Compra de servicios en la nube en el sector público

Manual con textos de ejemplo de una solicitud de propuesta (RFP) para un acuerdo marco de servicios en la nube

Versión 2: febrero de 2022

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 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 servicios en la nube. Este documento no supone ninguna garantía, manifestación, compromiso contractual, condición ni declaración.

Los ejemplos de documentos y de textos no se deben interpretar como una asesoría legal. Los clientes de la nube deben consultar a sus asesores jurídicos para conocer sus responsabilidades en virtud de la legislación aplicable del país en el que realizan operaciones. CISPE rechaza expresamente toda garantía, responsabilidad o daño asociado que pueda derivarse de la información proporcionada en este documento o esté relacionado con esta.

Acerca de CISPE

Cloud Infrastructure Services Providers in Europe (CISPE, Proveedores de servicios de infraestructura en la nube de Europa; https://cispe.cloud) es un grupo independiente del sector sin ánimo de lucro. Representamos a los proveedores de servicios de infraestructura en la nube de Europa y colaboramos 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.

Entre nuestro número creciente de miembros se incluyen empresas que operan en todos los países de la Unión Europea con sedes centrales en 16 países europeos. La asociación está abierta a todas 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. Juntos:

- Defendemos los beneficios de las políticas de adquisición pública que dan prioridad a la nube en la Unión Europea y los Estados miembros de la Unión Europea.
- Alentamos al sector de la infraestructura en la nube a lograr la neutralidad climática en 2030.
- Promovemos requisitos de seguridad y estándares técnicos coherentes en toda la Unión Europea.
- Apoyamos unos requisitos de privacidad exhaustivos con un código de conducta de protección de datos.
- Trabajamos para mantener el mercado de infraestructuras en la 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 «bloques de creación de TI» esenciales que permiten al gobierno, los organismos públicos y las empresas crear sus propios sistemas y ofrecer servicios esenciales a miles de millones de ciudadanos. De esta forma, 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 conducta de protección de datos de CISPE, lanzado públicamente en septiembre de 2016, se empezó a aplicar antes del Reglamento general de protección de datos (RGPD) de la Unión Europea. Se ajusta a los estrictos requisitos del RGPD, lo que permite a los proveedores de infraestructuras en la nube hacer efectivo el cumplimiento de la protección de datos y ofrecer un marco sólido para que los clientes puedan seleccionar proveedores de servicios en la nube y confiar en sus servicios. El Comité Europeo de Protección de Datos (EDPB) validó el Código de conducta de CISPE en mayo de 2021, y la CNIL francesa, en calidad de autoridad competente, lo aprobó en junio de 2021. https://www.codeofconduct.cloud/

Pacto por la neutralidad climática de los centros de datos

CISPE se comprometió con la Comisión Europea a finales de 2019 a desarrollar un conjunto de métricas y una iniciativa de autorregulación para garantizar la neutralidad climática de los centros de datos en 2030. Esta iniciativa, que se bautizó con el nombre «Pacto por la neutralidad climática de los centros de datos» cuando se lanzó en enero de 2021, la ha desarrollado la asociación

European Data Centre Association (EUDCA) junto con otras asociaciones comerciales y agentes del mercado de centros de datos. https://www.climateneutraldatacentre.net/

Iniciativa de software justo

Junto con la asociación de directores de información (CIO) franceses, CIGREF, y el respaldo de otras asociaciones comerciales de CIO y proveedores de toda Europa, CISPE ha publicado 10 principios de licencias de software justas para clientes que utilizan la nube, un conjunto de las prácticas recomendadas para las empresas que buscan innovación y flexibilidad de crecimiento en la nube. Con estos, CISPE reta a sus proveedores para que garanticen que aplican términos de licencias justos.
https://www.fairsoftware.cloud/

GAIA-X

CISPE fue uno de los veintidós miembros fundadores de GAIA-X, la iniciativa europea para ofrecer un ecosistema digital abierto, transparente y seguro. Desde sus inicios, CISPE se ha comprometido con la visión y los principios de la organización GAIA-X y, en junio de 2021, su secretario general fue reelegido para formar parte de la junta directiva. Algunas de las herramientas a las que se hace referencia en el manual, como el Código de conducta de protección de datos de CISPE y el Código de conducta IaaS de SWIPO, resultan útiles para demostrar el cumplimiento de los principios de GAIA-X. https://www.gaia-x.eu

CISPE y el sector público

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

Si bien los modelos de compra pública deben condicionar el proceso de adopción y uso de la computación en la nube, la adquisición de servicios en la nube difiere de la mayoría de las adquisiciones tecnológicas tradicionales que se conocen en el sector público. Conviene reconsiderar las estrategias 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 que «dan prioridad a la nube». De esta forma, contribuye a impulsar el crecimiento de un mercado único de infraestructuras en la 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 los organismos públicos 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 computación en la nube declarados en virtud del Código de conducta de CISPE:
https://www.codeofconduct.cloud/public-register/

Tabla de contenidos

Avisos 2
Acerca de CISPE 3
Tabla de contenidos 5
Resumen y finalidad de este manual 1
1.0 Información general de un acuerdo marco de servicios en la nube 4
2.0 Información general de la RFP de servicios en la nube 8
2.1 Redacción de una RFP de servicios en la nube 8
2.1.1 Introducción y objetivos estratégicos 8
2.1.2 Calendario de respuesta a la RFP 11
2.1.3 Definiciones 12
2.1.4 Descripción detallada del modelo de compra y competencia en el acuerdo marco 13
2.1.5 Requisitos administrativos mínimos del licitante 17
2.2 Requisitos técnicos 20
2.2.1 Requisitos mínimos 20
2.2.2 Comparación entre proveedores 23
2.2.3 Contratación 25
2.3 Seguridad 27
2.3.1 Requisitos mínimos 27
2.3.2 Comparación entre proveedores 33
2.3.3 Contratación 34
2.4 Precios 34
2.4.1 Requisitos mínimos 35
2.4.2 Comparación entre proveedores 36
2.5 Configuración y términos y condiciones de la suscripción del contrato 39
2.5.1 Términos y condiciones 39
2.5.2 Términos y condiciones del software 42
2.5.3 Cómo seleccionar los adjudicatarios por proyecto 44
2.5.4 Incorporación y baja 44
3.0 Prácticas recomendadas y lecciones aprendidas 45
3.1 Gobernanza de la nube 45
3.2 Elaboración de un presupuesto para la nube 45
3.3 Conocimiento del modelo empresarial basado en socios 47
3.4 Agentes en la nube 48
3.5 Aprovisionamiento y estudio de mercado previos a la RFP 48
3.6 Sostenibilidad 48
Apéndice A: requisitos técnicos para la comparación entre licitantes 50
1. Perfil del proveedor de servicios en la nube 50
2. Infraestructura global 50
3. Infraestructura 51

3.1 Computación 51
3.2 Redes 54
3.3 Almacenamiento 59
4. Administración 63
5. Seguridad 64
6. Cumplimiento de normas 66
7. Migraciones 72
8. Facturación 75
9. Gestión 75
10. Asistencia 77
Apéndice B: evaluación técnica en tiempo real 79
Plataforma: muestra de una evaluación técnica en tiempo real 81
Carga de trabajo: aplicación web; muestra de una evaluación técnica en directo 92

v2 de 2022: febrero

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 **(solicitud de propuesta [RFP] de servicios en la nube)**, pero que carecen de experiencia para redactar un acuerdo marco de servicios en la 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 analiza el texto de los criterios de selección para los **pedidos abiertos** o **minilicitaciones** cuando se realiza la compra a partir de un acuerdo marco de servicios en la nube. Las secciones del manual se organizan de forma similar a una RFP de TI genérica. El ejemplo de la RFP genérica y el texto de los criterios de selección incluyen comentarios que ayudan a comprender por qué una RFP de la nube difiere de una RFP de TI tradicional.

Después de la publicación de la estrategia en la nube de la Comisión Europea que establece cómo las instituciones y agencias europeas modernizarán sus infraestructuras de TI a través de una estrategia que prioriza la nube, CISPE entregó el manual a la Comisión Europea en julio de 2019 durante el evento «*How to transform governments through a smart cloud policy*» (Cómo transformar los gobiernos a través de una política en la nube inteligente).

La **versión 2** de este manual incluye nuevas instrucciones en relación con la protección de datos (sección 2.3.1.1), el cambio de proveedores de servicios en la nube y datos de portabilidad (sección 2.3.1.2), los términos y condiciones de software (sección 2.5.2), la sostenibilidad en la nube (sección 3.6) y una actualización del apéndice B sobre la evaluación técnica en tiempo real.

«Servicios en la nube» *hace referencia a todas las tecnologías de la nube y a los servicios relacionados a los que pueda requerir acceso el usuario final. Incluyen los servicios de consultoría, profesionales o administrados necesarios para permitir y realizar la migración a la nube y admitir las cargas de trabajo en la nube, además de la propia infraestructura en la nube, así como servicios de mercado en la nube, como los productos de software como servicio (SaaS).*

La creciente necesidad de usar la computación en la nube como opción predeterminada para las TI del sector público presenta una oportunidad de modernizar las estrategias de adquisición existentes. Los procesos de adquisición centrados en la nube permiten a las entidades del sector público aprovechar todos los beneficios de la nube, como el acceso a innovaciones de vanguardia, un aumento de la velocidad y 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. Todas las estrategias de precios, gobernanza de contratos, términos y condiciones, seguridad, requisitos técnicos y acuerdos de nivel de servicio, entre otras, son distintas en un modelo en la nube, por lo que el uso de los 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 servicios en la nube, una adjudicación a varias organizaciones de una serie de nubes de las que los compradores afiliados a la organización de compras que reúnen los requisitos pueden adquirir tecnologías de la nube y servicios asociados que satisfagan sus necesidades y se adapten a estas. Dichos acuerdos marco, que actúan como medio de compra de los contratos en la nube, permiten la compra de servicios en la nube de manera eficiente y eficaz. De esta manera, las organizaciones de compras y las entidades de usuarios finales pueden acceder a una amplia gama de servicios en la nube y, en última instancia, obtener todas las ventajas de la nube: agilidad, beneficios de las enormes economías de escala, escalabilidad para lograr una mejor disponibilidad con un coste más bajo, un amplio abanico de funcionalidades, velocidad de innovación y escalabilidad a nuevas regiones geográficas.

Tenga en cuenta que este documento se centra en la compra de las tecnologías de la nube de infraestructura como servicio (IaaS) y plataforma como servicio (PaaS) que proporcionan los *proveedores de servicios de infraestructura en la nube (CISP).* Estas tecnologías de la nube se pueden comprar directamente a los CISP o a través de distribuidores de CISP. *Se requieren algunas consideraciones adicionales en la RFP para los distribuidores de servicios de mercado en la nube (PaaS y SaaS) y los servicios de consultoría en la nube.*

Así mismo, tenga en cuenta que este documento no cubre todos los aspectos de la creación de un marco de adquisición en la nube completo. Existen muchos otros documentos del sector y de analistas que cubren cuestiones como prácticas recomendadas de adquisición en la nube, cómo elaborar presupuestos de servicios en la nube, la gobernanza de la nube, etc. Por este motivo, recomendamos encarecidamente tener en cuenta este asesoramiento y estos documentos durante el desarrollo de una estrategia global de adquisición de la nube. En la Tabla 1 siguiente se proporciona un esquema del manual de RFP de servicios en la nube y la ubicación de los ejemplos de los textos de la RFP de cada componente de una RFP de servicios en la nube.

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

Sección	Información general y texto de ejemplo de una RFP
1.0 Información general de un acuerdo marco de servicios en la nube	Introducción general del modelo de acuerdo marco de servicios en la nube (lotes, cómo competir y contratación)
2.0 Información general de la RFP de servicios en la nube	Texto de ejemplo genérico de la RFP que cubre las secciones siguientes, junto con comentarios que explican los motivos de la estructura y el texto de la RFP de servicios en la nube.
2.1 Redacción de una RFP de servicios en la nube	2.1.1 Introducción y objetivos estratégicos 2.1.2 Calendario de respuesta a la RFP 2.1.3 Definiciones 2.1.4 Descripción detallada del modelo de compra y competencia en el acuerdo marco 2.1.5 Requisitos administrativos mínimos del licitante
2.2 Requisitos técnicos	2.2.1 Requisitos mínimos 2.2.2 Comparación entre proveedores 2.2.3 Contratación
2.3 Seguridad	2.3.1 Requisitos mínimos 2.3.1.1 Protección de datos 2.3.1.2. Cambio de proveedores de servicios en la nube y datos de portabilidad 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 términos y condiciones de la suscripción del contrato	2.5.1 Términos y condiciones 2.5.2 Términos y condiciones de software 2.5.3 Cómo seleccionar los adjudicatarios 2.5.4. Incorporación y baja
3.0 Prácticas recomendadas y lecciones aprendidas	3.1 Gobernanza de la nube 3.2 Elaboración de un presupuesto para la nube 3.3 Conocimiento del modelo empresarial basado en socios 3.4 Agentes en la nube 3.5 Aprovisionamiento y estudio de mercado previos a la RFP 3.6 Sostenibilidad
Apéndice A: requisitos técnicos para la comparación entre licitantes	Lista de requisitos genéricos de tecnología de la nube para pedidos abiertos o minilicitaciones
Apéndice B: evaluación técnica en tiempo real	Ejemplo de un script de un producto de tecnología de la nube que muestra la puntuación (demostraciones de la nube como parte de un pedido abierto o una minilicitación)

1.0 Información general de un acuerdo marco de servicios en la nube

Un acuerdo marco de servicios en la nube bien diseñado puede ofrecer beneficios tanto a las organizaciones del sector público como a los proveedores de servicios en la nube que participen en la compra de servicios en la nube. Entre los beneficios que puede aportar un acuerdo marco de servicios en la nube bien diseñado se incluyen los siguientes:

- Cooperación:
    - El hecho de que varias organizaciones se asocien para realizar pedidos con requisitos similares resulta conveniente y eficaz y permite reducir los costes, al tiempo que simplifica el proceso de los pedidos. Establece un método eficaz de agrupar la demanda de tecnologías de la nube comunes y los servicios en la nube asociados de varias organizaciones del sector público, como pueden ser las soluciones del mercado y los servicios de consultoría.
- Amplia gama de servicios en la nube:
    - Puede incluir todos los servicios de consultoría, profesionales o administrados necesarios para permitir y realizar una migración a la nube completa y admitir las cargas de trabajo en la nube, así como las tecnologías de la nube que proporcionan los CISP y los servicios de mercado.
    - Estas tecnologías de la nube se pueden comprar directamente a un CISP o a través de un distribuidor designado.
- Gobernanza de contratos:
    - Permite aplicar una serie de términos y condiciones comunes y adjudicar un contrato maestro único para que las distintas organizaciones y compradores vayan en consonancia, en lugar de emplear unos diferentes para cada organización.
    - También resulta beneficioso para los proveedores, ya que estandariza el proceso de adquisición, los términos y condiciones y el mecanismo de pedido para evitar que se usen unos distintos para cada organización del sector público.
    - Ofrece flexibilidad. La creación, aprobación y formalización de un contrato de la nube efectivo en el marco de las políticas o reglamentos gubernamentales actuales requiere experimentación y una rápida capacidad de adaptación. Resulta mucho más beneficioso crear un acuerdo marco que permita que el sector público y los proveedores de servicios en la nube trabajen juntos para mejorar el contrato, de una manera 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 servicios en la nube.

- Capacidad de elección:
    - Permite que los compradores elijan entre varios CISP cualificados y establece un estándar de calidad alto para todos los servicios en la nube y los servicios asociados, como el mercado de PaaS y SaaS en la nube y la consultoría en la nube.
    - Esto permite controlar los distintos proveedores de un acuerdo marco y, de este modo, garantizar que se revisa adecuadamente el estándar de cada adjudicatario.

Un acuerdo marco para la compra de servicios en la nube resulta eficaz si incluye las principales tecnologías de IaaS o PaaS que proporciona el CISP, junto con el mercado de SaaS 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, utilizar y mantener una carga de trabajo que se ejecute en la nube, así como realizar una transición de esta. Por este motivo, aconsejamos dividir en tres lotes la RFP de servicios en la nube para elaborar un acuerdo marco de servicios en la nube, tal como se describe a continuación:

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

- LOTE 2: MERCADO
  Acceso a un mercado de servicios de PaaS y SaaS.

- LOTE 3: CONSULTORÍA EN LA NUBE
  Servicios de consultoría relacionados con la nube (formación, servicios profesionales, servicios administrados, etc.) y asistencia técnica.

*Como se ha señalado anteriormente, este documento se centra en la compra de las tecnologías de la nube de IaaS y PaaS (**LOTE 1**) según las proporcionan los CISP (tanto si se adquieren directamente de un CISP o a través de un distribuidor de CISP). Se exigen requisitos de idoneidad distintos para los distribuidores de los LOTES 2 y 3 en una RFP de servicios en la nube.*

En la Figura 1 siguiente se proporciona una vista general de cómo una RFP de servicios en la nube bien estructurada y dividida en estos tres lotes puede dar lugar a un acuerdo marco de servicios en la 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.

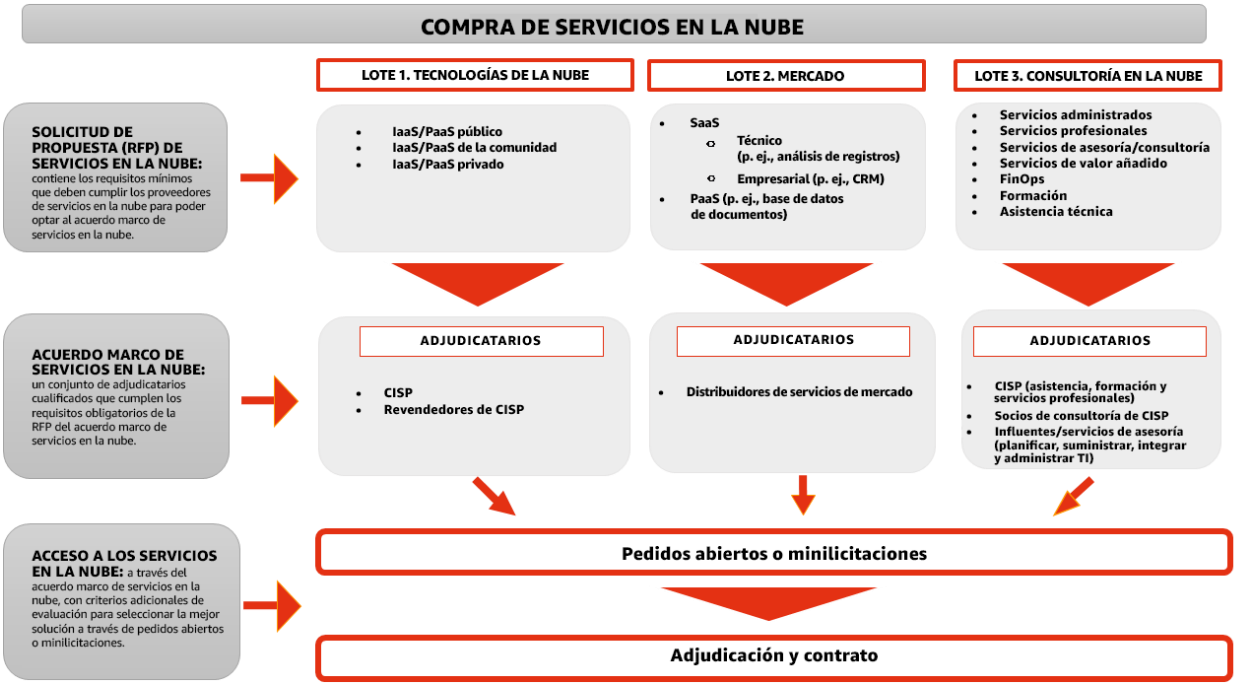

Figura 1: una RFP de servicios en la nube satisfactoria se divide en tres lotes. Cada lote presenta categorías o «tipos de ofertas» debajo del lote correspondiente, lo cual garantiza la adecuación técnica y contractual para satisfacer los requisitos del usuario final cuando se realiza la compra a partir del acuerdo marco de servicios en la nube.

Observe que:

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

Categorías del LOTE 1

Un acuerdo marco de servicios en la nube satisfactorio solicita a los CISP que describan el modelo de nube que ofrecen dividido en categorías debajo de cada lote. Recomendamos utilizar el estándar del sector para la computación en la nube (las características esenciales de la nube según el Instituto Nacional de Estándares y Tecnología [NIST]) para las definiciones de nube **pública**, nube **comunitaria** y nube **privada**. Esta estructuración del acuerdo marco de servicios en la nube permite a la agencia de compras y a los organismos públicos utilizar el marco para seleccionar entre una serie de modelos en la nube que se ajusten a sus necesidades.

Consulte la *Sección 2.1.3 Definiciones* para ver las definiciones que NIST propone para cada modelo en la nube del LOTE 1 (IaaS o PaaS pública, IaaS o PaaS comunitaria e IaaS o PaaS privada).

Cómo competir: ¿pedidos abiertos o minilicitaciones?

Los criterios de idoneidad de una RFP de servicios en la nube deben cubrir los elementos críticos y los estándares mínimos y deben excluir los estándares «deseables». Si se añaden estándares adicionales superiores a los de la base de referencia para los proveedores que cumplen los

requisitos del marco, es posible que algunos queden excluidos de la licitación y que, como consecuencia, se reduzcan las opciones para los compradores.

Una vez realizada la RFP y formalizado el acuerdo marco de servicios en la nube, los organismos del sector público que formen parte del marco pueden realizar un pedido o un «pedido abierto» de los servicios en la nube que necesiten cuando les convenga. La celebración de un contrato de entrega sucesiva en virtud de un acuerdo marco permite a los compradores precisar 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 en virtud del acuerdo marco e invita a todos los proveedores de un lote a responder a una serie de requisitos. El cliente invitará a todos los proveedores aptos del lote a realizar una oferta. Por este motivo, son importantes los requisitos mínimos de los adjudicatarios de una RFP de servicios en la nube, ya que garantizan que haya opciones de gran calidad 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. Si se aplica un «criterio uniforme» para la contratación de todos los lotes, se producirán problemas de viabilidad y compatibilidad técnica.*

2.0 Información general de la RFP de servicios en la nube

En esta sección se describe el modelo y el ámbito de la RFP de servicios en la nube, lo que incluye lo siguiente: 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 Redacción de una RFP de servicios en la nube

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

2.1.1 Introducción y objetivos estratégicos

A fin de lograr claridad en lo referente a los objetivos estratégicos, se recomienda exponer lo siguiente en la introducción de la RFP de los servicios en la nube: **(1)** los objetivos y los beneficios empresariales que prevé obtener la organización con el uso de la nube; **(2)** la estructura del acuerdo marco: quién compra, quién realiza operaciones, quién elabora los presupuestos, etc.; **(3)** una clara comprensión del modelo de responsabilidad compartida entre el sector público y los proveedores de servicios en la nube, que sienta las bases de una compra y un uso de la nube satisfactorios; y **(4)** el tipo de relación establecida entre los proveedores de servicios en la nube (CISP), los distribuidores de servicios de mercado, los socios consultores, las agencias de adquisición o contratación gubernamentales y los usuarios finales gubernamentales. Al exponer estos cuatro aspectos, las organizaciones pueden desarrollar una RFP que satisfaga mejor sus necesidades. Además, ello garantiza que tanto los clientes como los proveedores comprenden con claridad en qué consiste la entrega de la RFP.

La RFP de servicios en la nube difiere de forma intencionada de las RFP de TI tradicionales. La tecnología de la nube no se limita a sustituir los métodos de computación tradicionales por otros equivalentes, sino que presenta una manera completamente novedosa de consumir la tecnología. Las RFP de servicios en la nube bien diseñadas pueden ayudar a las entidades del sector público a tomar medidas rápidamente para poder beneficiarse de la nube.

Entre todas las prácticas recomendadas que hemos citado en relación con la compra de servicios en la nube, probablemente el mejor punto de partida sea comprender a la perfección el modelo de responsabilidad compartida. El modelo de responsabilidad compartida[1] se emplea principalmente a la hora de analizar la seguridad y el cumplimiento en la nube, pero esta delimitación de responsabilidades se aplica a todos los aspectos de las tecnologías de la nube. La RFP de servicios en la nube debe ser clara en cuanto a las competencias que tiene el CISP en un entorno de la nube y las responsabilidades del cliente. Por ejemplo, un CISP proporciona capacidades para supervisar recursos y aplicaciones que se ejecutan en la nube. ***Sin embargo***, es responsabilidad del cliente utilizar esas capacidades que le proporciona el CISP, dado que un CISP que opera a gran escala no está capacitado para hacerlo para millones de clientes.

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

Además, los clientes de la nube deben comprender de qué forma la red de socios del CISP les ayuda a utilizar la nube y a administrar sus responsabilidades. Por ejemplo, un proveedor de servicios administrados (MSP) en la nube puede ayudar a un cliente a configurar y utilizar las capacidades de supervisión que proporciona el CISP para satisfacer sus requisitos únicos de cumplimiento y auditoría.

En resumen, las responsabilidades del modelo en la nube son las siguientes:

Un CISP proporciona la tecnología de la nube.

Un cliente utiliza la tecnología de la nube.

Las **empresas consultoras** (si corresponde) ayudan al cliente a acceder a la tecnología de la 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 administrar sus cargas de trabajos 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 una compra en una ferretería. En una ferretería dispone de una amplia gama de materiales y herramientas para hacer lo que necesite. Puede hacer un armario o construir 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 a hacerle el trabajo. Por lo tanto, dispone de una serie de opciones:

1. Ir a comprar los materiales y las herramientas y hacer algo por su cuenta.
2. Ir a comprar los materiales y las herramientas y contratar a alguien que le haga o le ponga en funcionamiento algo.
3. Contratar a alguien para que le haga o le ponga en funcionamiento algo y pedirle que incluya los materiales y las herramientas como parte de su oferta global.

Si una organización dispone internamente de las capacidades necesarias para crear y administrar su entorno y soluciones en la nube por su cuenta, solo necesitará acceder a las tecnologías y herramientas de la 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 un mercado en la nube (**LOTE 2**). En el caso de que se necesite ayuda adicional con la consultoría, la migración, la implementación o la administración, el siguiente paso será acudir a la red de socios del CISP (**LOTE 3**).

Texto de ejemplo de una RFP: introducción y objetivos estratégicos

La computación en la nube proporciona a las organizaciones del sector público acceso rápido a una amplia gama de recursos de TI de pago por uso, de bajo coste y flexibles. Las organizaciones pueden aprovisionarse de los recursos del tipo y tamaño adecuados que necesiten para poner en marcha sus últimas ideas brillantes y gestionar sus departamentos de TI, a la vez que eliminan la necesidad de realizar grandes inversiones en hardware o en contratos de licencias de software a largo plazo.

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

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

1. *LOTE 1. Proveedores de servicios en la nube (CISP) o distribuidores del CISP que compran tecnologías de la nube*
2. *LOTE 2. Proveedores de servicios de mercado.*
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 licitadoras (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 las semanas o meses que requieren los plazos tradicionales.*
- ***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 inversión de capital [CapEx] a gastos operativos [OpEx]). 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, junto con los patrones de gasto a lo largo del tiempo, además de la previsión del gasto en el futuro.*
- ***Elasticidad:** obtener costes variables más bajos gracias a las economías de escala más altas que proporciona la nube.*
- ***Capacidad:** eliminar las suposiciones en lo que se refiere a las necesidades de capacidad de infraestructura.*
- ***Eliminación de la dependencia en 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 proteger las instalaciones y el hardware físico.*
- ***Responsabilidad compartida:** aliviar la carga operativa cuando el CISP gestiona, administra y controla los componentes desde el sistema operativo de host 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 en la nube para mejorar la capacidad de realizar un escalado seguro de manera más rápida y rentable.*
- ***Gobernanza de la nube:** (1) comenzar por un inventario completo de todos los recursos de TI; (2) administrar todos estos recursos 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 recursos, la administración de inventario, la administración de cambios, la administración y el análisis de registros y la gobernanza integral de la visibilidad y la nube.*

- ***Control:*** *obtener visibilidad completa sobre cómo se consumen los servicios de TI y cómo se pueden ajustar para mejorar la seguridad, la fiabilidad y el rendimiento, así como reducir los costes.*
- **Reversibilidad:** *herramientas y servicios de portabilidad que permiten realizar la migración a y desde la infraestructura del CISP y reducir así la dependencia del proveedor, además de respetar los códigos de conducta del sector.*
- ***Protección de datos:*** *capacidad de demostrar el cumplimiento del Reglamento general de protección de datos (*RGPD*) mediante un código de conducta del sector exclusivo para los servicios de infraestructura en la 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 (zona urbana).*
- ***Neutralidad climática:*** *los clientes deben comprometerse con los CISP en que siguen pasos específicos y de eficacia probada para alcanzar las metas de neutralidad climática antes de 2030 y que son firmantes del Pacto por la neutralidad climática de los centros de datos. De este modo, podrán alcanzar sus propias metas de neutralidad climática.*

2.1.2 Calendario de respuesta a la RFP

Se recomienda proporcionar a los licitantes un calendario de la actividad de licitación anticipada al crear un acuerdo marco de la nube, así como la RFP de servicios en la nube asociada. Cuanto mayor sea la interacción con el sector, mejor, ya que contribuirá a garantizar que todas las partes comprenden perfectamente los requisitos de la RFP 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 RFP está sujeto a las obligaciones legales y la legislación local, y que la lista que se proporciona a continuación se ha concebido como una guía de prácticas recomendadas en lugar de una lista obligatoria de actividades y plazos.

Texto de ejemplo de una RFP: calendario de respuesta

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

Calendario de la RFP de servicios en la nube
• *Publicación de la solicitud de información (RFI):* • *Respuesta a la RFI:* • *Publicación del borrador de la solicitud de propuesta (RFP):* • *Fecha límite de la respuesta al borrador de la RFP:* • *Fase de consulta del sector: <plazos>* • *Publicación de la RFP de idoneidad previa:* • *Respuesta a la RFP de idoneidad previa:* • *Publicación de la RFP:* • *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 RFP:*
- *Periodo de clarificación de la propuesta:*
- *Periodo de negociación:*
- *Fecha de intención de adjudicación:*
- *Adjudicación del contrato:*
- *Duración del contrato (opciones de ampliación):*

Tenga en cuenta que el calendario de la RFP está sujeto a las obligaciones legales y la legislación local, y que la lista que se proporciona a continuación se ha concebido como una guía de prácticas recomendadas en lugar de una lista obligatoria de actividades y plazos.

2.1.3 Definiciones

Una RFP de servicios en la nube debe incluir una lista detallada de definiciones. Esta lista incluye los roles del proveedor (por ejemplo, proveedor de servicios en la nube, distribuidor en la 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 ejemplo de una RFP: definiciones

Las siguientes definiciones son definiciones de computación en la nube del Instituto Nacional de Estándares y Tecnología (NIST).[2]

- *Infraestructura como servicio (IaaS). Se proporciona al consumidor la capacidad de aprovisionar el procesamiento, el almacenamiento, las redes y otros recursos de computación 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 en la nube subyacente, pero tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones implementadas, además de un posible control limitado de determinados componentes de red (por ejemplo, firewalls de host).*

- *Plataforma como servicio (PaaS). Se proporciona al consumidor la capacidad de realizar implementaciones en la infraestructura en la nube que ha creado o las aplicaciones adquiridas creadas con lenguajes de programación, bibliotecas, servicios y herramientas que admite el proveedor. El consumidor no administra ni controla la infraestructura en la 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 host 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 en la nube. Estas aplicaciones son accesibles desde diversos dispositivos de cliente mediante una interfaz de cliente ligero, como un navegador web (por ejemplo, correo electrónico basado en web), o una interfaz de programa. El consumidor no administra ni controla la infraestructura en la 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.*

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

- ***Nube pública.*** *La infraestructura en la nube se aprovisiona para que pueda usarla abiertamente el público general. Una organización empresarial, académica o gubernamental o cualquier combinación de estas pueden ser sus propietarias y encargarse de su administración y funcionamiento. Se encuentra ubicada en las instalaciones del proveedor de servicios en la nube.*

- ***Nube comunitaria.*** *La infraestructura en la nube se aprovisiona para que la use exclusivamente una comunidad específica de consumidores de organizaciones con inquietudes similares (por ejemplo, aspectos relativos al objetivo, los requisitos de seguridad, la política y el cumplimiento de la normativa). Una o varias organizaciones de la comunidad, un tercero o cualquier combinación de estos pueden ser sus propietarios y encargarse de su administración y funcionamiento. Así mismo, dicha nube puede estar ubicada en las instalaciones o fuera de ellas.*

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

- ***Nube privada.*** *La infraestructura en la nube se aprovisiona para el uso exclusivo de una sola organización formada por múltiples consumidores (por ejemplo, las unidades empresariales). La organización, un tercero o cualquier combinación de estos pueden ser sus propietarios y encargarse de su administración y funcionamiento. Así mismo, dicha nube puede estar ubicada en las instalaciones o fuera de ellas.*

2.1.4 Descripción detallada del modelo de compra y competencia en el acuerdo marco

Como se ha señalado anteriormente, las organizaciones del sector público deben identificar el modelo que determine cómo debe funcionar un 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 RFP de servicios en la nube de modo que los proveedores de tecnología de la nube, las organizaciones de servicios de consultoría relacionadas, los distribuidores del mercado y las entidades compradoras conozcan sus respectivas funciones.

En cuanto al alcance del acuerdo marco, así como 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 en virtud del 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 proporcionar acceso directo y oportuno a los datos de uso y facturación asociados a la utilización de los servicios del proveedor de servicios en la nube?

- ¿Se exige algún requisito a un distribuidor de valor añadido de servicios globales, un integrador de sistemas, un 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 los roles y las responsabilidades en un modelo de servicios en la nube.

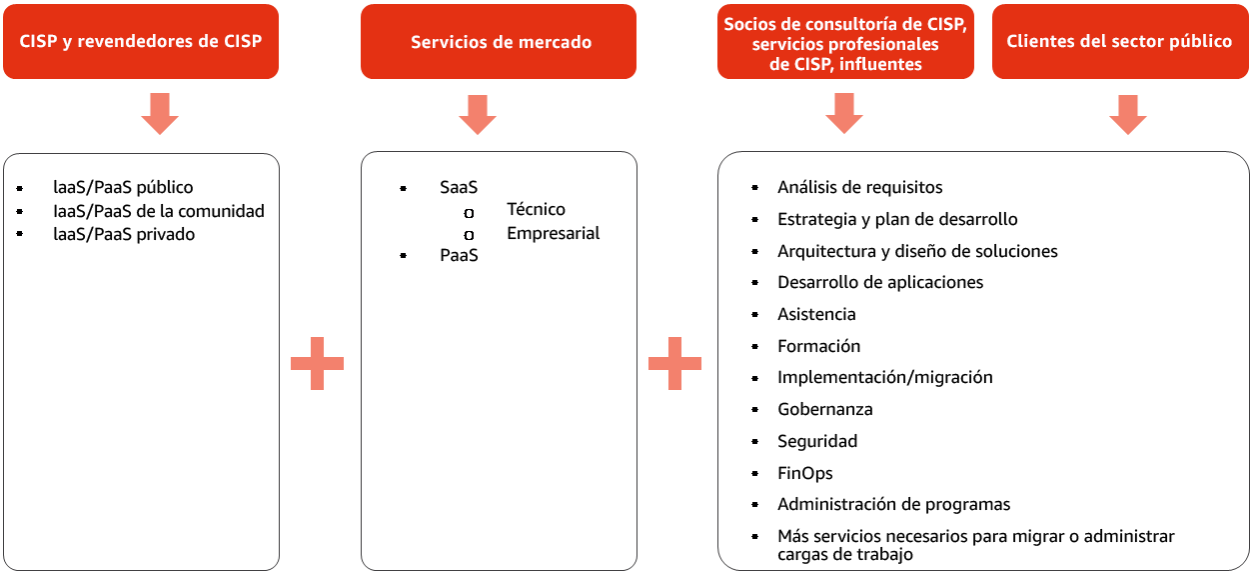

Figura 2: una RFP de servicios en la nube debe proporcionar a los usuarios finales un listado con todos los servicios en la nube que necesitan. Los clientes del sector público precisarán un CISP para las tecnologías de la nube y, si es necesario, un mercado para los productos de PaaS y SaaS. A continuación,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

En el siguiente ejemplo de contenido se plasman los roles y las responsabilidades, tal y como se muestra en la Figura 2 anterior. Un acuerdo marco de la nube, así como la RFP de servicios en la nube asociada, debe garantizar que los compradores tienen 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. Para lograrlo, se deben separar los servicios en lotes, como ya se ha comentado, y se debe exponer claramente cómo se realizan los pedidos abiertos y las minilicitaciones en virtud del acuerdo marco.

Texto de ejemplo de una RFP: modelo de compra

*Este contrato se utilizará como medio de compra del **Acuerdo marco**. Este acuerdo marco de servicios en la nube, que utilizarán distintos compradores aptos afiliados a <**ORGANIZACIÓN**>, incluirá múltiples **lotes**, según lo defina <**ORGANIZACIÓN**>, de tecnologías de la nube y servicios o productos de mercado relacionados; de servicios de consultoría; de servicios profesionales, integración de sistemas, servicios administrados o servicios profesionales de migración; y de formación y asistencia, según lo defina <**ORGANIZACIÓN**>. De este modo, se simplificará el proceso de adquisición y también se optimizarán las economías de escala.*

Una vez suscrito, este acuerdo marco permitirá a la organización comprar las tecnologías de la nube y los servicios relacionados con la nube específicos que desee cuando los necesite, en lugar de realizar la compra mediante adquisiciones independientes. De esta manera, 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 con las posibles renovaciones incluidas. La duración máxima de un contrato marco de pedido abierto suele ser de **<x>** meses; el plazo se puede ampliar en **<x>** meses y, posteriormente, en **<x>** meses adicionales con las correspondientes aprobaciones internas de ampliación de contrato, en caso de ser necesarias. Esto se especificará en cada **pedido abierto** específico.*

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

1. *LOTE 1: TECNOLOGÍAS DE LA NUBE: gama completa de tecnologías del proveedor de servicios en la nube (directamente de un CISP, de un distribuidor o de un distribuidor con asistencia o servicios 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 paquetes de soluciones de tecnología de la nube, como DR/COOP, almacenamiento, macrodatos y análisis, DevOps, etc.*
2. *LOTE 2: MERCADO: gama completa de productos y servicios de PaaS y SaaS, como contabilidad, CRM, diseño, recursos humanos, sistema de información geográfica (GIS) y cartografía, computación de alto rendimiento (HPC), inteligencia empresarial (BI), gestión de contenido, análisis de registros, etc.*
3. *LOTE 3: CONSULTORÍA EN LA NUBE: gama completa de servicios de consultoría (servicios administrados, servicios profesionales, servicios de asesoramiento y consultoría, servicios de valor añadido, operaciones financieras, asistencia técnica) relacionados con la migración a la nube y su uso. Estos servicios pueden incluir lo siguiente: planificación, diseño, migración, administración, asistencia, 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.

COMPETENCIA EN EL 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. La celebración de un contrato de entrega sucesiva en virtud de un acuerdo marco permite a los compradores precisar los requisitos con especificaciones funcionales adicionales para un pedido abierto, a la vez que conservan los beneficios que se ofrecen en virtud de dicho acuerdo marco.

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

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 mixtos de usuarios finales empresariales, especialistas en compras y expertos técnicos para elaborar una lista de requisitos imprescindibles y deseables. Estos requisitos servirán para decidir los lotes que son aplicables, así como el proveedor 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 en línea (un portal donde figurarán los adjudicatarios cualificados del acuerdo marco y sus servicios) para buscar productos o servicios que satisfagan las necesidades que han identificado. Seleccionarán los lotes adecuados y, a continuación, 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 lo siguiente:

- *Documento de definición del servicio o enlaces a definiciones del 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 a petición).*

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 siempre 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).

En virtud del acuerdo marco, los compradores pueden ponerse en contacto con los proveedores para solicitarles información sobre la descripción del servicio, los términos y condiciones, los precios o los documentos o el modelo de definición de servicio. Se conservará 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 necesitar lo siguiente:

- *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 siempre debe ser 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 completa: *relación coste-eficacia, precio y costes de funcionamiento*
Mérito técnico y ajuste funcional: *cobertura, capacidad de red y rendimiento según se especifican 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 amplia 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 en virtud del acuerdo marco e invita a todos los proveedores de un lote a responder a una serie de requisitos. El cliente invitará a todos los proveedores aptos del lote a realizar una oferta. Consulte información comparativa adicional en las secciones siguientes sobre aspectos técnicos, seguridad y precios o valor.

CONTRATO

*Tanto el comprador como el proveedor deberán firmar una copia del contrato para poder empezar a utilizar el servicio. La duración máxima de un contrato marco suele ser de **<x>** meses; el plazo se puede ampliar en **<x>** meses y, posteriormente, en **<x>** meses adicionales con las correspondientes aprobaciones internas de ampliación de contrato, en caso de ser necesarias.*

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 administrativos mínimos del licitante

El uso de una redacción clara y sencilla para establecer los criterios de idoneidad del acuerdo marco contribuirá a garantizar que no haya ninguna propuesta de centros de datos tradicionales o proveedores de hardware que empaqueten una solución tradicional en forma de «nube». Los participantes en la RFP deben demostrar que cumplen los requisitos administrativos mínimos del licitante.

De nuevo, tenga 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: MERCADO y el LOTE 3: CONSULTORÍA EN LA NUBE en los casos en que contribuye a ofrecer un contexto global en cuanto a los requisitos y el alcance de la RFP. Por ejemplo, es importante incluir los criterios mínimos de idoneidad de un distribuidor de CISP, un MSP, un SI o una empresa consultora, entre otros. Esto contribuye a garantizar que (1) están afiliados directamente al CISP como distribuidores o socios de canal, (2) están certificados por un CISP para distribuir el acceso directo a las ofertas del CISP a entidades terceras, y (3) cuentan con certificaciones de estos CISP que acreditan sus capacidades y conocimientos.

Texto de ejemplo de una RFP: requisitos administrativos mínimos del licitante

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 mercado o un proveedor de servicios para poder utilizar un CISP (por ejemplo, consultoría, servicios de migración, servicios administrados, operaciones financieras, etc.). Identifique los roles para los que presenta la oferta:

LOTE 1

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

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

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

____ - Distribuidor externo del CISP (capacidad para proporcionar acceso directo a las ofertas en la nube en línea 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 usted es un distribuidor autorizado de sus ofertas: _____*

LOTE 2

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

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

LOTE 3

____ - CISP que proporciona servicios profesionales

____ - Proveedor de asistencia técnica del CISP

____- Socio del CISP que proporciona servicios que se utilizan o gestionan en un CISP

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

Especifique el tipo de oferta:

- *Servicios administrados de cargas de trabajo en un CISP (S/N): _____*
  - *Identifique las especialidades si procede: _____*
- *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 (especifíquelo): _____*

Especifique los CISP para los que proporciona servicios: _____
Proporcione una carta del CISP que confirme su nombramiento como socio según el modelo del CISP: _____

LOTE 1 REQUISITOS ADMINISTRATIVOS MÍNIMOS

Proveedores de servicios en la nube (CISP)
Para optar a ser CISP, un proveedor debe demostrar que cumple los siguientes requisitos.

Criterios de idoneidad 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 y 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 de clientes (especifique el tipo o número de requisitos)	*El cliente puede evaluar si el CISP cuenta con suficiente experiencia para ofrecer los servicios solicitados.*
Responsabilidades sociales corporativas	*Deben ser versiones accesibles públicamente que proporcione el CISP.*
Compromisos y prácticas de sostenibilidad disponibles públicamente.	*El cliente puede ver si un CISP muestra compromiso para dirigir su empresa de la manera más respetuosa con el medio ambiente posible.*
El CISP debe demostrar una trayectoria probada en innovación y lanzamiento de nuevos servicios y características útiles a lo largo de los últimos 5 años, especialmente en el ámbito de PAAS, machine learning y análisis, macrodatos, servicios administrados y en las características de optimización de uso de la nube. Para demostrarlo, se pueden utilizar los registros de cambios o las fuentes de actualización de acceso público.	*Demuestra que el CISP se esfuerza para poner nuevos productos a disposición de los clientes con rapidez y que, luego, los renueva y mejora rápidamente. Esto permite a los clientes mantener una infraestructura de TI de vanguardia sin tener que realizar inversiones de recapitalización.*

Relación del distribuidor o el socio con el CISP
<ORGANIZACIÓN> requiere que el contratista principal esté afiliado directamente al CISP como distribuidor o socio de canal, que esté certificado por el CISP para distribuir el acceso directo a ofertas del CISP a entidades terceras y que cuente con certificaciones de dicho CISP que acrediten sus capacidades y conocimientos. *De este modo, <ORGANIZACIÓN> no debe revisar los términos y servicios asociados a una capa adicional de la subcontratación entre el contratista principal del Acuerdo marco y el CISP. Así mismo, este requisito reduce la complejidad que generan las capas adicionales de distribuidores cuando (1) <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) <ORGANIZACIÓN> lleva a cabo las actividades diarias que implican el consumo de servicios en la nube.*

[3] Tenga en cuenta que la RFP de servicios en la nube se centra en información empresarial general, 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 RFP en la nube se centran en el tamaño global de la empresa para satisfacer los requisitos (la escala adecuada) y en una experiencia y un rendimiento probados.

2.2 Requisitos técnicos

Una RFP de servicios en la nube debe elevar el nivel de exigencia de los CISP y exigirles que proporcionen las tecnologías de la 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 durante el planteamiento de una RFP de servicios en la nube. Los CISP ofrecen servicios estandarizados a millones de clientes. Por ello, las personalizaciones de una RFP de servicios en la nube se centran en soluciones y resultados superiores a los estándares, en lugar de en los métodos, la infraestructura o el hardware subyacentes empleados para ofrecer servicios en la nube que se utilizan para obtener resultados resolutivos.

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 la organización lleva a cabo sus actividades en ese momento. Reunir estos requisitos a la perfección es un proceso complejo en el mejor de los casos. Si dichas sesiones de requisitos se realizan correctamente, documentan el proceso empresarial histórico que podría estar anticuado y ser ineficaz. Así mismo, si dichos requisitos pasan a formar parte de una RFP que replicará el CISP, la única solución podría ser una personalizada. Este modelo no es compatible con las adquisiciones en la nube.

Las organizaciones del sector público deben conocer sus necesidades de rendimiento y objetivos empresariales, pero estos no deben ser prescriptivos en una RFP en la que se determine 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, en si cubren sus necesidades de rendimiento, así como en la capacidad de ajustar las reglas de negocio mediante la configuración.

Las RFP en la nube deben formular las preguntas adecuadas a fin de obtener las mejores soluciones. Dado que en un modelo en la nube no se compran activos físicos, muchos de los requisitos de adquisición de los centros de datos tradicionales no son aplicables. ***Si se reutilizan las preguntas de los centros de datos, inevitablemente se obtendrán sus respuestas****.*
Como consecuencia, los CISP no podrán presentar ninguna oferta o se generarán contratos con un diseño deficiente que impedirán a los clientes del sector público obtener todas las capacidades y los beneficios de la nube.

La RFP de servicios en la nube se centra en los requisitos clave que se exigen de un CISP y de los servicios en la nube. Además, garantiza que los proveedores que optan al LOTE 1 cumplen un alto estándar de calidad. También se debe evitar que los requisitos sean demasiado prescriptivos a fin de que el sector público no tenga limitaciones para acceder a una amplia variedad de CISP cualificados.

Texto de ejemplo de una RFP: capacidades del proveedor de servicios en la nube

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

Criterios de idoneidad 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 entre sí en caso de error.	*El CISP debe poder ofrecer una infraestructura adecuada para crear aplicaciones de alta disponibilidad en las que se puedan 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 sus centros de datos.	*La conectividad privada es un requisito fundamental para poder crear una infraestructura híbrida y segura.*
El CISP debe proporcionar mecanismos suficientes, como el cifrado de los datos en tránsito.	*El cliente puede exigir que haya una capacidad que impida el tránsito de los datos que no estén cifrados.*
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 cumplir con el Código de conducta de protección de datos de CISPE, para proporcionar características y servicios que se puedan utilizar conforme al RGPD y que permitan a los clientes crear aplicaciones que cumplan con el RGPD.	*El cliente debe poder crear o ejecutar aplicaciones que cumplan con el RGPD.*
El CISP debe facilitar informes auditados de terceros, como los informes SOC 1 y 2 (que cubren las ubicaciones y los servicios que utiliza el usuario final), que ofrezcan transparencia en relación con 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.*
El CISP debe cumplir con el Pacto por la neutralidad climática de los centros de datos.	*El Pacto por la neutralidad climática de los centros de datos compromete al CISP a alcanzar la neutralidad climática en 2030 y, por lo tanto, permitir al usuario cumplir sus propias metas de sostenibilidad. Los auditores externos son obligatorios para los proveedores con más de 250 empleados a tiempo completo (no se aplica en el caso de las pymes).*

El CISP debe cumplir el Código de conducta de portabilidad de IaaS de SWIPO.	*El Código de conducta de portabilidad de IaaS de SWIPO garantiza que los servicios cumplen los requisitos del artículo 6 «Portabilidad de datos» del Reglamento de libre circulación de datos no personales.*
Características del servicio	
La infraestructura del CISP debe ser accesible a través de interfaces programáticas (API) y la consola de administración basada en Web.	*El acceso de autoservicio y las interfaces programáticas son un estándar obligatorio de los proveedores CISP a fin de eliminar en la medida posible la necesidad de intermediarios en el acceso de los usuarios y los proveedores.*
El CISP debe ofrecer un conjunto básico de servicios que incluyan almacenamiento de objetos, una base de datos relacional administrada, una base de datos no relacional administrada, equilibradores de carga administrados, supervisión y escalado automático integrado.	*Una simple oferta de máquinas virtuales no es suficiente para que un proveedor sea apto para convertirse en como proveedor de servicios en la nube. Los proveedores en la nube deben ofrecer un conjunto de servicios PAAS e IAAS para acelerar y mejorar las aplicaciones del cliente.*
El CISP debe permitir que el cliente cambie libremente el uso y la configuración de sus servicios o traslade los datos dentro y fuera del CISP (oferta de autoservicio).	*El acceso de autoservicio a los servicios y los datos es un requisito obligatorio que otorga una independencia completa al cliente.*
El CISP debe permitir facturar sus servicios con la opción de «pago por uso».	*El pago por 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 (PoC) de corta duración.*
Seguridad de los datos y el sistema	
El CISP debe permitir al cliente mantener el control absoluto de sus datos, ofrecerle libertad para elegir dónde se almacenan los datos (área urbana de la ciudad) y garantizarle que no se trasladará ninguno de sus datos a menos que dicho traslado lo inicie el propio cliente.	*El cliente debe tener control sobre dónde se almacenan los datos y cómo se administra el acceso al contenido, así como disponer de acceso de usuario a los servicios y los recursos.*
Las características del CISP deben proporcionar al cliente un control absoluto de sus políticas de seguridad, incluida la confidencialidad, la integridad y la disponibilidad de los datos y el sistema del cliente.	*El cliente debe poder 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 supervisar 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 enviar una alerta 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 sobre requisitos técnicos que se muestran a continuación.

SOLUCIONES

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

- *Almacenamiento*
- *DevOps*
- *Seguridad o cumplimiento*
- *Macrodatos 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 de desastres*
- *Desarrollo y pruebas*
- *Archivado*
- *Copia de seguridad y recuperación*
- *Macrodatos*
- *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 RFP de servicios en la nube, es importante proporcionar criterios con los que se puedan comparar las tecnologías del CISP durante una evaluación competitiva.

Las RFP de servicios en la nube deben exigir las capacidades en la nube que necesita una organización, con el entendimiento de que el cliente puede usar dichas capacidades para crear su solución. Las funcionalidades que superen los estándares que puede proporcionar un CISP (como las soluciones predefinidas a través del CISP o las características de automatización) se pueden utilizar para hacer un análisis más significativo de las «opciones de valor añadido» o el «mejor valor» de una RFP de servicios en la nube.

El sector público suele exigir que en la competencia entre los licitantes se utilicen criterios de evaluación como el mejor valor, la oferta económicamente más ventajosa (MEAT) o el precio más bajo. En la fase de planificación de esta parte de la RFP de servicios en la nube, es importante que las entidades del sector público adopten un enfoque que tenga en cuenta las características únicas de la nube. Por ejemplo, hay que comprender que la simple comparación de las partidas presupuestarias entre las ofertas de los proveedores de servicios en la nube (p. ej.: computación o almacenamiento) no es una forma efectiva de comparar las ofertas. En su lugar, recomendamos encarecidamente un enfoque en soluciones más generales, como las mencionadas previamente en la sección *2.2.1*. De

este modo, las entidades del sector público pueden considerar los requisitos específicos de la nube, como los que se muestran en el *Apéndice A: requisitos técnicos para la comparación entre licitantes*.

Las RFP 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 Instituto Nacional de Estándares y Tecnología (NIST), además de informes de analistas de terceros, para garantizar que el CISP cuente con la oferta de la «nube verdadera» más adecuada que opere a gran escala.

Texto de ejemplo de una RFP: comparación entre proveedores

*Los CISP deben responder TODAS las preguntas sobre 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 automáticamente sin necesidad de interacción humana con cada proveedor de servicios. Los proponentes deben proporcionar una capacidad que permita aprovisionar servicios automáticamente al realizar pedidos (es decir, sin la revisión ni la aprobación del proveedor). Explique cómo se integra este requisito en su oferta 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 se integra este requisito en 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 varios consumidores mediante un modelo multiinquilino con diferentes recursos virtuales asignados y reasignados de forma dinámica en función de la demanda del consumidor. El usuario puede especificar la ubicación con un nivel superior de abstracción (p. ej.: el condado, la región o el centro de datos). El proponente debe admitir el escalado de estos recursos en cuestión de minutos u horas desde el momento en que se realiza una solicitud de aprovisionamiento. Explique cómo se integra este requisito en su oferta o la oferta que representa.*

4) ***Rápida elasticidad:** el CISP del proponente debe admitir capacidades de aprovisionamiento y desaprovisionamiento de servicios (escalado y reducción verticales) y poner el servicio a disposición en los plazos mínimos designados (un máximo de «x» horas) desde el momento de la solicitud de aprovisionamiento. El proponente deberá admitir los ajustes de facturación que se deriven de estas solicitudes de aprovisionamiento con una frecuencia diaria u horaria.*

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

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

Además, el CISP debe:

- *Ser un líder reconocido en la prestación 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 sus capacidades y fiabilidad probadas.*

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

2.2.2.1 Acuerdos de nivel de servicio (SLA)

Los CISP proporcionan acuerdos de nivel de servicio comerciales estandarizados a millones de clientes, por lo que no pueden ofrecer contratos personalizados, como ocurre en el modelo de centro de datos local. No obstante, los clientes del CISP (a menudo con la asistencia de los socios del CISP) pueden utilizar su nube para aprovechar los acuerdos de nivel de servicio comerciales del CISP y, de este modo, cumplir y superar los requisitos y los acuerdos de nivel de servicio únicos específicos del cliente.

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

Texto de ejemplo de una RFP: acuerdos de nivel de servicio

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

<ORGANIZACIÓN> se mantendrá al día de los acuerdos de nivel de servicio del CISP e implementará las aplicaciones y cargas de trabajo importantes de tal forma que sigan funcionando en caso de que no se cumpla un acuerdo de nivel de servicio.

<ORGANIZACIÓN> será responsable de mantener los acuerdos de nivel de servicio adecuados asociados con todo el equipamiento que posee <ORGANIZACIÓN> o con los servicios que preste <ORGANIZACIÓN> que se utilicen con el CISP.

El CISP debe proporcionar a <ORGANIZACIÓN> las capacidades necesarias para disponer de visibilidad continua e informes del rendimiento de su acuerdo de nivel de servicio operativo. Además, debe facilitarle prácticas recomendadas documentadas que permitan utilizar la infraestructura del CISP para diseñar servicios que ofrezcan rendimiento, durabilidad y fiabilidad.

2.2.3 Contratación

Los términos y condiciones del CISP se han diseñado para reflejar el funcionamiento de un modelo de servicios en la nube (no se compran activos físicos y los CISP operan a gran escala ofreciendo servicios estandarizados). Por este motivo, es fundamental que dichos términos y condiciones del CISP se incorporen y se utilicen en la mayor medida posible. Consulte la sección *2.5* que hay a continuación para obtener más información sobre los términos y condiciones y la contratación.

2.2.3.1 Servicios nuevos y cambiantes

Los CISP ofrecen rendimiento a través de un servicio. A diferencia de las soluciones locales tradicionales, que precisan actualizaciones y contratos de mantenimiento de servicios que caducan, los proveedores de servicios en la nube únicamente ofrecen un servicio estandarizado. Para que el

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

modelo en la nube logre economías de escala, se implementan actualizaciones y cambios en la infraestructura subyacente de todos los clientes, no solo de usuarios determinados, y, luego, dichos clientes seleccionan los servicios que utilizan. El servicio funciona mejor que los sistemas locales anteriores, y los proveedores de servicios en la nube añaden constantemente servicios nuevos y mejorados para que los clientes los utilicen como deseen.

Si se impide la adición de servicios del CISP nuevos o mejorados después de la fecha límite de presentación de la RFP, las organizaciones del sector público no podrán utilizar servicios nuevos ni características mejoradas hasta que se emita la siguiente versión del acuerdo marco. Por ello, recomendamos encarecidamente que la prestación de servicios descrita en el acuerdo marco sea lo más amplia posible a fin de permitir 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 de nuevos servicios significativamente diferentes del CISP al acuerdo marco, no obstante, se pueden añadir actualizaciones y nuevas versiones de los servicios que no se consideren cambios sustanciales sin que se impugnen las adquisiciones.

Texto de ejemplo de una RFP: 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 que evolucionan constantemente. ***<ORGANIZACIÓN>*** *reconoce y acuerda que las tecnologías de la nube se pueden proporcionar como servicio compartido a* ***<ORGANIZACIÓN>*** *y a otros clientes del CISP mediante un código base o un entorno común, y que el CISP puede ocasionalmente: cambiar, añadir o suprimir las funciones, las características, el rendimiento u otras características de los servicios en la nube. Además, 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 ámbito de este pedido 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 que proporciona el CISP 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, ya que no se compran activos físicos, lo que permite a los clientes trasladar sus datos de un proveedor de servicios en la 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, puede que un CISP ofrezca servicios y capacidades que otro simplemente no puede proporcionar. De este modo, se reduce la posibilidad de utilizar dichos servicios con otro proveedor. Una enfoque prudente consiste en solicitar a los CISP que proporcionen las características y los servicios necesarios para dejar de utilizar 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.

Consulte la sección 2.3.1.2 para obtener información sobre códigos de conducta del sector para abordar la «portabilidad de datos» y el «cambio de proveedores de servicios en la nube» a fin de cumplir con los requisitos del artículo 6 del Reglamento para la libre circulación de datos no personales en la Unión Europea.

Texto de ejemplo de una RFP: incorporación y baja

<ORGANIZACIÓN> está estudiando propuestas que ofrezcan una estrategia de salida razonable para evitar la dependencia. <ORGANIZACIÓN> no compra activos físicos, y el CISP ofrecerá tanto la posibilidad de ampliar la pila de TI como de reducirla. El CISP proporcionará las herramientas y los servicios de portabilidad necesarios para ayudar a realizar la migración hacia y desde su plataforma, lo que reducirá la dependencia. La documentación detallada sobre cómo utilizar las herramientas y los servicios de portabilidad que proporciona el CISP se empleará 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> trasladar los datos cuando sea necesario al almacenamiento del CISP y fuera de este. El CISP también permitirá que se descarguen imágenes de la máquina virtual y que se migren a un nuevo proveedor de servicios en la nube. <ORGANIZACIÓN> puede exportar sus imágenes de la máquina y utilizarlas en el entorno local 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 cumplimiento. En este modelo, los clientes de la nube pueden controlar el diseño y la seguridad de sus aplicaciones y de los datos que se almacenan en la infraestructura, mientras que los CISP son responsables de prestar servicios en una plataforma controlada de alta seguridad y de proporcionar una amplia gama de características de seguridad adicionales. El nivel de responsabilidad del CISP y del cliente en este modelo depende del modelo de implementación de la nube (IaaS, PaaS o SaaS). Además, los clientes deben tener claras sus responsabilidades en cada modelo.

Comprender este modelo de responsabilidad compartida es fundamental para poder elaborar una RFP de servicios en la nube satisfactoria. Las organizaciones del sector público deben asegurarse de que comprenden las responsabilidades del CISP y las suyas propias y cómo pueden ayudarles los socios consultores o los proveedores de software independientes.

2.3.1 Requisitos mínimos

La palabra clave en lo que respecta a la 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 responsabilidad compartida. Como se puede ver en la lista de requisitos representativa siguiente, se solicita al CISP que proporcione capacidades estandarizadas que pueda utilizar el cliente para hacer que su entorno en la 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 que permite elegir entre la posibilidad de que el CISP administre las claves de cifrado o que el cliente tenga el control absoluto de estas.*

- *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 características que permitan a los clientes ver exactamente lo que ocurre en el entorno de su CISP.*
- *Permitir una mayor visibilidad de las llamadas a la API, que incluya las llamadas realizadas, su autor y cuándo y desde dónde se hicieron.*
- *Proporcionar opciones de agregación de registros, investigaciones de optimización y generación de informes de cumplimiento.*
- *Proporcionar la capacidad de configurar notificaciones de alerta para 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 final.*

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

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

Las organizaciones del sector público deben comprobar las certificaciones y evaluaciones de acreditación de la nube para asegurarse de que se han implantado los controles de seguridad necesarios del CISP. Por ejemplo, supongamos que un auditor independiente ha validado y certificado un CISP para confirmar que cumple con el estándar de certificación ISO 27001. En el anexo A de la ISO 27001, el dominio 14 profundiza en los controles específicos a los que debe ceñirse el CISP de acuerdo con los requisitos de la ISO respecto 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 RFP relacionada con la TI. Por ello, resulta lógico que una organización únicamente requiera 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 RFP de servicios en la nube.

Este enfoque basado en utilizar informes de cumplimiento de terceros se puede aplicar a la mayoría de los controles de seguridad y cumplimiento, como, por ejemplo, el código de conducta del RGPD de CISPE, ISO, SOC, etc.

Texto de ejemplo de una RFP: seguridad

El CISP debe comunicar los procesos de seguridad que no sean de su propiedad y las limitaciones técnicas a <ORGANIZACIÓN> a fin de lograr una protección y una flexibilidad adecuadas entre <ORGANIZACIÓN> y el proveedor de servicios.

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

- *Describa los roles y las responsabilidades del CISP y <ORGANIZACIÓN> relacionados con la seguridad en la oferta propuesta. Exponga con claridad la delimitación de las responsabilidades y presente los servicios del CISP para ayudar a <ORGANIZACIÓN> a crear y automatizar las funciones de seguridad en su entorno en la nube.*
- *Proporcione las respuestas a las especificaciones técnicas del APÉNDICE 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 datos de <ORGANIZACIÓN>. Incluya los controles implantados para abordar la protección del contenido de <ORGANIZACIÓN>. El CISP debe proporcionar un aislamiento regional sólido, de modo que los objetos almacenados en una región nunca salgan de ella a menos que <ORGANIZACIÓN> los transfiera explícitamente a otra.

- *<ORGANIZACIÓN> administrará el acceso a sus contenidos, servicios y recursos. El CISP debe proporcionar un conjunto avanzado de características de acceso, cifrado y registro a fin de que <ORGANIZACIÓN> pueda implementar estos requisitos de forma eficaz. El CISP no accederá al contenido de <ORGANIZACIÓN> ni lo utilizará para ningún propósito, excepto en la medida en que sea necesario según la legislación y para el mantenimiento de los servicios del CISP y su prestación a <ORGANIZACIÓN> y a sus usuarios finales.*
- *<ORGANIZACIÓN> seleccionará las regiones en las que se almacenará el contenido. El CISP no trasladará ni replicará el contenido de <ORGANIZACIÓN> fuera de las regiones elegidas, salvo en la medida en que sea necesario según la legislación y para el mantenimiento de los servicios del CISP y su prestación a <ORGANIZACIÓN> y a sus usuarios finales.*
- <ORGANIZACIÓN> *elegirá cómo se protegerá su contenido. El CISP debe proporcionar un cifrado sólido para el contenido de <ORGANIZACIÓN> en tránsito o en reposo, así como 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 datos y privacidad para que <ORGANIZACIÓN> establezca, gestione 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 de terceros.*

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 RFP 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 en la nube.

Las RFP en la nube deben ofrecen a los CISP la posibilidad de demostrar que cumplen con las acreditaciones y las evaluaciones de cumplimiento. 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. Además, 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 el cumplimiento en una RFP en lugar de doblar esfuerzos en elaborar la lista de dichos controles individuales (**muchos de los cuales se pueden tomar de RFP anteriores que se encuentran directamente en los centros de datos locales, por lo que podrían no ser aplicables a la computación en la nube**).

NOTA: También es fundamental comprender cómo se accede a los informes que se enumeran a continuación. Por ejemplo, los informes SOC 1 y SOC 2 suelen ser documentos confidenciales. Debe comprender los acuerdos que necesita para acceder a ellos (p. ej.: el acuerdo de confidencialidad [NDA]) en lugar de pedir simplemente que le adjunten dichos documentos junto con la respuesta a una RFP (estos documentos se podrían hacer públicos mediante leyes de registros abiertos o similares que comprometen la seguridad de la nube).

Texto de ejemplo de una RFP: cumplimiento de la normativa

El uso de estándares operativos, de seguridad y de cumplimiento 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.), optimiza la adquisición de la tecnología basada en la nube.

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

Exigir al CISP que mantenga el cumplimiento mínimo de la normativa durante el tiempo de vigencia del contrato permite a su vez mantener al día el cumplimiento del servicio.

El CISP que realiza la oferta (directamente o a través de un distribuidor) debe ser capaz de demostrar que cumple con las siguientes atestaciones, informes y certificaciones de terceros independientes. (Nota: Si alguna de estas atestaciones, informes y certificaciones tiene restricciones de divulgación por problemas de seguridad, <Organización> colaborará con el CISP para acordar el acceso de forma conjunta):

Certificaciones y atestaciones	*Leyes, reglamentos y privacidad*	*Conformidad y marcos*
☐ C5 (Alemania)		*☐ CDSA*
☐ Código de conducta de protección de datos de CISPE (RGPD)		
☐ CNDCP (Pacto por la neutralidad climática de los centros de datos)		
☐ DIACAP	*☐ Directiva de protección de datos de la UE*	*☐ CIS*
☐ SRG del DoD; niveles 2 y 4	*☐ Cláusulas modelo de la UE*	*☐ Servicio de información de justicia criminal (CJIS)*

☐ *HDS (Francia, sanidad)*		
☐ *FedRAMP*	☐ *FERPA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *RGPD*	☐ *Escudo de la 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)*
☐ *Regla 17-a-4(f) de la SEC*	☐ *PIPEDA [Canadá]*	☐ *MARS – E*
☐ *SecNumCloud (Francia)*		
☐ *SOC1/ISAE 3402*	☐ *Ley de privacidad (Australia)*	☐ *MITA 3.0*
☐ *SOC2/SOC3*	☐ *Ley de privacidad (Nueva Zelanda)*	☐ *MPAA*
☐ *Código IaaS de SWIPO*		
	☐ *Autorización del DPA español*	☐ *NIST*
	☐ *DPA del Reino Unido (1988)*	☐ *Niveles de Uptime Institute*
	☐ *VPAT/Sección 508*	☐ *Principios de seguridad en 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.

2.3.1.1 Protección de datos

Una consideración clave que hay que tener en cuenta al utilizar servicios en la nube es que el procesamiento de datos personales se lleva a cabo de acuerdo con las leyes de protección de datos vigentes de la UE, incluido el Reglamento General de Protección de Datos (RGPD). El RGPD es un reglamento basado en principios y, por tanto, no proporciona instrucciones específicas del sector para poder garantizar el cumplimiento. No obstante, el RGPD recomienda adoptar herramientas de cumplimiento, como los códigos de conducta, a fin de proporcionar estas instrucciones. CISPE, en colaboración con la Autoridad de Protección de Datos de Francia (CNIL), ha desarrollado un código de conducta de protección de datos (Código CISPE [6]) avalado por el Comité Europeo de Protección de Datos y con vigencia general en Europa. La finalidad del Código es ayudar a los CISP a cumplir con el RGPD y guiar a los clientes en la evaluación de la idoneidad de los CISP para el procesamiento de datos personales que dichos clientes quieren realizar.

- El Código se centra exclusivamente en el sector de IaaS y aborda las responsabilidades y los roles específicos de los proveedores de IaaS.

[6] https://cispe.cloud/code-of-conduct/

- Ayuda a aclarar los aspectos del procesamiento justo y transparente y las medidas de seguridad adecuadas en el contexto de los servicios de infraestructura en la nube (RGPD, Artículo 40 [2]).
- Ayuda a los clientes a comprender cómo pueden retener la soberanía de sus datos, para lo cual deben asegurarse de que permanecen en la UE.
- Fomenta las prácticas recomendadas de protección de datos que respaldan la iniciativa GAIA-X de la UE para desarrollar servicios de datos en la nube europea.

El cumplimiento del CISP de los códigos de conducta de protección de datos, como el Código CISPE, garantiza que los datos personales se procesarán en estricto cumplimiento del RGPD.

Texto de ejemplo de una RFP: protección de datos

El CISP que realiza la oferta (directamente o a través de un distribuidor) debería poder demostrar su capacidad de cumplir con un código de conducta de protección de datos, como el Código CISPE. El código de protección de datos debe ajustarse a los requisitos establecidos en el marco del RGPD. El código debe incluir como mínimo: (1) una definición clara de los roles y las responsabilidades del CISP, (2) el requisito de que el CISP no utilizará datos de clientes con fines de marketing o publicidad, y la (3) capacidad de los clientes para seleccionar servicios del CISP que permitan procesar los datos completamente en el Espacio Económico Europeo. El cumplimiento del código deben verificarlo auditores independientes externos (organismos de supervisión) acreditados por auditores externos independientes, los cuales también tienen que estar acreditados por la Autoridad Europea de Protección de Datos.

2.3.1.2 Cambio de proveedores de servicios en la nube y datos de portabilidad

Los clientes deben tener la libertad de elegir los servicios en la nube que quieren utilizar, en lugar de estar limitados por un CISP o un proveedor de PaaS o SaaS.

Los servicios en la nube que proporciona el CISP se estandarizan y ofrecen según un modelo de «uno a varios», con servicios que configura, aprovisiona y controla el cliente. Una ventaja de la computación en la nube es que los clientes pueden elegir los servicios estandarizados que necesitan para desarrollar sus aplicaciones y soluciones únicas. Esta ventaja incluye la posibilidad de obtener servicios nuevos o diferentes que satisfagan de manera óptima las necesidades de los clientes en cualquier momento dado.

Al igual que la protección de datos, los códigos de conducta permiten proporcionar a los clientes garantías y confianza para la transición a la nube desde una infraestructura local o bien al cambiar entre CISP. CISPE presidió junto con EuroCIO (la asociación europea de directores de información [CIO]) el desarrollo del código de conducta de portabilidad de datos y cambio de servicios en la nube para los servicios en la nube de IaaS (Código IaaS de SWIPO[7,8]). La primera versión del código se desarrolló de acuerdo con el Reglamento para la libre circulación de datos no personales en la Unión Europea, entregado a la Comisión Europea en noviembre de 2019 bajo la presidencia finlandesa de la UE y publicado por la asociación SWIPO AISBL en mayo de 2020. En abril de 2021, SWIPO AISBL declaró la conformidad de los primeros servicios con el código y, en mayo de 2021, se anunció el cumplimiento con dicho código de los primeros servicios prestados por los miembros de CISPE.

[7] https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security
[8] https://swipo.eu/

Texto de ejemplo de una RFP: cambio de proveedores de servicios en la nube y portabilidad de datos

El CISP que realiza la oferta (directamente o a través de un distribuidor) debería poder demostrar su capacidad de cumplir con un código de conducta de «cambio y portabilidad de datos», como el Código IaaS de SWIPO. El código debe detallar cómo un CISP puede transferir de forma segura los datos empresariales de los clientes, en caso de que decidan cambiar de CISP.

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 RFP 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 entidades del sector público que evalúan a los CISP consideren las siguientes capacidades como aspectos clave de la seguridad:

Texto de ejemplo de una RFP: consideraciones clave de seguridad

- *La comprensión del modelo de responsabilidad compartida y la documentación por parte del CISP, 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 que no es de propiedad y que está disponible públicamente sobre los controles físicos y lógicos y la posición de seguridad del CISP.*
- *Asistencia del CISP específica para la seguridad de la nube.*
- *Servicios que permiten a los clientes formalizar el diseño de la cuenta, automatizar la seguridad y los controles de gobernanza de la nube, así como optimizar la auditoría.*
- *Capacidad de crear, aprovisionar y administrar un conjunto de recursos mediante plantillas (incluye plantillas de seguridad de referencia creadas por el CISP o por el socio del CISP).*
- *Capacidad de establecer un funcionamiento fiable y repetible de los controles.*
- *Características para una auditoría continua y en tiempo real.*
- *Capacidad de crear scripts técnicos de políticas de gobernanza de la nube.*
- *Capacidad de crear funciones forzadas que no puedan anular los usuarios que no tengan permiso para modificar dichas funciones.*
- *Capacidad de implementar de forma fiable lo que se describió previamente en las políticas, los estándares y los reglamentos, además de crear unas normas de seguridad y cumplimiento 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 comunes más frecuentes de denegación de servicio distribuido (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.*
- *Servicio administrado de detección de amenazas.*

2.3.3 Contratación

Como se ha indicado anteriormente, los términos y condiciones del CISP se han diseñado para reflejar el funcionamiento de un modelo de servicios en la nube (no se compran activos físicos y los CISP operan a gran escala ofreciendo servicios estandarizados). Por este motivo, es fundamental que dichos términos y condiciones del CISP se incorporen y se utilicen en la mayor medida posible. Consulte la sección *2.5* que hay a continuación para obtener más información sobre los términos y condiciones y la contratación.

En materia de seguridad, de nuevo recomendamos encarecidamente que se permita que los CISP actualicen constantemente sus ofertas o que los proveedores añadan productos después de la fecha límite de presentación, siempre y cuando se ajusten a los parámetros originales de la RFP. El motivo de ello es que las características y los servicios de seguridad evolucionan con rapidez y los CISP a menudo lanzan nuevos servicios centrados en la seguridad, que en muchos casos se pueden utilizar de forma gratuita. Tenga en cuenta que es importante contar con un nivel de seguridad de referencia (consulte los requisitos mínimos anteriores) que permita garantizar que los cambios en las ofertas de seguridad no resulten perjudiciales.

Evidentemente, el modelo de responsabilidad compartida constituye la piedra angular de la seguridad en una RFP 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 que proporciona el CISP, junto con documentación para ayudar a los clientes a integrar y automatizar las prácticas de seguridad recomendadas.

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

2.4 Precios

A fin de contratar tecnología de la nube que tenga en cuenta la fluctuación de la demanda, las organizaciones del sector público necesitan un contrato que les permita pagar los servicios a medida que los consumen (con la visibilidad y la gobernanza de la nube necesarias respecto al uso y al gasto).

Es importante que las RFP de servicios en la nube consideren el valor y el coste total de propiedad (TCO), en lugar de realizar sencillas comparaciones homogéneas de precios unitarios. La práctica tradicional de considerar el precio unitario más bajo no es aplicable al modelo en la nube, ya que no suele reflejar la oferta económicamente más ventajosa ni el precio global más bajo.

Para evaluar el precio del CISP, resulta útil contar en primer lugar con una idoneidad previa o una preselección de CISP, con los ***requisitos mínimos en cuanto a precios,*** *de modo que CISP con capacidades similares puedan ser candidatos para el acuerdo marco. De este modo, en el proceso de evaluación de los pedidos abiertos o las minilicitaciones, se puede consultar una selección de arquitecturas en la 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 tiempo real 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 un guion de pruebas de demostración de las tecnologías de la nube.*

2.4.1 Requisitos mínimos

La sección de precios de la RFP de servicios en la nube consta de 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 que resulta 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 respalda la innovación y las reducciones de precios.
4. **Control de gastos:** los CISP deben suministrar herramientas de generación de informes, supervisión y previsión que permitan a los clientes (1) supervisar el uso y el gasto tanto a nivel de resumen como de detalle, (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 la nube futuros.

Texto de ejemplo de una RFP: precios

<ORGANIZACIÓN> solicita que los CISP que respondan incluyan el método que proponen y el modelo de precios que usarán para prestar cada uno de sus servicios como una capacidad de la nube comercial a los usuarios finales.

El CISP debe proporcionarlo siguiente:

- *Documento de definición del servicio o enlaces a definiciones del servicio.*
- *Documento de términos y condiciones.*
- *Documento de precios (se aceptarán enlaces a los precios públicos siempre que haya una lista o un documento de precios exhaustivos disponibles a petición).*

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).

En virtud del acuerdo marco, los compradores pueden ponerse en contacto con los proveedores para solicitarles información sobre la descripción del servicio, los términos y condiciones, los precios o los documentos o el modelo de definición de servicio. Se conservará 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 un servicio de pago por uso bajo demanda al estilo de los servicios públicos? Describa su modelo de precios.*
  - *¿Puede ofrecer descuentos adicionales si existe un compromiso de uso o se realiza una compra de gran volumen? Especifique cómo.*

- *¿Los precios son 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 constante tendencia de reducción de precios en las tecnologías de la 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 servicios en la nube aplicable cuando el cliente consume la unidad de servicio.*

Presupuestos e informes y alertas de facturación
*Para demostrar la entrega y el uso de las tecnologías de la nube, los CISP deben proporcionar 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 según las etiquetas que defina el cliente. **<ORGANIZACIÓN>** reconoce que como parte del modelo de responsabilidad compartida en la nube, **<ORGANIZACIÓN>** será responsable de utilizar las características de facturación y elaboración de presupuestos, así como las herramientas para satisfacer los requisitos únicos de previsión y generación de informes que proporcione el CISP.*

- *Proporcione información sobre cómo puede **<ORGANIZACIÓN>** visualizar la información de facturación y uso tanto a nivel de detalle como de resumen, así como consultar 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, así como 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 en la nube utilizará a lo largo de un periodo de tiempo definido en función del uso anterior. Los CISP deben ofrecer una **estimación** de qué facturarán a **<ORGANIZACIÓN>**. De este modo, **<ORGANIZACIÓN>** puede utilizar alarmas y presupuestos para las cantidades que prevé utilizar a fin de tener un mayor control de los costes y los gastos.*

2.4.2 Comparación entre proveedores

Las organizaciones del sector público a menudo exigen 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. Al planificar 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, hay que comprender que la simple comparación de las partidas presupuestarias entre las ofertas de los proveedores de servicios en la nube (p. ej., computación o almacenamiento) no es un método eficaz de realizar la comparación, ya que no tiene en cuenta funciones como el rendimiento, la optimización de costes mediante los servicios nativos en la nube ni las herramientas de supervisión del CISP, así como tampoco 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 prestar atención al coste total de propiedad (TCO) de los casos de uso definidos y tener en cuenta todos los aspectos de una solución en la nube (incluidos los 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

En el proceso de evaluación también se pueden 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 a fin de incluir el ámbito de la tecnología y los servicios que utilizará 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 recuperación de desastres (DR) 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 un x % más caro debido al coste que conlleva tener en cuenta las necesidades de recuperación de desastres. Examine la siguiente alternativa de comparación homogénea directa como ejemplo de por qué un enfoque holístico de los precios que incluye funciones técnicas adicionales es crucial para evaluar a los CISP.

Ejemplo: un cliente desea comparar el precio del almacenamiento de objetos que ofrecen los 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 unidades, el cliente no formularía preguntas clave como:

1. ¿Cuántas copias de redundancia del objeto hay disponibles en caso de fallo? En el ejemplo anterior, el CISP 1 se ha diseñado para admitir 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 los objetos almacenados? El del CISP 1 es del 99,999999999 %; el del CISP 2, del 99 %.
3. Tenga en cuenta el coste durante la vigencia de la propiedad del proyecto o de la carga de trabajo global, además de cómo pueden las características de optimización de costes reducir los costes en relación con cómo se almacenan y utilizan los datos (por ejemplo, el aumento del uso de las funciones sin servidor de un CISP puede reducir los costes en un x %).

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

Entre las consideraciones de los escenarios de precios se incluyen las siguientes:

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, entre 3 y 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 SKU suelen resultar 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).

Los clientes de la nube que deseen obtener el mejor valor deberán evaluar el conjunto de capacidades globales del CISP. Por ejemplo, es posible que los CISP ofrezcan varios servicios de forma gratuita o esencialmente gratuita. Una evaluación de precios debe tener en cuenta dichos servicios, así como que puede que otros CISP cobren por funciones similares.

Los criterios de evaluación se pueden redactar de manera que los CISP puedan anunciar las características que «incluyen por defecto» y de qué modo dichos servicios tienen un impacto en el coste global. Los criterios de evaluación también pueden tener en cuenta los precios por volumen o por niveles del CISP y los descuentos disponibles comercialmente, como las instancias reservadas o de spot. Por ejemplo:

- x % de ahorro si los clientes compran una capacidad de computación reservada (para 1 año, 3 años, etc.)
- x % de descuento en precios por volumen o por niveles
- x % de ahorro según las revisiones de arquitectura y la optimización de la infraestructura, como el cambio a la opción de computación más adecuada
- como se ha mencionado anteriormente, debe tenerse en cuenta el coste de la vigencia completa y cómo pueden reducirlo las características de optimización de costes

ESCENARIO DE PRECIOS

Los licitantes deben indicar los 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, con el conocimiento explícito de que durante el periodo de vigencia del contrato cambiarán estos requisitos nominales. Indique los precios para una capacidad bajo demanda de 12 y 36 meses y reservada de 12 y 36 meses.

Indique:

- *Nombre de las soluciones propuestas:*
- *Mejor precio del licitante:*

- *Horas de servicio: 24 x 7 x 365*
- *Disponibilidad del servicio: 99,95 %*

Además, los escenarios de precios pueden incluir ejemplos de clientes actuales 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 supervisión 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 términos y condiciones de la suscripción del contrato

Las operaciones y las tecnologías de la nube que ofrece el CISP están estandarizadas por defecto, por lo que también lo están 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 para no ser rechazados. También pueden incluir 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 tienden a fracasar.

2.5.1 Términos y condiciones

El primer paso de la contratación en una RFP de servicios en la nube es revisar y comprender los términos comerciales existentes del CISP que, en muchos casos, están disponibles públicamente en los sitios web del CISP. Las entidades del sector público están cada vez más habituadas a aceptar los términos comerciales de los CISP. Parte de este esfuerzo para comprender los términos 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 términos específicos. Algunos de estos términos podrían parecer diferentes de los términos de TI tradicionales, pero hay motivos específicos que «explican» por qué forman parte de un contrato de la nube. Si no se pueden aceptar los términos disponibles públicamente, los CISP suelen disponer de acuerdos ligeramente modificables que se pueden explorar para los clientes empresariales.

Además de revisar los términos y condiciones de los CISP, es importante comprender las políticas existentes, los reglamentos o las leyes (por ejemplo, los relacionados con la tecnología, la clasificación de los datos, la privacidad, el personal, etc.). A menudo, existen políticas, reglamentos o leyes diseñados para comprar y utilizar ofertas de TI tradicionales que pueden entrar en conflicto con el modelo del CISP. Por ejemplo, al permitir únicamente el uso de las tecnologías de la nube que se incluían en la licitación de acuerdo marco a través de la RFP de servicios en la nube. Los CISP añaden constantemente nuevos servicios y características. El hecho de impedir el acceso a estos nuevos servicios simplemente porque se sigue un enfoque tradicional de actualización de productos de TI no tiene sentido para el cliente final. Si es este el caso, es importante debatir en profundidad con los CISP estas políticas, reglamentos o leyes.

Ventajas de las discusiones previas a la RFP

Como se ha indicado anteriormente, antes de elaborar un borrador de la RFP, deberá reunirse con los CISP y los proveedores relacionados a fin de conocer sus términos y condiciones e informarles del enfoque, las políticas, los reglamentos y las leyes de su entidad. Lo más importante de estas discusiones es que ambas partes descubran «por qué» los términos pertinentes funcionan de la manera que lo hacen. Por ejemplo, los términos y condiciones de la nube difieren de los términos de los centros de datos, los servicios administrados, el hardware, el software listo para usar y la integración de sistemas tradicionales. Dado que se trata de modelos únicos que requieren una innovación constante, sus modelos de negocio precisan de un proceso de RFP lo suficientemente flexible que permita mantener negociaciones o discusiones a fin de obtener aclaraciones.

Al incluir la posibilidad de aclarar los términos y condiciones mediante discusiones o negociaciones, las organizaciones del sector público pueden conocer mejor los modelos en la nube y evitan rechazar proveedores que en realidad podrían satisfacer las necesidades de la organización. Un proceso típico sería que la organización identificase determinados términos por adelantado que desee debatir y negociar antes de la adjudicación. Al negociar por adelantado los términos aceptables con los licitantes, 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, reglamentos 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 discusiones mucho antes de la RFP y de cualquier negociación contractual posterior).

Flexibilidad de la negociación

Para poder firmar los contratos conforme a la legislación local y, a su vez, a 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 RFP 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 que exige la legislación).

Nota: El ámbito de la responsabilidad compartida es inherente en el modelo en la nube y se debe reflejar en los términos del contrato (p. ej.: el CISP confirma que los clientes son propietarios de sus datos y que tienen control del lugar donde residen, así mismo proporciona herramientas para garantizar que la elección de ubicaciones de datos sea limitada, NO OBSTANTE, 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 servicios en la nube. Si se aplica un «criterio uniforme» para la contratación de todos los LOTES, se producirán problemas de viabilidad y compatibilidad técnica.*

Como se ha indicado anteriormente, las RFP que incluyen términos obligatorios que no son negociables son básicamente una propuesta de tipo «tómela o déjela» para los proveedores, lo que provocar el rechazo de una propuesta que de otro modo sería aceptada. Las organizaciones del sector público deberían analizar detenidamente 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 vendrán determinadas por su clasificación como obligatoria. El uso de requisitos o de términos obligatorios debe limitarse al mínimo estrictamente necesario a fin de dotar a la organización de la flexibilidad necesaria para adquirir la mejor tecnología y solución.

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

Compras indirectas

Una alternativa a la compra de tecnologías de la nube directamente de un CISP es adquirirlas a 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 ejemplo de una RFP: términos y condiciones

Los CISP o los proveedores representativos deben proporcionar los términos y condiciones que tienen disponibles públicamente y ofrecer información sobre los términos y condiciones clave que proporciona <ORGANIZACIÓN>.

<ORGANIZACIÓN> pretende celebrar un contrato por escrito con el licitante elegido en función de los términos contractuales del licitante. El licitante debe proponer a <ORGANIZACIÓN> una serie de términos contractuales, que representen su mejor propuesta comercial y legal, para que los revise. Los oferentes y <ORGANIZACIÓN> pueden debatir las dos series de términos y condiciones durante la fase de <DEBATE/NEGOCIACIÓN>.

- *Los términos generales principales del acuerdo marco constarían principalmente de los siguientes componentes:*
  - *Duración del marco.*
  - *Gobernanza del marco.*
  - *Rendimiento del marco.*
  - *Finalización del marco.*
  - *Ámbito 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.*
- *Las especificaciones del servicio del CISP se pueden tener en cuenta y 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 añadir nuevos servicios o mejoras. Dado que los servicios en la nube evolucionan de forma constante, se realizarán mejoras en estos de forma continua, lo que puede contribuir a brindar una mayor eficiencia a los clientes.*
- *El cliente no debe especificar los acuerdos de nivel de servicio (SLA). Los términos del cliente no deben definir los SLA personalizados específicos de la comisión que difieran de los modelos estándar de prestación de servicios de los CISP. Si se permiten los SLA estándar de los CISP, estos podrán mantener los costes bajos y trasladarlos a los clientes, lo que a su vez permitirá que los clientes confíen en que el CISP podrá cumplir el SLA.*
- *Los límites de responsabilidad deben ser proporcionales. La responsabilidad debe ser proporcional a los servicios que se compran, por lo que no deben establecerse límites de responsabilidad que resulten demasiado desproporcionados. Los límites muy desproporcionados pueden disuadir a los CISP de aceptar proyectos de bajo valor. Con frecuencia, estos proyectos son una buena introducción y funcionan como un caso de «prueba» que permite a los clientes determinar si ciertas soluciones en la nube son eficaces para su organización.*
- *Los clientes deben ser 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, podrán evitar depender del proveedor y podrán trasladar los datos libremente a nuevos proveedores.*

2.5.2 Términos y condiciones del software

Aunque este manual se centra en la compra de tecnologías de la nube de IaaS y PaaS tal y como las proporciona un CISP, es importante resaltar los términos y condiciones del software que las organizaciones del sector público pueden tener en cuenta al comprar software a proveedores. Consulte la Figura 1 (página 5) para ver cómo se compra el software como parte de una RFP de servicios en la nube bien estructurada.

El software desempeña un rol crítico en casi cualquier empresa, incluidas las del sector público. Incluir obligaciones como los términos y condiciones de licencia de software en una RFP de servicios en la nube permite garantizar que las entidades del sector público reciben el mejor valor y pueden elegir a los proveedores cuando adquieren software.

Consulte los diez principios de licencias de software justas para clientes de la nube[9] a fin de obtener más información. Los principios han sido desarrollado por Cigref[10], una asociación de las principales empresas y administraciones públicas de Francia, que representa a los usuarios de la tecnología digital, en colaboración con CISPE y con el apoyo de otras asociaciones comerciales europeas de directores de TI (CIO) y proveedores. Su objetivo es abordar las prácticas que ambas asociaciones consideran perjudiciales para la transformación digital de organizaciones de cualquier tamaño en su transición a la nube.

[9] https://www.fairsoftware.cloud/principles/
[10] https://www.cigref.fr/

Texto de ejemplo de una RFP: software

*<**ORGANIZACIÓN**> pretende celebrar un contrato por escrito con el licitante elegido en función de los términos contractuales del licitante. El licitante debe proponer a <**ORGANIZACIÓN**> una serie de términos contractuales, que representen su mejor propuesta comercial y legal, para que los revise. Los proveedores de software y <ORGANIZACIÓN> pueden debatir las dos series de términos y condiciones durante la fase de <DISCUSIÓN O NEGOCIACIÓN>.*

***Requisito 1.0.** Los proveedores de software deben proporcionar términos de licencia claros, que incluyan un desglose de los costes en los niveles de resumen y detalle.*

***Requisito 1.1.** Todos los cargos relacionados con cualquier incumplimiento de los términos de licencia deben indicarse en los niveles de resumen y detalle.*

***Requisito 2.0.** Las licencias de software deben proporcionar a <Organización> la capacidad de migrar el software con licencia del entorno local a la nube de su elección, sin tener que adquirir otras licencias duplicadas del mismo software.*

***Requisito 2.1.** Las licencias de software deben estar libres de restricciones de licencia y costes incrementados que restrinjan la capacidad de <Organización> para ejecutar el software con licencia en la nube de su elección.*

***Requisito 3.0.** Las licencias de software deben permitir que <Organización> ejecute el software con licencia en su propio hardware (generalmente denominado software «local»), así como en la nube de su elección.*

***Requisito 4.0.** Las licencias de software no deben exigir que el software con licencia solo se ejecute en hardware destinado exclusivamente a <Organización>.*

***Requisito 5.0.** Los proveedores de software no deben penalizar a <Organización> si su software con licencia se utiliza en la oferta en la nube de otro proveedor, por ejemplo, mediante la inclusión de derechos para iniciar auditorías de software invasivas o adicionales o para imponer tarifas de licencias de software más altas.*

***Requisito 6.0.** El software de directorio debe admitir estándares abiertos para la sincronización y autenticación de identidades de usuario de manera no discriminatoria con otros servicios de identidades.*

***Requisito 7.0.** Los proveedores de software no deben cobrar precios diferentes por el mismo software únicamente a juzgar por el propietario del hardware al que se instala.*

***Requisito 7.1.** Los precios del software no deben discriminar entre el software instalado en el centro de datos propio de <Organización>, un centro de datos administrado por un tercero, ordenadores alquilados a terceros o el proveedor de servicios en la nube elegido por <Organización>.*

***Requisito 8.0.** Durante la vigencia del contrato, los proveedores de software no deben realizar cambios sustanciales en los términos de licencia que limiten a <Organización> los usos permitidos anteriormente, salvo que lo exija la legislación o en caso de problemas de seguridad.*

***Requisito 9.0.** Los proveedores de software no deben confundir a <Organización> y manifestar que las licencias de software cubrirán el uso del software previsto por parte de <Organización> como se detalla en los <Requisitos de la organización>, si la cobertura de dicho uso puede requerir la compra de licencias adicionales.*

Requisito 10.0. *Si <Organización> tiene el derecho de distribuir y transferir licencias de software, los proveedores de software deben seguir ofreciendo asistencia y revisiones con términos justos a la organización que adquiera legalmente una licencia distribuida (<Organización>).*

2.5.3 Cómo seleccionar 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. La celebración de un contrato de entrega sucesiva en virtud de un acuerdo marco permite a los compradores precisar 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 en virtud del acuerdo marco e invita a todos los proveedores de un lote a responder a una serie de requisitos. El cliente invitará a todos los proveedores aptos del lote a realizar una oferta. Por este motivo, son importantes los requisitos mínimos de los adjudicatarios de una RFP de servicios en la nube, ya que garantizan que haya opciones de gran calidad bajo cada lote.

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

Consulte en la sección *2.1.4* un texto de la RFP de ejemplo relativo a la elección entre adjudicatarios.

2.5.4 Incorporación y baja

Un aspecto que hay que tener en cuenta al definir un acuerdo marco de servicios en la nube es la opción de un sistema dinámico de adquisición (DPS). Con un modelo de DPS, 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. Además, a diferencia del modelo tradicional, los proveedores también pueden solicitar unirse al «marco DPS» en cualquier momento durante su vigencia.

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

3.0 Prácticas recomendadas y lecciones aprendidas

A continuación destacamos algunas lecciones aprendidas sobre cómo definir un acuerdo marco de servicios en la nube satisfactorio con una RFP de servicios en la nube bien redactada.

3.1 Gobernanza de la nube

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

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 con un inventario completo de todos los recursos de TI; (2) administrar de forma centralizada todos estos recursos, y (3) crear alertas relacionadas con el uso, la facturación, la seguridad, etc. Todos estos beneficios fundamentales de la nube permiten a los clientes disponer de una arquitectura optimizada y automatizada al máximo sin necesidad de adquirir e instalar continuamente nuevo hardware. De ello se encarga el CISP, lo que permite a los clientes olvidarse de realizar las tareas de administración generales de la infraestructura y centrarse en el nivel operativo esencial.

Una forma útil de concebir la nube del CISP es considerarla una API de grandes dimensiones. Cuando lanza un nuevo servidor o cambia la configuración de seguridad, lo que hace es llamar a la API. Cada cambio realizado se registra y se graba en el entorno (quién hizo el cambio, en qué consistió, dónde se hizo y cuándo). Esto proporciona un nivel de gobernanza, control y visibilidad que solo es posible lograr en un entorno en la nube. De este modo, los clientes pueden replantear sus modelos de gobernanza de TI existentes, así como determinar de qué manera se pueden optimizar y mejorar, de acuerdo con los beneficios que aporta la nube.

La gobernanza de la nube también puede consistir en comunicar e incorporar los cambios positivos en los procesos y los nuevos conjuntos de capacidades que aporta la nube. Por ejemplo, los gestores de proyectos están habituados a esperar meses para que se implemente un entorno de TI, de modo que podrían sobrestimar considerablemente los plazos de la creación de un entorno de desarrollo o prueba en la nube (que con la nube apenas tarda unos minutos). La adaptación a esta nueva agilidad será progresiva y se realizará por programas. Estas lecciones aprendidas se deben compartir para que el acuerdo marco de servicios en la nube pueda seguir evolucionando a fin de que los requisitos resulten idóneos 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 constatado que resulta útil agrupar los servicios del CISP en una única partida (computación, almacenamiento, redes, base de datos, IoT, etc.), que denominamos 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, a su vez, proporciona a los usuarios un rápido acceso a los recursos necesarios en cualquier momento. También se adapta a la fluctuación de la demanda, lo que permite optimizar el uso y reducir los costes.

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

También se puede proporcionar mayor flexibilidad contractual si se utilizan partidas contractuales opcionales en las categorías de recursos adecuadas a fin de dar cabida al crecimiento en un futuro. Así mismo, si una organización desea agrupar tecnologías de la nube con servicios de consultoría, profesionales o administrados en una misma partida, puede hacerlo 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 financiar en función de las estimaciones de uso actuales y previstas.

Tabla 3: ejemplo de la estructura de precios de las partidas individuales

N.º 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	3000 €	3000 €
1005	Mercado en 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 utilizará la organización. La organización acepta los términos del proveedor, por ejemplo, 10 millones de euros en un plazo de 5 años, lo que equivale a 2 millones de euros al 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 supervisa la tasa de gasto mediante las herramientas de supervisión y previsión del CISP. Si quedan pocos fondos, la organización solicita fondos adicionales al director financiero (CFO) que pueden asignarse al mantenimiento de los servicios.

Texto de ejemplo de una RFP: precios (contratación)

TÉRMINOS DE PAGO
Los términos de pago deben estructurarse según corresponda de manera que se paguen únicamente los recursos que utilice <ORGANIZACIÓN>, como se indica a continuación:

1. *El pago mensual se debe basar en el uso o consumo real de los servicios y en los precios que haya disponibles públicamente 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 unitarias 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. Para ello, se modificará este pedido con diferentes cantidades a fin de que **<ORGANIZACIÓN>** tenga 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 forma periódica de cantidades suficientes para cubrir el coste estimado de las tecnologías de la nube que se utilizarán para satisfacer una serie de necesidades.*

N.º de artículo	Descripción	Cantidad	Unidad	Precio
01	Tecnologías de la nube del CISP	1000	Por unidad	1000,00 €

PEDIDO MÍNIMO E INCREMENTAL

*Los pedidos de diversas cantidades de **<10 000>** unidades por partida se realizarán de forma periódica en función del uso de tecnologías de la nube que estime **<ORGANIZACIÓN>**. Este acuerdo dotará a **<ORGANIZACIÓN>** de flexibilidad para realizar pedidos anticipados de **<10 000>** unidades de «Tecnologías de la nube» según sea necesario a fin de respaldar las operaciones y mantener coherencia con las prácticas comerciales de «pago por uso» de la computación en la nube.*

*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 un pedido no puede superar las **<x>**. No obstante, este número nunca puede superar el valor del pedido abierto cuando se combina con todas las unidades solicitadas previamente.**<ORGANIZACIÓN>** será responsable de garantizar que todos los pedidos se realicen conforme a los límites especificados en esta sección.*

VALOR 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 en 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, administrados o de distribución, entre muchos otros, son fundamentales en el proceso. Muchos clientes requieren un proveedor de servicios en la nube por su infraestructura y subcontratan el trabajo práctico de planificación, migración y administración a un integrador de sistemas (SI) 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 servicios en la nube, como las cláusulas de responsabilidad solidaria con los subcontratistas.

Tomaremos 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 de responsabilidad solidaria a todos sus socios o subcontratistas. Normalmente, los CISP no se ofertarán como socios subcontratistas formales, ya que su servicio estandarizado a gran escala no está adaptado a los requisitos únicos de un cliente final en particular (incluidas las necesidades de un cliente del sector público en virtud de 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 por el motivo de que no son aplicables a un proveedor de «segundo nivel» de servicios comerciales. En este caso, el CISP no realiza el volumen de trabajo por sí mismo en virtud del contrato, sino que, en su lugar, un socio del CISP es quien utiliza la infraestructura del CISP para hacerlo. 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 normalmente rechazaría 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 Agentes en la nube

El uso del concepto de «agente en la nube» para reducir la posibilidad de dependencia de un proveedor puede ser problemático. Aunque un agente 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 conlleva inevitablemente concesiones en la capacidad (no existe ninguna piedra Rosetta para la nube). En definitiva, este enfoque puede añadir una capa innecesaria de complejidad entre los clientes del sector público y sus servicios en la nube, lo que podría comprometer las eficiencias y las mejoras en seguridad que esperan obtener, así como dar lugar a una reducción de la escalabilidad y la agilidad, un aumento de los costes y la desaceleración de la innovación.

3.5 Aprovisionamiento y estudio de mercado previos a la RFP

Cuando una entidad del sector público planifica una RFP de servicios en la nube, debe incluir las partes interesadas de todos los aspectos de la organización desde el inicio del proceso: el personal directivo, las partes interesadas de la empresa, la tecnología, las finanzas, las adquisiciones, los aspectos legales y los contratos. Este enfoque garantiza que todas las partes interesadas comprenden el modelo en la nube y que, por tanto, tienen una visión fundamentada que les permite 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 del mercado 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. Otras formas eficaces de obtener un profundo conocimiento sobre la adquisición en la nube son mediante la publicación de una RFI o, preferiblemente, la elaboración de un documento borrador de una RFP. A menudo hay problemas potenciales que se pueden identificar, discutir y ajustar antes de que se publique la RFP de servicios en la nube finalizada.

3.6 Sostenibilidad

La sostenibilidad es algo inherente en la computación en la nube, y la transición a la nube proporciona un beneficio en términos de eficiencia energética, en comparación con los centros de datos empresariales o los servidores locales. Identificar a un CISP que priorice la sostenibilidad y haya contraído compromisos públicos para lograr los objetivos de sostenibilidad proporciona una

garantía adicional de la sostenibilidad de la nube. Los CISP y operadores de centros de datos europeos (con el apoyo de la Comisión Europea) crearon el Pacto por la neutralidad climática de los centros de datos[11], una iniciativa de autorregulación para establecer criterios de sostenibilidad claros, simples y trascendentes para el sector de los centros de datos y garantizar que los operadores de centros de datos y proveedores de servicios en la nube sean climáticamente neutros en 2030. La iniciativa de autorregulación incluye objetivos claros de eficiencia energética de los centros de datos, conservación del agua, reutilización y reparación de servidores y uso de energía libre de carbono para alimentar los centros de datos. Los CISP que se registran en la iniciativa de autorregulación aceptan cumplir estos objetivos y certificar el cumplimiento de los criterios para considerarse operadores climáticamente neutros.

Una RFP de servicios en la nube debería pedir a los CISP si se han comprometido con estos criterios, específicamente si se han registrado para la autorregulación, y cuándo lo han hecho.

Texto de ejemplo de una RFP: sostenibilidad

¿Se ha comprometido para dirigir centros de datos climáticamente neutros a través de la iniciativa de autorregulación de neutralidad climática en los centros de datos? Si es así, ¿cuándo la firmó?

¿Puede probar que se le ha concedido el sello del Pacto por la neutralidad climática de los centros de datos?

[11] https://www.climateneutraldatacentre.net/self-regulatory-initiative/

Apéndice A: requisitos técnicos para la comparación entre licitantes

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

1. Perfil del proveedor de servicios en la nube

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

2. Infraestructura global

	Requisito
1.	*ALCANCE GLOBAL:* *¿Ofrece el proveedor de servicios en la nube una infraestructura global para ayudar a los usuarios a lograr una baja latencia y un alto rendimiento?*
2.	*REGIONES:* *¿Tiene el proveedor de servicios en la nube presencia regional en las regiones geográficas necesarias?*
3.	*DOMINIOS O ZONAS:* *¿Implementa el proveedor de servicios en la nube el concepto de dominios o zonas en los 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 servicios en la 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 DISEÑADOS:* *¿Ofrece el proveedor de servicios en la nube centros de datos diseñados para que queden aislados de los errores de otros centros de datos con alimentación redundante, refrigeración y redes?*
6.	*REPLICACIÓN EN CENTROS DE DATOS:* *¿Ofrece el proveedor de servicios en la nube replicación de datos en todos los centros de datos de un domino o una zona con conmutación por error automática?*
7.	*REPLICACIÓN EN DOMINIOS O ZONAS:* *¿Ofrece el proveedor de servicios en la nube replicación de datos en todos los dominios o las zonas de una región?*

3. Infraestructura

3.1 Computación

	Requisito
1.	*COMPUTACIÓN – INSTANCIA NORMAL – USO GENERAL:* *¿Ofrece el proveedor de servicios en la nube los siguientes tipos de instancia?* • *Uso general: optimizada para las aplicaciones genéricas; proporciona un equilibrio de recursos de computación, memoria y redes.* o *En caso afirmativo, ¿cuál es la instancia de mayor tamaño?*
2.	*COMPUTACIÓN – INSTANCIA NORMAL – OPTIMIZADA PARA LA MEMORIA:* *¿Ofrece el proveedor de servicios en la nube los siguientes tipos de instancia?* • *Optimizada para la memoria: optimizada para aplicaciones que hacen un uso intensivo de la memoria.* o *En caso afirmativo, ¿cuál es la instancia de mayor tamaño?*
3.	*COMPUTACIÓN – INSTANCIA NORMAL – OPTIMIZADA PARA LA COMPUTACIÓN:* *¿Ofrece el proveedor de servicios en la nube los siguientes tipos de instancia?* • *Optimizada para la computación: optimizada para aplicaciones que exigen una alta capacidad de computación.* o *En caso afirmativo, ¿cuál es la instancia de mayor tamaño?*
4.	*COMPUTACIÓN – INSTANCIA NORMAL – OPTIMIZADA PARA EL ALMACENAMIENTO:* *¿Ofrece el proveedor de servicios en la nube los siguientes tipos de instancia?* • *Optimizada para el almacenamiento: ofrece una gran capacidad de almacenamiento local.* o *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 en una instancia y asociarse a esta?*
5.	*COMPUTACIÓN – INSTANCIA NORMAL – OPTIMIZADA PARA GRÁFICOS:* *¿Ofrece el proveedor de servicios en la nube los siguientes tipos de instancia?* • *Gráficos de bajo coste: ofrece aceleración de gráficos de bajo coste en las instancias de computación.* o *En caso afirmativo, ¿cuál es la instancia de mayor tamaño?*
6.	*COMPUTACIÓN – INSTANCIA NORMAL – OPTIMIZADA PARA GPU:* *¿Ofrece el proveedor de servicios en la nube los siguientes tipos de instancia?* • *GPU: ofrece unidades de procesamiento de gráficos (GPU) de hardware para aplicaciones que hacen un uso intensivo de gráficos.* o *En caso afirmativo, ¿cuántas GPU y qué modelos de GPU puede ofrecer el proveedor de servicios en la nube por instancia?*
7.	*COMPUTACIÓN – INSTANCIA NORMAL – OPTIMIZADA PARA FPGA:* *¿Ofrece el proveedor de servicios en la nube los siguientes tipos de instancia?* • *FPGA: ofrece matrices de puertas programables de campo (FPGA) para el desarrollo y la implementación de la aceleración de hardware personalizado para las aplicaciones.* o *En caso afirmativo, ¿cuántas FPGA puede ofrecer el proveedor de servicios en la nube por instancia?*

8.	*COMPUTACIÓN – INSTANCIA AMPLIABLE:* *¿Ofrece el proveedor de servicios en la nube instancias ampliables que proporcionen un nivel de referencia de rendimiento de la unidad de procesamiento central (CPU) con capacidad para ampliarse por encima de la base de referencia?* • *En caso afirmativo, ¿cuál es la instancia con mayor capacidad de ampliación?*
9.	*COMPUTACIÓN – INSTANCIA DE E/S INTENSIVA:* *¿Ofrece el proveedor de servicios en la nube instancias que utilicen unidades de estado sólido (SSD) de memoria exprés no volátil (NVMe) optimizadas para la 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 operaciones de entrada/salida por segundo (IOPS) de la instancia de mayor tamaño?*
10.	*COMPUTACIÓN – ALMACENAMIENTO LOCAL TEMPORAL:* *¿Ofrece el proveedor de servicios en la 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 TARJETAS NIC:* *¿Permite el proveedor de servicios en la nube que se asignen varias tarjetas de interfaz de red (NIC) (primaria y adicional) 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 servicios en la nube a los usuarios la capacidad de agrupar instancias de forma lógica en el mismo centro de datos?*
13.	*COMPUTACIÓN – ANTIAFINIDAD DE INSTANCIAS:* *¿Ofrece el proveedor de servicios en la nube a los usuarios la capacidad de agrupar instancias de forma lógica y situarlas en diferentes centros de datos de una región?*
14.	*COMPUTACIÓN – APROVISIONAMIENTO DE AUTOSERVICIO:* *¿Ofrece el proveedor de servicios en la nube un aprovisionamiento de autoservicio de varias 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 servicios en la nube instancias personalizables; por ejemplo, la capacidad de modificar ajustes de configuración como unidades centrales de procesamiento virtual (vCPU) y memoria de acceso aleatorio (RAM)?*
16.	*COMPUTACIÓN – TENENCIA:* *¿Ofrece el proveedor de servicios en la nube instancias de inquilino único que se ejecuten en hardware dedicado para un solo usuario?* • *En caso afirmativo, ¿cuál es la instancia de inquilino único de mayor tamaño disponible?*
17.	*COMPUTACIÓN – AFINIDAD DEL HOST:* *¿Ofrece el proveedor de servicios en la nube la capacidad de ejecutar una instancia y de especificar que siempre se reinicie en el mismo host físico?*
18.	*COMPUTACIÓN – ANTIAFINIDAD DEL ANFITRIÓN:* *¿Ofrece el proveedor de servicios en la nube la capacidad de dividir y hospedar instancias específicas en los diferentes hosts físicos?*

19.	*COMPUTACIÓN – ESCALADO AUTOMÁTICO:* *¿Ofrece el proveedor de servicios en la 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 servicios en la nube a los usuarios la capacidad de importar sus imágenes existentes y de guardarlas como imágenes nuevas disponibles 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 servicios en la nube la capacidad de exportar una instancia en ejecución existente o una copia de una instancia a un formato de máquina virtual?* • *En caso afirmativo, ¿cuáles son los formatos admitidos?*
22.	*COMPUTACIÓN – INTERRUPCIÓN DEL SERVICIO:* *¿Ofrece el proveedor de servicios en la nube mecanismos para evitar interrupciones y tiempos de inactividad en la instancia cuando este realiza algún tipo de mantenimiento del servicio o el hardware a nivel de host?*
23.	*COMPUTACIÓN – REINICIO DE INSTANCIAS:* *¿Ofrece el proveedor de servicios en la nube mecanismos para reiniciar las instancias de forma automática en un host en buen estado si falla el host físico original?*
24.	*COMPUTACIÓN – NOTIFICACIONES:* *Si se produce un evento de computación resistente, ¿tiene el proveedor de servicios en la nube la capacidad de notificar al usuario que se ha producido dicho evento? Así mismo, ¿puede el usuario participar en esta comunicación o salir de ella mediante opciones de autoservicio?*
25.	*COMPUTACIÓN – PROGRAMACIÓN DE EVENTOS:* *¿Ofrece el proveedor de servicios en la nube la capacidad 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 servicios en la nube un mecanismo integrado de copia de seguridad y recuperación?*
27.	*COMPUTACIÓN – MECANISMO DE INSTANTÁNEA:* *¿Ofrece el proveedor de servicios en la nube un mecanismo manual de instantánea bajo demanda?*
28.	*COMPUTACIÓN – METADATOS:* *¿Ofrece el proveedor de servicios en la 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 servicios en la nube un servicio de metadatos de instancia que proporcione una interfaz de programa de aplicación (API) que pueda llamar la instancia para buscar información sobre sí misma?*
30.	*COMPUTACIÓN – MECANISMO DE LICITACIÓN:* *¿Ofrece el proveedor de servicios en la nube un mecanismo de licitación para ofertar instancias de coste más bajo de las que se puedan crear instancias de forma inmediata para alojar cargas de trabajo no esenciales?*
31.	*COMPUTACIÓN – MECANISMO DE PROGRAMACIÓN:* *¿Ofrece el proveedor de servicios en la 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 servicios en la 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 servicios en la 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 servicios en la nube con las dos versiones principales más recientes de Windows Server (Windows Server 2017 y Windows Server 2016)?*
35.	***COMPUTACIÓN – PORTABILIDAD DE LICENCIAS:*** *¿Ofrece el proveedor de servicios en la nube asistencia y portabilidad para las licencias?* • *En caso afirmativo, indique el proveedor de software, los nombres del software, las ediciones y sus versiones.*
36.	***COMPUTACIÓN – CUOTAS DE SERVICIO:*** *¿Establece el proveedor de servicios en la nube alguna restricción (p. ej., cuotas de servicio) en cuanto a la sección de computación anterior?* *Ejemplo:* *Número máximo de instancias por cuenta.* *Número máximo de hosts dedicados por cuenta.* *Número máximo de direcciones de protocolo de Internet (IP) reservadas.*

3.2 Redes

	Requisito
1.	***REDES – REDES VIRTUALES:*** *¿Ofrece el proveedor de servicios en la nube la capacidad de crear una red virtual lógica aislada que represente la red de la empresa en la nube?*
2.	***REDES – CONECTIVIDAD EN LA MISMA REGIÓN:*** *¿Admite el proveedor de servicios en la nube la conexión de dos redes virtuales dentro de la misma región para enrutar el tráfico entre ellas mediante direcciones privadas de protocolo de Internet (IP)?*
3.	***REDES – CONECTIVIDAD ENTRE DIFERENTES REGIONES:*** *¿Admite el proveedor de servicios en la nube la conexión de dos redes virtuales de diferentes regiones para enrutar el tráfico entre ellas mediante direcciones privadas de protocolo de Internet (IP)?*
4.	***REDES – SUBRED PRIVADA:*** *¿Ofrece el proveedor de servicios en la 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 – INTERVALO DE DIRECCIONES DE RED VIRTUAL:* *¿Admite el proveedor de servicios en la nube los intervalos 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 servicios en la nube varios protocolos tales como el protocolo de control de transmisión (TCP), el protocolo de datagramas de usuario (UDP) y el protocolo de mensajes de control de Internet (ICMP)?*
7.	*REDES – ASIGNACIÓN AUTOMÁTICA DE DIRECCIONES IP:* *¿Ofrece el proveedor de servicios en la 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 servicios en la nube direcciones del protocolo de Internet (IP) asociadas con la cuenta de usuario y no con una instancia determinada? La dirección IP debe permanecer asociada con la cuenta hasta que se publique de forma explícita.*
9.	*REDES – COMPATIBILIDAD CON IPV6:* *¿Admite el proveedor de servicios en la nube el protocolo de Internet versión 6 (IPv6) con respecto a la puerta de enlace o la instancia y expone esta funcionalidad a los usuarios?*
10.	*REDES – VARIAS DIRECCIONES IP POR NIC:* *¿Ofrece el proveedor de servicios en la nube la capacidad de asignar una dirección de protocolo de Internet (IP) primaria y una secundaria a una tarjeta de interfaz de red (NIC) asociada a una instancia determinada?*
11.	*REDES – VARIAS NIC:* *¿Ofrece el proveedor de servicios en la 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 servicios en la nube la capacidad de mover las tarjetas de interfaz de red (NIC) y las direcciones de protocolo de Internet (IP) entre instancias?*
13.	*REDES – COMPATIBILIDAD CON SR-IOV:* *¿Ofrece el proveedor de servicios en la 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 una menor vibración?*
14.	*REDES – FILTRADO DE ENTRADA:* *¿Permite el proveedor de servicios en la nube añadir o eliminar reglas aplicables al tráfico de entrada a las instancias?*
15.	*REDES – FILTRADO DE SALIDA:* *¿Permite el proveedor de servicios en la nube añadir o eliminar reglas aplicables al tráfico de salida que se origina en las instancias?*
16.	*REDES – ACL:* *¿Ofrece el proveedor de servicios en la nube acceso a las listas de control de acceso (ACL) para controlar el tráfico entrante y saliente de las subredes?*
17.	*REDES – COMPATIBILIDAD CON EL REGISTRO DE FLUJO:* *¿Ofrece el proveedor de servicios en la nube la capacidad de capturar los registros de flujo de tráfico de red?*

18.	*REDES – NAT:* *¿Proporciona el proveedor de servicios en la nube un servicio administrado de puerta de enlace de traducción de direcciones de red (NAT) en una red privada para conectarse a Internet o a otros servicios en la nube, pero que evita que Internet inicie una conexión con dichas instancias?*
19.	*REDES – COMPROBACIÓN DE ORIGEN/DESTINO:* *¿Tiene el proveedor de servicios en la nube la capacidad de desactivar la comprobación de origen/destino en las tarjetas de interfaz de red (NIC)?*
20.	*REDES – COMPATIBILIDAD CON VPN:* *¿Ofrece el proveedor de servicios en la nube conectividad de red privada virtual (VPN) entre sí mismo y el centro de datos del usuario?*
21.	*REDES – TÚNELES DE VPN:* *¿Admite el proveedor de servicios en la nube varias conexiones de red privada virtual (VPN) por red virtual?*
22.	*REDES – COMPATIBILIDAD CON VPN de IPSEC:* *¿Permite el proveedor de servicios en la 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 capa de sockets seguros (SSL)?*
23.	*REDES – COMPATIBILIDAD CON BGP:* *¿Utiliza el proveedor de servicios en la nube el protocolo de puerta de enlace 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 servicios en la nube un servicio de conectividad privada directa entre las ubicaciones de dicho proveedor y el centro de datos, la oficina o el entorno de coubicación de un usuario que permita transferencias de datos rápidas y de gran volumen?*
25.	*REDES – EQUILIBRADOR DE CARGA DE FRONT-END:* *¿Ofrece el proveedor de servicios en la nube un servicio de equilibrio 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 equilibrador de carga?*
26.	*REDES – EQUILIBRADOR DE CARGA DE BACK-END:* *¿Ofrece el proveedor de servicios en la nube un servicio de equilibrio de carga de back-end (privado) que enrute el tráfico hacia instancias alojadas en subredes privadas?*
27.	*REDES – EQUILIBRADOR DE CARGA DE CAPA 7:* *¿Ofrece el proveedor de servicios en la nube un servicio de equilibrio de carga de capa 7 (protocolo de transferencia de hipertexto [HTTP]) que pueda equilibrar la carga del tráfico de red en varias instancias?*
28.	*REDES – EQUILIBRADOR DE CARGA DE CAPA 4:* *¿Ofrece el proveedor de servicios en la nube un servicio de equilibrio de carga de capa 4 (protocolo de control de transmisión [TCP]) que pueda equilibrar la carga del tráfico de red en varias instancias?*
29.	*REDES – AFINIDAD DE SESIÓN DE LOS EQUILIBRADORES DE CARGA:* *¿Ofrece el proveedor de servicios en la nube un servicio de equilibrio de carga que admita la afinidad de sesión?*
30.	*REDES – EQUILIBRADOR DE CARGA BASADO EN DNS:* *¿Ofrece el proveedor de servicios en la nube un servicio de equilibrio de carga que pueda equilibrar la carga del tráfico a las instancias alojadas en varios hosts que pertenecen a un solo dominio?*

31.	***REDES – REGISTROS DEL EQUILIBRADOR DE CARGA:*** *¿Proporciona el proveedor de servicios en la nube registros que capturen información detallada sobre todas las solicitudes enviadas a un equilibrador de carga?*
32.	***REDES – DNS:*** *¿Ofrece el proveedor de servicios en la nube un servicio de sistema de nombres de dominio (DNS) de alta disponibilidad y escalable?*
33.	***REDES – ENRUTAMIENTO DE DNS BASADO EN LA LATENCIA:*** *¿Ofrece el proveedor de servicios en la nube un servicio de sistema de nombres de dominio (DNS) que admita un enrutamiento basado en la latencia (p. ej., el servicio DNS responde a 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 servicios en la 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 a 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 servicios en la 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 que está activo actualmente, 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 servicios en la 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 servicios en la nube un servicio de sistema de nombres de dominio (DNS) que utilice comprobaciones de estado para supervisar el estado y el rendimiento de los recursos?*
38.	***REDES – INTEGRACIÓN DEL DNS Y EL EQUILIBRADOR DE CARGA:*** *¿Ofrece el proveedor de servicios en la nube un servicio de sistema de nombres de dominio (DNS) que se integre con el equilibrador de carga de dicho proveedor?*
39.	***REDES – EDITOR VISUAL:*** *¿Ofrece el proveedor de servicios en la nube una herramienta que permita a los usuarios crear políticas de administración del tráfico?*
40.	***RED DE ENTREGA DE CONTENIDO (CDN):*** *¿Ofrece el proveedor de servicios en la nube un servicio de red de entrega de contenido (CDN) 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 servicios en la nube un servicio de red de entrega de contenido (CDN) que permita eliminar un objeto de las cachés perimetrales antes de que caduque y que incluya características como la invalidación de objetos y el control de versiones de objetos?*
42.	***REDES – ORÍGENES EXTERNOS DE CDN:*** *¿Ofrece el proveedor de servicios en la 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 servicios en la 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 localizadores uniformes de recursos (URL)?*
44.	*REDES – CDN CON RESTRICCIÓN GEOGRÁFICA:* *¿Ofrece el proveedor de servicios en la 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 servicios en la nube un servicio de red de entrega de contenido (CDN) que admita localizadores uniformes de recursos (URL) firmados que suelan incluir información adicional, como la fecha y hora de vencimiento, para otorgar a los usuarios mayor control sobre el acceso a su contenido?*
46.	*REDES – CERTIFICADOS DE CDN:* *¿Ofrece el proveedor de servicios en la nube un servicio de red de entrega de contenido (CDN) que admita certificados personalizados de capa de sockets seguros (SSL) para entregar el contenido de forma segura mediante un protocolo seguro de transferencia de hipertexto (HTTPS) desde ubicaciones de borde?*
47.	*REDES – CACHÉ DE VARIAS CAPAS DE CDN:* *¿Ofrece el proveedor de servicios en la 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 regionales para reducir la latencia?*
48.	*REDES – COMPRESIÓN DE CDN:* *¿Ofrece el proveedor de servicios en la 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 servicios en la nube una red de entrega de contenido (CDN) que permita a los usuarios cargar su información confidencial de forma segura de manera que solo puedan verla determinados componentes y servicios en la infraestructura de origen del usuario?*
50.	*REDES – PUNTOS DE CONEXIÓN:* *¿Ofrece el servicio de red del proveedor de servicios en la nube a los usuarios puntos de conexión 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 – CUOTAS DE SERVICIO:* *¿Establece el proveedor de servicios en la nube alguna restricción (p. ej., cuotas de servicio) en cuanto a la sección de redes anterior?* *Ejemplo:* *Número máximo de redes virtuales por cuenta.* *Tamaño máximo de una red virtual.* *Número máximo de subredes por cuenta.* *Número máximo de equilibradores de carga por cuenta.* *Número máximo de entradas de la lista de control de acceso (ACL).* *Número máximo de túneles de la red privada virtual (VPN).* *Número máximo de orígenes por distribución.* *Número máximo de certificados por equilibrador de carga.*

3.3 Almacenamiento

	Requisito
1.	*SERVICIO DE ALMACENAMIENTO EN BLOQUES:* *¿Ofrece el proveedor de servicios en la nube volúmenes de almacenamiento con respecto a bloques para utilizarlos con las instancias de computación?*
2.	*ALMACENAMIENTO EN BLOQUES – IOPS:* *¿Ofrece el proveedor de servicios en la 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/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 servicios en la nube medios de almacenamiento basados 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 pueden asociar por instancia?*
4.	*ALMACENAMIENTO EN BLOQUES – ESCALADO:* *¿Ofrece el proveedor de servicios en la 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 servicios en la nube de capacidad de instantáneas para su servicio de almacenamiento en bloques?*
6.	*ALMACENAMIENTO EN BLOQUES – ERRADICACIÓN DE DATOS:* *¿Ofrece el proveedor de servicios en la nube una erradicación completa de datos de manera que los usuarios no autorizados o terceros ya no puedan leerlos ni acceder a ellos?*
7.	*ALMACENAMIENTO EN BLOQUES – CIFRADO EN REPOSO:* *¿Ofrece el proveedor de servicios en la nube cifrado de datos en reposo del lado del servidor para los datos almacenados en volúmenes y sus instantáneas?* • *En caso afirmativo, ¿qué algoritmo de cifrado se emplea?*
8.	*SERVICIO DE ALMACENAMIENTO DE OBJETOS:* *¿Ofrece el proveedor de servicios en la 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 servicios en la 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 servicios en la 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 servicios en la nube un nivel para los datos a los que se accede con menor frecuencia pero que igualmente requieren un acceso rápido?*

12.	*ALMACENAMIENTO DE OBJETOS – NIVELES DE OBJETOS:* *¿Ofrece el proveedor de servicios en la nube la capacidad de organizar en niveles 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:* *¿Permite el proveedor de servicios en la nube administrar el 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 servicios en la 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 servicios en la 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 servicios en la 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 servicios en la nube el cifrado del lado del servidor (SSE) de datos en reposo, en el que dicho proveedor administra las claves de cifrado?* • *En caso afirmativo, ¿qué algoritmo de cifrado se emplea?*
18.	*ALMACENAMIENTO DE OBJETOS – CIFRADO CON CLAVES DE USUARIO:* *¿Ofrece el proveedor de servicios en la nube capacidades de cifrado del lado del servidor (SSE) mediante las claves criptográficas suministradas por el cliente?*
19.	*ALMACENAMIENTO DE OBJETOS – SERVICIO DE ADMINISTRACIÓN DE CLAVES:* *¿Admite el proveedor de servicios en la nube el cifrado del lado del servidor (SSE) mediante un servicio de administración de claves que permita crear claves de cifrado, definir las políticas que controlan cómo se pueden utilizar dichas claves y auditar el uso de las claves para comprobar que se utilizan correctamente?*
20.	*ALMACENAMIENTO DE OBJETOS – CLAVE MAESTRA DEL LADO DEL CLIENTE:* *¿Ofrece el proveedor de servicios en la nube a los usuarios la opción de retener el control de las claves de cifrado y completar el cifrado o descifrado de los objetos del lado del cliente?*
21.	*ALMACENAMIENTO DE OBJETOS – ALTA COHERENCIA:* *¿Es compatible el proveedor de servicios en la 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 servicios en la 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?*
23.	*ALMACENAMIENTO DE OBJETOS – REPLICACIÓN:* *¿Ofrece el proveedor de servicios en la nube una característica 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 servicios en la 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 servicios en la nube al usuario marcar un elemento como recuperable?*
26.	*ALMACENAMIENTO DE OBJETOS – ELIMINACIÓN CON MFA:* *¿Admite el proveedor de servicios en la nube la autenticación multifactor (MFA) para las operaciones de eliminación como opción de seguridad adicional?*
27.	*ALMACENAMIENTO DE OBJETOS – CARGA MULTIPARTE:* *¿Admite el proveedor de servicios en la 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 dichas partes de los objetos se pueden cargar de forma independiente y en cualquier orden?*
28.	*ALMACENAMIENTO DE OBJETOS – ETIQUETAS:* *¿Ofrece el proveedor de servicios en la nube la capacidad de crear y asociar etiquetas dinámicas mutables a nivel de objeto?*
29.	*ALMACENAMIENTO DE OBJETOS – NOTIFICACIONES:* *¿Ofrece el proveedor de servicios en la nube la capacidad de enviar notificaciones cuando se producen determinados eventos a nivel de objeto (p. ej., operaciones de adición o eliminación)?*
30.	*ALMACENAMIENTO DE OBJETOS – REGISTROS:* *¿Ofrece el proveedor de servicios en la nube la capacidad de generar registros de auditoría que incluyan detalles sobre una solicitud de acceso individual, como el solicitante, la hora de la solicitud, la acción de la solicitud, el estado de la respuesta y el código de error?*
31.	*ALMACENAMIENTO DE OBJETOS – INVENTARIO DE OBJETOS:* *¿Ofrece el proveedor de servicios en la 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 aquellos con acceso público?*
32.	*ALMACENAMIENTO DE OBJETOS – INVENTARIO DE METADATOS:* *¿Ofrece el proveedor de servicios en la 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 servicios en la nube la capacidad de enrutar los datos desde las ubicaciones de borde hasta el servicio de almacenamiento mediante una ruta de red optimizada?*
34.	*ALMACENAMIENTO DE OBJETOS – CAPACIDAD DE CONSULTA:* *¿Ofrece el proveedor de servicios en la 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 servicios en la 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 servicios en la 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 servicios en la 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 servicios en la nube una erradicación completa de datos de almacenamiento de archivos de manera que los usuarios no autorizados o terceros ya no puedan leerlos ni acceder a ellos?*
39.	*ALMACENAMIENTO DE ARCHIVOS – ALTA DISPONIBILIDAD:* *¿Proporciona el sistema de archivos administrados del proveedor de servicios en la nube un alto grado de alta disponibilidad?*
40.	*ALMACENAMIENTO DE ARCHIVOS – NFS:* *¿Admite el proveedor servicios en la nube el protocolo de sistema de archivos de red (NFS)?*
41.	*ALMACENAMIENTO DE ARCHIVOS – SMB:* *¿Admite el proveedor de servicios en la nube el protocolo de bloque de mensajes del servidor (SMB)?*
42.	*ALMACENAMIENTO DE ARCHIVOS – CIFRADO EN REPOSO:* *¿Es compatible el servicio de almacenamiento de archivos del proveedor de servicios en la nube con el cifrado en reposo?*
43.	*ALMACENAMIENTO DE ARCHIVOS – CIFRADO EN TRÁNSITO:* *¿Es compatible el servicio de almacenamiento de archivos del proveedor de servicios en la nube con el cifrado de datos en tránsito?*
44.	*ALMACENAMIENTO DE ARCHIVOS – HERRAMIENTA DE MIGRACIÓN DE DATOS:* *¿Ofrece el proveedor de servicios en la 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 servicios en la 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 servicios en la nube tolerancia a errores para su servicio de almacenamiento de archivado?*
47.	*ALMACENAMIENTO DE ARCHIVOS – INMUTABILIDAD:* *¿Ofrece el proveedor de servicios en la nube inmutabilidad para los objetos y los archivos archivados?*
48.	*ALMACENAMIENTO DE ARCHIVOS – WORM:* *¿Ofrece el proveedor de servicios en la nube la capacidad de escritura única y lectura múltiple (WORM)?*
49.	*ALMACENAMIENTO DE ARCHIVOS – RECUPERACIÓN DE SUBCONJUNTOS:* *¿Ofrece el proveedor de servicios en la 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 servicios en la 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 servicios en la nube con el cifrado en reposo?*
52.	*ALMACENAMIENTO – CUOTAS DE SERVICIO:* *¿Establece el proveedor de servicios en la nube alguna restricción (p. ej., cuotas de servicio) en cuanto a la sección de almacenamiento anterior?* *Ejemplo:* *Tamaño de volumen máximo.* *Número máximo de unidades asociadas a una instancia.* *Número máximo de operaciones de entrada/salida por segundo (IOPS).* *Tamaño máximo del objeto.* *Número máximo de objetos por cuenta de almacenamiento.* *Número máximo de instantáneas.*

4. Administración

	Requisito
1.	*ADMINISTRACIÓN – USUARIOS Y GRUPOS:* *¿Ofrece el proveedor de servicios en la nube un servicio para crear y administrar usuarios y grupos de usuarios de su infraestructura y recursos?*
2.	*ADMINISTRACIÓN – RESTABLECIMIENTO DE CONTRASEÑAS:* *¿Permite el proveedor de servicios en la nube a los usuarios restablecer su propia contraseña en modo de autoservicio?*
3.	*ADMINISTRACIÓN – PERMISOS:* *¿Ofrece el proveedor de servicios en la nube la capacidad de añadir permisos a usuarios y grupos a nivel de recursos?*
4.	*ADMINISTRACIÓN – PERMISOS TEMPORALES:* *¿Ofrece el proveedor de servicios en la nube la capacidad de crear permisos que sean válidos para un intervalo de tiempo específico?*
5.	*ADMINISTRACIÓN – CRECENCIALES TEMPORALES:* *¿Ofrece el proveedor de servicios en la nube a los usuarios la capacidad de crear y proporcionar credenciales de seguridad temporales a los usuarios de confianza configuradas para durar entre unos minutos y varias horas?*
6.	*ADMINISTRACIÓN – CONTROL DE ACCESO:* *¿Ofrece el proveedor de servicios en la nube controles de acceso específicos para 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 servicios en la nube políticas de acceso integradas que se pueden asociar a usuarios y grupos?*

8.	*ADMINISTRACIÓN – POLÍTICAS PERSONALIZADAS:* *¿Permite la infraestructura del proveedor de servicios en la 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 servicios en la nube un mecanismo para probar los efectos de las políticas de control de acceso antes de remitir dichas políticas a la fase de producción?*
10.	*ADMINISTRACIÓN – MFA EN LA NUBE:* *¿Admite el proveedor de servicios en la nube el uso de la autenticación multifactor (MFA) como capa adicional de control de acceso y autenticación para su infraestructura?*
11.	*ADMINISTRACIÓN – CUOTAS DE SERVICIO:* *¿Aplica el proveedor de servicios en la nube alguna restricción (p. ej., cuotas de 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 servicios en la nube que tienen acceso a la infraestructura de servicios (tanto física como no física)?*
2.	*SEGURIDAD – ACCESO FÍSICO:* *¿Restringe el proveedor de servicios en la nube que el personal acceda a la infraestructura de servicios 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 servicios en la nube el acceso del personal a su infraestructura, donde dicho acceso siempre se registra y los registros se conservan durante un mínimo de 90 días?*
4.	*SEGURIDAD – INICIOS DE SESIÓN EN EL HOST:* *¿Restringe el proveedor de servicios en la nube que el personal inicie sesión en los hosts de computación, en lugar de automatizar todas las tareas realizadas en los hosts 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 servicios en la 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 servicios en la 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 servicios en la 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 servicios en la nube con otros servicios en la nube para ofrecer la capacidad de cifrado de datos en reposo?*
9.	*SEGURIDAD – HSM:* *¿Ofrece el proveedor de servicios en la nube módulos de seguridad de hardware (HSM) dedicados; por ejemplo, dispositivos de hardware que proporcionen un almacenamiento seguro de claves y operaciones criptográficas dentro de un módulo de hardware a prueba de manipulaciones?*
10.	*SEGURIDAD – DURABILIDAD DE LAS CLAVES CRIPTOGRÁFICAS:* *¿Ofrece el proveedor de servicios en la nube durabilidad de claves, como el almacenamiento de varias copias para que las claves estén disponibles cuando sea necesario?*
11.	*SEGURIDAD – SSO:* *¿Ofrece el proveedor de servicios en la 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 servicios en la 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 servicios en la nube la renovación de los certificados?*
14.	*SEGURIDAD – CERTIFICADOS COMODÍN:* *¿Admite el servicio de administración de certificados del proveedor de servicios en la nube el uso de certificados comodín?*
15.	*SEGURIDAD – ENTIDAD DE CERTIFICACIÓN:* *¿Actúa el servicio de administración de certificados del proveedor de servicios en la nube también como entidad de certificación (CA)?*
16.	*SEGURIDAD – ACTIVE DIRECTORY:* *¿Ofrece el proveedor de servicios en la 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 servicios en la nube la integración con Active Directory (AD) de Microsoft local?*
18.	*SEGURIDAD – LDAP:* *¿Es compatible el servicio administrado de Active Directory (AD) de Microsoft del proveedor de servicios en la 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 servicios en la nube con el lenguaje de marcado de aserción de seguridad (SAML)?*

20.	***SEGURIDAD – ADMINISTRACIÓN DE CREDENCIALES:*** *¿Ofrece el proveedor de servicios en la nube un servicio administrado que ayude a los usuarios a rotar, administrar y recuperar credenciales fácilmente, como las claves de la interfaz de programa de aplicación (API), las credenciales de base de datos y otros secretos?*
21.	***SEGURIDAD – WAF:*** *¿Ofrece el proveedor de servicios en la nube un firewall para aplicaciones web (WAF) que ayude a proteger las aplicaciones web de vulnerabilidades de seguridad web habituales que podrían afectar a la disponibilidad de la aplicación, poner en peligro la seguridad o consumir demasiados recursos?*
22.	***SEGURIDAD – DDOS:*** *¿Ofrece el proveedor de servicios en la nube un servicio para protegerse de los ataques comunes más frecuentes de denegación de servicio distribuido (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 servicios en la nube un servicio para evaluar de forma automática las posibles vulnerabilidades en las aplicaciones y los recursos?*
24.	***SEGURIDAD – DETECCIÓN DE AMENAZAS:*** *¿Ofrece el proveedor de servicios en la nube un servicio administrado de detección de amenazas?*
25.	***SEGURIDAD – CUOTAS DE SERVICIO:*** *¿Aplica el proveedor de servicios en la nube alguna restricción (p. ej., cuotas de servicio) en cuanto a la sección de seguridad anterior?* *Ejemplo:* *Número máximo de claves maestras del 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 cumplimiento internacionales y específicos del sector que cumple el proveedor de servicios en la nube.

Certificaciones y atestaciones	*Leyes, reglamentos 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*	
☐ CNDCP (Pacto por la neutralidad climática de los centros de datos)		
☐ DIACAP	*☐ FERPA*	*☐ CIS*

☐ *SRG del DoD; niveles 2 y 4*	☐ *RGPD*	☐ *Servicio de información de justicia criminal (CJIS)*
☐ *FedRAMP*	☐ *GLBA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *HIPAA*	☐ *Escudo de la privacidad entre la UE y los EE. UU.*
☐ *HDS (Francia, sanidad)*	☐ *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*
☐ *Regla 17-a-4(f) de la SEC*	☐ *Autorización del DPA español*	☐ *MITA 3.0*
☐ *SOC1/ISAE 3402*	☐ *DPA del Reino Unido (1988)*	☐ *MPAA*
☐ *SOC2/SOC3*	☐ *VPAT/Sección 508*	☐ *NIST*
☐ *Código IaaS de SWIPO*		
		☐ *Niveles de Uptime Institute*
		☐ *Principios de seguridad en la nube del Reino Unido*

El uso de los informes de cumplimiento anteriores permite a las organizaciones del sector público evaluar las ofertas individuales con respecto a los estándares aceptados de seguridad, de cumplimiento y operativos. Dichos informes pueden mostrar que el CISP, mediante su cumplimiento, también cumple los controles de funcionamiento del centro de datos siguientes que se exigen al proveedor de servicios en la nube pública. Al exigir el cumplimiento de dichos informes, las entidades del sector público pueden tener la seguridad de que se implementan los controles siguientes.

- *Acceso verificado: el CISP debe limitar el acceso físico solo a aquellas personas que deban estar en una ubicación por razones empresariales justificadas. Si se concede acceso, este se debe revocar tan pronto como se complete el trabajo necesario.*
- *Entrada controlada y supervisada: el acceso a la capa perimetral del centro de datos debe realizarse mediante un proceso controlado. El CISP debe contar con agentes de seguridad y supervisores de empleados en las puertas de entrada que supervisen a los agentes y visitantes mediante cámaras de seguridad. Cuando haya personas autorizadas en las instalaciones, se les debe entregar una credencial que requiera una autenticación multifactor y les 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 pertinentes de las instalaciones según el puesto de trabajo. Dicho acceso se controlará de manera estricta y periódica. 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 necesita estar de manera continua en el centro de datos, se le debe pedir que siga el proceso para visitantes.*

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

- *Supervisión de la seguridad global por parte de los centros de operaciones de seguridad del CISP: los centros de operaciones de seguridad del CISP deben estar distribuidos por todo el mundo y son responsables de supervisar, clasificar y ejecutar los programas de seguridad de los centros de datos del CISP. Deberán supervisar la administración del acceso físico y la respuesta a la detección de intrusiones. También deberán proporcionar asistencia global de forma ininterrumpida a los equipos de seguridad locales del centro de datos, además de realizar actividades de supervisión continuas, como el seguimiento de las actividades de acceso, la revocación de permisos de acceso y estar disponibles para responder a un posible incidente de seguridad y analizarlo.*

- *Revisión del acceso por capas: se debe restringir el acceso a la capa de infraestructura en función de las necesidades empresariales. Al implementar una revisión de acceso por capas, 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 equipamiento 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 equipamiento y los servicios del centro de datos deben formar parte de las operaciones habituales de los centros de datos del CISP.*

- *Equipamiento de reserva preparado para emergencias: el abastecimiento de agua, el suministro eléctrico, las telecomunicaciones y la conectividad de Internet se deben diseñar para ofrecer redundancia, de modo que el CISP pueda seguir realizando las operaciones continuas en caso de emergencia. Los sistemas eléctricos se deben diseñar de modo que sean completamente redundantes. De esta manera, en caso de interrupción, se pueden utilizar unidades de suministro ininterrumpido de energía para determinadas funciones hasta que los generadores puedan suministrar alimentación auxiliar a toda la instalación. Las personas y los sistemas deben supervisar y controlar la temperatura y la humedad para evitar sobrecalentamientos y, de este modo, reducir aún más la posibilidad de que se produzcan interrupciones en el servicio.*

- *Colaboración entre la tecnología y las personas para ofrecer una mayor seguridad: se deben establecer procedimientos obligatorios para obtener autorización de acceso a la capa de datos. Estos incluyen la revisión y aprobación de la solicitud de acceso de una persona por parte de los sujetos autorizados. Por su parte, los sistemas de detección de amenazas e intrusiones electrónicas deben supervisar las amenazas identificadas o cualquier actividad sospechosa y activar automáticamente alertas para estas. Por ejemplo, debe activarse una alarma si una puerta se mantiene abierta o si se fuerza su apertura. Los CISP deben instalar cámaras de seguridad y guardar las grabaciones de acuerdo con los requisitos legales y de cumplimiento.*

- *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 multifactor. El CISP también debe estar preparado para prevenir las intrusiones tecnológicas. Los servidores del CISP deben ser capaces de avisar a los empleados de cualquier intento de eliminación de datos. En el caso poco probable de que se produzca una infracción de seguridad, el servidor debe desactivarse de forma automática.*

- *Atención rigurosa a los servidores y los soportes físicos: el CISP debe clasificar como críticos los dispositivos de almacenamiento multimedia utilizados para guardar los datos de los clientes y tratarlos según 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 llegue al final de su vida útil, el CISP retirará los soportes físicos mediante las*

técnicas detalladas en NIST 800-88. Los soportes físicos que almacenan datos del cliente no se quitarán de la unidad de control del CISP hasta que se hayan retirado de forma segura.

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

- *Preparación ante imprevistos: el CISP debe prepararse de forma proactiva para posibles amenazas ambientales, como pueden ser los desastres naturales y los incendios. Dos formas en las que el CISP puede proteger los centros de datos son mediante la instalación de sensores automáticos y de equipamiento con capacidad de respuesta. Se deben instalar equipos de detección de agua que permitan avisar a los empleados de la existencia de problemas mientras las bombas automáticas retiran el líquido a fin de evitar daños. De igual modo, el equipamiento automático de detección y extinción de incendios reduce los riesgos y puede enviar una notificación a los empleados del CISP y a los bomberos sobre 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 rápidas de fibra óptica a fin de diseñar aplicaciones que realicen conmutaciones por error de forma automática entre las zonas de disponibilidad sin interrupciones.*

- *Simulación de interrupciones y medición de la respuesta: el CISP debe contar con un plan de continuidad del negocio que se utilice como guía del proceso operativo. Dicho plan debe describir cómo evitar y reducir las interrupciones causadas por desastres naturales, además de incluir los pasos detallados que se deben seguir antes, durante y después de un evento. Para mitigar y prepararse para los imprevistos, 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 y, a continuación, informar 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.*

- *Ayuda para 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, además de información sobre cómo pueden sus clientes reducir las emisiones de carbono con respecto a sus centros de datos.*

- *Selección del sitio: antes de seleccionar una ubicación, el CISP debe realizar evaluaciones geográficas y medioambientales iniciales. Las ubicaciones de los centros de datos se deben elegir cuidadosamente a fin de mitigar los 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: los centros de datos se deben diseñar 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 error en el centro de datos, se disponga de capacidad suficiente para equilibrar la carga del tráfico en los sitios restantes.*

- *Disponibilidad: el CISP debe identificar los componentes críticos del sistema necesarios para mantener su disponibilidad 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 que funcione de manera independiente con una alta fiabilidad. Las zonas de disponibilidad deben estar conectadas para que las aplicaciones puedan realizar conmutaciones por error de forma automática entre las zonas de disponibilidad sin interrupciones. La alta resistencia y, por tanto, la disponibilidad del servicio, deben*

ser características del diseño del sistema. El diseño del centro de datos con zonas de disponibilidad y replicación de datos debe permitir que los clientes del CISP logren 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 supervisar el uso del servicio de forma continua para implementar una 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 DE 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 con el objetivo de realizar mejoras continuas.*
- ***Respuesta en caso de pandemia:** el CISP debe incorporar políticas y procedimientos de respuesta frente a pandemias en su planificación de recuperación de 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 la región, así como 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 sanidad y los reglamentos sanitarios internacionales, incluidos los puntos de contacto de los organismos internacionales.*

SUPERVISIÓN y REGISTRO

- ***Revisión del acceso a los centros de datos:** el acceso a los centros de datos se debe revisar con regularidad. Este acceso se revocará de forma automática cuando se dé por finalizado 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 duración de la solicitud aprobada, se debe revocar su acceso aunque siga siendo empleado del CISP.*
- ***Registros de acceso a los centros de datos:** es necesario registrar, supervisar y conservar el acceso físico a los centros de datos del CISP. El CISP debe correlacionar la información obtenida de sistemas de supervisión lógicos y físicos para mejorar la seguridad según sea necesario.*
- ***Supervisión del acceso a los centros de datos:** el CISP debe supervisar los centros de datos a través de centros de operaciones de seguridad globales responsables de supervisar, clasificar y ejecutar programas de seguridad. Estos deben proporcionar asistencia global de forma ininterrumpida en la administración y supervisión de las actividades de acceso a los centros de datos, así como preparar a los equipos locales y otros equipos de asistencia para responder ante incidentes de seguridad mediante la clasificación, la consulta, el análisis y el envío de respuestas.*

VIDEOVIGILANCIA y DETECCIÓN

- ***CCTV:** una cámara de circuito cerrado de televisión (CCTV) 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 cumplimiento.*
- ***Puntos de entrada a los centros de datos:** en los puntos de acceso al edificio debe haber personal de seguridad profesional que controle el acceso físico mediante sistemas de videovigilancia y de detección y otros medios electrónicos. El personal autorizado debe utilizar mecanismos de autenticación multifactor para acceder a los centros de datos. Las entradas a las salas de los servidores deben estar protegidas con dispositivos que disparen alarmas sonoras a fin de iniciar una respuesta a un incidente en el caso de que se fuerce la puerta o se mantenga abierta.*
- ***Detección de intrusiones:** se deben instalar sistemas electrónicos de detección de intrusiones dentro de la capa de datos para supervisar y detectar los incidentes de seguridad y alertar de forma automática al personal adecuado sobre estos. Los puntos de entrada y salida de las salas de servidores se deben proteger con dispositivos que requieran la autenticación multifactor a cualquier persona que entre o salga. Estos dispositivos dispararán alarmas*

sonoras en el caso de que se fuerce la apertura de la puerta sin autenticación o esta se mantenga abierta. Los dispositivos de alarma para puertas también se deben configurar a fin de detectar los casos en que alguien salga de una capa de datos o entre a esta sin proporcionar la autenticación multifactor. Las alarmas se deben notificar 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 recursos del CISP se deben administrar de forma centralizada mediante un sistema de administración de inventario que almacene la información sobre el propietario, la ubicación, el estado, el mantenimiento y la descripción de los recursos que posee el CISP, así como que realice un seguimiento de esta. Después de su adquisición, es necesario examinar los recursos y realizar un seguimiento de ellos, mientras que, durante su mantenimiento, se debe comprobar y supervisar su propiedad, estado y resolución.*

- *Destrucción de los soportes físicos: el CISP debe clasificar como críticos los dispositivos de almacenamiento multimedia utilizados para guardar los datos de los clientes y tratarlos según 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 llegue al final de su vida útil, el CISP deberá retirar los soportes físicos mediante las técnicas detalladas en NIST 800-88. Los soportes físicos que almacenan datos del cliente no se deben quitar de la unidad de control del CISP hasta que se hayan retirado de forma segura.*

SISTEMAS DE SOPORTE OPERATIVO

- *Suministro eléctrico: los sistemas de suministro eléctrico de los centros de datos del CISP deben ser completamente redundantes y su mantenimiento debe poder realizarse sin causar ningún impacto en las operaciones que se ejecutan de manera ininterrumpida. El CISP debe asegurarse de que los centros de datos cuenten con suministro eléctrico auxiliar con el fin de garantizar que dicho suministro esté disponible para mantener las operaciones en el caso de que se produzca un fallo eléctrico que afecte a las 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. De este modo, se evitan sobrecalentamientos y se reduce la posibilidad de que se produzcan interrupciones en el servicio. El personal y los sistemas deben supervisar y controlar que se mantienen los niveles adecuados de temperatura y humedad.*

- *Detección y extinción de incendios: los centros de datos del CISP deben contar con equipamiento automático de detección y extinción de incendios. Los sistemas de detección de incendios deben utilizar sensores de detección de humo en los espacios de redes, de infraestructura y mecánicos. Estas áreas también deben estar protegidas mediante sistemas de extinción.*

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

MANTENIMIENTO DE LA INFRAESTRUCTURA

- *Mantenimiento del equipamiento: el CISP debe supervisar el equipo eléctrico y mecánico y llevar a cabo un mantenimiento preventivo de este para mantener la capacidad operativa continua de los sistemas en los centros de datos del CISP. Los procedimientos de mantenimiento del equipamiento 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 supervisar los sistemas y los equipos eléctricos y mecánicos para poder identificar los problemas de forma inmediata. Para ello, se deben utilizar herramientas de auditoría continua y la información que proporcionan los sistemas de administración de edificios y supervisión eléctrica del CISP. Así mismo, 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 periódicas de las amenazas y las vulnerabilidades de los centros de datos. La evaluación y mitigación continuas de las vulnerabilidades potenciales deben realizarse a través de actividades de evaluación de riesgos de los centros de datos. Esta evaluación se debe llevar a cabo junto con el proceso de evaluación de riesgos en el ámbito de empresa, que se utiliza para identificar y administrar los riesgos que se presentan en la empresa en general. En este proceso también se deben tener en cuenta los riesgos medioambientales y los relacionados con la normativa regional.*

- ***Certificación de seguridad de terceros:*** *las evaluaciones externas de los centros de datos del CISP, como se documentan en los informes de terceros, deben 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 cumplimiento y sus requisitos, los auditores externos pueden realizar pruebas de eliminación 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 servicios en la nube?*
2.	***MIGRACIONES – SUPERVISIÓN CENTRALIZADA:*** *¿Ofrece el proveedor de servicios en la nube a las organizaciones un servicio centralizado (p. ej., un solo panel) donde puedan supervisar el estado del servidor y las migraciones de aplicaciones, así como realizar un seguimiento de este?*
3.	***MIGRACIONES – PANEL:*** *¿Ofrece la herramienta de migración del proveedor de servicios en la 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 SERVICIOS EN LA NUBE:*** *¿Ofrece la herramienta de migración del proveedor de servicios en la nube integración con otras herramientas de migración de dicho proveedor que permitan realizar migraciones de servidores y aplicaciones?*
5.	***MIGRACIONES – HERRAMIENTAS DE TERCEROS:*** *¿Permite la herramienta de migración del proveedor de servicios en la 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 servicios en la nube una capacidad de seguimiento y supervisión 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 servicios en la nube un modo de migrar los servidores virtualizados locales a la nube?* • *En caso afirmativo, ¿qué entornos virtualizados se admiten actualmente?*
8.	***MIGRACIONES – DETECCIÓN DE SERVIDORES:*** *¿Tiene la herramienta de migración del proveedor de servicios en la nube una capacidad de detección que permita buscar automáticamente servidores virtuales locales para migrarlos a la nube?*

9.	*MIGRACIONES – DATOS DE RENDIMIENTO DEL SERVIDOR:* *¿Tiene la herramienta de migración del proveedor de servicios en la nube la capacidad de recopilar y mostrar el rendimiento del servidor o la máquina virtual, como el 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 servicios en la nube la capacidad de almacenar todos los datos recopilados en una base de datos centralizada?* • *En caso afirmativo, ¿las organizaciones pueden exportar estos datos? ¿A qué formatos?*
11.	*MIGRACIONES – CIFRADO EN REPOSO:* *¿Realiza el proveedor de servicios en la nube el cifrado en reposo de toda la información recopilada y almacenada en la base de datos de detección?*
12.	*MIGRACIONES – REPLICACIÓN PROGRESIVA DEL SERVIDOR:* *¿Ofrece la herramienta de migración del proveedor de servicios en la nube replicaciones del servidor progresivas en tiempo real y automatizadas durante la migración del servidor o la máquina virtual a fin de garantizar 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 servicios en la nube la realización de migraciones de la máquina virtual de VMWare del entorno local a la nube?*
14.	*MIGRACIONES – HYPER-V:* *¿Admite la herramienta de migración del proveedor de servicios en la nube la realización de migraciones de la máquina virtual de Hyper-V del entorno local a la nube?*
15.	*MIGRACIONES – DETECCIÓN DE APLICACIONES:* *¿Tiene la herramienta de migración del proveedor de servicios en la 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 servicios en la 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 servicios en la nube la capacidad de migrar bases de datos locales a la nube?*
18.	*MIGRACIONES – TIEMPO DE INACTIVIDAD DE LA MIGRACIÓN DE LAS BASES DE DATOS:* *¿Tiene la herramienta de migración del proveedor de servicios en la nube la capacidad de realizar una migración de las 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 servicios en la nube la migración de diferentes orígenes de bases de datos 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 servicios en la 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 servicios en la 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 servicios en la 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 servicios en la nube un servicio para integrar a la perfección el centro de datos de un cliente con servicios de almacenamiento en la nube a fin de poder transferir y almacenar datos en el servicio de almacenamiento del proveedor de servicios en la nube?*
24.	*MIGRACIONES – COPIAS DE SEGURIDAD EMPRESARIALES – ALMACENAMIENTO DE OBJETOS:* *¿Ofrece el servicio de copia de seguridad empresarial del proveedor de servicios en la 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 servicios en la nube a los usuarios almacenar y recuperar objetos mediante protocolos de archivos como el protocolo del 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 servicios en la nube a los usuarios almacenar y recuperar objetos mediante protocolos de bloques como el de interfaz para sistemas informáticos pequeños de Internet (iSCSI)?*
27.	*MIGRACIONES – COPIAS DE SEGURIDAD EMPRESARIALES – ACCESO A CINTAS:* *¿Permite el servicio de copia de seguridad empresarial del proveedor de servicios en la 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 servicios en la 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 servicios en la nube con el software de copia de seguridad de terceros que se usa habitualmente?*
30.	*MIGRACIONES – CUOTAS DE SERVICIO:* *¿Aplica el proveedor de servicios en la nube alguna restricción (p. ej., cuotas de 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 servicios en la nube un servicio de facturación con seguimiento y generación de informes que ayude a los usuarios a administrar y supervisar el uso que realizan de las ofertas en la nube?*
2.	***FACTURACIÓN – ALARMAS Y NOTIFICACIONES:*** *¿Ofrece el proveedor de servicios en la nube a los usuarios un mecanismo para configurar alarmas con notificaciones que alerten a los usuarios cuando su gasto ha superado un umbral específico?*
3.	***FACTURACIÓN – ADMINISTRACIÓN DE COSTES:*** *¿Ofrece el proveedor de servicios en la nube un mecanismo para crear y mostrar gráficos que resuman los costes y los gastos?*
4.	***FACTURACIÓN – PRESUPUESTOS:*** *¿Ofrece el proveedor de servicios en la nube un mecanismo para mostrar y administrar presupuestos y hacer previsiones de costes estimados?*
5.	***FACTURACIÓN – VISTA CONSOLIDADA:*** *¿Ofrece el proveedor de servicios en la nube un mecanismo para consolidar la facturación de varias cuentas en una sola cuenta de pago principal?*
6.	***FACTURACIÓN – CUOTAS DE SERVICIO:*** *¿Aplica el proveedor de servicios en la nube alguna restricción (p. ej., cuotas de 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 SUPERVISIÓN:*** *¿Ofrece el proveedor de servicios en la nube un servicio de supervisión para administrar los recursos y las aplicaciones en la nube que recopila, supervisa y para los que genera informes con métricas predefinidas?*
2.	***ADMINISTRACIÓN – ALARMAS:*** *¿Permite el servicio de supervisión del proveedor de servicios en la nube a los usuarios configurar alarmas?*
3.	***ADMINISTRACIÓN – MÉTRICAS PERSONALIZADAS:*** *¿Permite el servicio de supervisión del proveedor de servicios en la nube a los usuarios crear y supervisar métricas personalizadas?*
4.	***ADMINISTRACIÓN – DETALLES DE SUPERVISIÓN:*** *¿Proporciona el servicio de supervisión del proveedor de servicios en la nube varios niveles de detalle de supervisión, incluido el nivel de un minuto?*

5.	*ADMINISTRACIÓN – SERVICIO DE SEGUIMIENTO DE API:* *¿Ofrece el proveedor de servicios en la nube un servicio que registre, supervise y almacene la actividad de los recursos en la nube tanto con respecto a la consola como a la interfaz de programa de aplicación (API) para ofrecer una mejor visibilidad?* • *En caso afirmativo, ¿cuáles son los servicios del proveedor de servicios en la nube que se integran con este servicio de seguimiento?*
6.	*ADMINISTRACIÓN – NOTIFICACIÓN:* *¿Admite el proveedor de servicios en la nube la capacidad de enviar notificaciones según los niveles de actividad de la interfaz de programa de aplicación (API)?*
7.	*ADMINISTRACIÓN – COMPRESIÓN:* *¿Ofrece el proveedor de servicios en la nube un mecanismo para comprimir los registros que genera el sistema de seguimiento de la interfaz de programa de aplicación (API) a fin de ayudar a los usuarios a reducir los costes de almacenamiento asociados a este servicio?*
8.	*ADMINISTRACIÓN – AGRUPACIÓN DE REGIONES:* *¿Ofrece el proveedor de servicios en la nube la capacidad de registrar la actividad de la interfaz de interfaz de programa de aplicación (API) de la cuenta en todas las regiones y de presentar esta información de forma global para facilitar su uso?*
9.	*ADMINISTRACIÓN – INVENTARIO DE RECURSOS:* *Ofrece el proveedor de servicios en la nube un servicio para evaluar y auditar las configuraciones de los recursos que implementa un usuario?*
10.	*ADMINISTRACIÓN – CAMBIOS DE CONFIGURACIÓN:* *¿Registra el proveedor de servicios en la nube de forma automática un cambio de configuración en los recursos cuando este se produce?*
11.	*ADMINISTRACIÓN – HISTORIAL DE CONFIGURACIÓN:* *¿Ofrece el proveedor de servicios en la nube la capacidad de examinar la configuración de los recursos en cualquier momento del pasado?*
12.	*ADMINISTRACIÓN – REGLAS DE CONFIGURACIÓN:* *¿Ofrece el proveedor de servicios en la nube directrices y recomendaciones para el aprovisionamiento, la configuración y la supervisión continua del cumplimiento de la normativa?*
13.	*ADMINISTRACIÓN – PLANTILLAS DE RECURSOS:* *¿Ofrece el proveedor de servicios en la nube a los usuarios la capacidad de crear, aprovisionar y administrar una recopilación de recursos mediante plantillas?*
14.	*ADMINISTRACIÓN – REPLICACIÓN DE PLANTILLAS DE RECURSOS:* *¿Ofrece el proveedor de servicios en la nube la capacidad de replicar rápidamente estas plantillas de recursos en diferentes regiones para su posible uso en situaciones de recuperación de desastres (DR)?*
15.	*ADMINISTRACIÓN – DISEÑADOR DE PLANTILLAS:* *¿Ofrece el proveedor de servicios en la 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 servicios en la 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 servicios en la nube una interfaz de usuario basada en Web para facilitar la administración y supervisión de los servicios en la nube?*
18.	***ADMINISTRACIÓN – ACCESO DESDE LA CLI:*** *¿Ofrece el proveedor de servicios en la nube una herramienta unificada para administrar y configurar varios servicios en la nube desde la interfaz de la línea de comandos (CLI) a fin de automatizar las tareas de administración mediante el uso de scripts?*
19.	***ADMINISTRACIÓN – ACCESO MÓVIL:*** *¿Ofrece el proveedor de servicios en la nube una aplicación para smartphones 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 servicios en la nube un servicio que ayude a los usuarios a comparar su uso de la nube en relación con las prácticas recomendadas?*
21.	***ADMINISTRACIÓN – CUOTAS DE SERVICIO:*** *¿Aplica el proveedor de servicios en la nube alguna restricción (p. ej., cuotas de 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. Asistencia

	Requisito
1.	***ASISTENCIA – SERVICIO:*** *¿Ofrece el proveedor de servicios en la nube asistencia ininterrumpida (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.	***ASISTENCIA – NIVELES DE ASISTENCIA:*** *¿Ofrece el proveedor de servicios en la nube diferentes niveles de asistencia?*
3.	***ASISTENCIA – ASIGNACIÓN DE NIVELES:*** *¿Permite el proveedor de servicios en la nube a los usuarios autoasignarse los recursos o los servicios consumidos en diferentes niveles de asistencia 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 asistencia?*
4.	***ASISTENCIA – FOROS:*** *¿Ofrece el proveedor de servicios en la nube foros de asistencia públicos donde los clientes pueden comentar problemas?*
5.	***ASISTENCIA – PANEL DE ESTADO DEL SERVICIO:*** *¿Ofrece el proveedor de servicios en la nube un panel de estado del servicio que muestre información actualizada sobre la disponibilidad del servicio en varias regiones?*

6.	*ASISTENCIA – PANEL PERSONALIZADO:* *¿Ofrece el proveedor de servicios en la nube un panel que muestre una vista personalizada del rendimiento y la disponibilidad de los servicios subyacentes a los recursos específicos del usuario?*
7.	*ASISTENCIA – HISTORIAL DEL PANEL:* *¿Ofrece el proveedor de servicios en la nube un historial del panel de estado del servicio de 365 días?*
8.	*ASISTENCIA – ASESOR EN LA NUBE:* *¿Ofrece el proveedor de servicios en la nube un servicio que actúe como un experto en la nube personalizado y ayude a comparar el uso de recursos en relación con las prácticas recomendadas?*
9.	*ASISTENCIA – TAM:* *¿Ofrece el proveedor de servicios en la nube un administrador técnico de cuenta (TAM) que proporcione experiencia técnica para la gama completa de servicios en la nube?*
10.	*ASISTENCIA – ASISTENCIA PARA APLICACIONES DE TERCEROS:* *¿Ofrece el proveedor de servicios en la nube compatibilidad con los sistemas operativos comunes y los componentes de la pila de aplicaciones comunes?*
11.	*ASISTENCIA – API PÚBLICA:* *¿Ofrece el proveedor de servicios en la nube una interfaz de programa de aplicación (API) que interactúe de forma programática con casos de asistencia para crearlos, editarlos y cerrarlos?*
12.	*ASISTENCIA – DOCUMENTACIÓN DE LOS SERVICIOS:* *¿Ofrece el proveedor de servicios en la nube documentación técnica de calidad disponible públicamente para todos sus servicios, incluidos, entre otros, guías de usuario, tutoriales, preguntas frecuentes (FAQ) y notas de la versión?*
13.	*ASISTENCIA – DOCUMENTACIÓN DE LA CLI:* *¿Ofrece el proveedor de servicios en la nube documentación técnica de calidad disponible públicamente para su interfaz de línea de comandos (CLI)?*
14.	*ASISTENCIA – ARQUITECTURAS DE REFERENCIA:* *¿Ofrece el proveedor de servicios en la nube una serie de documentos de arquitectura de referencia en línea y gratuitos para ayudar a los clientes a crear soluciones específicas que combinen muchos de los servicios en la nube del proveedor de servicios en la nube?*
15.	*ASISTENCIA – IMPLEMENTACIONES DE REFERENCIA:* *¿Ofrece el proveedor de servicios en la nube una serie de documentos en línea y gratuitos que contengan procedimientos paso a paso detallados, probados y validados, además de las prácticas recomendadas, para implementar las soluciones comunes (p. ej., DevOps, macrodatos, almacenamiento de datos, cargas de trabajo de Microsoft, cargas de trabajo de SAP, etc.) en sus ofertas en la nube?*

Apéndice B: evaluación técnica en tiempo real

Al seleccionar un CISP, es importante evaluar las capacidades de la plataforma en la nube «en tiempo real» mediante los servicios y la infraestructura disponibles públicamente del CISP. Recomendamos dedicar al menos un día completo a realizar la evaluación técnica de cada CISP preseleccionado. Durante la evaluación se puede: 1) llevar a cabo una evaluación en profundidad para valorar si las capacidades demostradas se ajustan con los requisitos de su RFP y las respuestas escritas del CISP; 2) proporcionar una plataforma para que sus expertos prueben el CISP y se aseguren de que se ajusta y adapta a sus necesidades técnicas y organizativas específicas; y 3) ganar confianza en los servicios y la capacidad del CISP para escalar su capacidad, realizar operaciones de forma segura y resistente y continuar innovando para satisfacer las necesidades futuras.

Cuando los CISP responden a los requisitos de una RFP de servicios en la nube, pueden declarar el cumplimiento de acuerdo con una interpretación general de los requisitos, que carece del contexto completo de las necesidades del entorno operativo o aplicación de una organización. Recomendamos constituir un panel de evaluación técnica en tiempo real con los principales expertos técnicos, operativos, de seguridad y de aplicaciones. Los evaluadores deben poner a prueba al CISP a lo largo de la evaluación. Así mismo, como práctica recomendada, deben puntuar a los CISP de forma independiente y calificar los escenarios en una escala establecida, como, por ejemplo, de 0 a 4 (0 = inaceptable; 1 = mínimo; 2 = aceptable; 3 = bueno; 4 = excelente). Después, las puntuaciones de las demostraciones pueden consolidarse, de modo que la puntuación media de cada escenario de evaluación se sume a la evaluación global del CISP. Antes de finalizar la evaluación, el equipo de evaluación debe analizar los escenarios que presenten una desviación típica elevada. Una vez consolidadas las puntuaciones, se puede aplicar una ponderación basada en la criticidad de los escenarios.

En cuanto al ámbito de la demostración, recomendamos adoptar una visión holística de la plataforma del CISP y, luego, profundizar en la evaluación de las cargas de trabajo específicas que se ejecutan en la plataforma. A continuación, se presenta un ejemplo de un esquema de evaluación de la plataforma y carga de trabajo. Las organizaciones pueden basarse en esta referencia o personalizarla para asegurarse de que el CISP seleccionado cumpla sus requisitos funcionales y no funcionales específicos. Como práctica recomendada, se puede permitir que los proveedores a los que se facilite la lista de escenarios y requisitos propongan un programa para la evaluación en tiempo real que maximice la cobertura e incluya preguntas y respuestas en un 20 % del tiempo.

Evaluación de la plataforma: varios CISP han adoptado el término «bien estructurado» (en inglés, «Well Architected») para referirse a una estrategia de la nube que ofrece un valor óptimo y minimiza el riesgo. Los escenarios bien estructurados en una demostración técnica en directo pueden incluir lo siguiente:

1. **Seguridad:** identidad, gobernanza centralizada, detección automática de amenazas, protección de datos, preparación para eventos.
2. **Eficiencia del rendimiento:** ajuste de tamaño correcto, escalabilidad o elasticidad, modelo sin servidor.
3. **Fiabilidad:** disponibilidad alta (resistencia a los errores), reducción del riesgo de cambio, recuperación de desastres, copia de seguridad.
4. **Administración de costes:** operaciones financieras, optimización comercial, presupuestos y asignación de costes.
5. **Excelencia operativa:** automatización, supervisión, asistencia, administración y capacidades necesarias para migrar a la nube y operar en ella.

Evaluación de la carga de trabajo: un conjunto común de tipos de aplicaciones que pueden demostrarse sería el siguiente:

- Aplicación web: alojamiento público de un sitio web dinámico, que incluye la base de datos de back-end y el almacenamiento de objetos estáticos.
- Análisis de datos: una arquitectura de lago de datos o lake house que permite la consolidación de datos de distintos proveedores de datos y la capacidad de lidiar con un gran volumen (TB/PB de datos), una amplia variedad (estructurados, no estructurados, diferentes formatos, etc.) y una alta velocidad (ritmo de generación de datos, cambios y patrones de consulta).
- Plataforma de ciencia de datos: una plataforma que permite el desarrollo, la implementación y el uso de capacidades basadas en IA o ML en toda su organización.
- Aplicación IoT: una plataforma o capacidad de IoT que abarca la nube, una capacidad de red y los dispositivos.

Puede definir los escenarios que debe demostrar el CISP para cada carga de trabajo representativa que sea importante para su organización. Estos escenarios deben demostrar las capacidades generales que permiten la implementación de la carga de trabajo de una manera bien estructurada. En las siguientes páginas se incluyen ejemplos de criterios de evaluación técnica en tiempo real para: 1) la plataforma del CISP y 2) un ejemplo de una carga de trabajo de una aplicación web.

Plataforma: muestra de una evaluación técnica en tiempo real

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
Plat.Sec.1	Federación de identidades	4	Demostración de la capacidad de realizar la federación desde un almacén de identidades existente al servicio en la nube.	• Compatibilidad con protocolos estándar como SAML. • Compatibilidad con la replicación de identidades basada en SCIM. • Capacidad de definir diferentes niveles de acceso dentro del almacén de identidades corporativo y hacer que se apliquen dentro del proveedor de servicios en la nube. • Capacidad de limitar el acceso a ciertas cuentas, proyectos o cargas de trabajo a determinadas personas o equipos. • Capacidad de admitir el control de acceso basado en atributos (ABAC) y utilizar dichos atributos en el sistema de Identity and Access Management (IAM) del proveedor de servicios en la nube para controlar el acceso a los recursos en la nube.
Plat.Sec.2	Gobernanza centralizada	4	Demostración de la capacidad de definir la política y los requisitos de forma centralizada, en el ámbito de la organización (políticas globales) y también en el ámbito de la unidad empresarial y del proyecto.	• La política debe incluir la posibilidad de habilitar o deshabilitar servicios y aplicar restricciones geográficas (limitar regiones). • Las políticas también deben restringir a los usuarios, incluidos los administradores, la posibilidad de desactivar cualquier control de auditoría o gobernanza.
Plat.Sec.3	Limitación de los permisos de usuario	3	Demostración de las recomendaciones automáticas para reforzar los permisos de los usuarios.	• Capacidad de comparar los permisos actuales con los requeridos. • Generación automática de políticas para promover el privilegio mínimo.
Plat.Sec.4	Registro de auditoría	4	Demostración del registro de auditoría de la actividad en la nube, incluidas las acciones permitidas y no permitidas.	• Registros centralizados para toda la organización. • Registros específicos de la cuenta o el proyecto para respaldar el seguimiento y la responsabilidad básicos. • Herramientas que permiten la consulta de registros.

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
				• Herramientas que permiten desencadenar acciones basadas en eventos o entradas de registro específicos. • Capacidad de ver la actividad de asistencia a los proveedores. • Capacidad de impedir la eliminación de los registros, incluso por parte de los administradores.
Plat.Sec.5	Aislamiento de red	4	Demostración y pruebas cuando sea posible del aislamiento de los diferentes inquilinos en la nube. Demostración de la configuración de las subredes aisladas (sin conectividad), privadas (sin Internet) y públicas (con acceso a Internet).	• Separación de inquilinos, incluido en los servicios de VPN y de conexión cruzada. • Capacidad de controlar el flujo de tráfico desde fuera de la infraestructura de la nube (entorno local), dentro de ella y hacia Internet. • Cómo se aplica la separación cuando se utilizan servicios compartidos como el alojamiento de contenedores o la función como servicio.
Plat.Sec.6	Cifrado en reposo	4	Demostración de la capacidad de cifrar los datos en reposo, incluidas las opciones de cifrado BYOK y del lado del cliente.	• Capacidad de requerir el cifrado de la información confidencial. • Capacidad de utilizar claves administradas por el proveedor o el cliente. • Adherencia a FIPS 140-2. • Capacidad de alertar y registrar el incumplimiento de los requisitos de cifrado. • Impacto en el coste adicional. • Impacto en el rendimiento. • Compatibilidad con algoritmos de prueba cuántica y tamaños de clave.
Plat.Sec.7	Cifrado en tránsito	4	Demostración de la capacidad de cifrar los datos en tránsito.	• Cifrado predeterminado para las API de servicios. • Capacidad de activar el cifrado en tránsito (TLS) en los equilibradores de carga y las API administradas. • Compatibilidad con la autenticación mutua (cliente y servidor).

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
Plat.Sec.8	Administración de claves	4	Demostración de la capacidad de administración de claves. Inclusión del ciclo de vida completo de las claves. Inclusión de la integración con los servicios en la nube.	• Registro de la creación, el uso, la rotación y la destrucción de las claves.
Plat.Sec.9	Administración de la configuración	3	Demostración de las capacidades de administración de la configuración de la plataforma en la nube.	• Mantenimiento de una base de datos de administración de la configuración (CMBD) precisa. • Comprobación del cumplimiento. • Desencadenamiento automático de acciones basadas en el incumplimiento. • Capacidad de evaluar los cambios de configuración con respecto a las prácticas recomendadas o a las reglas personalizadas.
Plat.Sec.10	Seguridad de red	3	Demostración de la capacidad del firewall para aplicaciones web y de firewall, incluida la integración con conjuntos de reglas o firewalls de terceros y la protección contra ataques volumétricos.	• Capacidades de WAF (firewall para aplicaciones web): escalabilidad. • Compatibilidad con redes privadas y públicas. • Capacidad de suscribirse a las fuentes del sector o proveedores para los conjuntos de reglas. • Desencadenamiento automático de acciones dentro de la infraestructura en función de los eventos de WAF. • Capacidades de firewall, escalabilidad. • Firewalls basados en el host y en la red. • Capacidad de hacer referencia a grupos u objetos lógicos, además de poder especificar bloques IP CIDR. • Número de reglas admitidas en cada nivel o componente. • Capacidad de admitir un modelo operativo distribuido (equipo de red + equipo de desarrollo) mediante la configuración de políticas y redes.

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
Plat.Sec.11	Conectividad de red	3	Demostración de la capacidad de conectarse a redes locales, así como de que los puntos de conexión o los clientes se conecten a redes privadas en la nube.	• Conectividad privada (ancho de banda amplio > 10 GB). • Capacidad de controlar las políticas de enrutamiento y firewall en toda la organización. • Conectividad VPN (de sitio a sitio y basada en el cliente). • Compatibilidad con IPV6.
Plat.Sec.12	Administración de instancias	3	Demostración de la capacidad de administración de instancias.	• Capacidad de supervisar y administrar el estado de las revisiones de un gran volumen de instancias. • Compatibilidad con la administración de revisiones del sistema operativo Linux y Windows. • Capacidad de ejecutar comandos en una flota de servidores sin necesidad de SSH. • Capacidad de controlar y auditar el acceso remoto a las máquinas virtuales de forma centralizada. • Capacidad de cambiar el tamaño de una instancia, adjuntar volúmenes adicionales y cambiar la configuración de la red, etc. a través de la consola, la CLI y la API.
Plat.Sec.13	Aplicación de política	3	Demostración de la capacidad de configurar los servicios e impedir el acceso desde la red pública de Internet.	• Capacidad de aislar el tráfico en redes privadas de los servicios que puedan contener datos importantes o confidenciales. • Capacidad de definir políticas que controlen el acceso a los datos en función de la red de origen. • Aplicación de estas restricciones de acceso a todos los usuarios, incluidos los usuarios con credenciales importantes.
Plat.Sec.14	Análisis de vulnerabilidad	2	Demostración de la capacidad de analizar imágenes (contenedor y máquina virtual) en busca de vulnerabilidades.	• Capacidad de analizar automáticamente los contenedores en un registro. • Capacidad de analizar las máquinas virtuales en busca de vulnerabilidades conocidas. • Capacidad de hacer un análisis de la red.

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
Plat.Sec.15	Inspección de la red	2	Demostración de la capacidad de capturar o reflejar el tráfico de red (NetFlow y paquete completo) desde un entorno de cliente.	• Capacidad de reflejar todo el tráfico o una parte de este en la infraestructura del proveedor de servicios en la nube (desde la perspectiva del inquilino), incluida la captura de paquetes completos. • Capacidad de seleccionar simplemente el tráfico que se desea capturar. • Capacidad de escalar la capacidad a volúmenes de tráfico de gran tamaño (>50 Gbps).
Plat.Sec.16	Detección de amenazas	3	Demostración de la capacidad de detección de intrusiones de su plataforma, que incluye las amenazas de una red, el uso de credenciales y el análisis de patrones de uso, entre otros.	• Capacidad de detectar actividades sospechosas, como la «minería». • Capacidad de detectar ataques de autenticación por fuerza bruta, como los inicios de sesión SSH. • Capacidad de detectar la fuga o el abuso de credenciales. • Aplicación de ML, mediante el análisis de un gran número de eventos y la muestra de eventos prioritarios. • Esfuerzo para habilitar o configurar opciones (lo simple es mejor). • Capacidad de integración con servicios externos y activación de notificaciones. • Capacidad de configurar el IDS en todo el mundo para todos los proyectos o cuentas.
Plat.Perf.1	Optimización de la computación	2	Demostración de las recomendaciones automáticas para la optimización de los costes de las máquinas virtuales y de las funciones como servicio.	• Recomendaciones basadas en la utilización real y los patrones de la carga de trabajo. • Las recomendaciones incluyen una estimación del ahorro e información del nivel de carga previsto o implicaciones técnicas. • Las optimizaciones deben incluir tanto el ahorro como el «riesgo de rendimiento» cuando, por ejemplo, se puede reducir el tamaño de las máquinas virtuales.

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
Plat.Perf.2	Optimización del entorno	2	Demostración de las recomendaciones automáticas para otros componentes de la nube, como equilibradores de carga, redes, bases de datos, almacenamiento, etc.	• Las recomendaciones identifican el ahorro y las posibles oportunidades de eficiencia en el rendimiento en otros componentes más allá de la computación básica.
Plat.Perf.3	Escalado automático de la computación	4	Demostración de las capacidades de escalado automático de una aplicación implementada que se basa en un equilibrador de carga en un entorno de computación virtual. Demostración de las diferentes opciones o enfoques disponibles y la capacidad de desencadenar otras acciones (opcionales) antes o después de los eventos de escalado, como una notificación.	• Diferentes opciones de escalado manuales o basadas en el desencadenador, en el tiempo o en enfoques más inteligentes que aplican el machine learning para predecir la capacidad necesaria. • Escalado automático completo, incluido el registro con un equilibrador de carga y comprobaciones de estado. • Capacidad de ejecutar un código arbitrario en puntos específicos del ciclo de vida del escalado.
Plat.Perf.4	Escalado en línea para almacenamiento	3	Demostración de la capacidad de escalar tanto la capacidad como el rendimiento del almacenamiento en bloque sin interrumpir la carga de trabajo.	• Capacidad de transición del almacenamiento en bloque entre diferentes tipos de almacenamiento sin necesidad de reconstruir los servicios completamente. • Capacidad de aumentar el tamaño de los volúmenes presentados a las máquinas virtuales.
Plat.Perf.5	Escalado automático para servicios administrados	3	Demostración de la capacidad del almacén de objetos, la API Gateway, la plataforma FaaS y la base de datos NoSQL para escalar de unos pocos (10) a muchos (1000) usuarios a la vez.	• Escalado automático perfecto, idealmente sin intervención del administrador. • Rendimiento constante durante un periodo de escalado vertical que se ajusta a los requisitos de escalado de la fase de producción. • Para algunos componentes, como FaaS, busque opciones para la preparación y la administración de los límites de la ejecución simultánea, en el caso de que también resulte necesario.

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
Plat.Perf.6	Cargas de trabajo basadas en contenedores	3	Demostración de la capacidad de alojar cargas de trabajo basadas en contenedores.	• Opciones de plataformas de alojamiento de contenedores. • Integración con otros componentes de IaaS, como los equilibradores de carga. • Disponibilidad de una solución de malla de servicios. • Opciones que no son de propiedad para el alojamiento de contenedores, como Kubernetes. • Compatibilidad nativa con la alta disponibilidad dentro del plano de control del contenedor. • Capacidad de administrar hosts de contenedores de forma local.
Plat.Rel.1	Resiliencia regional	4	Demostración de la conmutación por error automatizada de una instancia de base de datos relacional en una región cuando se simula un error localizado geográficamente (como un corte en el suministro eléctrico).	• Conmutación por error automatizada. • Zonas de errores aisladas en una región de nubes. • Delimitación clara y diseño sencillo para ofrecer una alta disponibilidad.
Plat.Rel.2	Recuperación automática de instancias	2	Demostración de la recuperación automática de una instancia o conjunto de instancias tras una comprobación de estado fallida.	• Comprobaciones de estado configurables. • Recuperación o reaprovisionamiento de instancias totalmente automatizado.
Plat.Rel.3	Reconocimiento del estado del equilibrador de carga	3	Demostración de cómo un equilibrador de carga detecta automáticamente una instancia con errores y redirige el tráfico a otros hosts en buen estado.	• Comprobaciones de estado configurables. • Enrutamiento automático del tráfico hacia los hosts en buen estado.
Plat.Rel.4	Conmutación por error regional	3	Demostración de una arquitectura multirregional, que incluye el desplazamiento automático del tráfico a una región secundaria.	• Comprobaciones de estado con reconocimiento global. • Opciones de enrutamiento automatizado: latencia, ponderación y conmutación por error. • Compatibilidad con cargas de trabajo de máquinas virtuales, así como servicios administrados, como un servicio de base de datos de almacén de objetos o NoSQL.

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
Plat.Rel.5	Copia de seguridad y recuperación	4	Demostración de las opciones de copia de seguridad y recuperación para máquinas virtuales, bases de datos y servicios administrados.	• Nivel de automatización. • Capacidad de realizar una restauración en la misma región u otra de la nube. • Capacidad de copiar las copias de seguridad en otra región de la nube.
Plat.Cost.1	Presupuestos	3	Demostración de la capacidad de administración de presupuestos, incluida la forma de estructurarlos para las subcuentas y los proyectos.	• Consideración de la posibilidad de aplicar controles presupuestarios y realizar una supervisión en los diferentes niveles de su organización. • Comprobación de la flexibilidad, por ejemplo, la capacidad de agrupar componentes (mediante el etiquetado), establecer presupuestos para servicios en la nube específicos y configurar umbrales de alerta o supervisión.
Plat.Cost.2	Asignación de presupuesto	1	Demostración del aprovisionamiento de un nuevo entorno de proyecto (cuenta), incluido el proceso de asignación de presupuestos para el proyecto. El aprovisionamiento debe incluir pasos de aprobación manual para la 1) revisión técnica o de TI, 2) revisión comercial o de finanzas.	• Capacidad de autoaprovisionamiento, con las aprobaciones correspondientes. • Automatización de la configuración del ajuste de presupuesto, las notificaciones o las políticas presupuestarias adecuadas para su organización.
Plat.Cost.3	Informes de presupuestos	2	Demostración de la capacidad de informar sobre los presupuestos en toda la organización. Creación de informes para un departamento específico frente a informes para toda la organización (en función de a quién se deba informar). Los informes deben incluir los valores de los gastos «reales» y los previstos o estimados.	• Capacidad de proporcionar visibilidad a diferentes niveles de la organización, a fin de promover el conocimiento y ofrecer transparencia, teniendo en cuenta a quién se debe informar. • La previsión debe basarse en las tendencias de consumo actuales y pasadas y proporcionar una alerta preventiva de posibles excesos del presupuesto.

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
Plat.Cost.4	Controles de presupuesto	1	Demostración de la capacidad de tomar medidas cuando se alcanza un umbral de presupuesto. Las acciones podrían incluir notificaciones, la aplicación de restricciones o la intervención activa para evitar el exceso de gasto presupuestario.	• Capacidad de definir acciones de forma simple para diferentes proyectos. • Capacidad de que las acciones varíen de un proyecto a otro, por ejemplo, teniendo en cuenta las implicaciones de desarrollo frente a las de producción. • Capacidad de definir varias acciones y umbrales para el mismo presupuesto o proyecto. • Capacidad de definir acciones personalizadas además de las capacidades estándar.
Plat.Cost.5	Periodicidad del presupuesto	1	Demostración de la capacidad de aplicar presupuestos para diferentes periodos de tiempo: diarios, mensuales, anuales, etc. En el caso de los presupuestos anuales, demostración de la capacidad de aplicar una distribución variable de los gastos previstos a lo largo del año.	• Capacidad de definir presupuestos para diferentes periodos de tiempo. • Capacidad de configurar una distribución de los gastos a lo largo del año para los presupuestos anuales, especialmente importante para las cargas de trabajo estacionales o altamente elásticas, como, por ejemplo, una declaración de impuestos anual.
Plat.Cost.6	Mercado de terceros	3	Demostración de la capacidad de comprar e implementar productos de terceros. Demostración de cómo establecer un presupuesto para un conjunto de productos de terceros disponibles a través de un mercado y también la capacidad de restringir los productos disponibles.	• Capacidad de establecer un presupuesto para un producto específico, un presupuesto global, un presupuesto para un conjunto de proyectos o cuentas. • Capacidad de presentar solo un subconjunto del mercado más amplio a los usuarios de la nube.
Plat.Cost.7	Modelos de precios de computación	3	Demostración de los diferentes modelos de precios o comerciales que se pueden aplicar a las máquinas virtuales.	• Las capacidades deben incluir precios bajo demanda, detallados (por minuto/hora) y sin necesidad de un compromiso a largo plazo. • Compromisos opcionales a largo plazo a cambio de un descuento. • Capacidad de comprar instancias con la posibilidad de que se interrumpan a cambio de un descuento.

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
				• Es importante que se puedan mezclar estos modelos dentro del mismo proyecto o cuentas, así como compartir los beneficios entre diferentes cuentas.
Plat.Cost.8	Recomendaciones de optimización comercial	3	Demostración de la capacidad de recibir recomendaciones de optimización comercial para optimizar el gasto (sin tener que hacer cambios técnicos).	• Recomendaciones holísticas para varios servicios, que incluyen, por ejemplo, máquinas virtuales y bases de datos administradas. • Capacidad de llevar a cabo las recomendaciones de forma sencilla y comprender el ahorro o beneficio previsto.
Plat.Cost.9	Hosts dedicados	4	Demostración de la capacidad de aprovisionar un host dedicado para permitir el uso de licencias locales vinculadas a un host específico.	• Facilidad de aprovisionamiento. • Capacidad de administrar la utilización del host. • Capacidad de compartir el host entre diferentes proyectos o tenencias.
Plat.Ops.1	Migración de máquinas virtuales	3	Demostración de la importación de una máquina virtual del entorno local a un servicio de máquina virtual basado en la nube.	• Capacidad de importar sistemas operativos basados en Windows y Linux. • Capacidad de importar varias máquinas a la vez. • Capacidad de mantener una sesión de replicación para habilitar una «conmutación por error» rápida a la nube.
Plat.Ops.2	Capacidades de automatización y DevOps	4	Demostración de las capacidades de DevOps o automatización, que incluye cómo se definen los entornos como código, la compatibilidad de las implementaciones totalmente automatizadas, las pruebas automatizadas y las reversiones.	• Capacidad de definir todos los componentes de los sistemas como código, que incluye la red, máquinas virtuales, almacenamiento y bases de datos. • Capacidad de crear una canalización. • Capacidad de crear un repositorio de código. • Capacidad de automatizar las compilaciones. • Capacidad de llevar a cabo implementaciones azul-verde. • Capacidad de crear varios entornos y tener varias fases de implementación. • Reversión automatizada de las implementaciones erróneas.

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
Plat.Ops.3	Alojamiento de aplicaciones	2	Demostración del alojamiento de una aplicación sencilla de 2 niveles en un servicio de plataforma o que requiere poco código. Esto incluye una base de datos relacional y escalado automático para el nivel de aplicación o web.	• Configuración simple a través de IU. • Inclusión de comprobaciones de estado, escalado, disponibilidad alta. Compatibilidad con la plataforma, Windows y Linux.
Plat.Ops.4	Integración de seguridad	2	Demostración de las capacidades de integración de la plataforma desde la perspectiva de la administración de incidentes y eventos de seguridad.	• Capacidad de integrar y usar fácilmente los registros relacionados con la seguridad del proveedor de servicios en la nube y las API para la integración.
Plat.Ops.5	Integración de ITSM	3	Demostración de las capacidades de integración de la plataforma desde la perspectiva de la administración de servicios de TI (ITSM).	• Capacidad de plantear, supervisar y actualizar un caso de asistencia a través de una API. • Capacidad de aprovisionar servicios o conjuntos de servicios como «productos» a través de una API.
Plat.Ops.6	Asistencia	4	Demostración de la oferta de asistencia.	• Diferentes niveles de asistencia para distintos tipos de cargas de trabajo. • Capacidad de ofrecer asistencia también al sistema operativo o al motor de base de datos, etc., según convenga para un servicio determinado. • Capacidad de ofrecer una oferta excepcional con líderes de asistencia designados para las cargas de trabajo críticas. • Capacidad de ofrecer un proceso estructurado de preparación de eventos y revisión de la arquitectura. • Información sobre el plan de desarrollo de los proveedores.
Plat.Ops.7	Auditabilidad	4	Demostración de las herramientas de las que dispone para admitir las auditorías de cumplimiento.	• Capacidad de obtener detalles de la auditoría de cumplimiento a través de la consola. • Capacidad de administrar y automatizar las auditorías del entorno.

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
Plat.Ops.8	De la máquina virtual al contenedor	1	Demostración de la conversión de una aplicación de una máquina virtual a un contenedor y de su prestación mediante el uso de la plataforma de contenedores del proveedor de servicios en la nube.	• Facilidad de uso de la conversión. • Tiempo de la conversión. • Compatibilidad con la plataforma, .Net y Java.

Carga de trabajo: aplicación web; muestra de una evaluación técnica en directo

En la siguiente sección se proporciona un ejemplo de una hoja de evaluación de una carga de trabajo para una «aplicación web» específica. Cuando se desarrolla una hoja de evaluación para una aplicación determinada, se recomienda encarecidamente contar con la participación de los usuarios, desarrolladores y administradores de la aplicación, ya que son los que mejor suelen conocer los requisitos, los retos actuales y las limitaciones.

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
Web.Sec.1	Seguridad: protección de la aplicación	3	Demostración de la capacidad de bloquear los intentos maliciosos de aprovechamiento de la aplicación a través de la inyección de código SQL, el ataque de scripting entre sitios y otros ataques.	• Capacidad de protección contra los ataques comunes «predefinidos» con reglas o capacidades estándar. • Capacidad de crear comprobaciones, reglas y funciones personalizadas.
Web.Sec.2	Seguridad: protección basada en volumen	3	Demostración de la capacidad de impedir ataques que impliquen un gran volumen de solicitudes o de datos dirigidos a una aplicación, así como de protegerse de estos.	• Capacidad de configurar los límites y restringir las tasas de solicitudes desde una dirección IP determinada o una lista de direcciones.
Web.Sec.3	Seguridad: protección basada en el origen	3	Demostración de la capacidad de restringir el acceso en función de la red u origen geográfico.	• Capacidad de aplicar restricciones según el bloque de red o una lista de bloques de red. • Capacidad de aplicar restricciones según el país de origen (sin necesidad de administrar listas de IP).

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
Web.Sec.4	Seguridad: segmentación de red	4	Demostración de la capacidad de aislar o proteger los componentes (servidor web, servidor de aplicaciones o servidor de bases de datos) para protegerlos de la propagación norte-sur y este-oeste a través de la infraestructura.	• Capacidad de colocar componentes en diferentes subredes y controlar el flujo de tráfico entre diferentes subredes. • Capacidad de controlar el flujo de tráfico a nivel de interfaz de red. • Capacidad de hacer referencia a grupos lógicos, así como a bloques de CIDR.
Web.Sec.5	Seguridad: compatibilidad con TLS y administración de certificados	4	Demostración de la capacidad de ofrecer un punto de conexión protegido con TLS y administrar automáticamente los componentes complementarios para entregarlo, incluida, por ejemplo, la rotación automática de certificados.	• Compatibilidad con los protocolos TLS más recientes y la capacidad de desactivar las versiones heredadas si es necesario. • Generación, administración y rotación sencillas de certificados (idealmente, automatizados por completo).
Web.Perf.1	Rendimiento: escalabilidad	4	Demostración de su capacidad para escalar de 10 a 100 000 usuarios simultáneos de la aplicación web mediante el escalado automático dinámico.	• Capacidad de definir reglas de escalado basadas en el tiempo y en el desencadenador. • Escalado sencillo para el usuario final y el administrador. Escalado horizontal automático cuando la carga aumenta y vertical cuando la carga disminuye. • Asegúrese de que existe escalabilidad en cada capa de la aplicación web (equilibrador de carga, capa web, capa de datos, etc.). • Disponibilidad para los servicios de almacenamiento en caché en diferentes capas de la aplicación, según corresponda.
Web.Perf.2	Rendimiento: entrega global	3	Demostración de la capacidad de la red de distribución de contenidos (CDN), incluida la demostración de latencia desde diferentes puntos del mundo, que incluyen Australia, Asia, África, Oriente Medio, Norteamérica, Sudamérica y Europa.	• Capacidad para crear y configurar una CDN a través de la consola o las API del CISP. • Reglas de distribución configurables para distintas geografías. • Almacenamiento en caché configurable para diferentes casos de uso o aplicaciones.

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
Web.Rel.1	Fiabilidad: resiliencia de una sola región	4	Demostración de la capacidad de tolerar un evento localizado, como la pérdida de conectividad de la red al centro de datos del CISP.	• Conmutación por error automatizada y alta disponibilidad dentro de una región de la nube (ciudad).
Web.Rel.2	Fiabilidad: implementación multirregional	3	Demostración de una implementación multirregional de una aplicación web que incluya una base de datos replicada globalmente.	• Capacidad para implementar una aplicación multirregional mediante programación. • Replicación entre las regiones para el almacén de datos. • Enrutamiento automático de los usuarios a su región óptima.
Web.Rel.3	Fiabilidad: conmutación por error multirregional	3	Demostración de la conmutación por error automática de una aplicación web en caso de un problema en el servicio que afecte a la región.	• Conmutación por error automatizada y disponibilidad alta en varias regiones de la nube.
Web.Cost.1	Coste: visibilidad	2	Demostración de la capacidad de realizar un seguimiento del coste por aplicación.	• Capacidad de ver los costes históricos de una aplicación específica, lo que incluye cuándo escala vertical u horizontalmente.
Web.Cost.2	Coste: presupuestos	2	Demostración de la capacidad de establecer presupuestos y alertas relacionadas por aplicación.	• Presupuestos configurados por aplicación y capacidad de desencadenar acciones o alertas con base en los umbrales configurados.
Web.Ops.1	Operaciones: plazos de mantenimiento	3	Demostración de la capacidad de configurar plazos de mantenimiento que se ajusten a los requisitos de la empresa, especialmente cuando el mantenimiento puede afectar a la disponibilidad de la aplicación.	• Plazos de mantenimiento configurables para componentes como un servicio de base de datos relacional.
Web.Ops.2	Operaciones: registro	3	Demostración de la capacidad de centralizar el registro de una aplicación con varios componentes, incluida la persistencia de los registros después de la terminación o el error de las máquinas virtuales.	• Capacidad de configurar un servicio de registro centralizado que se pueda escalar junto con los requisitos de la aplicación. • Capacidad de definir reglas o filtros para desencadenar alertas o acciones basadas en eventos de registro específicos.

ID del escenario	Nombre del escenario	Criticidad (1 = baja; 4 = crítica)	Requisitos de demostración	Consideraciones de puntuación
Web.Ops.3	Operaciones: supervisión	3	Demostración de la supervisión de la aplicación, que incluye el rendimiento, la disponibilidad, tiempos de respuesta, recuentos de errores, etc. y la funcionalidad para tomar medidas o activar notificaciones basadas en diferentes umbrales de métricas.	• Una colección de métricas estándar disponibles, como E/S de disco, CPU, métricas de base de datos, red, equilibrador de carga, etc. • Capacidad de definir métricas y umbrales personalizados. • Capacidad de crear un panel personalizado para representar las métricas más importantes y compartir esos paneles con los usuarios pertinentes.