege sus claves de cuenta*
5. *Muestre cómo se puede seleccionar la ubicación física donde se almacenan la carga de trabajo y los datos.*
6. *Muestre la escala de su oferta mediante la configuración de soluciones de computación y almacenamiento a gran escala.*
7. *Ilustre cómo solicita un usuario final varios servicios de las ofertas de nube. Muestre:*
    - *Cómo se establecen las cuentas*
    - *Cómo se realizan las disposiciones de seguridad*
    - *Cuántas cuentas se pueden dividir en subcuentas*
    - *Cómo puede su Identity and Access Management (IAM, Administración de identidades y acceso) separar el acceso a varios recursos:*
        - *Cómo proteger una cuenta*
        - *Crear usuarios y grupos*
        - *Asociar una política*
        - *Configurar contraseñas*
8. *Muestre cómo se pueden aislar los entornos virtuales desde la perspectiva de la seguridad y las redes:*
    - *Crear subredes*
    - *Enrutamiento de Internet*
9. *Muestre cómo puede crear un entorno en dos o más ubicaciones aisladas independientes.*
    - *Muestre el balanceo de carga entre dos entornos.*
10. *Muestre la capacidad de utilizar varios métodos para interactuar con los servicios de computación en la nube (p. ej., la interfaz de programación de aplicaciones [API], la consola web o la línea de comandos).*
11. *Almacenamiento:*
    - *Describa las opciones de almacenamiento*
    - *Muestre los tipos de almacenamiento disponibles (p. ej., bloque, objeto) y los procesos del ciclo de vida de los datos*
    - *Establezca un volumen de almacenamiento y muestre cómo se cargan y recuperan los datos*
    - *Cree un volumen de almacenamiento de XGB con y sin opción de computación*

- *Muestre y valide los permisos para acceder a estos volúmenes:*

12. *Computación:*
    - *Describa las opciones de computación: tamaño y capacidades de los recursos de computación*
    - *Muestre la activación y desactivación, de un recurso de computación*
    - *Muestre las propiedades (capacidad de ejecutar X instancias de forma simultánea, selección de red, protección frente a finalizaciones accidentales, tenencia, etc.)*
    - *Muestre una opción de computación con el equivalente de X núcleos y X GB de RAM*
    - *Muestre el escalado de recursos según la carga mediante la ejecución de una carga de trabajo*
    - *Muestre las capacidades de escalado automático*
    - *Muestre cómo se puede detener y reiniciar posteriormente la computación*
    - *Muestre cómo se puede aumentar o reducir el tamaño de una opción de computación y mantener las configuraciones*
    - *Muestre cómo se puede copiar una opción de computación*
    - *Muestre cómo se configuran los grupos de seguridad*
    - *Describa los sistemas operativos que se encuentran disponibles en la oferta del CISP*
    - *Muestre un ejemplo de instalación del sistema operativo Linux*
    - *Describa sus capacidades para proporcionar imágenes para las ofertas de computación*
    - *¿Qué formatos de imagen admite?*
    - *Muestre cómo cargaría y operaría una imagen*
    - *Muestre la computación sin servidor*
    - *Muestre la capacidad de ejecutar un clúster de instancias de computación con precios variables en función del mercado de spot*
13. *Base de datos:*
    - *Describa sus capacidades de base de datos*
    - *Muestre las capacidades de MySQL, MS SQL Server, Oracle, y Postgres*
    - *Muestre todas las capacidades de almacenamiento de datos*
    - *Muestre las capacidades para realizar copias de seguridad de estos recursos*
14. *Redes: muestre las opciones de red definidas por el software y las capacidades de administración de redes*
15. *Administración y análisis*
    - *Describa las capacidades de administración y análisis de su nube*
    - *Muestre las opciones de monitorización*
    - *Muestre sus capacidades con marcos Hadoop*
16. *Seguridad: muestre la seguridad de la red*
    - *Describa su enfoque sobre seguridad*
    - *Firewalls*
    - *Grupos de seguridad*
    - *Gateways*
    - *NACL*
    - *Registros del sistema*
    - *Cifrado*
    - *Acreditaciones de conformidad disponibles*
    - *Almacenamiento de claves*
    - *Otras características*
17. *Aprovisionamiento: muestre cómo se puede crear un conjunto de recursos de nube relacionados y aprovisionarlos de manera ordenada y predecible mediante una plantilla reutilizable*

18. *Software: muestre sus capacidades para proporcionar acceso al software que se usa comúnmente y utilizarlo*
19. *Muestre cómo se puede realizar una transferencia de datos a gran escala*
20. *Muestre las opciones de facturación, incluyendo:*
    - *Vista de resumen, vista detallada, vista por recursos etiquetados*
    - *Gasto y uso previsto basado en el gasto y el uso actual*
21. *Muestre las capacidades de soporte y consultoría disponibles*
    - *Cuáles son las opciones de soporte disponibles*
    - *¿Se incluyen capacidades para realizar comprobaciones y proporcionar asesoramiento sobre el uso del servicio?*

Muestre cualquier otra característica de la oferta que piense que pueda diferenciarla.