

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.3502

(08/2014)

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA
INFORMACIÓN, ASPECTOS DEL PROTOCOLO
INTERNET, REDES DE PRÓXIMA GENERACIÓN,
INTERNET DE LAS COSAS Y CIUDADES
INTELIGENTES

Computación en la nube

**Tecnología de la información – Computación en
la nube – Arquitectura de referencia**

Recomendación UIT-T Y.3502

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET, REDES DE PRÓXIMA GENERACIÓN, INTERNET DE LAS COSAS Y CIUDADES INTELIGENTES

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899
Televisión IP sobre redes de próxima generación	Y.1900–Y.1999
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de la próxima generación	Y.2250–Y.2299
Mejoras de las NGN	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Redes basadas en paquetes	Y.2600–Y.2699
Seguridad	Y.2700–Y.2799
Movilidad generalizada	Y.2800–Y.2899
Entorno abierto con calidad de operador	Y.2900–Y.2999
REDES FUTURAS	Y.3000–Y.3499
COMPUTACIÓN EN LA NUBE	Y.3500–Y.3999
INTERNET DE LAS COSAS Y CIUDADES Y COMUNIDADES INTELIGENTES	
General	Y.4000–Y.4049
Definiciones y terminologías	Y.4050–Y.4099
Requisitos y casos de utilización	Y.4100–Y.4249
Infraestructura, conectividad y redes	Y.4250–Y.4399
Marcos, arquitecturas y protocolos	Y.4400–Y.4549
Servicios, aplicaciones, computación y proceso de datos	Y.4550–Y.4699
Gestión, control y calidad de funcionamiento	Y.4700–Y.4799
Identificación y seguridad	Y.4800–Y.4899
Examen y evaluación	Y.4900–Y.4999

Para más información, véase la Lista de Recomendaciones del UIT-T.

Tecnología de la información – Computación en la nube – Arquitectura de referencia

Resumen

La Recomendación UIT-T Y.3502 | ISO/CEI 17789 describe la arquitectura de referencia de la computación en la nube, que comprende las funciones y las actividades de la computación en la nube, así como sus componentes funcionales y sus relaciones.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T Y.3502	13-08-2014	13	11.1002/1000/12209

* Para acceder a la Recomendación, sírvase digitar el URL <http://handle.itu.int/> en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, <http://handle.itu.int/11.1002/1000/11830-en>.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT T disponibles en el sitio web del UIT T en <http://www.itu.int/ITU-T/ipr/>.

© UIT 2021

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

	<i>Página</i>
1 Alcance.....	1
2 Referencias normativas	1
2.1 Recomendaciones Normas Internacionales idénticas	1
2.2 Referencias adicionales	1
3 Definiciones.....	1
3.1 Términos definidos en otros documentos.....	1
3.2 Términos definidos en esta Recomendación Norma Internacional	1
4 Abreviaturas	2
5 Convenios.....	2
6 Metas y objetivos de la arquitectura de referencia de la computación en la nube	3
7 conceptos de la arquitectura de referencia	4
7.1 Perspectivas arquitectónicas de la CCRA	4
7.2 Perspectiva del usuario de la computación en la nube	5
7.3 Perspectiva funcional de la computación en la nube.....	7
7.4 Relación entre la perspectiva del usuario y la perspectiva funcional	8
7.5 Relación de la perspectiva del usuario y la perspectiva funcional con los aspectos transversales	9
7.6 Perspectiva de implementación de la computación en la nube.....	9
7.7 Perspectiva de despliegue de la computación en la nube	9
8 Perspectiva del usuario	9
8.1 Presentación de las funciones, subfunciones y actividades de la computación en la nube.....	9
8.2 Cliente de servicios en la nube	10
8.3 Proveedor de servicios en la nube	14
8.4 Asociado de servicios en la nube	22
8.5 Aspectos transversales.....	25
9 Perspectiva funcional.....	31
9.1 Arquitectura funcional.....	31
9.2 Componentes funcionales	33
10 Relación entre la perspectiva de usuario y la perspectiva funcional.....	42
10.1 Generalidades.....	42
10.2 Visión general	42
Anexo A – Pormenores de la perspectiva de usuario y la perspectiva funcional.....	48
A.1 Relación entre el cliente de servicios en la nube y el proveedor de servicios en la nube	48
A.2 Relación entre el proveedor y el proveedor par (o "entre nubes").....	51
A.3 Relación entre el creador de servicios en la nube y el proveedor de servicios en la nube.....	54
A.4 Relación entre el proveedor de servicios en la nube y el auditor	55
Bibliografía.....	57

**NORMA INTERNACIONAL ISO/CEI 17789
RECOMENDACIÓN UIT-T Y.3502**

Tecnología de la información – Computación en la nube – Arquitectura de referencia

1 Alcance

En esta Recomendación | Norma Internacional se especifica la arquitectura de referencia de la computación en la nube (CCRA), que comprende las **funciones de la computación en la nube y las actividades de la computación en la nube**, así como **los componentes funcionales de la computación en la nube** y sus relaciones.

2 Referencias normativas

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación | Norma Internacional. Al Efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y Normas Internacionales son objeto de revisiones, por lo que se insta a los participantes en acuerdos basados en la presente Recomendación | Norma Internacional a que investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y Normas Internacionales citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones de la UIT mantiene una lista de las Recomendaciones UIT-T actualmente vigentes.

2.1 Recomendaciones | Normas Internacionales idénticas

- Recomendación UIT-T Y.3500 (2014) | ISO/CEI 17788:2014, *Tecnología de la información – Computación en la nube – Visión general y vocabulario*.

2.2 Referencias adicionales

- ISO/CEI 29100:2011, *Information technology – Security techniques – Privacy framework*.

3 Definiciones

A los efectos de esta Recomendación | Norma Internacional, son de aplicación los términos y definiciones de la Recomendación UIT-T Y.3500 | ISO/CEI 17788 y las siguientes definiciones.

3.1 Términos definidos en otros documentos

El siguiente término está definido en ISO/CEI/IEEE 42010:

3.1.1 arquitectura: Conceptos o propiedades fundamentales de un sistema dentro de su entorno, encarnados en sus elementos, las relaciones entre ellos, y los principios de su diseño y evolución.

El siguiente término está definido en ISO/CEI 29100:

3.1.2 Información de identificación personal (IIP): toda información que a) puede utilizarse para identificar el titular de la información de identificación personal (IIP) con quien está relacionada esa información, o b) está o puede estar relacionada directa o indirectamente con el titular de la IIP.

NOTA – Para determinar si un titular de IIP es identificable, se deben tener en cuenta todos los medios utilizables, razonablemente, por el interesado en la privacidad que posea los datos, o por cualquier otra **parte**, para identificar a esa persona física.

3.2 Términos definidos en esta Recomendación | Norma Internacional

En esta Recomendación | Norma Internacional se definen los siguientes términos:

3.2.1 actividad: Serie o conjunto especificado de tareas.

3.2.2 producto de servicio en la nube: servicio en la nube conforme a los términos comerciales en virtud de los cuales se ofrece el servicio en la nube.

NOTA – Los términos comerciales pueden comprender la fijación de precios, la calificación y los niveles de servicio.

3.2.3 componente funcional: bloque de construcción funcional necesario para realizar una **actividad** (cláusula 3.2.1), respaldada por una implementación.

3.2.4 servicio en la nube par: servicio en la nube de un **proveedor de servicios en la nube** que se utiliza como parte de un **servicio en la nube** de uno o más **proveedores de servicios en la nube**.

3.2.5 proveedor de servicios en la nube par: proveedor de servicios en la nube que ofrece uno o más **servicios en la nube** para su utilización por uno o más **proveedores de servicios en la nube** como parte de sus **servicios en la nube**.

3.2.6 catálogo de productos: listado de todos los **productos de servicios en la nube** (cláusula 3.2.2) que los **proveedores de servicios en la nube** ponen a disposición de los **clientes de servicios en la nube**.

3.2.7 función: conjunto de **actividades** (cláusula 3.2.1) que sirven un fin común.

3.2.8 catálogo de servicios: listado de todos los servicios en la nube de un **proveedor de servicios en la nube** concreto.

3.2.9 subfunción: subconjunto de **actividades** (cláusula 3.2.1) de una **función** (cláusula 3.2.7) dada.

4 Abreviaturas

En esta Recomendación | Norma Internacional se utilizan las siguientes abreviaturas:

API	Interfaz de programación de aplicaciones (<i>application programming interface</i>)
CaaS	Comunicaciones como servicio (<i>communications as a service</i>)
CCRA	Arquitectura de referencia de la computación en la nube (<i>cloud computing reference architecture</i>)
CPU	Unidad central de procesamiento (<i>central processing unit</i>)
CS	Servicio en la nube (<i>cloud service</i>)
CSC	Cliente de servicio en la nube (<i>cloud service customer</i>)
CSN	Socio de servicio en la nube (<i>cloud service partner</i>)
CSP	Proveedor de servicios en la nube (<i>cloud service provider</i>)
IaaS	Infraestructura como servicio (<i>infrastructure as a service</i>)
TIC	Tecnología de la información y la comunicación
IFR	Indicador fundamental de rendimiento
MSA	Acuerdo de servicios maestro (<i>master service agreement</i>)
NaaS	Red como servicio (<i>network as a service</i>)
PaaS	Plataforma como servicio (<i>platform as a service</i>)
IIP	Información de identificación personal
QoS	Calidad de servicio (<i>quality of service</i>)
RAM	Memoria de acceso aleatorio (<i>random access memory</i>)
SaaS	Software como servicio (<i>software as a service</i>)
SLA	Acuerdo de nivel de servicio (<i>service level agreement</i>)
ToS	Términos de servicio (<i>terms of service</i>)
T&C	Términos y condiciones
VLAN	Red de área local virtual (<i>virtual local area network</i>)
VPN	Red privada virtual (<i>virtual private network</i>)
VM	Máquina virtual (<i>virtual machine</i>)

5 Convenios

Se utilizan los siguientes convenios:

- 1) A lo largo de esta Recomendación | Norma Internacional se utilizan diagramas para ilustrar la arquitectura de referencia de la computación en la nube (CCRA). En la Figura 5-1 se muestran los convenios utilizados para el contenido de los diagramas.

NOTA – En la Figura 5-1, por "aspecto" debe entenderse "aspecto transversal".

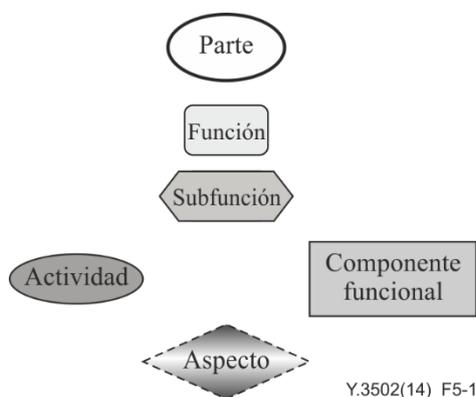


Figura 5-1 – Leyenda de los diagramas utilizados en esta Recomendación | Norma Internacional

- 2) En esta CCRA se utilizan los términos "TIC" y "sistemas de TIC", siendo TIC la abreviatura de "tecnología de la información y la comunicación", como se define en la cláusula 3.1332 de ISO/CEI/IEEE 24765. Este término se emplea para aclarar que la CCRA no sólo abarca las tecnologías de computación y almacenamiento asociadas a los sistemas informáticos, sino también las redes de comunicación que vinculan esos sistemas.
- 3) Se indican en **negrita** los términos definidos en la cláusula 3 y en la Recomendación UIT-T Y.3500 | ISO/CEI 17788.

6 Metas y objetivos de la arquitectura de referencia de la computación en la nube

La **computación en la nube** es un paradigma para dar acceso a la red a un conjunto elástico y ampliable de recursos físicos o virtuales compartibles con administración y configuración en autoservicio previa solicitud. Véase la Recomendación UIT-T Y.3500 | ISO/CEI 17788.

La arquitectura de referencia de la computación en la nube (CCRA, *cloud computing reference architecture*) presentada en esta Recomendación | Norma Internacional establece un marco arquitectónico eficaz para la descripción de las **funciones y subfunciones de la computación en la nube**, las **actividades de la computación en la nube**, los aspectos transversales, así como la arquitectura funcional y los **componentes funcionales de la computación en la nube**.

La CCRA tiene las siguientes metas:

- describir la comunidad de partes interesadas que participan en la **computación en la nube**;
- describir las características fundamentales de los sistemas de **computación en la nube**;
- especificar las **actividades y componentes funcionales de la computación en la nube** y describir las relaciones entre ellos y con el entorno;
- identificar los principios que rigen el diseño y la evolución de la **CCRA**.

La CCRA contribuye a alcanzar los siguientes importantes objetivos de normalización:

- permitir la elaboración de un conjunto coherente de normas internacionales en materia de **computación en la nube**;
- servir de punto de referencia independiente de la tecnología para la definición de normas sobre la **computación en la nube**;
- fomentar la apertura y la transparencia en la identificación de los beneficios y riesgos que conlleva la **computación en la nube**.

La CCRA se centra en los requisitos de "qué" ofrecen los **servicios en la nube** y no en "cómo" diseñar soluciones e implementaciones basadas en la nube. La CCRA no representa la arquitectura de sistema de ningún sistema de **computación en la nube** concreto, aunque puede imponer limitaciones a los sistemas específicos. La CCRA no está vinculada a ningún producto, servicio o implementación de referencia de un fabricante concreto, ni define prescriptivamente soluciones que impidan la innovación.

La CCRA también pretende:

- facilitar la comprensión de las complejidades operativas de la **computación en la nube**;
- ilustrar y facilitar la comprensión de los diversos **servicios en la nube**, su configuración y su uso;

- servir de referencia técnica que permita a la comunidad internacional entender, debatir, categorizar y comparar los **servicios en la nube**;
- servir de herramienta para describir, debatir y desarrollar una arquitectura específica de sistema a partir de un marco de referencia común;
- facilitar el análisis de eventuales normas relativas a la seguridad, la **interoperabilidad**, la portabilidad, la **reversibilidad**, la fiabilidad y la gestión de servicio, además de soportar el análisis de las implementaciones de referencia.

7 conceptos de la arquitectura de referencia

En esta Recomendación | Norma Internacional se define una CCRA que puede servir de punto de referencia fundamental para la normalización de la **computación en la nube** y que ofrece un marco general de los conceptos y principios básicos de un sistema de **computación en la nube**.

En esta cláusula se presenta una visión general de los enfoques arquitectónicos utilizados en esta Recomendación | Norma Internacional.

7.1 Perspectivas arquitectónicas de la CCRA

Los sistemas de **computación en la nube** pueden describirse desde distintas perspectivas.

En la CCRA se utilizan cuatro perspectivas (véase la Figura 7-1):

- perspectiva del usuario;
- perspectiva funcional;
- perspectiva de implementación; y
- perspectiva de despliegue.

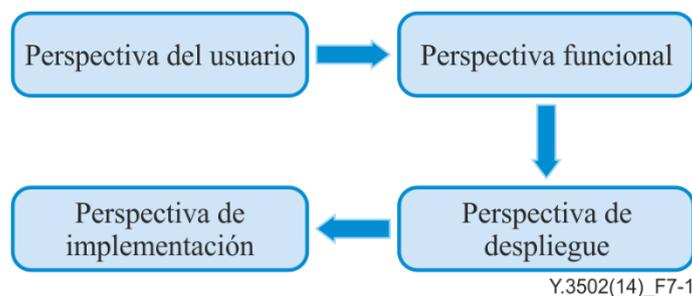


Figura 7-1 – Transformaciones entre perspectivas arquitectónicas

En el Cuadro 7-1 se describen cada una de estas perspectivas.

Cuadro 7-1 – Perspectivas de la CCRA

Perspectiva de la CCRA	Descripción de la perspectiva de la CCRA	Alcance
Perspectiva del usuario	Contexto del sistema, las partes , las funciones , las subfunciones y las actividades de la computación en la nube	Dentro del alcance
Perspectiva funcional	Funciones necesarias para el soporte de las actividades de la computación en la nube	Dentro del alcance
Perspectiva de implementación	Funciones necesarias para la implementación de un servicio en la nube dentro de partes del servicio y/o de partes de la infraestructura	Fuera del alcance
Perspectiva de despliegue	Cómo se implementan técnicamente las funciones de un servicio en la nube dentro de los elementos infraestructurales ya existentes o de nuevos elementos que se hayan de introducir en la infraestructura	Fuera del alcance
NOTA – Si bien en esta Recomendación Norma Internacional se detallan las perspectivas funcional y del usuario, las perspectivas de implementación y despliegue dependen de la tecnología y de las implementaciones y despliegues reales de la computación en la nube específicas del fabricante, por lo que quedan fuera del alcance de la presente Recomendación Norma Internacional.		

En la Figura 7-2 se ilustra la transición de la perspectiva del usuario a la perspectiva funcional, cuyos detalles se presentan en la cláusula 7.4.

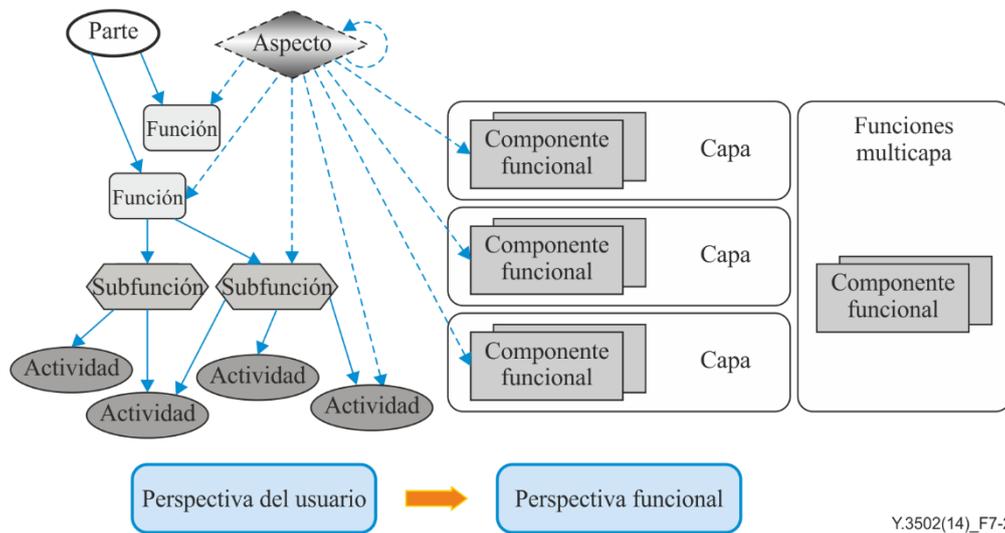


Figura 7-2 – Transición de la perspectiva del usuario a la perspectiva funcional

7.2 Perspectiva del usuario de la computación en la nube

La perspectiva del usuario contempla los siguientes conceptos de la **computación en la nube**:

- **actividades de la computación en la nube;**
- **funciones y subfunciones;**
- **partes;**
- **servicios en la nube;**
- **modelos de despliegue de la nube;**
- **aspectos transversales.**

En la Figura 7-3 se muestran las entidades definidas para la perspectiva del usuario.

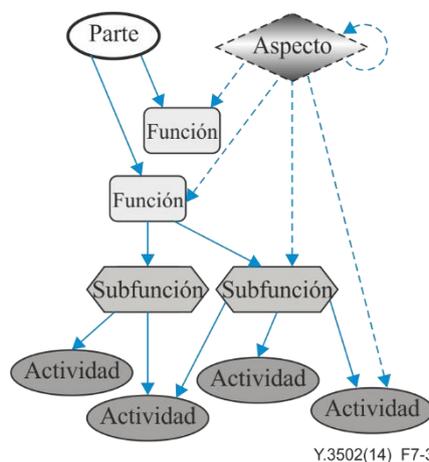


Figura 7-3 – Entidades de la perspectiva del usuario

7.2.1 Actividades de la computación en la nube

Una **actividad de la computación en la nube** se define como una serie o conjunto específico de tareas.

Las **actividades de la computación en la nube** deben tener un fin o genera uno o más resultados.

Las **actividades** dentro de un sistema de **computación en la nube** se realizan empleando los **componentes funcionales** (véase la cláusula 7.3.1).

Las **actividades de la computación en la nube** se identifican y describen más detalladamente en la cláusula 8.

7.2.2 Funciones y subfunciones

Una **función** es un conjunto de **actividades de la computación en la nube** que sirven un mismo fin.

En la CCRA se definen tres **funciones**:

- **cliente de servicios en la nube (CSC, *cloud service customer*): parte** que mantiene una relación empresarial a los efectos de utilizar **servicios en la nube**.
- **proveedor de servicios en la nube (CSP, *cloud service provider*): parte** que pone a disposición **servicios en la nube**.
- **asociado de servicios en la nube (CSN, *cloud service partner*): parte** que colabora o asiste en **actividades del proveedor de servicios en la nube** o del **cliente de servicios en la nube**, o de ambos.

Una **subfunción** es un subconjunto de **actividades de computación en la nube** para una **función** dada.

Las distintas **subfunciones** pueden compartir las **actividades de computación en la nube** asociadas a una **función** determinada.

En la cláusula 8 se describen las **funciones** y **subfunciones de la computación en la nube**.

7.2.3 Partes

Una **parte** es una persona física o moral, esté o no constituida, o un grupo de ellas. Las **partes** en un sistema de **computación en la nube** son sus interesados.

Una **parte** puede asumir más de una **función** en un momento dado y puede participar en un subconjunto específico de las **actividades** de esa **función**. Como ejemplo de partes pueden citarse, entre otras, las grandes empresas, las pequeñas y medianas empresas, los organismos estatales, las instituciones académicas y los particulares.

7.2.4 Servicios en la nube

Los **servicios en la nube** forman parte esencial de la **computación en la nube**. Los **servicios en la nube** son el objeto de la Recomendación UIT-T Y.3500 | ISO/CEI 17788. En esta cláusula se presenta un resumen.

Los **servicios en la nube** pueden describirse en términos de los **tipos de capacidades en la nube** que ofrecen, en función de los recursos facilitados por el **servicio en la nube**. Hay tres **tipos de capacidades en la nube**:

- **tipo de capacidades de aplicación;**
- **tipo de capacidades de plataforma;**
- **tipo de capacidades de infraestructura.**

Los **tipos de capacidades en la nube** y las **categorías de servicios en la nube** se abordan en la Recomendación UIT-T Y.3500 | ISO/CEI 17788.

Los **servicios en la nube** también se dividen en categorías, consistiendo cada una de ellas en un grupo de **servicios en la nube** que posee una serie de cualidades comunes. Los servicios de esas categorías pueden poseer capacidades de uno o más de los **tipos de capacidades en la nube** anteriores.

Algunas de las **categorías de servicios en la nube** son:

- **infraestructura como servicio (IaaS, *infrastructure as a service*);**
- **plataforma como servicio (PaaS, *platform as a service*);**
- **software como servicio (SaaS, *software as a service*);**
- **red como servicio (NaaS, *network as a service*).**

En la Recomendación UIT-T Y.3500 | ISO/CEI 17788 se describen otras **categorías de servicios en la nube**.

7.2.5 Modelos de despliegue de la nube

Los **modelos de despliegue de la nube** se tratan en la Recomendación UIT-T Y.3500 | ISO/CEI 17788. En esta cláusula se presenta un resumen.

Los **modelos de despliegue de la nube** son las maneras en que la **computación en la nube** puede organizarse en función del control y la compartición de los recursos físicos o virtuales.

Los **modelos de despliegue de la nube** son:

- **nube pública;**
- **nube privada;**

- **nube comunitaria;**
- **nube híbrida.**

7.2.6 Aspectos transversales

Los aspectos transversales son los comportamientos o capacidades que se han de coordinar entre las distintas **funciones** y que se implementan coherentemente en el sistema de **computación en la nube**.

Los aspectos transversales pueden compartirse y pueden afectar a múltiples **funciones, actividades de la computación en la nube y componentes funcionales**.

Los aspectos transversales atañen a múltiples **funciones o componentes funcionales** individuales.

Un ejemplo de aspecto transversal es la seguridad.

En la cláusula 8.5 se describen los aspectos transversales.

7.3 Perspectiva funcional de la computación en la nube

La perspectiva funcional es una perspectiva tecnológicamente neutra de las funciones necesarias para crear un sistema de **computación en la nube**. La perspectiva funcional describe la distribución de las funciones necesarias para soportar las **actividades de computación en la nube**.

La arquitectura funcional también define las dependencias entre las funciones.

La perspectiva funcional abarca los siguientes conceptos de la **computación en la nube**:

- **componentes funcionales;**
- capas funcionales; y
- funciones multicapa.

En la Figura 7-4 se ilustran los conceptos de función, capa y **componente funcional**.

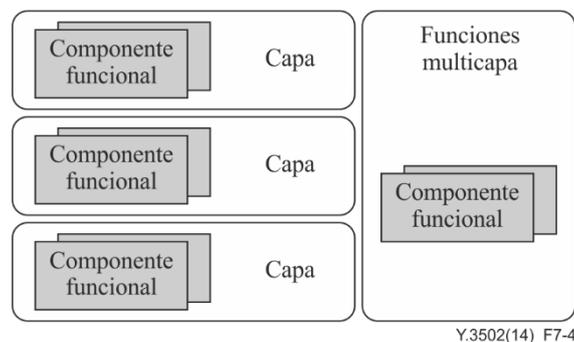


Figura 7-4 – Estratificación funcional

La arquitectura funcional de la **computación en la nube** se describe en la cláusula 9.1.

7.3.1 Componentes funcionales

Un **componente funcional** es un bloque de construcción funcional necesario para realizar una **actividad** en el marco de una implementación.

Las capacidades de un sistema de **computación en la nube** están plenamente definidas por el conjunto de **componentes funcionales** implementados.

Los **componentes funcionales** se detallan en la cláusula 9.2.

7.3.2 Capas funcionales

Una capa es un conjunto de **componentes funcionales** que ofrecen capacidades similares o sirven un fin común.

La arquitectura funcional se organiza parcialmente en capas (es decir, que tiene capas y un conjunto de funciones multicapa).

En la CCRA se definen cuatro capas distintas:

- la capa de usuario, que comprende los **componentes funcionales** que soportan las **actividades de la computación en la nube** de los **clientes de servicios en la nube** y **asociados de servicios en la nube**;
- la capa de acceso, que comprende los **componentes funcionales** que facilitan la distribución e interconexión de funciones;
- la capa de servicio, que comprende los **componentes funcionales** que ofrecen por sí mismos los **servicios en la nube**, además de las capacidades comerciales y administrativas conexas, y las capacidades de orquestación necesarias para la prestación;
- la capa de recursos, que comprende los **componentes funcionales** que representan los recursos necesarios para implementar el sistema de **computación en la nube**.

Téngase en cuenta que no todas las capas o **componentes funcionales** tienen que estar necesariamente presentes en un sistema de **computación en la nube** específico.

7.3.3 Funciones multicapa

Las funciones multicapa comprenden los **componentes funcionales** que ofrecen capacidades utilizadas en múltiples capas funcionales.

Las funciones multicapa se dividen en subconjuntos.

Se definen los siguientes subconjuntos de funciones multicapa:

- soporte de desarrollo;
- integración;
- sistemas de seguridad;
- sistemas de soporte operativo;
- sistemas de soporte comercial.

En la cláusula 9.2.5 se describen los **componentes funcionales** de las funciones multicapa.

7.4 Relación entre la perspectiva del usuario y la perspectiva funcional

En la Figura 7-5 se muestra cómo la perspectiva del usuario facilita el conjunto de **actividades de la computación en la nube** que se representan en la perspectiva funcional (y se llevan a cabo utilizando las tecnologías de la perspectiva de implementación).

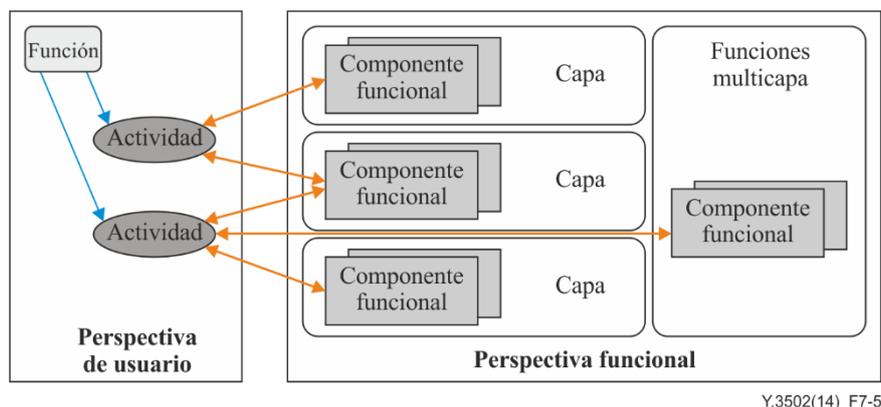


Figura 7-5 – De la perspectiva del usuario a la perspectiva funcional

Pueden encontrarse más detalles sobre la relación entre la perspectiva del usuario y la perspectiva funcional en la cláusula 10.

7.5 Relación de la perspectiva del usuario y la perspectiva funcional con los aspectos transversales

Los aspectos transversales, como su nombre indica, afectan tanto a la perspectiva del usuario como a la perspectiva funcional de la **computación en la nube**.

Los aspectos transversales atañen a las **funciones** y **subfunciones** en la perspectiva del usuario y afectan directa o indirectamente a las **actividades** que realizan esas **funciones**.

Los aspectos transversales también atañen a los **componentes funcionales** de la perspectiva funcional, que se utilizan al realizar las **actividades** descritas en la perspectiva del usuario.

Los aspectos transversales de la **computación en la nube** descritos en la cláusula 8.5 son:

- auditabilidad;
- **disponibilidad**;
- gobernanza;
- **interoperabilidad**;
- mantenimiento y gestión de versiones;
- calidad de funcionamiento;
- portabilidad;
- protección de **información de identificación personal**;
- reglamentación;
- resiliencia;
- **reversibilidad**;
- seguridad;
- niveles de servicio y **acuerdo de nivel de servicio**.

7.6 Perspectiva de implementación de la computación en la nube

En esta Recomendación | Norma Internacional se detallan la perspectiva del usuario y la perspectiva funcional. La perspectiva de implementación queda fuera del alcance de esta Recomendación | Norma Internacional.

7.7 Perspectiva de despliegue de la computación en la nube

En esta Recomendación | Norma Internacional se detallan la perspectiva del usuario y la perspectiva funcional. La perspectiva de despliegue queda fuera del alcance de esta Recomendación | Norma Internacional.

8 Perspectiva del usuario

8.1 Presentación de las funciones, subfunciones y actividades de la computación en la nube

Dado que los servicios distribuidos y su prestación son el núcleo de la **computación en la nube**, todas las **actividades** relacionadas con la **computación en la nube** pueden dividirse en tres grandes categorías: **actividades** que utilizan servicios, **actividades** que prestan servicios y **actividades** que soportan servicios.

En esta cláusula se describen algunas de las **funciones** y **subfunciones** asociadas a la **computación en la nube**.

Conviene señalar que una **parte** puede desempeñar más de una **función** en un momento dado. Al desempeñar una **función**, una **parte** puede limitarse a ejercer una o más **subfunciones**. Las **subfunciones** son un subconjunto de **actividades de computación en la nube** de una determinada **función**.

Como se muestra en la Figura 8-1, las **funciones** de la **computación en la nube** son:

- **cliente de servicios en la nube** (cláusula 8.2);
- **proveedor de servicios en la nube** (cláusula 8.3);
- **asociado de servicios en la nube** (cláusula 8.4).

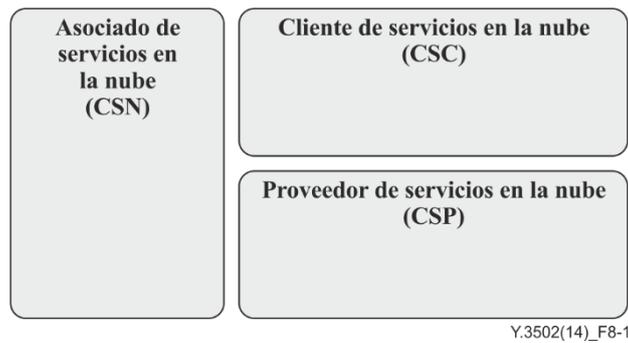


Figura 8-1 – Funciones de la computación en la nube

En la Figura 8-2 se muestran las **funciones** de la **computación en la nube** con sus **subfunciones** correspondientes. Cada una de las **subfunciones** indicadas en la figura se describe más detalladamente en las cláusulas siguientes.

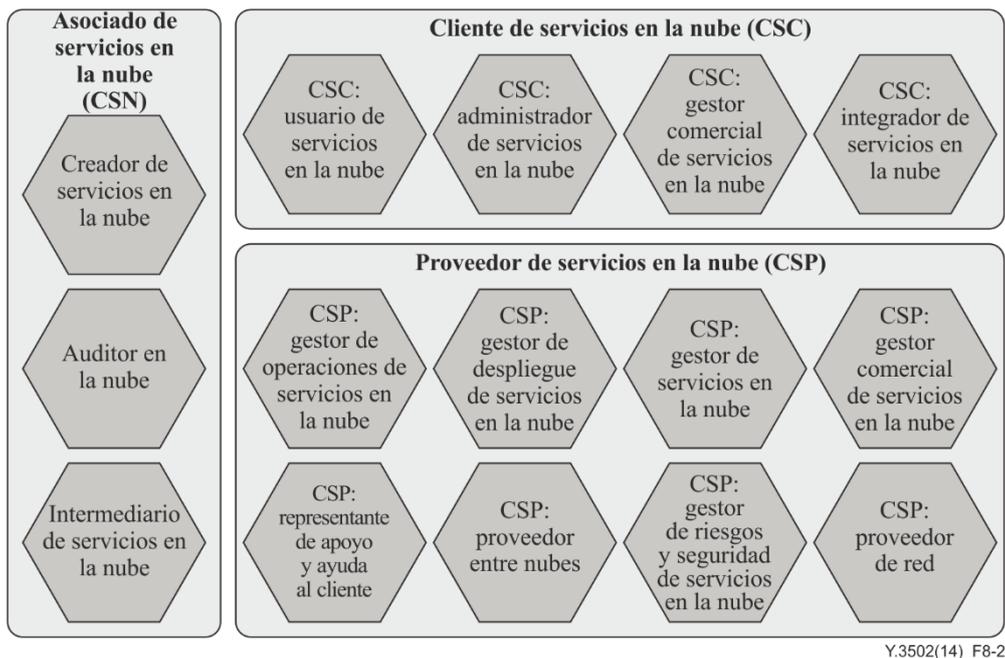


Figura 8-2 – Funciones y subfunciones

8.2 Cliente de servicios en la nube

8.2.1 Función

Un **cliente de servicios en la nube** (CSC, *cloud service customer*) tiene una relación comercial con un **proveedor de servicios en la nube** cuyo objetivo es la utilización de **servicios en la nube**. Un **cliente de servicios en la nube** también mantiene una relación comercial con un **asociado de servicios en la nube** con distintos fines.

Las **actividades del cliente de servicios en la nube** se enmarcan en las **subfunciones** descritas en las cláusulas 8.2.1.1 y 8.2.1.4.

8.2.1.1 CSC:usuario de servicios en la nube

CSC:usuario de servicios en la nube es una subfunción del **cliente de servicios en la nube** correspondiente a una persona física o a la entidad que actúa en su nombre, asociada al **cliente de servicios en la nube** que utiliza los **servicios en la nube**.

Las **actividades de computación en la nube** de CSC:usuario de servicios en la nube son:

- utilizar **servicio en la nube** (cláusula 8.2.2.1).

8.2.1.2 CSC:administrador de servicios en la nube

CSC:administrador de servicios en la nube es una **subfunción** del **cliente de servicios en la nube**, cuyo objetivo principal es garantizar que el usuario utiliza sin problemas los **servicios en la nube**, y que esos **servicios en la nube** funcionan adecuadamente con los sistemas y aplicaciones de TIC del cliente. CSC:administrador de servicios en la nube supervisa todos los procesos operativos relacionados con la utilización de los **servicios en la nube** y ejerce de coordinador de las comunicaciones técnicas entre el **cliente de servicios en la nube** y el **proveedor de servicios en la nube**.

Las **actividades de computación en la nube** de CSC:administrador de servicios en la nube son:

- realizar prueba de servicio (cláusula 8.2.2.2);
- supervisar servicio (cláusula 8.2.2.3);
- administrar seguridad del servicio (cláusula 8.2.2.4);
- generar informes de facturación y utilización (cláusula 8.2.2.5);
- tramitar informes de problemas (cláusula 8.2.2.6);
- administrar arrendamientos (cláusula 8.2.2.7).

8.2.1.3 CSC:gestor comercial de servicios en la nube

CSC:gestor comercial de servicios en la nube es una **subfunción** del **cliente de servicios en la nube** cuyo objetivo es alcanzar las metas comerciales del **cliente de servicios en la nube** mediante la adquisición y utilización de **servicios en la nube** de manera rentable. El ámbito de responsabilidad principal de CSC:gestor comercial de servicios en la nube son los aspectos financieros y jurídicos de la utilización de los **servicios en la nube**, incluidas la aprobación, la propiedad actual y la responsabilidad.

Las **actividades de computación en la nube** de CSC:gestor comercial de servicios en la nube son:

- administración comercial (cláusula 8.2.2.8);
- seleccionar y adquirir servicio (cláusula 8.2.2.9);
- solicitar informe de auditoría (cláusula 8.2.2.10).

8.2.1.4 CSC:integrador de servicios en la nube

CSC:integrador de servicios en la nube es una **subfunción** del **cliente de servicios en la nube** responsable de la integración de los **servicios en la nube** en los sistemas de TIC existentes del **cliente de servicios en la nube**, incluidas las funciones y datos de aplicación.

Las **actividades de computación en la nube** de CSC:integrador de servicios en la nube son:

- conectar sistemas de TIC a **servicios en la nube** (cláusula 8.2.2.11).

8.2.2 Actividades de computación en la nube

Las **actividades de computación en la nube** relacionadas con las **subfunciones** del **cliente de servicios en la nube** se ilustran en la Figura 8-3.

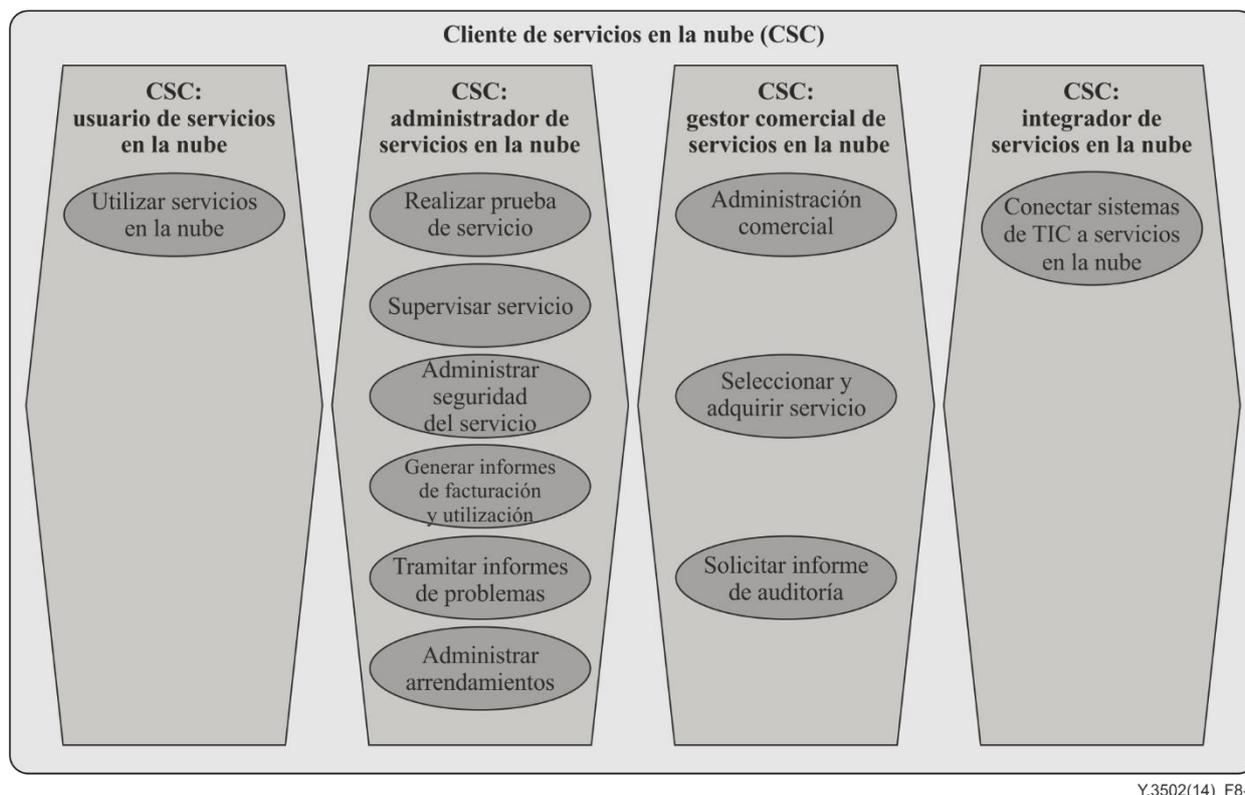


Figura 8-3 – Actividades de computación en la nube relacionadas con las subfunciones del cliente de servicios en la nube

8.2.2.1 Utilizar servicios en la nube

La **actividad** utilizar **servicios en la nube** implica la utilización de los servicios de un **proveedor de servicios en la nube** para realizar diversas tareas.

La **actividad** utilizar **servicios en la nube** suele implicar:

- 1) la configuración de credenciales de usuario para que el **proveedor de servicios en la nube** pueda autenticar al usuario y concederle acceso al **servicio en la nube**;
- 2) la invocación del **servicio en la nube** para su ejecución y la prestación de los resultados especificados.

8.2.2.2 Realizar prueba de servicio

La **actividad** realizar prueba de servicio implica la utilización de los servicios de un **proveedor de servicios en la nube** para garantizar que el **servicio en la nube** se adecúa a las necesidades comerciales del **cliente de servicios en la nube**. Los **servicios en la nube** se utilizan a título provisional con el acuerdo y entendimiento mutuos entre el **proveedor de servicios en la nube** y el **cliente de servicios en la nube**.

La **actividad** realizar prueba de servicio implica:

- 1) la configuración de las credenciales del usuario para que el **proveedor de servicios en la nube** pueda autenticar al usuario y concederle acceso al **servicio en la nube** "de prueba";
- 2) la invocación del **servicio en la nube** "de prueba" para que el **cliente de servicios en la nube** pueda probar su adecuación a sus necesidades comerciales.

8.2.2.3 Supervisar servicio

La **actividad** supervisar servicio controla la calidad del servicio prestado con respecto a los niveles de servicio definidos en el **acuerdo de nivel de servicio (SLA, service level agreement)** entre el **cliente de servicios en la nube** y el **proveedor de servicios en la nube**. Esta **actividad** utiliza las funciones de supervisión intrínsecas del sistema en la nube. Esta **actividad** implica:

- hacer un seguimiento cuantitativo de la utilización de cada **servicio en la nube** y de qué usuarios los utilizan. Se incluye aquí la verificación de que la utilización es adecuada;
- supervisar la integración de los **servicios en la nube** en los sistemas de TIC existentes del cliente para garantizar que se cumplen los objetivos comerciales;

- definir puntos de medición e indicadores de rendimiento para el servicio en cuestión (por ejemplo, **disponibilidad** del servicio, frecuencia de interrupciones del servicio, tiempo medio de reparación, reactividad del servicio técnico del proveedor, etc.);
- supervisar, analizar y archivar los datos de esos indicadores;
- comparar la calidad de servicio real que se presta con la calidad de servicio acordada.

8.2.2.4 Administrar seguridad del servicio

La **actividad** administrar seguridad del servicio implica:

- garantizar la adecuada seguridad de los **datos del cliente de servicios en la nube** que se depositan en un entorno de **computación en la nube**.
- definir planes para la copia de seguridad y recuperación de datos y, eventualmente, para la duplicación de datos y la conmutación por fallo;
- administrar las políticas de seguridad;
- definir las tecnologías de encriptación e integridad que se han de aplicar a los **datos del cliente de servicios en la nube** tanto en reposo como en movimiento;
- definir el tratamiento de toda **información de identificación personal (IIP)** de los **datos del cliente de servicios en la nube**.

8.2.2.5 Generar informes de facturación y utilización

La **actividad** generar informes de facturación y utilización implica la preparación de informes sobre la utilización de los **servicios en la nube** por la organización cliente, además de los informes de facturación/datos de facturación correspondientes a esa utilización. Dichos informes se presentan al CSC:gestor comercial.

8.2.2.6 Tramitar informes de problemas

La **actividad** tramitar informes de problemas implica la tramitación en el lado cliente de todo problema comunicado en relación con la utilización de los **servicios en la nube**. Esto implica:

- evaluar las consecuencias de cada problema;
- analizar el problema para determinar su(s) causa(s);
- generar un informe de problema ante el **proveedor de servicios en la nube** y hacer un seguimiento hasta su resolución;
- encontrar soluciones alternativas para el problema;
- poner en manos de entidades superiores los problemas no resueltos dentro de los plazos acordados o que tengan serias consecuencias comerciales.

8.2.2.7 Administrar arrendamientos

La **actividad** administrar arrendamientos implica la administración de los dominios arrendados por el **cliente de servicios en la nube** al **proveedor de servicios en la nube**. Esta **actividad** implica:

- configurar y controlar los aspectos de seguridad, incluidas las cuentas de usuario, las **funciones** de seguridad, las identidades y los permisos;
- identificar y controlar los datos compartidos entre usuarios dentro de un arrendamiento;
- crear y suprimir **arrendatarios**;
- gestionar los usuarios y los recursos atribuidos a los **arrendatarios**;
- definir las políticas de aplicación para cada **arrendatario**.

8.2.2.8 Administración comercial

La **actividad** administración comercial implica la gestión de los aspectos comerciales de la utilización de los **servicios en la nube**, incluida la gestión financiera y contable. Esta **actividad** implica:

- ajustar el plan comercial para acomodar la utilización de **servicios en la nube**;
- hacer un seguimiento de la utilización de los servicios y ocuparse de la gestión contable y financiera;
- tramitar los recibos/facturas recibidos del **proveedor de servicios en la nube** en concepto de la utilización de los **servicios en la nube**;
- garantizar que la facturación se ajusta a la utilización real de los **servicios en la nube** por el **cliente de servicios en la nube**;

- efectuar pagos al **proveedor de servicios en la nube**;
- llevar la contabilidad de la utilización de los **servicios en la nube**.

8.2.2.9 Seleccionar y adquirir servicio

La **actividad** seleccionar y adquirir servicio implica:

- examinar las ofertas de **servicios en la nube** de (uno o más) **proveedores de servicios en la nube** para determinar si el servicio ofrecido se ajusta a los requisitos comerciales y técnicos del **cliente de servicios en la nube**. Para ello suele ser necesario consultar un **catálogo de productos** y la documentación de cada servicio, que puede contener información técnica sobre el servicio y sus **SLA**, además de información comercial, incluida la tarifa de precios;
- negociar los términos del **servicio en la nube** (si el **proveedor de servicios en la nube** permite variar los términos del servicio);
- aceptar el contrato de **servicios en la nube** y proceder a la inscripción ante el **proveedor de servicios en la nube**.

8.2.2.10 Solicitar informe de auditoría

La **actividad** solicitar informe de auditoría implica que el **cliente de servicios en la nube** solicita un informe de auditoría del **servicio en la nube**, generalmente en el marco de una norma o esquema de auditoría en particular. El **cliente de servicios en la nube** puede solicitar el informe a un **auditor de la nube**, o a un **proveedor de servicios en la nube**, aunque probablemente el informe de auditoría lo prepare una entidad independiente del **proveedor de servicios en la nube** antes de que se complete la adquisición, y periódicamente una vez en uso el servicio.

8.2.2.11 Conectar sistemas de TIC a servicios en la nube

La **actividad** conectar sistemas de TIC a **servicios en la nube** implica la integración de los sistemas de TIC existentes y los **servicios en la nube**, así como la conexión de los componentes y aplicaciones de TIC existentes con el/los **servicio(s) en la nube** de que se trate, además de la conexión de los sistemas de supervisión y gestión del cliente con la supervisión y control de los **servicios en la nube** del **proveedor de servicios en la nube**.

La conexión de los componentes y aplicaciones de TIC existentes con el/los **servicio(s) en la nube** correspondientes implica:

- evaluar la repercusión del/de los **servicio(s) en la nube** en los procesos, sistemas y servicios existentes;
- introducir los datos comerciales residentes en los sistemas de TIC existentes del **cliente de servicios en la nube** en los **servicios en la nube**;
- invocar el **servicio en la nube** desde los componentes y aplicaciones de TIC existentes introduciendo datos y tratando los datos resultantes;
- configurar los derechos de acceso de los CSC:usuarios de servicios en la nube;
- definir e implementar los requisitos de seguridad correspondientes, incluidas la **confidencialidad e integridad** de los flujos de datos;
- integrar las operaciones del cliente para la administración de cuentas de usuario, **funciones** de seguridad, identidades y permisos con las operaciones equivalentes de los **servicios en la nube**;
- crear y supervisar cuentas de usuario e identidades específicas para la utilización de las interfaces de gestión de los **servicios en la nube**;
- integrar el registro y la gestión de incidentes de seguridad de los **servicios en la nube** en la infraestructura de supervisión y gestión del **cliente de servicios en la nube**.

8.3 Proveedor de servicios en la nube

8.3.1 Función

Un **proveedor de servicios en la nube** (CSP) pone **servicios en la nube** a disposición de los **clientes de servicios en la nube**. Esta **función** (y todas sus **subfunciones**) se centran en las **actividades de computación en la nube** necesarias para prestar **servicios en la nube** y en las **actividades de computación en la nube** necesarias para garantizar su prestación a los **clientes de servicios en la nube**, así como para el mantenimiento de los **servicios en la nube**.

El **proveedor de servicios en la nube** es responsable de las relaciones comerciales con los **clientes de servicios en la nube**.

Las **actividades del proveedor de servicios en la nube** se enmarcan en las **subfunciones** descritas en las cláusulas 8.3.1.1 a 8.3.1.8.

8.3.1.1 CSP:gestor de operaciones de servicios en la nube

CSP:gestor de operaciones de servicios en la nube es una **subfunción** del **proveedor de servicios en la nube**, responsable de realizar todos los procesos y procedimientos operativos del **proveedor de servicios en la nube**, garantizando que todos los servicios y las infraestructuras asociadas se ajustan a los objetivos operativos.

Las **actividades de computación en la nube** del CSP:gestor de operaciones de servicios en la nube son:

- preparar sistemas (cláusula 8.3.2.1);
- supervisar y administrar servicios (cláusula 8.3.2.2);
- gestionar activos e inventario (cláusula 8.3.2.3);
- facilitar datos de auditoría (cláusula 8.3.2.4).

8.3.1.2 CSP:gestor de despliegue de servicios en la nube

CSP:gestor de despliegue de servicios en la nube es una **subfunción** del **proveedor de servicios en la nube**, responsable de la planificación de la puesta en marcha de un servicio. Se incluye aquí la definición del entorno operativo del servicio, las primeras fases de despliegue del servicio y sus dependencias, y la facilitación de los procesos operativos utilizados durante la ejecución del servicio.

Las **actividades de computación en la nube** del CSP:gestor de despliegue de servicios en la nube son:

- definir entorno y procesos (cláusula 8.3.2.5);
- definir y recabar mediciones (cláusula 8.3.2.6);
- definir fases de despliegue (cláusula 8.3.2.7).

8.3.1.3 CSP:gestor de servicios en la nube

CSP:gestor de servicios en la nube es una **subfunción** del **proveedor de servicios en la nube**, responsable de garantizar que los servicios del **proveedor de servicios en la nube** están disponibles para su uso por los **clientes de servicios en la nube** y que funcionan correctamente, además de ajustarse a los objetivos especificados en el **acuerdo de nivel de servicio**. El CSP:gestor de servicios en la nube también es responsable de garantizar el adecuado funcionamiento del sistema de soporte comercial y el sistema de soporte operativo del **proveedor de servicios en la nube**, además del funcionamiento de las demás funcionalidades ofrecidas a los **clientes de servicios en la nube** y **asociados de servicios en la nube** para la gestión, la administración y demás **actividades de computación en la nube**.

Las **actividades de computación en la nube** del CSP:gestor de servicios en la nube son:

- prestar servicios (cláusula 8.3.2.8);
- desplegar y configurar servicios (cláusula 8.3.2.9);
- gestionar nivel de servicio (cláusula 8.3.2.10).

8.3.1.4 CSP:gestor comercial de servicios en la nube

CSP:gestor comercial de servicios en la nube es una **subfunción** del **proveedor de servicios en la nube**, responsable de los aspectos comerciales de la oferta de **servicios en la nube** a los **clientes de servicios en la nube**. El CSP:gestor comercial de servicios en la nube crea y hace el seguimiento del plan comercial, define la estrategia de oferta de servicio y gestiona las relaciones comerciales con los **clientes de servicios en la nube**.

Las **actividades de computación en la nube** del CSP:gestor comercial de servicios en la nube son:

- gestionar plan comercial para la prestación de **servicios en la nube** (cláusula 8.3.2.11);
- gestionar relaciones con los clientes (cláusula 8.3.2.12);
- gestionar procesamiento financiero (cláusula 8.3.2.13).

8.3.1.5 CSP:representante de apoyo y ayuda a los clientes

CSP:representante de apoyo y ayuda a los clientes es una **subfunción** del **proveedor de servicios en la nube**, que consiste la principal interfaz entre el **cliente de servicios en la nube** y el **proveedor de servicios en la nube**, y es responsable de reaccionar a los problemas y dudas de los clientes de manera puntual y rentable con el objetivo de mantener el nivel de satisfacción del cliente con el **proveedor de servicios en la nube** y los **servicios en la nube** ofrecidos.

Las **actividades de computación en la nube** del CSP:representante de apoyo y ayuda a los clientes son:

- tramitar solicitudes de los clientes (cláusula 8.3.2.14).

8.3.1.6 CSP:proveedor entre nubes

CSP:proveedor entre nubes es una **subfunción** del **proveedor de servicios en la nube**, que depende de uno o más **proveedores de servicios en la nube pares** para prestar total o parcialmente los **servicios en la nube** ofrecidos a los **clientes de servicios en la nube** por el CSP:proveedor entre nubes. Las principales actividades del CSP:proveedor entre nubes son la intermediación, la agregación, el arbitraje, la asociación o federación de los **servicios en la nube de proveedores de servicios en la nube pares** y sus capacidades comerciales y administrativas desde la perspectiva del **cliente de servicios en la nube**, de manera que el **cliente de servicios en la nube** sólo utilice el servicio y las interfaces comerciales y administrativas del proveedor de servicios entre nubes.

Las **actividades de computación en la nube** del CSP:proveedor entre nubes son:

- gestionar **servicios en la nube pares** (cláusula 8.3.2.15);
- asociar, federar, intermediar, agregar y arbitrar (cláusula 8.3.2.16).

8.3.1.7 CSP:gestor de riesgos y seguridad de servicios en la nube

CSP:gestor de riesgos y seguridad de servicios en la nube es una **subfunción** del **proveedor de servicios en la nube**, responsable de garantizar que el **proveedor de servicios en la nube** gestiona adecuadamente los riesgos asociados al desarrollo, la prestación, la utilización y el soporte de los **servicios en la nube**. Esto incluye la garantía de que las políticas de **seguridad de la información del cliente de servicios en la nube** y el **proveedor de servicios en la nube** están armonizadas y se ajustan a los requisitos de seguridad estipulados en el **SLA**.

Las **actividades de computación en la nube** del CSP:gestor de riesgos y seguridad de servicios en la nube son:

- gestionar riesgos y seguridad (cláusula 8.3.2.17);
- diseñar e implementar la continuidad del servicio (cláusula 8.3.2.18);
- garantizar el cumplimiento (cláusula 8.3.2.19).

8.3.1.8 CSP:proveedor de red

CSP:proveedor de red es una **subfunción** del **proveedor de servicios en la nube**, encargada de ofrecer la conectividad de red y los servicios de red al **cliente de servicios en la nube**, el **asociados de servicios en la nube** y el **proveedor de servicios en la nube**. CSP:proveedor de red puede ofrecer la conectividad de red entre sistemas dentro del centro de datos del **proveedor de servicios en la nube** o entre los sistemas del **proveedor de servicios en la nube** y sistemas fuera del centro de datos del proveedor, por ejemplo, los sistemas del **cliente de servicios en la nube** o sistemas pertenecientes a otros **proveedores de servicios en la nube**.

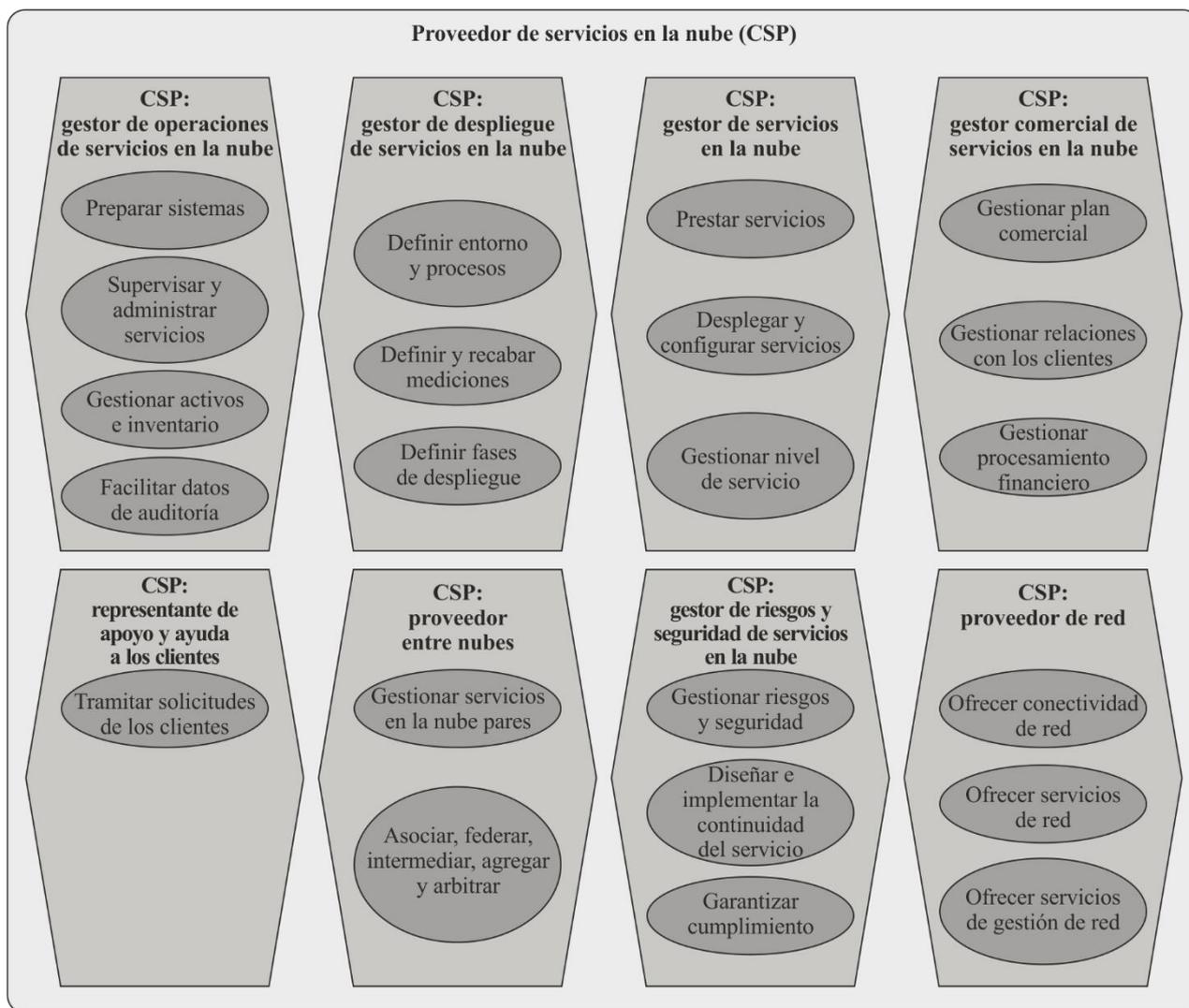
Las **actividades de computación en la nube** del CSP:proveedor de red son:

- ofrecer conectividad de red (cláusula 8.3.2.20);
- ofrecer servicios de red (cláusula 8.3.2.21);
- ofrecer servicios de gestión de red (cláusula 8.3.2.22).

CSP:proveedor de red puede optar también por ofrecer el control dinámico de la conectividad de red como **NaaS**.

8.3.2 Actividades de computación en la nube

Las **actividades de computación en la nube** relacionadas con las **subfunciones** del **proveedor de servicios en la nube** se muestran en la Figura 8-4.



Y.3502(14)_F8-4

Figura 8-4 – Actividades de computación en la nube relacionadas con las subfunciones del proveedor de servicios en la nube

8.3.2.1 Preparar sistemas

La **actividad** preparar sistemas se centra en preparar los sistemas del entorno del proveedor para el despliegue de nuevos **servicios en la nube**. Esta **actividad** implica:

- evaluar las repercusiones del despliegue de nuevos servicios o de incrementar la utilización de los servicios existentes;
- modificar o ampliar los recursos del centro de datos para cubrir las necesidades de nuevos despliegues.

8.3.2.2 Supervisar y administrar servicios

La **actividad** supervisar y administrar servicios se centra en la supervisión y administración de servicios y la infraestructura conexas, lo que incluye los privilegios de usuario y de sistema. Esta **actividad** implica:

- supervisar los servicios y la infraestructura del **proveedor de servicios en la nube**;
- registrar eventos y datos de importancia para el negocio del proveedor y presentar esos datos de manera útil para el CSP: gestor comercial de servicios en la nube. Esa información puede incluir, entre otras cosas, la utilización de los **servicios en la nube** por los **clientes de servicios en la nube** y el coste que supone su prestación;
- administrar la infraestructura de red, incluidos los encaminadores, servidores de nombres de dominio, direcciones IP, redes privadas virtuales (VPN, *virtual private networks*), cortafuegos y filtros de contenido;
- atribuir y administrar el almacenamiento;
- administrar los privilegios de usuarios y sistemas;

ISO/IEC 17789:2014 (E)

- configurar y mantener sistemas operativos e hipervisores;
- administrar un entorno de virtualización;
- supervisar el comportamiento del entorno de TIC del **proveedor de servicios en la nube** para garantizar su correcto funcionamiento y que los **servicios en la nube** prestados se ajustan a los términos del **SLA**;
- registrar problemas, dar cuenta adecuadamente de los problemas (lo que puede implicar el envío de mensajes a uno o más clientes) y hacer el seguimiento de los problemas hasta su resolución.

8.3.2.3 Gestionar activos e inventario

La **actividad** gestionar activos e inventario implica:

- rastrear todos los activos de computación, almacenamiento, red y software y de las relaciones entre ellos. Se incluye aquí el rastreo de datos como las versiones y el nivel de parcheado, además de la información de configuración, según proceda;
- introducir nuevos activos y descartar activos obsoletos. Puede incluirse aquí la garantía de que los nuevos activos son adecuados al fin que van a servir y se han verificado adecuadamente desde el punto de vista de la seguridad y la gestionabilidad; también puede incluirse la eliminación de activos que ya no sean necesarios, en cuyo caso se incluye la eliminación segura de los activos con datos.

8.3.2.4 Facilitar datos de auditoría

La **actividad** facilitar datos de auditoría consiste en la recopilación y comunicación de datos pertinentes en respuesta a una solicitud de auditoría, como los relacionados con los controles de seguridad o la calidad de funcionamiento del servicio. Los datos solicitados dependerán del esquema o norma de auditoría que se utilice. Esta **actividad** implica:

- crear y enviar la información de auditoría adecuada a partir de registros cronológicos, etc.;
- editar la información procedente de registros cronológicos u otros datos que pueda contener información sensible o **IIP**.

8.3.2.5 Definir entorno y procesos

La **actividad** definir entorno y procesos consiste en definir el entorno técnico y los procesos operativos necesarios que se utilizan durante la ejecución de un servicio. Esta **actividad** implica:

- definir el entorno técnico necesario en términos de computación, almacenamiento y recursos de red, además de las dependencias de software, incluida la configuración;
- definir las políticas y procesos para adaptar la cantidad de recursos a la evolución de la demanda de utilización;
- garantizar que el **servicio en la nube** cumple las normas adecuadas en materia de seguridad y conformidad comercial;
- definir los procesos que se han de seguir durante la ejecución del servicio, incluidos los planes de reparación, actualización y migración.

8.3.2.6 Definir y recabar mediciones

La **actividad** definir y recabar mediciones se centra en la definición de métricas del nivel de servicio y su gestión. Esta **actividad** implica:

- definir las métricas utilizadas para medir el funcionamiento de los **servicios en la nube**, que suelen incluirse en los **SLA** relativos a esos servicios;
- diseñar cómo se obtienen las mediciones en cada **servicio en la nube**;
- definir cómo se gestionan y generan los informes sobre las mediciones, en particular para garantizar el cumplimiento de los objetivos de los **SLA**.

8.3.2.7 Definir fases de despliegue

La **actividad** definir fases de despliegue consiste en definir las fases del despliegue de los servicios. Esta **actividad** implica la descripción de cada una de las fases que han de seguir los equipos de operaciones y soporte para desplegar el servicio y que los **clientes de servicios en la nube** lo puedan utilizar.

8.3.2.8 Prestar servicios

La **actividad** prestar servicios comprende todas las fases necesarias para la prestación de un **servicio en la nube** a los **clientes de servicios en la nube**. La **actividad** prestar servicios comprende la aceptación y procesamiento de las invocaciones de servicio emitidas por los usuarios previa autenticación y autorización de las identidades de los usuarios.

El procesamiento de una invocación de servicio se efectúa mediante una instancia de la implementación del servicio, que a su vez puede comprender la composición y demanda de otros servicios, según determinen el diseño y configuración de la implementación correspondiente.

La **actividad** prestar servicios implica:

- gestionar el proceso de tratamiento de fallos del servicio;
- gestionar el sistema de soporte comercial y el sistema de soporte operativo;
- mantener el servicio y la infraestructura subyacente;
- automatizar los procesos del sistema;
- gestionar la capacidad a largo plazo y las tendencias de calidad de funcionamiento;
- instalar, configurar y proceder a actualizaciones de mantenimiento del hardware necesario para la computación, el almacenamiento y las capacidades de red del centro de datos del **proveedor de servicios de red**;
- instalar y configurar el software necesario para el funcionamiento del centro de datos del proveedor de la nube y el soporte de las implementaciones de **servicios en la nube**. Esto incluye la reparación, actualización y mejora del software, según proceda.

8.3.2.9 Desplegar y configurar servicios

La **actividad** desplegar y configurar servicios implica la ejecución de una implementación de servicio y su puesta a disposición en un punto extremo de la red accesible para el CSC:usuario de servicios en la nube, de manera que pueda tramitar las solicitudes de servicio de los usuarios. Esta **actividad** implica:

- seguir los procesos de despliegue definidos para el servicio.

NOTA – Esta actividad también comprende los procesos necesarios para la supresión y desconfiguración de un servicio en la nube.

8.3.2.10 Gestionar nivel de servicio

La **actividad** gestionar nivel de servicio se centra en la gestión del cumplimiento de los objetivos de los **SLA**. Esta **actividad** implica:

- supervisar las mediciones de cada servicio y compararlas con los objetivos de servicios estipulados en el **SLA** para ese servicio;
- tomar medidas cuando las mediciones no se ajusten a los valores exigidos por el **SLA**, recuperar la conformidad del servicio con el **SLA**, por ejemplo, siguiendo los procedimientos establecidos por el CSP:gestor de despliegue de servicios en la nube;
- informar del problema si no se puede mantener el cumplimiento.

8.3.2.11 Gestionar plan comercial

La **actividad** gestionar plan comercial implica:

- definir una oferta de servicio, describir los aspectos técnicos de la oferta (interfaces funcionales, **SLA**, ...) y los aspectos comerciales de la oferta;
 - NOTA – Al establecer la oferta de servicio, el **proveedor de servicios en la nube** puede tomar en consideración los aspectos relacionados con la interacción con **proveedores de servicios en la nube pares**.
- crear un plan comercial que abarque la oferta de uno o más **servicios en la nube** a los clientes, comprendidos tanto los aspectos técnicos como financieros de los servicios, los clientes objetivo, los contratos y **SLA**, los canales de comercialización y los objetivos de ventas;
- hacer un seguimiento de las ventas y la utilización del servicio en relación con el plan para garantizar que se alcanzan los objetivos financieros del **proveedor de servicios en la nube**;
- preparar un plan comercial y ajustarlo para la prestación de **servicios en la nube**.

8.3.2.12 Gestionar relaciones con los clientes

La **actividad** gestionar relaciones con los clientes implica la gestión de la relación comercial entre el **proveedor de servicios en la nube** y el **cliente de servicios en la nube** y, entre otras cosas:

- crear y mantener el contenido del **catálogo de productos**;
- captar clientes;
- servir de punto de contacto con los clientes para todas las cuestiones comerciales;

ISO/IEC 17789:2014 (E)

- considerar y resolver las inquietudes o problemas comunicados por los clientes;
- procesar las solicitudes de cambio (por ejemplo, cambio de titularidad).

8.3.2.13 Gestionar procesamiento financiero

La **actividad** gestionar procesamiento financiero implica:

- tramitar las actualizaciones o problemas relacionados con la facturación;
- generar facturas y/o recibos correspondientes a la utilización de los **servicios en la nube** y transmitir dichas facturas o recibos al **cliente de servicios en la nube**;
- tramitar los pagos recibidos de los **clientes de servicios en la nube** y llevar la contabilidad.

8.3.2.14 Tramitar solicitudes de los clientes

La **actividad** tramitar solicitudes de los clientes implica:

- tramitar las solicitudes de ayuda, los informes e incidentes de los **clientes de servicios en la nube**, sea cual sea su medio de transmisión. Se puede ofrecer a los clientes una amplia variedad de medios de comunicación, desde los foros de correo electrónico hasta los sistemas de asistencia técnica, pasando por los portales web para la comunicación en tiempo real con el personal de atención al cliente del proveedor.

NOTA – Algunas solicitudes o informes pueden necesitar únicamente la comunicación o aclaración de información. Otras solicitudes e informes pueden requerir un análisis de los problemas o la emisión de una solicitud de cambio.

8.3.2.15 Gestionar servicios en la nube pares

La **actividad** gestionar **servicios en la nube** pares consiste en la gestión de la utilización de los **servicios en la nube** de un **proveedor de servicios en la nube par**. Esta **actividad** implica:

- seleccionar y utilizar uno o más servicios de un **proveedor de servicios en la nube par**;
- supervisar y gestionar los **servicios en la nube** del **proveedor de servicios en la nube par** para garantizar que cumplen los objetivos estipulados en el **SLA**, incluidas la comunicación y resolución de problemas de esos servicios;
- gestionar los aspectos comerciales de los **servicios en la nube** de un **proveedor de servicios en la nube par**, incluidos el plan comercial y el procesamiento financiero;
- hacer un seguimiento cuantitativo de la utilización de cada **servicio en la nube** de un **proveedor de servicios en la nube par**, y de qué usuarios lo utilizan, y garantizar que la utilización es adecuada y se ajusta al plan comercial;
- supervisar la integración de los **servicios en la nube** de un **proveedor de servicios en la nube par** con las implementaciones de servicio para garantizar que se cumplen los objetivos comerciales;
- coordinar las identidades y credenciales de seguridad entre los **clientes de servicios en la nube** y todos los **proveedores de servicios en la nube pares**.

8.3.2.16 Asociar, federar, intermediar, agregar y arbitrar

La **actividad** asociar, federar, intermediar, agregar y arbitrar implica la utilización de los **servicios en la nube** de **proveedores de servicios en la nube pares** de manera particular:

- asociar consiste en la utilización de los **servicios en la nube** de un **proveedor de servicios en la nube par**;
- federar implica la utilización de los **servicios en la nube** de un grupo de **proveedores de servicios en la nube pares** que combinan sus capacidades de servicio para ofrecer el conjunto de **servicios en la nube** exigido por los clientes;
- intermediar supone que un **proveedor de servicios en la nube** ofrece un **servicio en la nube** basado en el condicionamiento o mejora del **servicio en la nube** de un **proveedor de servicios en la nube par**. Ejemplos de mejora pueden ser la gestión del acceso a los **servicios en la nube**, la facilitación de una interfaz de programación de aplicación (*API, application programming interface*) de un **servicio en la nube**, la gestión de identidades, la rendición de informes de calidad de funcionamiento, la mejora de la seguridad, etc.;
- agregar implica que un **proveedor de servicios en la nube** ofrece un **servicio en la nube** componiendo un conjunto de servicios ofrecidos por **proveedores de servicios en la nube pares**;
- arbitrar consiste en la oferta por un **proveedor de servicios en la nube** de un **servicio en la nube** basado en la selección de una de las ofertas de servicio de **proveedores de servicios en la nube pares**.

8.3.2.17 Gestionar riesgos y seguridad

La **actividad** gestionar riesgos y seguridad se centra en la gestión de los riesgos y la seguridad asociados con el desarrollo, la prestación, la utilización y el soporte de **servicios en la nube**. Esta **actividad** implica:

- definir la política de **seguridad de la información** habida cuenta de los requisitos de servicio, los requisitos estatutarios y reglamentarios y las obligaciones contractuales y dimanantes del **SLA**;
- definir los riesgos de **seguridad de la información** de un **servicio en la nube** y el enfoque adoptado al respecto para cumplir los objetivos comerciales del **proveedor de servicios en la nube**. Cabe destacar aquí que la gestión de los riesgos de **seguridad de la información** supone un coste y que el proveedor puede optar a nivel comercial por no asumir determinados riesgos, traspasando la responsabilidad sobre ellos al **cliente de servicios en la nube** mediante un acuerdo de servicio, a fin de asumir los costes de otra parte del mercado;
- seleccionar puntos de diseño y los controles de **seguridad de la información** asociados, necesarios para paliar los riesgos asociados con el servicio y el punto de diseño escogido. Los controles suelen abarcar una serie de categorías, como son las siguientes:
 - gestión de identidad y acceso;
 - descubrimiento, clasificación y protección de datos y activos de información;
 - adquisición, desarrollo y mantenimiento de sistemas de información;
 - protección de la infraestructura contra amenazas y vulnerabilidades;
 - gestión de problemas e incidentes de **seguridad de la información**;
 - gobernanza y cumplimiento en materia de seguridad;
 - seguridad física y del personal;
 - seguridad de redes y comunicaciones;
 - asilamiento (entre **arrendatarios** en caso de multidivisión).
- garantizar la aplicación de los controles identificados para el servicio desplegado y la infraestructura subyacente;
- diseñar, implementar y evaluar la seguridad de sistemas y aplicaciones;
- gestionar, diseñar, implementar y evaluar la seguridad de los **servicios en la nube** de **proveedores en la nube pares**;
- evaluar la eficacia de los controles aplicados y modificarlos en función de la experiencia;
- garantizar que los sistemas operativo y de soporte comercial facilitan al personal del **proveedor de servicios en la nube** datos sobre los **arrendatarios clientes de servicios en la nube** a los que se presta el servicio.

8.3.2.18 Diseñar e implementar la continuidad del servicio

La **actividad** diseñar e implementar la continuidad del servicio implica:

- considerar posibles modos de fallo de un **servicio en la nube** y su infraestructura subyacente y establecer procesos de recuperación que permitan la disponibilidad del **servicio en la nube** de acuerdo con los términos del **SLA**, empleando técnicas como la conmutación por fallo y la redundancia.

8.3.2.19 Garantizar cumplimiento

La **actividad** garantizar cumplimiento se centra en la implementación del cumplimiento reglamentario y normativo. Esta **actividad** implica:

- garantizar que la implementación del **servicio en la nube** y su infraestructura subyacente se ajusta a los requisitos de todas las normas aplicables, por ejemplo, por exigencia del conjunto de clientes objetivo o del esquema de certificación escogido por el proveedor para asegurar el servicio;
- garantizar que la implementación del **servicio en la nube** y su infraestructura subyacente (incluido el tratamiento de datos) se ajusta a todos los requisitos reglamentarios aplicables a ese servicio y a los datos que éste almacena o procesa.

8.3.2.20 Ofrecer conectividad de red

La **actividad** ofrecer conectividad de red implica el establecimiento de las conexiones de red solicitadas y las capacidades conexas, incluidas (entre otras) las conexiones entre el **cliente de servicios en la nube** y el sistema del **proveedor de servicios en la nube** y entre un sistema del **proveedor de servicios en la nube** y otro sistema del **proveedor de servicios**

en la nube. Puede incluirse aquí el establecimiento de facilidades como una VPN o de conexiones con ancho de banda dedicado.

Entre las capacidades de red se incluye la posibilidad de ofrecer el retardo limitado, la fluctuación de fase, el ancho de banda, la calidad de servicio y la fiabilidad adecuados para todas las **categorías de servicios en la nube**, tanto con fines relacionados y no relacionados con la nube en el caso de la **NaaS**.

8.3.2.21 Ofrecer servicios de red

La **actividad** ofrecer servicios de red implica la prestación de servicios de red, como los cortafuegos o el equilibrio de carga.

8.3.2.22 Ofrecer servicios de gestión de red

La **actividad** ofrecer servicios de gestión de red implica la gestión de la infraestructura de red empleada para el transporte de **servicios en la nube**. Esta **actividad** ofrece métodos, herramientas y procedimientos que permiten el funcionamiento, la administración, el mantenimiento y la configuración de la infraestructura de red en la nube, e implica:

- mantener la red activa y en adecuado funcionamiento;
- hacer un seguimiento de los recursos de red y de su modo de atribución;
- proceder a reparaciones y actualizaciones, por ejemplo, cuando es necesario sustituir los equipos o añadirles nuevas funciones;
- configurar los recursos de la red para soportar un **servicio en la nube**.

8.4 Asociado de servicios en la nube

8.4.1 Función

Un **asociado de servicios en la nube (CSN)** es una **parte** implicada en el soporte de las **actividades** del **proveedor de servicios en la nube** o del **cliente de servicios en la nube**, o de ambos, o que ejerce funciones auxiliares a dichas **actividades**.

Las **actividades de computación en la nube** de un **asociado de servicios en la nube** pueden variar en función del tipo de asociado y de su relación con el **proveedor de servicios en la nube** y el **cliente de servicios en la nube**.

8.4.1.1 Creador de servicios en la nube

Creador de servicios en la nube es una **subfunción** del **asociado de servicios en la nube**, responsable del diseño, el desarrollo, las pruebas y el mantenimiento de la implementación de un **servicio en la nube**. Esto puede implicar también la composición de la implementación del servicio a partir de implementaciones de servicios existentes.

Las **actividades de computación en la nube** del creador de servicios en la nube son:

- diseñar, crear y mantener los componentes del servicio (cláusula 8.4.2.1);
- componer servicios (cláusula 8.4.2.2);
- probar servicios (cláusula 8.4.2.3).

NOTA 1 – Integrador de servicios en la nube y creador de componentes de servicios en la nube son **subfunciones** del creador de servicios en la nube. El integrador de servicios en la nube se ocupa de la composición de un servicio a partir de otros servicios, mientras que el creador de componentes de servicios en la nube se encarga del diseño, la creación, las pruebas y el mantenimiento de cada uno de los componentes del servicio.

NOTA 2 – Comprende las implementaciones de servicio y los componentes de servicio que implican interacciones con **proveedores de servicios en la nube pares**.

8.4.1.2 Auditor de la nube

Auditor de la nube es una **subfunción** del **asociado de servicios en la nube**, responsable de auditar la prestación y utilización de los **servicios en la nube**. Una auditoría de la nube suele comprender las operaciones, la calidad de funcionamiento y la seguridad, y considerar si se cumple un conjunto específico de criterios de auditoría. Hay múltiples especificaciones sobre los criterios de auditoría; por ejemplo, ISO/CEI 27002 se ocupa de las consideraciones de seguridad.

Las **actividades de computación en la nube** del **auditor de la nube** son:

- auditar (cláusula 8.4.2.4);
- comunicar resultados de auditoría (cláusula 8.4.2.5).

8.4.1.3 Intermediario de servicios en la nube

Intermediario de servicios en la nube es una **subfunción del asociado de servicios en la nube** que negocia las relaciones entre los **clientes de servicios en la nube** y los **proveedores de servicios en la nube**. El **intermediario de servicios en la nube** no es en sí mismo un **proveedor de servicios en la nube** y no debe confundirse con la función de proveedor entre nubes (véase la cláusula 8.3.1.6). La función **intermediario de servicios en la nube** puede combinarse con la de proveedor entre nubes u operar de manera independiente.

Las **actividades de computación en la nube del intermediario de servicios en la nube** son:

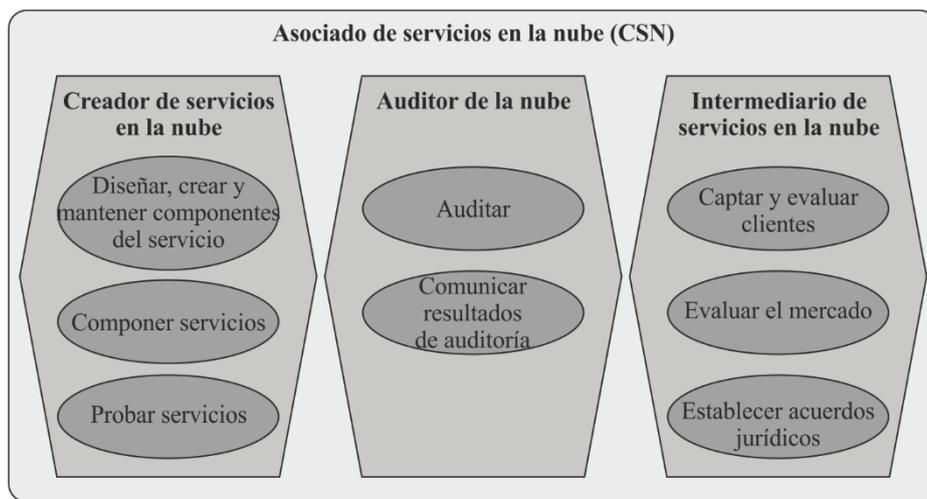
- captar y evaluar clientes (cláusula 8.4.2.6);
- evaluar el mercado (cláusula 8.4.2.7);
- establecer acuerdos jurídicos (cláusula 8.4.2.8);

La evaluación del mercado puede efectuarse antes de captar a los clientes. Se crean entonces preacuerdos con los **proveedores de servicios en la nube** y los **clientes de servicios en la nube** pueden entonces seleccionar a los **proveedores de servicios en la nube** a partir de un **catálogo de servicios**, posiblemente negociando los detalles del servicio (por ejemplo, objetivos de nivel de servicio) en el momento de la selección.

En cualquier caso, el **intermediario de servicios en la nube** sólo participa en la fase de contratación del servicio entre el **cliente de servicios en la nube** y el **proveedor de servicios en la nube**. El **intermediario de servicios en la nube** no interviene en el consumo del servicio. En tal caso, las **actividades** son las del **proveedor de servicios en la nube**.

8.4.2 Actividades de computación en la nube

En la Figura 8-5 se muestran las **actividades de computación en la nube** relacionadas con las **subfunciones del asociado de servicios en la nube**.



Y.3502(14)_F8-5

Figura 8-5 – Actividades de computación en la nube relacionadas con las subfunciones del asociado de servicios en la nube

8.4.2.1 Diseñar, crear y mantener componentes de servicio

La **actividad** diseñar, crear y mantener componentes de servicio implica:

- diseñar y crear componentes de software que forman parte de la implementación de un servicio;
- crear la funcionalidad que se ofrece a los usuarios del servicio, lo que conlleva asimismo conectar los componentes de servicio a los sistemas de soporte operativo del proveedor a fin de poder supervisar y controlar la implementación del servicio;
- procesar informes de problemas relacionados con el funcionamiento de una implementación de servicio;
- reparar las implementaciones de servicios;
- mejorar las implementaciones de servicios.

8.4.2.2 Componer servicios

La **actividad** componer servicios consiste en componer servicios a partir de servicios existentes. Esta **actividad** implica:

- crear funcionalidades de servicio mediante la adición de uno o más servicios existentes de otros proveedores;
- describir los aspectos técnicos del servicio (interfaces funcionales, **SLA**, ...);
- diseñar una interfaz para el **cliente de servicios en la nube** que lleve a los servicios compuestos a partir de múltiples ofertas de **proveedores de servicios en la nube**;
- proceder a la composición, lo que puede implicar la intermediación, la agregación o el arbitraje de servicios existentes.

8.4.2.3 Probar servicios

La **actividad** probar servicios se centra en las pruebas de los componentes y servicios preparados por el creador de servicios en la nube. Esta **actividad** implica:

- probar los componentes que forman una implementación de servicio para garantizar que cumplen correcta y completamente la funcionalidad del servicio;
- garantizar la **interoperabilidad** con los **servicios en la nube** ofrecidos por **proveedores de servicios en la nube pares**;
- realizar las pruebas, lo que debe incluir la verificación de que las conexiones a los sistemas de soporte operativo del **proveedor de servicios en la nube** funcionan correctamente. En función del resultado, suele ser necesario realizar pruebas en la zona de pruebas del centro de datos del **proveedor de servicios en la nube**.

8.4.2.4 Auditar

La **actividad** auditoría implica:

- solicitar u obtener pruebas de auditoría;
- proceder a las pruebas necesarias del sistema auditado;
- obtener pruebas programáticamente a través de una serie de interfaces del sistema auditado;
- editar las pruebas, de ser necesario, para proteger la información sensible o sujeta al control reglamentario (por ejemplo, **IIP**);
- comparar las pruebas de auditoría obtenidas con los criterios de auditoría descritos en el esquema o norma sobre auditoría que se utilice.

El tipo de pruebas de auditoría necesarias y los criterios utilizados para evaluarlas están determinados por el esquema o norma de auditoría que se utilice. Son, por ejemplo, los datos relacionados con los controles de seguridad y los datos de calidad de funcionamiento de cada servicio concreto. Además de la obtención de los datos, la **actividad** auditar puede implicar la evaluación de los servicios prestados por un **proveedor de servicios en la nube**, incluidos los controles de seguridad, la influencia en la privacidad, la calidad de funcionamiento y demás **actividades de computación en la nube** relacionadas con los **servicios en la nube** que determine el solicitante de la auditoría. El solicitante puede ser el **proveedor de servicios en la nube** mismo cuando desea obtener pruebas de la calidad de sus **servicios en la nube** para poder presentarlos a **clientes de servicios en la nube** potenciales.

8.4.2.5 Comunicar resultados de auditoría

La **actividad** comunicar resultados de auditoría implica la presentación de un informe documentado de los resultados de la auditoría realizada, por ejemplo, de un **servicio en la nube** determinado, de un **proveedor de servicios en la nube** o de la utilización de un **servicio en la nube** por un **cliente de servicios en la nube**. El formato del informe documentado puede estar definido por el esquema de auditoría que se utilice. En función de la situación comercial o del contexto jurídico, los resultados de la auditoría podrán comunicarse al **proveedor de servicios en la nube** o, previa demanda, al **cliente de servicios en la nube**.

8.4.2.6 Captar y evaluar clientes

La **actividad** captar y evaluar clientes comprende las tareas necesarias para comercializar y vender **servicios en la nube** de manera que un **cliente de servicios en la nube** entabla una relación contractual para la utilización de uno o más servicios. Esta **actividad de computación en la nube** implica:

- informar a los clientes potenciales acerca de los servicios disponibles y los correspondientes **SLA** y términos contractuales;
- negociar términos y precios con los clientes;

- evaluar las necesidades y requisitos de los clientes en relación con los **servicios en la nube**.

NOTA – La actividad evaluación de las necesidades del **cliente de servicios en la nube** comprende las medidas adoptadas para determinar y responder a los requisitos del **cliente de servicios en la nube**, identificados en el análisis de carencias realizado comparando las capacidades vigentes del cliente y las capacidades que desea en el futuro.

8.4.2.7 Evaluar mercado

La **actividad** evaluar mercado consiste en la evaluación del mercado de **servicios en la nube** vigente para determinar el/los **servicio(s) en la nube** que se ajustan a los requisitos de los clientes. Esta **actividad de computación en la nube** implica:

- conocer las ofertas de productos de los **proveedores de servicios en la nube**, tanto a nivel técnico como comercial;
- abonarse a los **catálogos de productos** de los **proveedores de servicios en la nube** y recibir notificaciones cuando cambie su contenido;
- ajustar las ofertas de productos a las necesidades y requisitos de los clientes tanto a nivel técnico como comercial y reglamentario.

8.4.2.8 Establecer acuerdos jurídicos

La **actividad** establecer acuerdos jurídicos atañe al acuerdo de servicio concluido entre el **cliente de servicios en la nube** y el/los **proveedor(es) de servicios en la nube**. Esto implica la negociación de acuerdos de servicio entre los **clientes de servicios en la nube** y el/los **proveedor(es) de servicios en la nube** escogidos con el objetivo de colmar las necesidades de los clientes.

8.5 Aspectos transversales

8.5.1 Generalidades

Los aspectos transversales atañen tanto a la arquitectura como al funcionamiento e influyen en múltiples elementos de la CCRA o están relacionados con su funcionamiento en un sistema real. Estos aspectos transversales afectan tanto a las **funciones** como a las **actividades** y **componentes funcionales**. Por ejemplo, la seguridad es un aspecto transversal porque atañe a la infraestructura, a los servicios, a los **proveedores de servicios en la nube**, a los **clientes de servicios en la nube** y a los **asociados de servicios en la nube** (**auditores de la nube**, creadores de servicios en la nube, etc.). Todos ellos necesitan seguridad, pero ésta es distinta en función de lo que se protege. Así, la seguridad de la infraestructura y los servicios infraestructurales difiere en gran medida de la seguridad de los servicios de software.

Algunos aspectos transversales se aplican a otros aspectos transversales. Por ejemplo, la gobernanza se aplica tanto a los elementos funcionales como a los aspectos transversales que son la calidad de funcionamiento y la seguridad.

Los aspectos transversales suelen afectar a las **actividades de computación en la nube** que llevan a cabo las **funciones**. Las **funciones** pueden coordinar el soporte de un aspecto transversal entre ellas y sus **actividades de computación en la nube**. Para soportar aspectos transversales también es necesario que los **componentes funcionales** soporten las **actividades de computación en la nube**, las capacidades técnicas y las implementaciones.

Para cada aspecto transversal se define una serie de **actividades de computación en la nube** y **componentes funcionales** que los soportan. Cada **función** y solución podrá utilizar uno o varios de los siguientes.

Los aspectos transversales son, entre otros, los siguientes:

- auditabilidad (cláusula 8.5.2);
- **disponibilidad** (cláusula 8.5.3);
- gobernanza (cláusula 8.5.4);
- **interoperabilidad** (cláusula 8.5.5);
- mantenimiento y gestión de versiones (cláusula 8.5.6);
- calidad de funcionamiento (cláusula 8.5.7);
- portabilidad (cláusula 8.5.8);
- protección de la **información de identificación personal** (cláusula 8.5.9);
- reglamentación;
- resiliencia (cláusula 8.5.10);
- **reversibilidad** (cláusula 8.5.11);
- seguridad (cláusula 8.5.12);

- niveles de servicio y **acuerdo de nivel de servicio** (cláusula 8.5.13).

8.5.2 Auditabilidad

Auditabilidad es la capacidad de recabar y poner a disposición información de pruebas relacionada con el funcionamiento y la utilización de un **servicio en la nube**, necesaria a los efectos de realizar una auditoría. En relación con la gobernanza de **servicios en la nube** es la garantía de que esos servicios se presta y utilizan de conformidad con los acuerdos de servicio correspondientes establecidos entre los **clientes de servicios en la nube**, **proveedores de servicios en la nube** y **asociados de servicios en la nube**. Esta garantía suele lograrse mediante la auditoría independiente de los servicios. Una auditoría suele consistir en un informe o certificación de auditoría que se facilita a las partes de los acuerdos de servicio en cuestión: los **clientes de servicios en la nube**, los **proveedores de servicios en la nube** y los **asociados de servicios en la nube**.

La auditoría misma depende de los datos y pruebas que se ponen a disposición, relacionados con la utilización, el entorno, la **disponibilidad** y la calidad de funcionamiento de los servicios y recursos asociados. Esos datos y pruebas comprenden los registros, cronológicos y de otro tipo, de las actividades y condiciones de los entornos operativos de todas las partes en dichos acuerdos. Esos registros han de llevarse y mantenerse de manera segura.

8.5.3 Disponibilidad

La **disponibilidad** es la propiedad de ser accesible y utilizable por solicitud de una entidad autorizada. La "entidad autorizada" suele ser un **cliente de servicios en la nube**.

8.5.4 Gobernanza

La gobernanza es el sistema mediante el cual se dirige y controla la prestación y utilización de **servicios en la nube**.

El término gobernanza interna en la nube se utiliza para la aplicación de políticas en tiempo de ejecución y de diseño destinadas a garantizar que las soluciones basadas en la **computación en la nube** se diseñen e implementen, y que los servicios basados en la **computación en la nube** se suministren con arreglo a expectativas específicas. Esas expectativas pueden abarcar cualquiera de los aspectos transversales o todos ellos.

Las prácticas de gobernanza individuales de los **clientes de servicios en la nube** y **proveedores de servicios en la nube** pueden ir de las más simples a las más sofisticadas y se enmarcan dentro de su **función**. Corresponde a cada **función** implementar la gobernanza en función de sus necesidades. La gobernanza en la nube se considera un aspecto transversal por el requisito de transparencia y la necesidad de racionalizar prácticas de gobernanza con **SLA** y otros elementos contractuales del **cliente de servicios en la nube** con el **proveedor de servicios en la nube**.

La gobernanza externa en la nube se utiliza para formalizar un acuerdo entre el **cliente de servicios en la nube** y el **proveedor de servicios en la nube** relativo a la utilización de **servicios en la nube** por el **cliente de servicios en la nube**. Ese acuerdo puede hacer referencia a un **acuerdo de nivel de servicio** que consigne información detallada sobre los aspectos funcionales y no funcionales de los servicios.

8.5.5 Interoperabilidad

La **interoperabilidad** en el marco de la **computación en la nube** significa que el **cliente de servicios en la nube** tiene la capacidad de interactuar con un **servicio en la nube**, intercambiar información y obtener resultados previsibles, siguiendo un método determinado. Normalmente, la **interoperabilidad** supone que un **servicio en la nube** funciona según una especificación acordada, probablemente normalizada. El **cliente de servicios en la nube** debe poder utilizar ampliamente sus propias instalaciones de TIC al interactuar con los **servicios en la nube**, evitando así la necesidad de utilizar software privado o muy especializado.

La **interoperabilidad** también incluye la capacidad de un **servicio en la nube** de interactuar con otros **servicios en la nube**, ya sea a través de una relación de CSP:proveedor entre nubes, o en el marco de un **cliente de servicios en la nube** que utiliza múltiples **servicios en la nube** para lograr sus objetivos comerciales.

La **interoperabilidad** va más allá de los **servicios en la nube** propiamente dichos y, además, abarca la interacción del **cliente del servicio en la nube** con la infraestructura de gestión del **servicio en la nube** del **proveedor de servicios en la nube**. Idealmente, el **cliente de servicios en la nube** dispondrá de una interfaz coherente e interoperable a la funcionalidad de gestión del **servicio en la nube** y podrá interactuar con dos o más **proveedores de servicios en la nube** sin necesidad de tratar con cada uno de ellos de manera particular.

Las normas se implementan para soportar la **interoperabilidad** entre componentes o para soportar la portabilidad de datos o componentes de programas. Esas implementaciones deben soportar la evolución de las normas utilizadas, desde su versión más temprana a la más actual, o el cambio de una norma por otra, minimizando al mismo tiempo las interrupciones.

8.5.6 Mantenimiento y gestión de versiones

Un punto importante en relación con la gobernanza es el mantenimiento de los servicios y recursos subyacentes. El mantenimiento puede llevarse a cabo por muy diversos motivos, incluida la necesidad de reparar fallos o la necesidad de actualizar o ampliar las funcionalidades por motivos comerciales. Las operaciones de mantenimiento pueden modificar el comportamiento de los **servicios en la nube**, sobre todo cuando afectan al funcionamiento de un servicio cuando lo utiliza un cliente.

Conviene distinguir entre el mantenimiento realizado por el **proveedor de servicios en la nube** y el mantenimiento realizado por el **cliente de servicios en la nube**. En el caso de un servicio **SaaS**, es probable que prácticamente todas las operaciones de mantenimiento procedan del proveedor. En el caso de los servicios **IaaS** y **PaaS**, los componentes de aplicación pertenecen al **cliente de servicios en la nube** y es éste el responsable de su mantenimiento. El proveedor es responsable del entorno en el que se ejecutan los componentes de aplicación, que varía en función de los detalles del servicio, pero que puede incluir elementos como los recursos de hardware, el sistema operativo o el middleware.

Por un lado, puede convenir al cliente que un servicio o plataforma de servicio se actualice o arregle. Por otra parte, todo cambio del comportamiento de un servicio puede repercutir negativamente en el cliente, que posiblemente deberá modificar los componentes de aplicación o los sistemas de TIC clientes, o tendrá que volver a formar a los usuarios del servicio clientes. Así, es importante que el mantenimiento de los servicios esté sujeto a prácticas de gobernanza transparentes para el cliente.

Las prácticas de mantenimiento de **servicios en la nube** deben documentarse en los **SLA** e incluir la capacidad del cliente de comunicar problemas y exigir reparaciones, así como un mecanismo para que el **proveedor de servicios en la nube** notifique al cliente los cambios de mantenimiento por hacer y el calendario para ello.

La gestión de versiones es el adecuado etiquetado de un servicio (o sus componentes, como el nivel de sistema operativo utilizado en un servicio **IaaS**), a fin de que el cliente tenga claro qué versión concreta está utilizando. También es importante dar al servicio una nueva etiqueta de versión tras el mantenimiento de un **servicio en la nube**.

Cuando se aportan modificaciones importantes a un servicio entre dos versiones, la versión más antigua del servicio debe estar disponible en paralelo a las nuevas versiones durante un periodo de tiempo acordado.

8.5.7 Calidad de funcionamiento

La calidad de funcionamiento comprende una serie de facetas no funcionales relacionadas con el funcionamiento de un **servicio en la nube**, como son las siguientes:

- **disponibilidad** del servicio;
- tiempo de respuesta para completar las solicitudes de servicio;
- velocidad de transacción a la que se ejecutan las solicitudes de servicio;
- latencia de las solicitudes de servicio;
- velocidad del caudal de datos (entrante y saliente);
- número de solicitudes de servicio concurrentes (adaptabilidad);
- capacidad de almacenamiento de datos;
- (para **IaaS** y **PaaS**) número de hilos de ejecución concurrentes disponibles para una aplicación;
- (para **IaaS** y **PaaS**) cantidad de memoria (RAM) disponible para la ejecución del programa;
- conjunto de direcciones IP de la red del centro de datos y/o capacidad de alcance VLAN.

Cuando el servicio implica la ejecución de una aplicación (**IaaS**, **PaaS**), las mismas facetas de la calidad de funcionamiento se aplican al comportamiento de la aplicación que se ejecuta en el entorno del **proveedor de servicios en la nube**.

En función del modelo de cobro, también puede ser una faceta importante de la calidad de funcionamiento la capacidad del **servicio en la nube** para adaptar su utilización de los recursos de conformidad con los términos del **SLA**. Las métricas de la calidad de funcionamiento deben estar definidas en el **SLA** para cada una de las condiciones identificadas, y esas métricas deben supervisarse durante el funcionamiento del **servicio en la nube** para garantizar que el servicio cumple los términos de calidad de funcionamiento previstos en el **SLA**.

8.5.8 Portabilidad

La portabilidad es importante en la **computación en la nube** pues a los eventuales **clientes de servicios en la nube** les interesa evitar las ataduras cuando optan por utilizar **servicios en la nube**. Los **clientes de servicios en la nube** necesitan saber que pueden trasladar sus **datos de clientes de servicios en la nube** o sus aplicaciones entre múltiples **proveedores de servicios en la nube** a bajo coste y con una mínima interrupción. El coste y la interrupción aceptables podrán variar en función del tipo de **servicio en la nube** que se utilice.

Por ejemplo, si una organización **cliente de servicios en la nube** considera la posibilidad de cambiar de un **proveedor de servicio IaaS en la nube** a otro, el **cliente de servicios en la nube** debe poder coger sus datos e imagen de máquina virtual (VM, *virtual machine*) y activarlos y ejecutarlos en un servicio **IaaS** equivalente de manera relativamente directa. En un entorno **SaaS**, cuando la organización **cliente de servicios en la nube** desea trasladar una aplicación **SaaS** a un **proveedor de servicios en la nube** distinto (es decir, cambiar de proveedor de servicio **SaaS**), el **cliente de servicios en la nube** necesita poder llevarse sus datos, pero el resto del coste que implica el cambio incluirá la exportación, la correspondencia y la importación de los datos en la aplicación **SaaS** del nuevo **proveedor de servicios en la nube**, y ese coste será una función de hasta qué punto los modelos y formatos de datos de los dos **proveedores de servicios SaaS en la nube** concuerdan. En una configuración ideal, los **proveedores de servicios SaaS en la nube** deben adoptar formatos de intercambio de datos normalizados para su dominio de aplicación. El cambio de una aplicación **SaaS** a otra también puede implicar que el **cliente de servicios en la nube** deba adaptarse a una nueva interfaz de servicio (este aspecto concierne a la **interoperabilidad** del servicio).

Sin embargo, como cada **tipo de capacidad en la nube** puede tener sus propios requisitos de portabilidad, suele ser más útil centrarse en los tipos de portabilidad específicos, como la **portabilidad de datos en la nube** y la **portabilidad de aplicaciones en la nube**.

Datos de cliente de servicios en la nube es una clase de objetos de datos que controla el **cliente de servicios en la nube**. La **portabilidad de datos en la nube** permite a los **clientes de servicios en la nube** copiar o suprimir los **datos de cliente de servicios en la nube** de un **servicio en la nube** mediante acceso de red o transferencia física de los dispositivos de almacenamiento.

La **portabilidad de aplicaciones en la nube** permite la migración de elementos como las instancias de máquinas virtuales totalmente detenidas o una imagen de máquina (servicio **IaaS**) de un **proveedor de servicios en la nube** a otro **proveedor de servicios en la nube**, o la migración de componentes de aplicación (servicio **PaaS**) de un **proveedor de servicios en la nube** a otro. En ambos casos hay que tener en cuenta el soporte de la portabilidad de metadatos relacionados con los componentes de aplicación, que dan información sobre las relaciones de los componentes de programa y sobre la infraestructura necesaria para esos componentes (por ejemplo, configuración de equilibrio de carga, parámetros del cortafuegos).

8.5.9 Protección de la información de identificación personal (IIP)

Los **proveedores de servicios en la nube** deben proteger adecuada, debida y coherentemente la recopilación, procesamiento, comunicación, utilización y eliminación de **información de identificación personal (IIP)** en relación con los **servicios en la nube**.

De acuerdo con las directrices establecidas, uno de los principales imperativos comerciales de una organización es garantizar la protección de la **información de identificación personal (IIP)**. Aunque la **computación en la nube** ofrece una solución flexible para compartir recursos, software e información, también plantea problemas de **confidencialidad** para los **clientes de servicios en la nube** que utilizan **servicios en la nube**, así como para los **proveedores de servicios en la nube**.

En muchos países se aplican normas y reglamentos estrictos en materia de tratamiento de la **IIP** y la utilización de **servicios en la nube** para almacenar y procesar la **IIP** con frecuencia deben conformarse a esas normas y reglamentos.

Los requisitos jurídicos, reglamentarios y legislativos varían en función del sector del mercado y la jurisdicción, y pueden modificar las responsabilidades de los **clientes de servicios en la nube** y de los **proveedores de servicios en la nube**. La conformidad con tales requisitos está a menudo relacionada con la gobernanza y las **actividades** de gestión de riesgos.

8.5.10 Resiliencia

La resiliencia es la capacidad de un sistema de proporcionar y mantener un nivel aceptable de servicio en caso de averías (involuntarias, deliberadas o de causa natural) que afectan al funcionamiento normal.

Por resiliencia se entiende el conjunto de procesos de supervisión, prevención y respuesta que permiten a un **servicio en la nube** ofrecer un funcionamiento continuo, o interrupciones predecibles y verificables, aplicando medidas de fallo y recuperación. Se incluyen aquí los fallos de hardware, comunicación y/o software, que pueden ocurrir de manera puntual o combinada, incluidos los fallos en serie. Estos procesos pueden ser automáticos o manuales y suelen afectar a múltiples sistemas, por lo que su descripción y aplicación forman parte de la infraestructura global de la nube y no de una función independiente.

Inherente a la resiliencia es la gestión de riesgos, pues la resiliencia está determinada por el componente menos resiliente del sistema y la relación coste/calidad de funcionamiento u otros factores pueden limitar la medida en que la resiliencia es posible o factible. La asociación del riesgo al valor depende de las opciones implementadas para lograr la resiliencia.

8.5.11 Reversibilidad

La **reversibilidad** es el proceso que siguen el **cliente de servicios en la nube** para recuperar sus **datos de cliente de servicios en la nube** y artefactos de aplicación y el **proveedor de servicios en la nube** para suprimir todos **datos de cliente de servicios en la nube**, así como los **datos derivados de servicios en la nube** especificados por contrato tras un periodo acordado. El principio aplicable es el del "derecho al olvido", en la medida en que el **cliente de servicios en la nube** tiene derecho a esperar que, una vez comunicada al **proveedor de servicios en la nube** su intención de cesar la utilización de los servicios, se iniciará un proceso normalizado para que el **cliente de servicios en la nube** extraiga sus **datos de cliente de servicios en la nube** y artefactos de aplicación, y que el **proveedor de servicios en la nube** suprima todas las copias y no conserve material alguno perteneciente al **cliente de servicios en la nube** tras un periodo acordado.

La actividad relacionada con la **reversibilidad** en la mayoría de los casos implicará una serie de fases, en las que normalmente el **cliente de servicios en la nube** solicitará la extracción de sus datos e informará al **proveedor de servicios en la nube** de que puede borrar sus copias de **datos de cliente de servicios en la nube** – conservando copias de seguridad hasta ese punto por si ocurre un fallo en el proceso de extracción. Esas fases se aplicarán también necesariamente a los servicios pares utilizados por el **proveedor de servicios en la nube** para soportar sus propios servicios.

8.5.12 Seguridad

8.5.12.1 Generalidades

Resulta fundamental reconocer que la seguridad es un aspecto transversal de la arquitectura que atañe a todas las perspectivas del modelo de referencia, desde la seguridad física hasta la seguridad de aplicación. Por consiguiente, la seguridad en la arquitectura de **computación en la nube** no es simplemente un aspecto transversal que controlan los **proveedores de servicios en la nube**, sino que también afecta a los **clientes de servicios en la nube**, los **asociados de servicios en la nube** y sus **subfunciones**.

Los **sistemas de computación en la nube** pueden tener que cumplir requisitos de seguridad como la autenticación, la autorización, la **disponibilidad**, la **confidencialidad**, el no repudio, la gestión de identidades, la **integridad**, la auditoría, la supervisión de seguridad, la respuesta a incidentes y la gestión de políticas de seguridad. En esta cláusula se describen las perspectivas propias de la **computación en la nube** para ayudar a analizar e implementar la seguridad en sistemas de **computación en la nube**.

Entre las capacidades de seguridad de los **servicios en la nube** se cuentan el control de acceso, la **confidencialidad**, la **integridad** y la **disponibilidad**. La seguridad de la **computación en la nube** se describe detalladamente en otras especificaciones.

Las capacidades de seguridad comprenden también las funciones de gestión y administración empleadas para controlar los **servicios en la nube**, los recursos subyacentes y la utilización de los **servicios en la nube**, prestando una atención especial al control de acceso para los usuarios de esas funciones. Se incluyen además:

- funcionalidades que permitan la detección temprana, el diagnóstico y la reparación de los **servicios en la nube** y los problemas relacionados con los recursos;
- el registro seguro de registros de acceso, informes de actividad, supervisión de sesión e inspecciones de paquetes en la red;
- la instalación de cortafuegos y sistemas de detección y prevención de ataques malignos en los sistemas de los **proveedores de servicios en la nube**. Un usuario no debe poder interrumpir la utilización que otros usuarios hacen de los **servicios en la nube**.

La red que conecta al **cliente de servicios en la nube** con el **proveedor de servicios en la nube** (por ejemplo, mediante capacidades VPN) debe contar con un nivel de seguridad intrarred.

Las medidas de seguridad en la **computación en la nube** se aplican contra una serie de amenazas a la utilización de los **servicios en la nube** por los **clientes de servicios en la nube**, que afectan tanto a éstos como a los **proveedores de servicios en la nube**. Esas amenazas se describen pormenorizadamente en otras especificaciones, como ISO/CEI 27018.

8.5.12.2 Distribución de las responsabilidades en materia de seguridad

Un **proveedor de servicios en la nube** y un **cliente de servicios en la nube** no tienen el mismo grado de control sobre los recursos de computación de un sistema de **computación en la nube**. A diferencia de los sistemas de tecnología de la información tradicionales, donde sólo una de las partes controla la totalidad de los recursos de computación durante toda la vida útil de los sistemas, los **proveedores de servicios en la nube** y los **clientes de servicios en la nube** colaboran para diseñar, construir, desplegar y explotar los sistemas de **computación en la nube**.

La división del control implica que ambas **funciones** comparten responsabilidades a la hora de proteger adecuadamente los sistemas de **computación en la nube**. La seguridad es una responsabilidad compartida. Es necesario analizar los controles de seguridad, es decir, las medidas adoptadas para ofrecer protección, a fin de determinar qué **función** se

encuentra en mejor postura para aplicar esos controles. Este análisis debe tener en cuenta la perspectiva de categorías de servicio, pues las distintas **categorías de servicios en la nube** implican distintos grados de control entre los **proveedores de servicios en la nube** y los **clientes de servicios en la nube**. es importante definir claramente las responsabilidades tanto del cliente como del proveedor para garantizar que se abarcan todos los aspectos de la seguridad y evitar toda ambigüedad en relación con dichas responsabilidades.

Por ejemplo, los controles de gestión de cuentas para los usuarios con privilegios iniciales de un sistema del servicio **IaaS** suelen ser ejecutados por el **proveedor del servicio IaaS en la nube**, mientras que la gestión de cuentas de usuario de aplicación para la aplicación desplegada de dicho servicio **IaaS** suele ser responsabilidad del **cliente de servicios en la nube** que despliega la aplicación mediante el servicio **IaaS**. Por el contrario, en el caso de un servicio de aplicación **SaaS**, los controles de gestión de cuentas de todos los tipos de usuarios dependen del **proveedor de servicios en la nube** (aunque los **clientes de servicios en la nube** pueden ofrecer capacidades como la autenticación de terceros).

8.5.12.3 Perspectivas de categorías de servicios en la nube

Una **categoría de servicios en la nube**, según se define en la Recomendación UIT-T Y.3500 | ISO/CEI 17788, es un grupo de **servicios en la nube** que posee un conjunto común de cualidades. Las **categorías de servicios en la nube** ofrecen a los **clientes de servicios en la nube** distintos tipos de operaciones de gestión de servicio, además de diferentes puntos de entrada a los sistemas de **computación en la nube**, lo que a su vez supone que hay más superficies susceptibles de ser atacadas. Por consiguiente, es importante considerar las consecuencias que las **categorías de servicios en la nube**, y los distintos problemas que plantean, tienen para el diseño y la implementación de la seguridad.

Por ejemplo, el **SaaS** ofrece a los usuarios acceso a ofertas de **computación en la nube** a través de una conexión de red, posiblemente por Internet y la utilización de un navegador web. Al considerar la seguridad de los sistemas de **computación en la nube SaaS** se ha hecho mucho hincapié en la seguridad de los navegadores web. Los CSC:usuario de servicios en la nube de los servicios **IaaS** suelen contar con máquinas virtuales (VM) que se ejecutan en los hipervisores de los anfitriones, por lo que la seguridad de los hipervisores para lograr el aislamiento de las VM ha sido objeto de amplios estudios por parte de los **proveedores de servicios IaaS en la nube** que utilizan tecnologías de virtualización.

8.5.12.4 Implicaciones de los modelos de despliegue en la nube

Los distintos **modelos de despliegue en la nube** tienen importantes implicaciones de seguridad. Una manera de considerarlas desde la perspectiva de los modelos de despliegue es distinguiendo el nivel de exclusividad de los **arrendatarios** en el modelo de despliegue. Una **nube privada** está dedicada a una organización **cliente de servicios en la nube**, mientras que una **nube pública** puede tener **arrendatarios** de múltiples organizaciones diferentes coexistentes.

Otra manera de analizar las consecuencias para la seguridad de los **modelos de despliegue en la nube** es utilizar el concepto de fronteras de acceso. Por ejemplo, un sistema de **nube privada** en los locales propios puede necesitar o no controladores de frontera adicionales en la frontera del **servicio en la nube** cuando el sistema de **red privada** está albergado en los locales propios dentro de los límites de la red de la organización **cliente de servicios en la nube**, mientras que una **nube privada** externalizada suele exigir el establecimiento de un perímetro de protección en la frontera de los **servicios en la nube**.

8.5.12.5 Estrategia y responsabilidad de protección de datos

La protección de los datos supone una nueva dimensión de la **computación en la nube**. una organización puede optar por almacenar sus datos en un **servicio en la nube**, pero en tal caso la responsabilidad de protección de los datos deberá acordarse claramente de antemano. En primer lugar el **cliente de servicios en la nube** debe catalogar adecuadamente los datos y determinar su sensibilidad, así como el riesgo comercial que supondría su fuga, pérdida o corrupción. (Véase ISO/CEI 27002 como referencia para determinar la sensibilidad de los datos.)

En una configuración ideal, recae en el **cliente de servicios en la nube** la responsabilidad de proteger los datos antes de su traslado a un sistema de **computación en la nube**. Sin embargo, el proveedor será responsable de cualquier manipulación o robo de los datos. La encriptación es una técnica que se puede utilizar, pero entonces se ha de considerar la gestión de claves cuando es el **cliente de servicios en la nube** o un tercero quien gestiona las claves. Si las claves están gestionadas por el **proveedor de servicios en la nube**, éste es responsable del control lógico y físico de las claves, así como de los datos.

8.5.13 Acuerdos de servicio y acuerdos de nivel de servicio

Los **acuerdos de nivel de servicio** son componentes importantes de la gobernanza de la **computación en la nube** y representan elementos mensurables necesarios para garantizar la calidad de servicio acordada entre el **cliente de servicios en la nube** y el **proveedor de servicios en la nube**.

El **acuerdo de nivel de servicio de la computación en la nube (SLA nube)** es un **acuerdo de nivel de servicio** entre un **proveedor de servicios en la nube** y un **cliente de servicios en la nube** basado en una taxonomía de condiciones específicas de la **computación en la nube** para establecer la calidad de los **servicios en la nube** suministrados. Caracteriza la calidad de los **servicios en la nube** suministrados en lo que respecta a:

- un conjunto de propiedades cuantificables específicas de la **computación en la nube** (comercial y técnica);
- un determinado conjunto de **funciones de computación en la nube** (**cliente de servicios en la nube** y **proveedor de servicios en la nube**, y sus **subfunciones** correspondientes).

Por ejemplo, los **clientes de servicios en la nube** necesitan un **SLA** nube para especificar los requisitos de calidad de funcionamiento técnicos de uno o más **servicios en la nube**. Un **SLA** nube puede prever las condiciones aplicables a la calidad de servicio, la seguridad, la calidad de funcionamiento y las compensaciones por incumplimiento de los términos del **SLA**. Un **proveedor de servicios en la nube** también puede incluir en el **SLA** nube una serie de promesas no explícitamente formuladas a los **clientes de servicios en la nube**, es decir, limitaciones y obligaciones que el **cliente de servicios en la nube** debe aceptar. En un **SLA** nube se debe definir la clasificación de objetos de datos (es decir, **datos de clientes de servicios en la nube**, **datos de proveedores de servicios en la nube** y **datos derivados de servicios en la nube**), quién puede acceder y controlar los objetos de datos en cada clasificación y cómo se utilizarán esos datos.

El **acuerdo de nivel de servicio** debe especificar información relativa a la **disponibilidad** de los servicios, la **confidencialidad** e **integridad** de los servicios y los controles de acceso aplicables a esos servicios. En el **acuerdo de nivel de servicio** se debe especificar cómo se tratará la **información de identificación personal** relacionada con los **servicios en la nube**.

El acuerdo de servicio, también denominado acuerdo de servicio maestro (MSA, *master service agreement*), términos de servicio (ToS, *terms of service*), términos y condiciones (T&C) o, simplemente, "contrato", es el documento más importante en los acuerdos entre las partes y de él depende el **acuerdo de nivel de servicio (SLA)**. Es importante establecer esta distinción, pues con frecuencia se utiliza erróneamente el acrónimo **SLA** para hacer referencia a la relación contractual en su conjunto, **función** que el **SLA** por sí solo es incapaz de realizar. El acuerdo de servicio prevé la totalidad de la relación contractual, por lo que contiene elementos contractuales no directamente relacionados con la **computación en la nube**.

9 Perspectiva funcional

9.1 Arquitectura funcional

La arquitectura funcional de la **computación en la nube** describe la **computación en la nube** en términos de un conjunto de alto nivel de **componentes funcionales**. Los **componentes funcionales** son series de funciones necesarias para realizar las **actividades de computación en la nube** descritas en la cláusula 8 para las diversas **funciones** y **subfunciones** implicadas en la **computación en la nube**.

La arquitectura funcional describe los **componentes funcionales** en un marco estratificado donde cada tipo específico de función se agrupa en una capa y donde hay interfaces entre los **componentes funcionales** de capas contiguas.

9.1.1 Marco estratificado

El marco estratificado utilizado en la CCRA tiene cuatro capas, además de una serie de funciones que se aplican a todas las capas. Las cuatro capas son:

- capa de usuario;
- capa de acceso;
- capa de servicio;
- capa de recursos.

Las funciones que se aplican a todas las capas se denominan funciones multicapa.

En la Figura 9-1 se ilustra el marco estratificado.

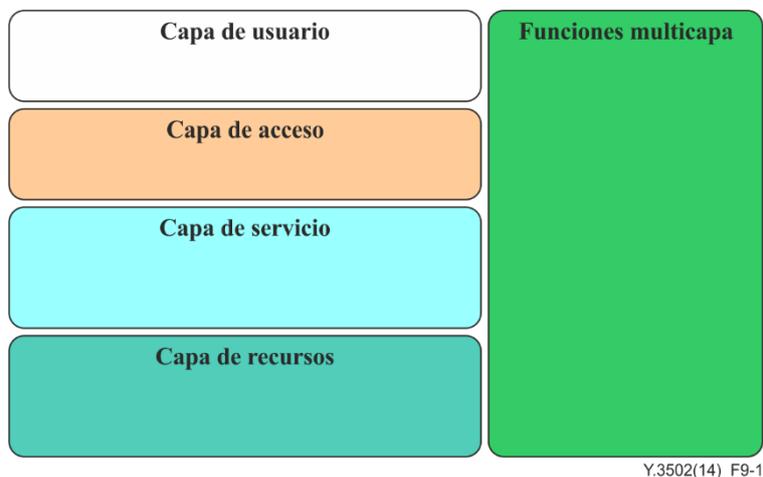


Figura 9-1 – Marco estratificado de computación en la nube

En las siguientes subcláusulas se describen las capas de este marco.

9.1.1.1 Capa de usuario

La capa de usuario es la interfaz de usuario a través de la que el **cliente de servicios en la nube** interactúa con el **proveedor de servicios en la nube** y con los **servicios en la nube**, realiza las **actividades** administrativas relacionadas con el cliente y supervisa los **servicios en la nube**. También se pueden ofrecer los resultados de los **servicios en la nube** a otra instancia de la capa de recursos.

9.1.1.2 Capa de acceso

La capa de acceso ofrece una interfaz común para el acceso manual y automatizado a las capacidades disponibles en la capa de servicio. Esas capacidades son tanto las de los servicios como las capacidades administrativas y comerciales.

La capa de acceso es responsable de presentar las capacidades de **servicios en la nube** por uno o más mecanismos de acceso, por ejemplo, como un conjunto de páginas web a las que se accede a través de un navegador o como un conjunto de servicios web a los que se accede programáticamente en una comunicación protegida. Otra responsabilidad de la capa de acceso es aplicar la adecuada funcionalidad de seguridad para acceder a las capacidades de **servicios en la nube**. La capa de acceso es responsable de autenticar las solicitudes utilizando credenciales de usuario y de validar la autorización para que el usuario emplee unas capacidades concretas. La capa de acceso también se ocupa de la encriptación y de verificar la **integridad** de las solicitudes, cuando procede.

La capa de acceso también puede encargarse de las políticas de QoS aplicables al tráfico procedente de la capa de usuario (por ejemplo, las solicitudes de servicio al **proveedor de servicios en la nube**) y al tráfico saliente hacia la capa de usuario (por ejemplo, resultado de los **servicios en la nube**).

La capa de acceso transmite las solicitudes validadas a los componentes de la capa de servicio. La capa de acceso acepta las solicitudes de consumo de **servicios en la nube** de los **clientes de servicios en la nube** o los **proveedores de servicios en la nube** para acceder a los servicios y recursos del CSP.

9.1.1.3 Capa de servicio

La capa de servicio contiene la implementación de los servicios prestados por un **proveedor de servicios en la nube**. La capa de servicio contiene y controla los componentes de software que implementan los servicios (pero no los hipervisores subyacentes, los sistemas operativos anfitriones, los controladores de dispositivos, etc.) y hace lo necesario para ofrecer a los usuarios los **servicios en la nube** a través de la capa de acceso.

El software de implementación de servicios de la capa de servicio depende a su vez de las capacidades disponibles en la capa de recursos para prestar los servicios ofrecidos y garantizar el cumplimiento de los requisitos estipulados en los **SLA** relativos a esos servicios, por ejemplo, utilizando suficientes recursos.

9.1.1.4 Capa de recursos

La capa de recursos es donde residen los recursos, que son, entre otros, los equipos normalmente utilizados en los centros de datos, como los servidores, los conmutadores de interconexión de redes y encaminadores, y los dispositivos de almacenamiento, además del correspondiente software no específico de la nube que se ejecuta en los servidores y demás equipos como sistemas operativos anfitriones, hipervisores, controladores de dispositivos y software de gestión de sistemas genérico.

La capa de recursos también representa y alberga la funcionalidad de red de transporte en la nube, necesaria para ofrecer la conectividad de red subyacente entre el **proveedor de servicios en la nube** y los usuarios, así como dentro del **proveedor de servicios en la nube**, y entre **proveedores de servicios en la nube pares**.

Téngase en cuenta que para que un **proveedor de servicios en la nube** preste servicios coherentes con el **SLA**, puede ser necesario que las conexiones entre los usuarios y el **proveedor de servicios en la nube** sean exclusivas y/o seguras.

9.1.1.5 Funciones multicapa

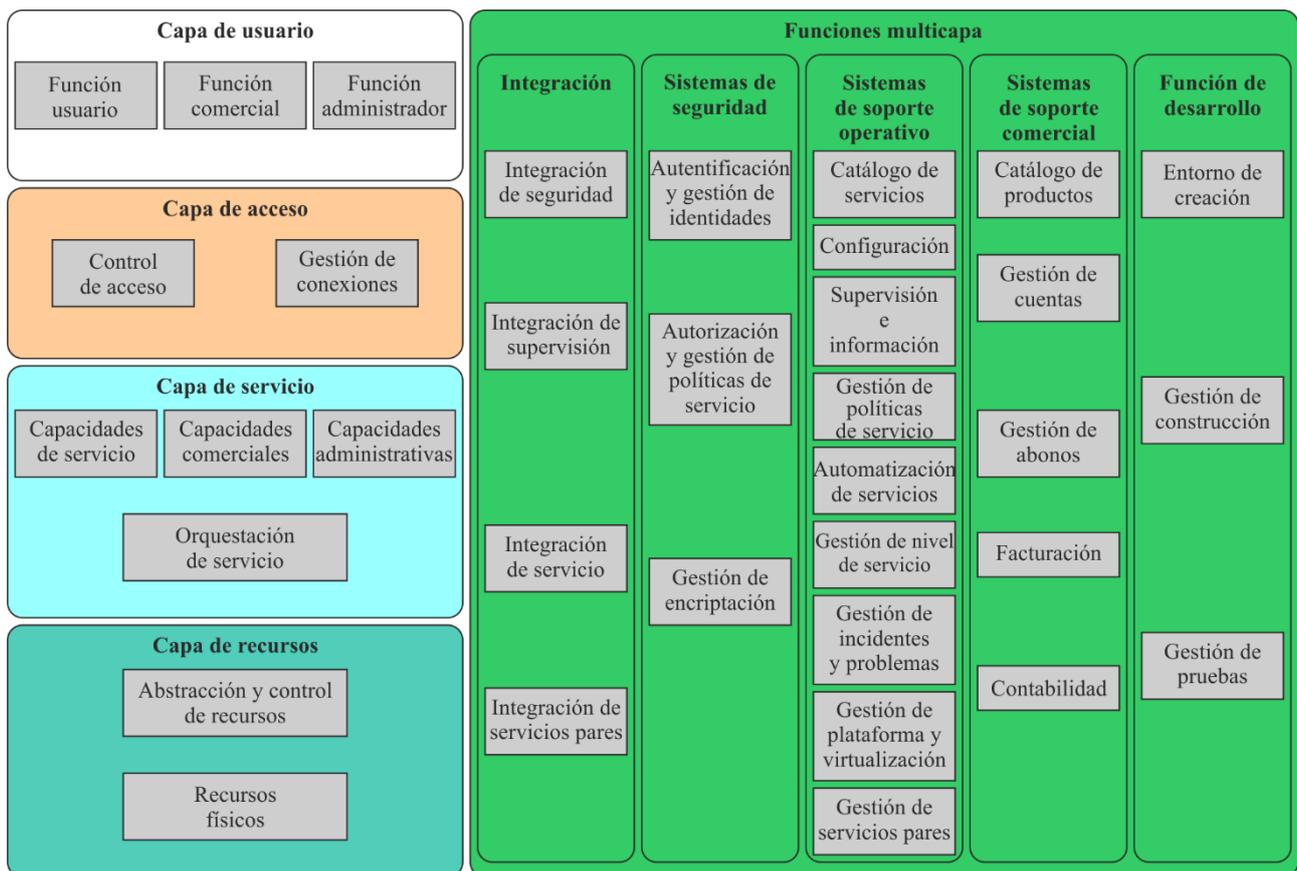
Las funciones multicapa comprenden una serie de **componentes funcionales** que interactúan con los **componentes funcionales** de las otras cuatro capas anteriores para ofrecer capacidades de soporte entre las que se cuentan las siguientes:

- capacidades de sistemas de soporte operativo (administración de tiempo de ejecución, supervisión, configuración y mantenimiento);
- capacidades de sistemas de soporte comercial (**catálogo de productos**, gestión financiera y de la facturación);
- capacidades de sistemas de seguridad (autenticación, autorización, auditoría, validación, encriptación);
- capacidades de integración (vinculación de los distintos componentes para lograr la funcionalidad necesaria);
- capacidades de soporte de desarrollo (implica la creación, las pruebas y la gestión de la vida útil de los servicios y los componentes de servicio).

9.2 Componentes funcionales

En esta cláusula se describe la arquitectura de la nube en términos de un conjunto común de **componentes funcionales de computación en la nube**. Un **componente funcional** es un elemento funcional de la CCRA que se utiliza para realizar una **actividad** o parte de una **actividad** y que tiene un artefacto de implementación en la materialización concreta de la arquitectura, por ejemplo, un componente de software, un subsistema o una aplicación.

La Figura 9-2 contiene una representación de alto nivel de los **componentes funcionales** de la CCRA, organizados según el marco estratificado.



Y.3502(14)_F9-2

Figura 9-2 – Componentes funcionales de la CCRA

9.2.1 Componentes funcionales de la capa de usuario

Los **componentes funcionales** de la capa de usuario son:

- función usuario;
- función comercial;
- función administrador.

Los **servicios en la nube** presentados al CSC:usuario de servicios en la nube pueden dividirse en dos grandes categorías, servicios funcionales y servicios de gestión de autoservicio. Estos últimos pueden dividirse, además, en servicios comerciales y servicios administrativos.

La interfaz que se presenta al usuario de los **servicios en la nube** comprende la función primaria de los **servicios en la nube** y es distinta de la interfaz utilizada para gestionar la utilización de los **servicios en la nube**. No obstante, en todos los casos se trata de **servicios en la nube** adaptados a distintos tipos de capacidades.

9.2.1.1 Función usuario

El **componente funcional** función usuario soporta que el CSC:usuario de servicios en la nube acceda a los **servicios en la nube** y los utilice (**actividad utilizar servicio**). En algunos casos, el **componente funcional** función usuario puede ser tan simple como un navegador que se ejecuta en un dispositivo de usuario. Sin embargo, en otros casos puede implicar un sistema empresarial sofisticado que ejecuta procesos comerciales, aplicaciones, middleware y la infraestructura asociada.

9.2.1.2 Función comercial

El **componente funcional** función comercial soporta las **actividades de computación en la nube** del CSC:gestor comercial, incluida la selección y adquisición de **servicios en la nube**, así como la gestión contable y financiera relativa a la utilización de los **servicios en la nube**. Cabe señalar que las capacidades comerciales en sí mismas se ofrecen a través de los **servicios en la nube**.

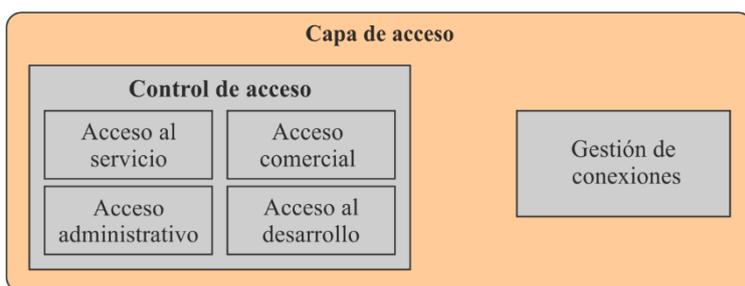
9.2.1.3 Función administrador

El **componente funcional** función administrador soporta las **actividades de computación en la nube** del CSC:administrador de servicios en la nube, lo que incluye las funciones de administración de las identidades y perfiles de usuario, la supervisión de la actividad y utilización de los servicios, el tratamiento de eventos y la comunicación de problemas. A las capacidades de administración de la nube sólo se puede acceder mediante **servicios en la nube**.

9.2.2 Componentes funcionales de la capa de acceso

En la Figura 9-3 se muestran los **componentes funcionales** de la capa de acceso, que son los siguientes:

- Control de acceso:
 - acceso al servicio;
 - acceso comercial;
 - acceso administrativo;
 - acceso al desarrollo.
- Gestión de conexiones.



Y.3502(14)_F9-3

Figura 9-3 – Componentes funcionales de la capa de acceso

9.2.2.1 Control de acceso

El control de acceso limita la utilización de servicios concretos por los usuarios. Principalmente, el control de acceso implica la autenticación del usuario mediante la presentación y validación de credenciales, y la posterior autorización del usuario autenticado para utilizar unos servicios específicos. La gestión de identidades está asociada a este proceso.

Es necesario aplicar un control de acceso a los **servicios en la nube**, los recursos de que dependen y las funciones de control conexas.

9.2.2.2 Acceso al servicio

El **componente funcional** acceso de servicio da acceso a los **servicios en la nube** ofrecidos por el **proveedor de servicios en la nube**.

9.2.2.3 Acceso comercial

El **componente funcional** acceso comercial da acceso a las capacidades comerciales del **proveedor de servicios en la nube**, implementadas por los sistemas de soporte comercial.

9.2.2.4 Acceso administrativo

El **componente funcional** acceso administrativo da acceso a las capacidades administrativas ofrecidas por el **proveedor de servicios en la nube**, implementadas por el sistema de soporte operativo.

9.2.2.5 Acceso al desarrollo

El **componente funcional** acceso al desarrollo da acceso a una serie de capacidades del sistema del proveedor que soportan el desarrollo, las pruebas y el mantenimiento de las implementaciones de **servicios en la nube**.

9.2.2.6 Gestión de conexiones

El **componente funcional** gestión de conexiones se encarga de aplicar las políticas de QoS aplicables al tráfico entrante y/o saliente de los **componentes funcionales** de la capa de usuario. El **componente funcional** gestión de conexiones interactúa con las funciones multicapa para extraer las políticas almacenadas y aplicarlas localmente en la capa de acceso.

9.2.3 Componentes funcionales de la capa de servicio

Los **componentes funcionales** de la capa de servicio son:

- capacidades de servicio;
- capacidades comerciales;
- capacidades administrativas;
- orquestación de servicios.

9.2.3.1 Capacidades de servicio

El **componente funcional** capacidades de servicio consiste en el software necesario para implementar el servicio ofrecido a los **clientes de servicios en la nube**. implementa la funcionalidad definida por la interfaz de servicio, es decir, la interfaz ofrecida a los **clientes de servicios en la nube**, independiente de la implementación del servicio.

9.2.3.2 Capacidades comerciales

El **componente funcional** capacidades comerciales ofrece una serie de capacidades para acceder a la función comercial relacionada con la prestación de **servicios en la nube**. La función comercial misma reside en los **componentes funcionales** sistemas de soporte comercial.

9.2.3.3 Capacidades administrativas

El **componente funcional** capacidades administrativas ofrece una serie de capacidades para acceder a la función administrativa relacionada con la prestación de **servicios en la nube**.

La función administrativa misma reside en los **componentes funcionales** sistemas de soporte operativo y sistemas de soporte comercial.

9.2.3.4 Orquestación de servicios

El **componente funcional** orquestación de servicios se ocupa de la coordinación, agregación y composición de múltiples componentes de servicio para la prestación de **servicios en la nube**.

9.2.4 Componentes funcionales de la capa de recursos

Los **componentes funcionales** de la capa de recursos son:

- abstracción y control de recursos;
- recursos físicos.

9.2.4.1 Abstracción y control de recursos

El **componente funcional** abstracción y control de recursos lo utilizan los **proveedores de servicios en la nube** para dar acceso a los recursos de computación físicos mediante la abstracción de software. La abstracción de recursos debe garantizar una utilización eficiente, segura y fiable de la infraestructura subyacente. La parte control del **componente funcional** permite la gestión de la parte abstracción de recursos.

El **componente funcional** abstracción y control de recursos permite al **proveedor de servicios en la nube** ofrecer funcionalidades como elasticidad rápida, **agrupación de recursos** y **autoservicio a la demanda**. El **componente funcional** abstracción y control de recursos puede incluir elementos de software como hipervisores, máquinas virtuales, almacenamiento de datos virtuales y compartición del tiempo.

El **componente funcional** abstracción y control de recursos ofrece una funcionalidad de control que activa capacidades de supervisión y control en el **componente funcional** sistema de soporte operativo (véase la cláusula 9.2.5.3). Por ejemplo, puede haber un algoritmo centralizado para controlar, correlacionar y conectar diversas unidades de procesamiento, almacenamiento e interconexión de redes en los recursos físicos a fin de poder, en conjunto, ofrecer un entorno donde puedan ofrecerse las **categorías de servicios en la nube NaaS, IaaS, PaaS o SaaS**. El controlador puede decidir qué CPU y/o bastidores contienen qué máquinas virtuales que ejecutan una u otra parte de la carga de trabajo de un **servicio en la nube**, cómo esas unidades de procesamiento están conectadas entre sí y en qué momento se reasignan de manera dinámica y transparente partes de la carga de trabajo a nuevas unidades en función de la evolución de las condiciones.

La decisión de si se virtualizan o no los recursos físicos depende de las características de la carga de trabajo. Para muchas cargas de trabajo de **servicios en la nube** (por ejemplo, de **computación como servicio** y de **almacenamiento de datos como servicio**), conviene virtualizar los recursos físicos subyacentes, sobre todo porque la virtualización permite realizar operaciones que esencialmente no pueden llevarse a cabo con una infraestructura física (por ejemplo, que impliquen la gestión de imágenes o la adaptación dinámica de la capacidad de CPU en función de las necesidades). Para otras cargas de trabajo (por ejemplo, análisis y/o búsquedas) se necesita disponer de la máxima capacidad de computación y utilizar cientos o miles de nodos para ejecutar una única carga de trabajo especializada. En esos casos es más conveniente no virtualizar los recursos físicos.

9.2.4.2 Recursos físicos

El **componente funcional** recursos físicos representa los elementos que necesita el **proveedor de servicios en la nube** para ejecutar y gestionar los **servicios en la nube** que ofrece.

Los recursos físicos son, entre otros, las computadoras (CPU y memoria), las redes (encaminadores, cortafuegos, conmutadores, enlaces de red y conectores de red, componentes de almacenamiento (discos duros)) y otros elementos de la infraestructura de computación física. Esos recursos pueden incluir los que residen en los centros de datos en la nube (por ejemplo, servidores de computación, servidores de almacenamiento y redes internas del centro de datos) y los que residen fuera de los centros de datos, que suelen ser recursos de interconexión de redes, como redes entre centros de datos y redes de transporte núcleo.

Todos los elementos de los recursos físicos se gestionan desde el **componente funcional** sistema de soporte operativo, que puede situar instancias de cada **servicio en la nube** en los recursos según sea necesario para satisfacer los requisitos de los clientes. Téngase en cuenta que normalmente el **componente funcional** sistema de soporte operativo se ejecuta en parte de los recursos físicos.

9.2.5 Funciones multicapa

9.2.5.1 Componente funcional integración

El **componente funcional** integración es responsable de conectar los **componentes funcionales** a la arquitectura para crear una arquitectura unificada. El **componente funcional** integración se ocupa del encaminamiento de mensajes y de los mecanismos de intercambio de mensajes dentro de la arquitectura de la nube y sus **componentes funcionales**, así como con **componentes funcionales** externos. El encaminamiento de mensajes puede basarse en diversos criterios, por ejemplo, el contexto o las políticas.

El **componente funcional** integración comprende:

- integración de seguridad;

- integración de supervisión;
- integración de servicio;
- integración de servicios pares.

9.2.5.1.1 Integración de seguridad

El **componente funcional** integración de seguridad supone la integración de las capacidades de seguridad, incluidas la autenticación, la autorización, la encriptación y la verificación de **integridad**, así como de los mecanismos políticos relacionados con las capacidades de seguridad.

9.2.5.1.2 Integración de supervisión

El **componente funcional** integración de supervisión establece la conexión entre los **componentes funcionales** de la capa de acceso, la capa de servicio y la capa de recursos y las capacidades de supervisión e información de los sistemas de soporte operativo.

9.2.5.1.3 Integración de servicio

El **componente funcional** integración de servicio establece la conexión con los servicios que se ejecutan en el entorno del proveedor. El **componente funcional** integración de servicio es un aspecto esencial de la virtualización de los servicios a fin de que, por ejemplo, su ubicación y detalles de implementación estén ocultos para los componentes que dependen de esos servicios.

9.2.5.1.4 Integración de servicios pares

El **componente funcional** integración de servicios pares se utiliza para conectar los servicios de **proveedores de servicios en la nube pares** de manera controlada, con la seguridad conveniente y la contabilidad adecuada a su utilización, vinculada a la identidad del **cliente de servicios en la nube**. El **componente funcional** integración de servicios pares también virtualiza los enlaces a los servicios objetivo a fin de que los detalles de esos servicios puedan cambiar dinámicamente sin consecuencias para los **componentes funcionales** que referencian esos servicios.

9.2.5.2 Componente funcional sistemas de seguridad

El **componente funcional** sistemas de seguridad es responsable de aplicar los controles de seguridad convenientes para mitigar las amenazas a la seguridad en los entornos de **computación en la nube**. El **componente funcional** sistemas de seguridad comprende todas las funcionalidades de seguridad necesarias para el soporte de los **servicios en la nube**.

El **componente funcional** sistemas de seguridad comprende:

- autenticación y gestión de identidades;
- autorización y gestión de políticas de seguridad;
- gestión de encriptación.

9.2.5.2.1 Autenticación y gestión de identidades

El **componente funcional** autenticación y gestión de identidades ofrece capacidades relacionadas con las identidades y credenciales del usuario necesarias para autenticar a los usuarios cuando acceder a los **servicios en línea** y sus capacidades administrativas y comerciales conexas.

La gestión de identidades puede implicar la gestión de identidades federadas a fin de que los usuarios puedan emplear las mismas identidad y credenciales para acceder a múltiples **servicios en línea** gracias a capacidades como "inicio de sesión único".

9.2.5.2.2 Autorización y gestión de políticas de seguridad

El **componente funcional** autorización y gestión de políticas de seguridad ofrece capacidades para el control y aplicación de la autorización de los usuarios para acceder a capacidades o datos específicos. La gestión de políticas de servicio permite la definición y aplicación de políticas de seguridad relativas a los **servicios en la nube**.

9.2.5.2.3 Gestión de encriptación

El **componente funcional** gestión de encriptación ofrece capacidades relacionadas con la encriptación de los datos, ya sean datos estáticos o en movimiento. La gestión de claves de encriptación y la selección del esquema de encriptación son algunas de las capacidades que ofrece.

9.2.5.3 Componente funcional sistemas de soporte operativo

El **componente funcional** sistemas de soporte operativo comprende el conjunto de capacidades de gestión relacionadas con el funcionamiento, necesarias para gestionar y controlar los **servicios en la nube** ofrecidos a los clientes.

El **componente funcional** sistemas de soporte operativo comprende:

- **catálogo de servicios;**
- configuración;
- supervisión e información;
- gestión de políticas de servicio;
- automatización de servicio;
- gestión de nivel de servicio;
- gestión de incidentes y problemas;
- gestión de plataformas y virtualización;
- gestión de servicios pares.

9.2.5.3.1 Catálogo de servicios

El **componente funcional** **catálogo de servicios** ofrece un listado de todos los **servicios en la nube** de un determinado **proveedor de servicios en la nube**. Un **catálogo de servicios** puede contener/referenciar toda la información técnica pertinente necesaria para desplegar, configurar y ejecutar un **servicio en la nube**.

9.2.5.3.2 Configuración

El **componente funcional** configuración ofrece capacidades para la configuración de los servicios, tanto en términos de implementaciones de servicio como de puntos extremos de acceso y de flujo de trabajo necesarios para garantizar que los elementos se configuran en la secuencia correcta.

9.2.5.3.3 Supervisión e información

El **componente funcional** supervisión e información ofrece capacidades para:

- supervisar las **actividades de computación en la nube** de otros **componentes funcionales** a lo largo y ancho del sistema del **proveedor de servicios en la nube**. Esto incluye los **componentes funcionales** implicados en la utilización directa de los **servicios en la nube** por el CSC:usuario de servicios en la nube, como el acceso al servicio y la implementación de servicio (por ejemplo, la invocación del funcionamiento de un **servicio en la nube** por un usuario concreto). Esto incluye también los **componentes funcionales** que participan en el soporte de los **servicios en la nube**, como los **componentes funcionales** del OSS mismo, como el **componente funcional** automatización de servicio (por ejemplo, la configuración de una instancia de servicio para un cliente en concreto);
- presentar informes sobre el comportamiento del sistema del **proveedor de servicios en la nube**, que pueden tomar la forma de alertas cuando el comportamiento se ha de señalar con urgencia (por ejemplo, un fallo o la finalización de una tarea) o presentarse como la agregación de datos históricos (por ejemplo, datos de utilización del servicio);
- almacenar y extraer datos de supervisión y eventos, como los registros cronológicos.

Es necesario garantizar la **disponibilidad, confidencialidad e integridad** de los registros cronológicos que mantiene el **componente funcional** supervisión e información. En el caso de los **servicios en la nube** multidivisión, también es necesario diseñar el acceso a los registros a fin de que cada **arrendatario** concreto sólo pueda acceder a la información que concierne a su división y no a la de las demás divisiones.

9.2.5.3.4 Gestión de políticas de servicio

El **componente funcional** gestión de políticas de servicio ofrece capacidades para definir, almacenar y extraer políticas aplicables a los **servicios en la nube**. Las políticas en cuestión pueden ser las políticas comerciales, técnicas, de seguridad, de privacidad y de certificación aplicables a los **servicios en la nube** y su utilización por los **clientes de servicios en la nube**.

Algunas políticas pueden ser de alcance general y aplicarse a un **servicio en la nube** independientemente del cliente concernido. Otras políticas pueden aplicarse específicamente a un cliente en particular.

9.2.5.3.5 Automatización de servicio

El **componente funcional** automatización de servicio ofrece capacidades para la prestación de servicios, incluidas la gestión y ejecución de plantillas de servicio y la orquestación de servicios. El **componente funcional** automatización de servicio posee las plantillas de servicio que definen las **actividades de computación en la nube** y los flujos de trabajo necesarios para la configuración y entrega de una entrada concreta del **catálogo de servicios**.

La configuración de **servicios en la nube** puede automatizarse para soportar el funcionamiento adaptable de los recursos, incluidas su configuración y tarificación.

Las **actividades** de administración de **servicios en la nube** del **cliente de servicios en la nube** han de poder automatizarse y no necesitar la intervención del **proveedor de servicios en la nube**.

El **componente funcional** automatización de servicio colabora con el **componente funcional** configuración y el **componente funcional** integración de servicio para alcanzar sus objetivos.

9.2.5.3.6 Gestión de nivel de servicio

El **componente funcional** gestión de nivel de servicio ofrece capacidades para gestionar los niveles de servicio de un **servicio en la nube** concreto con el objetivo de garantizar que el **servicio en la nube** cumple los requisitos estipulados en el **SLA** aplicable a ese servicio.

El **componente funcional** gestión de nivel de servicio gestiona la capacidad y la calidad de funcionamiento de un **servicio en la nube**, lo que puede implicar la aplicación de políticas de servicio (por ejemplo, una norma de ubicación cuyo objetivo sea evitar puntos de fallo únicos).

El **componente funcional** gestión de nivel de servicio obtiene información de supervisión del **componente funcional** supervisión e información con el fin de medir y registrar los indicadores fundamentales de rendimiento (IFR) del **servicio en la nube**. De acuerdo con esos IFR se atribuye o retira la capacidad.

El **componente funcional** gestión de nivel de servicio también hace un seguimiento del estado general de los recursos atribuidos y disponibles. Gracias a la comparación entre la capacidad atribuida y los IFR de calidad de funcionamiento del **servicio en la nube** es posible identificar los atascos potenciales o en curso en auxilio de la planificación de la capacidad.

9.2.5.3.7 Gestión de incidentes y problemas

El **componente funcional** gestión de incidentes y problemas ofrece capacidades para la recepción de informes de incidentes o problemas y su gestión hasta la resolución de los mismos.

Tanto los sistemas del **proveedor de servicios en la nube** como los **clientes de servicios en la nube** puede detectar los incidentes y problemas y dar cuenta de ellos.

9.2.5.3.8 Gestión de plataforma y virtualización

El **componente funcional** gestión de plataforma y virtualización ofrece capacidades para la gestión de los recursos subyacentes del **proveedor de servicios en la nube** (computación, almacenamiento, interconexión de redes) y para la virtualización de la utilización de esos recursos (por ejemplo, utilizando hipervisores).

Los recursos suelen organizarse en grupos con características comunes:

- composición y configuración de hardware normalizadas;
- fácil ampliación mediante la adición de nueva capacidad de hardware;
- conmutación automática de recursos en función de la carga de trabajo;
- protección y aislamiento de cargas de trabajo y datos contiguos;
- reducción y/o eliminación de interrupciones mediante el traslado de cargas de trabajo y datos entre recursos;
- gestión del consumo de recursos en función de los objetivos (por ejemplo, calidad de funcionamiento, **disponibilidad**, licencias, consumo energético).

9.2.5.3.9 Gestión de servicios pares

El **componente funcional** gestión de servicios pares ofrece capacidades para conectar los sistemas de soporte operativo y de soporte comercial del proveedor con las capacidades administrativas y comerciales de los **proveedores de servicios en la nube pares** con respecto a los **servicios en la nube pares** utilizados por el proveedor.

ISO/IEC 17789:2014 (E)

El **componente funcional** gestión de servicios pares es responsable de establecer el/los trayecto(s) de comunicación necesarios y de transmitir las identidades y credenciales adecuadas con las solicitudes formuladas a los **proveedores de servicios en la nube pares**.

9.2.5.4 Componente funcional sistemas de soporte comercial

El **componente funcional** sistemas de soporte comercial comprende las capacidades de gestión comercial relacionadas con los clientes y los procesos de soporte.

El **componente funcional** sistemas de soporte comercial incluye:

- **catálogo de productos;**
- gestión de cuentas;
- gestión de abonos;
- facturación;
- contabilidad.

9.2.5.4.1 Catálogo de productos

El **componente funcional catálogo de productos** ofrece a los **clientes de servicios en la nube** capacidades para navegar por una lista de ofertas de servicio disponibles para su adquisición, y al personal del **proveedor de servicios en la nube** una serie de capacidades para gestionar el contenido del catálogo.

El **catálogo de productos** contiene información técnica sobre cada una de las ofertas de servicio (capacidades ofrecidas por el servicio, definiciones de las interfaces del servicio, incluidas las operaciones disponibles, información de seguridad), además de información comercial conexas, como el precio o la valoración.

9.2.5.4.2 Gestión de cuentas

El **componente funcional** gestión de cuentas ofrece capacidades para gestionar la relación con el **cliente de servicios en la nube**, incluido lo siguiente:

- gestión de contratos;
- abonos a **servicios en la nube;**
- derechos;
- precios, incluidas condiciones aplicables a clientes específicos, como los descuentos;
- políticas aplicables al tratamiento de los **datos de cliente de servicios en la nube**.

El **componente funcional** gestión de cuentas y su(s) base(s) de datos conexas(s) están sujetas a requisitos muy estrictos de **disponibilidad** y seguridad, dada la importancia y sensibilidad de los datos de las cuentas de cliente.

9.2.5.4.3 Gestión de abonos

El **componente funcional** gestión de abonos se ocupa de los abonos de los **clientes de servicios en la nube** a **servicios en la nube** concretos con el objetivo de registrar toda novedad o modificación de la información de abono del cliente y garantizar la prestación de los servicios a que está abonado el cliente.

9.2.5.4.4 Facturación

El **componente funcional** facturación ofrece capacidades para:

- medir y valorar la utilización de **servicios en la nube** por los **clientes en la nube**. Por medir se entiende la medición del consumo de **servicios en la nube** por cada uno de los **clientes de servicios en la nube**, mientras que valorar consiste en la aplicación de tarifas a los resultados de las mediciones. La forma de medir los datos dependerá de la naturaleza del **servicio en la nube** y las tarifas pueden prever condiciones aplicables específicamente al cliente (por ejemplo, descuentos) y exigen la aplicación de un algoritmo a los datos medidos;
- generar facturas a partir del resultado de la medición de la utilización de los **servicios en la nube** y de la correspondiente valoración, y enviar las facturas a los **clientes de servicios en la nube**. Los datos de las facturas también interesan al **componente funcional** contabilidad y el **componente funcional** gestión de cuentas.

9.2.5.4.5 Contabilidad

El **componente funcional** contabilidad comprende las capacidades relacionadas con el libro mayor y las funciones de contabilidad general, incluidas las cuentas acreedoras y deudoras. Téngase en cuenta que el **componente funcional**

contabilidad atañe a la contabilidad de la organización del **proveedor de servicios en la nube** y no comprende el mantenimiento de las cuentas de clientes individuales (de las que se ocupa el **componente funcional** gestión de cuentas).

9.2.5.5 Componente funcional soporte de desarrollo

El **componente funcional** soporte de desarrollo soporta las **actividades de computación en la nube** del creador de servicios en la nube, lo que incluye el soporte de la creación y/o composición de implementaciones de servicio, la gestión de la construcción y la gestión de las pruebas.

El **componente funcional** soporte de desarrollo comprende:

- entorno de creación;
- gestión de construcción;
- gestión de pruebas.

9.2.5.5.1 Entorno de creación

El **componente funcional** entorno de creación ofrece capacidades para soportar la creación del software de implementación de servicio. Se soporta la creación de componentes de software y se ofrecen herramientas que ayudan a componer un servicio a partir de una serie de servicios.

El **componente funcional** entorno de creación soporta la utilización de las capacidades ofrecidas por el entorno del **proveedor de servicios en la nube**, incluidas las conexiones a los recursos y la red, la integración con otros servicios (incluidos servicios de **proveedores de servicios en la nube pares**), la integración con capacidades de supervisión y gestión, y la integración con capacidades de seguridad.

El **componente funcional** entorno de creación también soporta la creación de metadatos de configuración relacionados con el servicio que se crea, además de la creación de guiones y demás artefactos utilizados por los sistemas de soporte operativo del proveedor para ofrecer y configurar el servicio.

9.2.5.5.2 Gestión de construcción

El **componente funcional** gestión de construcción soporta la construcción de un paquete de software listo para el despliegue, que puede transmitirse al **proveedor de servicios en la nube** para su despliegue en el entorno de **servicios en la nube**. El paquete de software contiene tanto el software de implementación de servicio como los metadatos y guiones de configuración.

9.2.5.5.3 Gestión de pruebas

El **componente funcional** gestión de pruebas soporta la ejecución de pruebas en las implementaciones de servicio. El **componente funcional** gestión de pruebas genera informes de las pruebas realizadas, que pueden comunicarse a los **proveedores de servicios en la nube** junto con las implementaciones de servicio.

Las pruebas suelen realizarse en un entorno de pruebas especial, que se aproxima lo más posible al entorno de producción sin interferir con él. En el caso de la **computación en la nube**, suele ser el **proveedor de servicios en la nube** el que pone a disposición el entorno de pruebas.

10 Relación entre la perspectiva de usuario y la perspectiva funcional

10.1 Generalidades

Además de especificar la perspectiva de las **funciones** y **actividades de computación en la nube** en la cláusula 8 y la perspectiva funcional, incluidos los **componentes funcionales** de la arquitectura, en la cláusula 9, en esta Recomendación | Norma Internacional se describen a continuación las relaciones lógicas entre las **funciones** y **actividades de computación en la nube** y los **componentes funcionales**.

Algunas de estas relaciones pueden estar normalizadas. Las normas aplicables a una relación pueden emplearse para i) especificar grados del flujo de información u otros tipos de **interoperabilidad**, y/o ii) garantizar grados especificados de calidad (por ejemplo, nivel de seguridad o de servicio).

Las relaciones lógicas definidas en esta arquitectura son importantes para especificar la CCRA y su comportamiento. La relación describe asuntos como los flujos de información requerida entre los **componentes funcionales** de la CCRA.

10.2 Visión general

En la Figura 10-1 se ilustran los principales elementos de la CCRA: **funciones, actividades de computación en la nube y componentes funcionales** en una configuración común.

En la Figura 10-1 se utilizan los convenios gráficos de la cláusula 5. Los cuadros con bordes continuos y esquinas redondeadas representan las **funciones**, los hexágonos denotan las **subfunciones**, los cuadros con borde discontinuo y esquinas redondeadas son las **actividades de computación en la nube** y los recuadros son los **componentes funcionales**. Los cuadros en forma de "L" dentro del **componente funcional** capacidades de servicio representan las interfaces de **servicios en la nube** basadas en los **tipos de capacidades en la nube** fundamentales. De la Figura 10-1 se deduce claramente que las **funciones** son grupos de **actividades de computación en la nube** que a su vez implementan o materializan los **componentes funcionales**.

La proximidad entre los elementos gráficos que representan las **funciones** es significativa e indica una estrecha interacción entre las **funciones** vecinas. Por ejemplo, la **función proveedor de servicios en la nube** está en el centro del diagrama para enfatizar que interactúa con todas las demás **funciones**. Lo mismo se aplica al posicionamiento de las **actividades de computación en la nube** dentro de una determinada **función**, así como al posicionamiento relativo de los **componentes funcionales** dentro de una misma **actividad**. Por ejemplo, el **componente funcional** capacidades de servicio se sitúa encima del **componente funcional** abstracción y control de recursos para indicar la dependencia del primero con respecto al segundo.

Los aspectos transversales, a saber, auditabilidad, **disponibilidad**, gobernanza, **interoperabilidad**, mantenimiento y gestión de versiones, calidad de funcionamiento, portabilidad, protección de la **información de identificación personal**, reglamentación, resiliencia, **reversibilidad**, seguridad, niveles de servicio y **acuerdo de nivel de servicio** figuran en el cuadro exterior de la Figura 10-1 para indicar que los aspectos transversales se aplican a todos los demás elementos de la Figura 10-1: **funciones, actividades y componentes funcionales**. Por ejemplo, el CSC:usuario de servicio en la nube debe tener una identidad, además de unas credenciales, que deben transmitirse al **componente funcional** función usuario a la hora de realizar la **actividad servicio en la nube**. La identidad y las credenciales se presentan al **componente funcional** control de acceso y la autenticación y autorización se realizan como parte de la **actividad** prestar servicios, invocando las capacidades correspondientes del **componente funcional** seguridad antes de facilitar el **servicio en la nube** al CSC:usuario de servicios en la nube.

El **componente funcional** capacidades de servicio de la Figura 10-1 representa la implementación del **servicio en la nube** mismo.

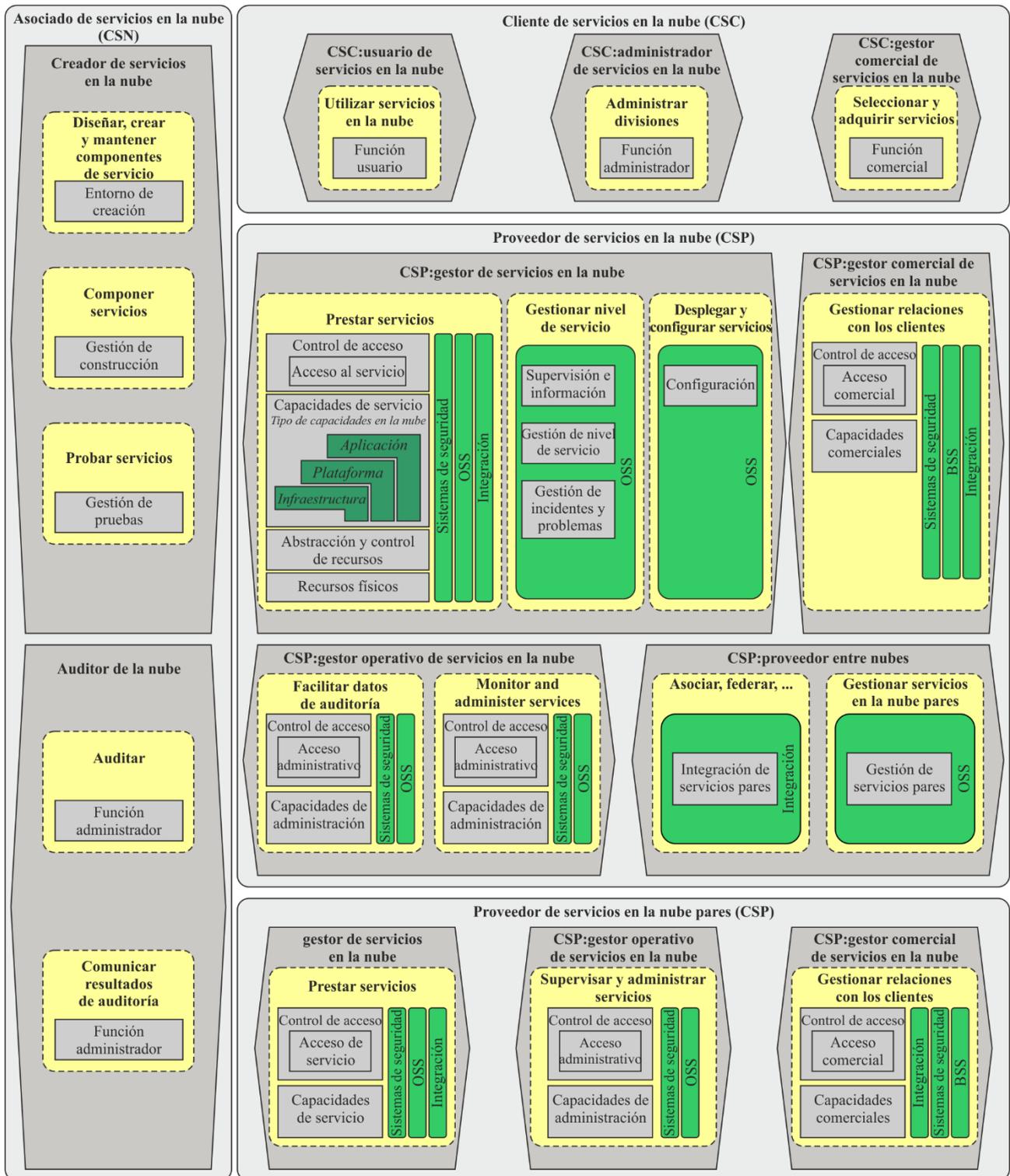
10.2.1 Componente funcional capacidades de servicio

El **servicio en la nube** se ofrece a través de una interfaz de servicio y puede facilitar uno o más **tipos de capacidades en la nube**, representados por los recuadros en forma de "L" invertida situados dentro del **componente funcional** capacidades de servicio. La L superior representa el **tipo capacidades de aplicación**, la "L" del medio son el tipo capacidades de plataforma y la última "L" representan el tipo capacidades de infraestructura.

Lo que implican las "L" es que es posible utilizar un **tipo capacidades de aplicación** utilizando o no el tipo capacidades de plataforma (al escoger el **proveedor de servicios en la nube**) y que el tipo capacidades de plataforma puede implementarse utilizando o no el tipo capacidades de infraestructura.

En el caso de las **categorías de servicios en la nube SaaS o CaaS**, el **componente funcional** capacidades de servicio contiene el software de aplicación específico o las aplicaciones de comunicación que se despliegan en la capa de recursos de manera que se alcancen los niveles de servicio identificados en el **SLA**.

Para las demás **categorías de servicios en la nube**, véase la visión general y el vocabulario de la computación en la nube en la Recomendación UIT-T Y.3500 | ISO/CEI 17788.



Y.3502(14)_F10-1

Auditabilidad, disponibilidad, gobernanza, interoperabilidad, mantenimiento y gestión de versiones, calidad de funcionamiento, portabilidad, protección de información de identificación personal, reglamentación, resiliencia, reversibilidad, seguridad, niveles de servicio y acuerdo de nivel de servicio

Figura 10-1 – Visión general de las funciones, actividades de computación en la nube y componentes funcionales

10.2.2 Funciones, actividades y componentes funcionales comunes

En la Figura 10-1, el **proveedor de servicios en la nube** tiene una **subfunción**, CSP:gestor de servicios en la nube, que realiza la **actividad** prestar servicios, que consiste en la prestación del servicio al CSC:usuario de servicios en la nube del **cliente de servicios en la nube** para su utilización efectiva. Sin embargo, antes de poder utilizar el servicio, es necesario crear y desplegar el **servicio en la nube**.

En ello participan dos **subfunciones** del **asociado de servicios en la nube**, el creador de servicios en la nube y el **auditor de la nube**. El creador de servicios en la nube desarrolla la implementación de los **servicios en la nube** empleando el **componente funcional** herramientas de creación y prueba el servicio gracias al **componente funcional** gestión de pruebas. El **servicio en la nube** se une en un paquete con la información de despliegue y se entrega al CSP:gestor de servicios en la nube para que éste proceda a la **actividad** despliegue y prestación de servicios, cuyo resultado será la oferta del **componente funcional** capacidades de servicio en la **actividad** prestar servicios. El **auditor de la nube**, mientras tanto, realiza las **actividades** auditar y comunicar resultados de auditoría en el creador de servicios en la nube, el **proveedor de servicios en la nube** o el **cliente de servicios en la nube**, en función de las políticas y regímenes de gobernanza de cada uno de ellos.

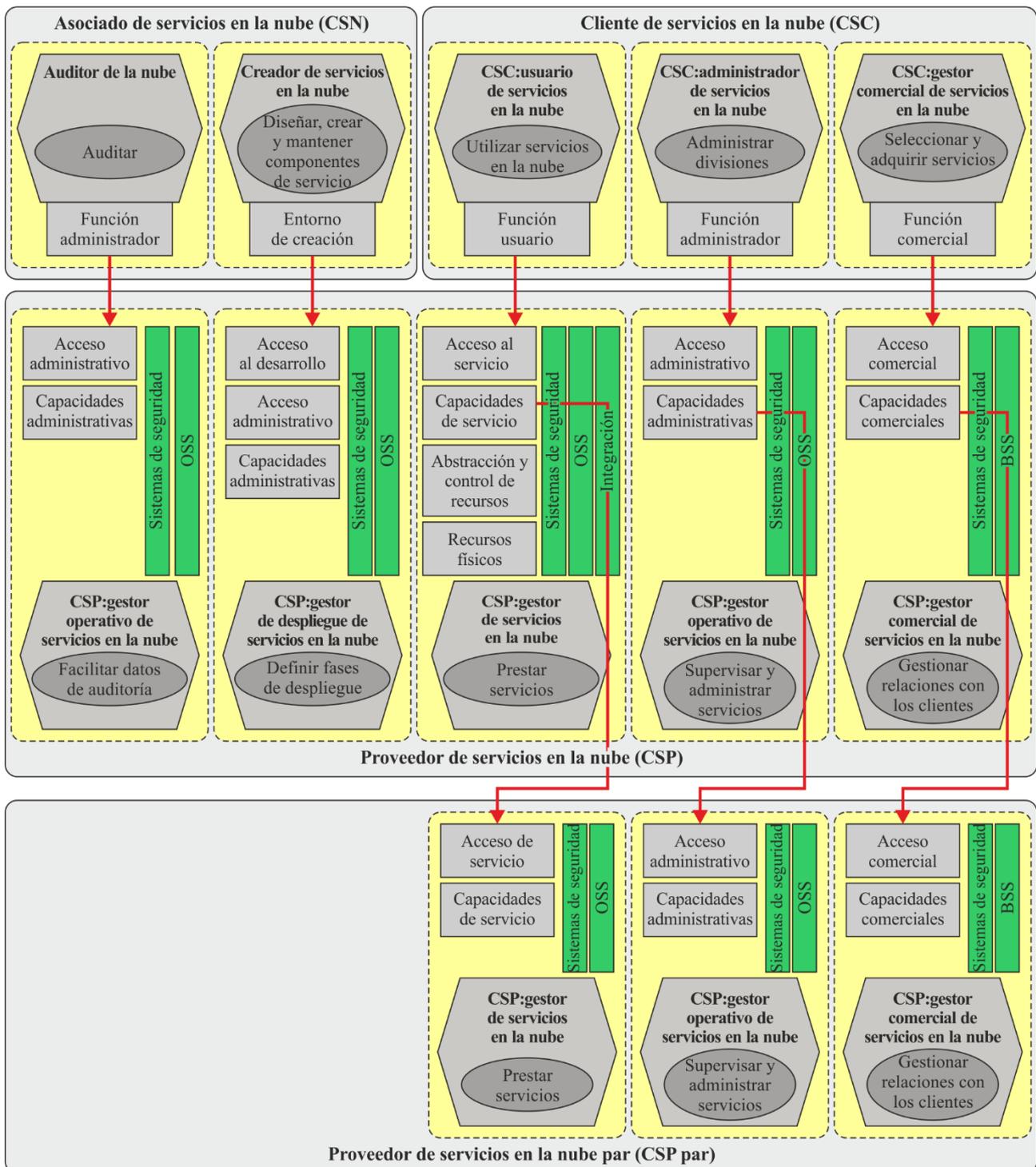
Una vez que el CSP:gestor de servicios en la nube realiza la **actividad** desplegar y prestar servicios, la **actividad** prestar servicios utiliza el **componente funcional** capacidades de servicio, que es la implementación del servicio y que, a su vez, utiliza los **componentes funcionales** de la capa de recursos para que los recursos de computación, almacenamiento y red necesarios ejecuten el servicio. La **actividad** prestar servicios también implica la integración del **componente funcional** capacidades de servicio con el **componente funcional** sistemas de seguridad a fin de ofrecer las capacidades de seguridad y protección de la **información de identificación personal**, como la encriptación de datos. El **componente funcional** sistemas de soporte operativo soporta la gestión, supervisión, automatización y configuración de los servicios y recursos. Además, el CSP:gestor de servicios en la nube realiza la **actividad** gestión de nivel de servicio. La **actividad** gestión de nivel de servicio gestiona la **disponibilidad** y calidad de funcionamiento del **servicio en la nube** a fin de que se ajuste a los objetivos definidos en el **SLA** aplicable al **servicio en la nube**. El **componente funcional** gestión de nivel de servicio, el **componente funcional** supervisión e información y el **componente funcional** gestión de incidentes y problemas se emplean para realizar esa tarea.

En ocasiones el CSP:gestor de servicios en la nube ofrece el servicio en colaboración con otro CSP:gestor de servicios en la nube invocando los **servicios en la nube** de un **proveedor de servicios en la nube par**. A continuación, el CSP:gestor de servicios en la nube realiza la **actividad** gestionar **servicios en la nube pares** para definir los contratos y **SLA** necesarios para utilizar los **servicios en la nube pares**. El **proveedor de servicios en la nube par** también realiza **actividades de computación en la nube** de carácter administrativo y operativo: las **actividades** prestar servicio y gestionar nivel de servicio, como cualquier otro **proveedor de servicios en la nube**.

Este es el conjunto común de **actividades de computación en la nube** del CSP:gestor de servicios en la nube, pero hay otras **actividades de computación en la nube** que pueden realizarse y que se documentan en esta especificación.

Una vez disponible para su uso el **servicio en la nube**, dos **subfunciones** del **cliente de servicios en la nube** realizan varias actividades. En primer lugar, el CSC:administrador de servicios en la nube se ocupa de administrar la **actividad** divisiones gracias al **componente funcional** función administrador a fin de crear una división y conceder derechos de acceso al CSC:usuario de servicios en la nube. Una vez hecho esto, el CSC:usuario de servicios en la nube realiza la **actividad** utilizar servicio en la nube mediante el **componente funcional** función usuario para interactuar con el **servicio en la nube**. Mientras tanto, el CSC:administrador de servicios en la nube suele supervisar el servicio para asegurarse de que se ejecuta correctamente y cumple los términos del **SLA** nuevamente utilizando el **componente funcional** función administrador.

En la Figura 10-2 se muestran las relaciones entre las **funciones, actividades de computación en la nube** y **componentes funcionales** y las **actividades de computación en la nube** de las diversas **funciones**. En el Anexo A se describe cada una de estas relaciones.



Y.3502(14)_F10-2

Figura 10-2 – Ejemplos de relaciones e interacciones entre actividades y componentes funcionales

10.2.3 Multidivisión y aislamiento

La **computación en la nube** implica la compartición de algunos recursos, lo que supone que normalmente esos recursos se comparten con otros clientes de los **servicios en la nube** en cuestión. Los términos **división** y **multidivisión** se utilizan para describir la compartición de los recursos.

Un **arrendatario** de un **servicio en la nube** no es exactamente lo mismo que un **cliente de servicios en la nube** – un **arrendatario** es un grupo de CSC:usuario de servicios en la nube que comparten el acceso a una serie de recursos físicos y virtuales. Normalmente el grupo de CSC:usuario de servicios en la nube estará asociado a un **cliente de servicios en la nube** concreto, pero un **cliente de servicios en la nube** muy bien puede tener múltiples **arrendatarios**, es decir, grupos de usuarios de distintos departamentos de la organización cliente, por ejemplo.

ISO/IEC 17789:2014 (E)

Multidivisión es la atribución de recursos físicos o virtuales de manera que cada **arrendatario**, y sus cálculos y datos, está aislado e inaccesible con respecto a los demás **arrendatarios**. Dicho de otro modo, los usuarios que pertenecen a una división desconocerán por completo la presencia de usuarios de otra división.

La **multidivisión** no sólo afecta a los **servicios en la nube** mismos, sino también a las capacidades comerciales y administrativas que el **proveedor de servicios en la nube** ofrece a los **clientes de servicios en la nube**. Toda la información sobre las cuentas de usuario, los abonos, la utilización y la facturación debe mantenerse aislada y ser visible sólo para los clientes que poseen las divisiones correspondientes. Se ha de tener mucho cuidado con recursos tales como archivos cronológicos, que pueden contener registros de múltiples **arrendatarios**. Si un cliente determinado necesita acceder a los registros cronológicos, por ejemplo en caso de incidente, esos registros deberán filtrarse para que el cliente sólo pueda ver los que se refieren a sus divisiones.

Anexo A

Pormenores de la perspectiva de usuario y la perspectiva funcional

(Este anexo de la presente Recomendación | Norma Internacional es de carácter informativo.)

En este anexo se presentan más detalles acerca de la relación entre la perspectiva de usuario y la perspectiva funcional.

A.1 Relación entre el cliente de servicios en la nube y el proveedor de servicios en la nube

En la relación **cliente de servicios en la nube-proveedor de servicios en la nube** hay tres elementos esenciales:

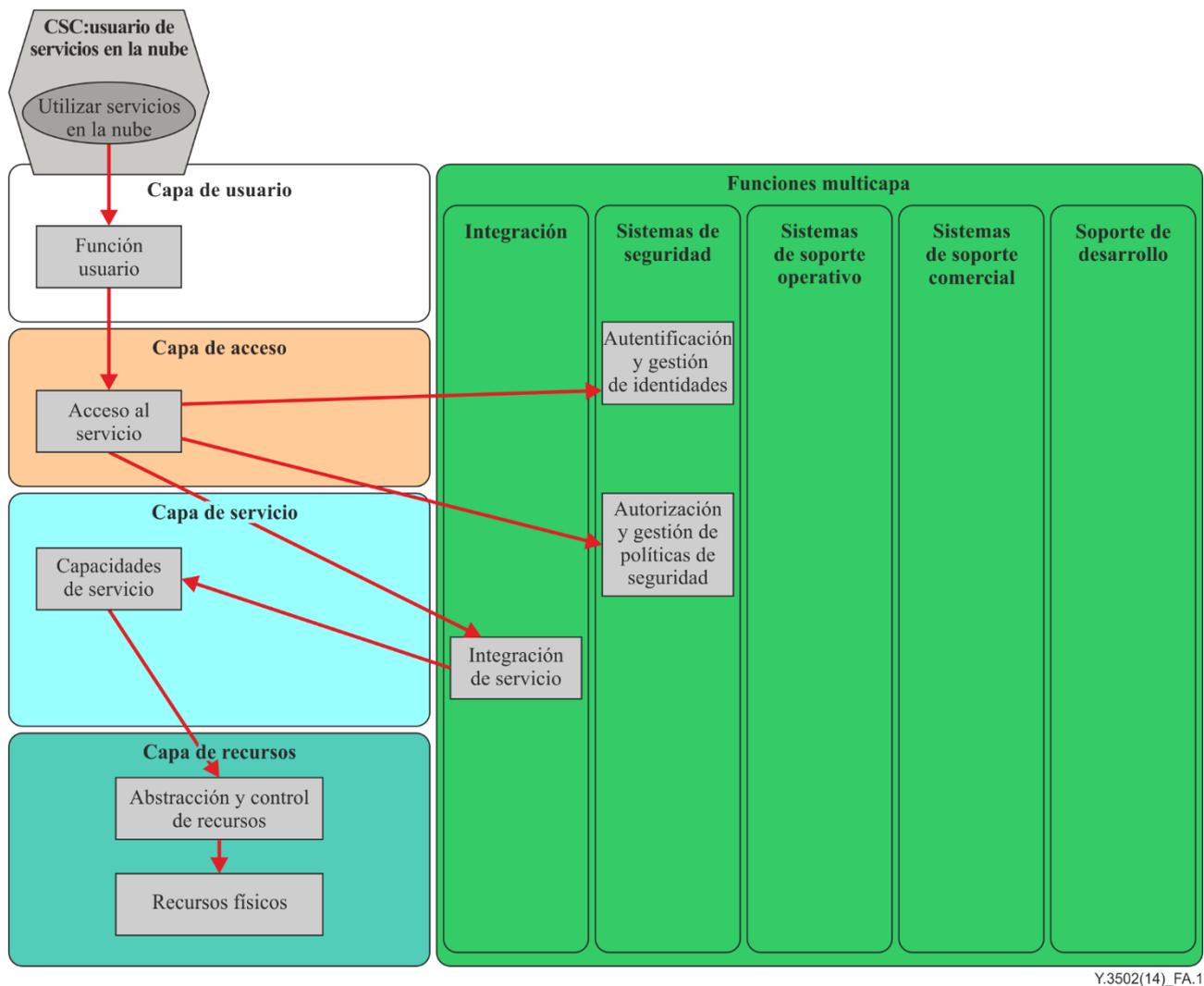
- 1) el CSC:usuario de servicios en la nube que utiliza los **servicios en la nube** del proveedor para lograr sus objetivos comerciales;
- 2) el CSC:gestor comercial que utiliza las capacidades comerciales del **proveedor de servicios en la nube** para abonarse a **servicios en la nube** y gestionar su utilización desde un punto de vista comercial;
- 3) el CSC:administrador de servicios en la nube que utiliza las capacidades administrativas del **proveedor de servicios en la nube** para administrar la utilización de los **servicios en la nube** desde el punto de vista del **cliente de servicios en la nube**.

A.1.1 Relación funcional

Los **servicios en la nube** se ponen a disposición del CSC:usuario de servicios en la nube a través de un punto extremo y una interfaz facilitada por el **componente funcional** acceso al servicio. Las funciones de esta interfaz y los flujos de información asociados son propios de cada **servicio en la nube** por lo que no se contemplan en la arquitectura de referencia. Sin embargo, algunos aspectos de carácter amplio que deben reflejarse en la interfaz de servicio, sobre todo la necesidad de identificar y autenticar al CSC:usuario de servicios en la nube.

El CSC:usuario de servicios en la nube realiza la **actividad** utilizar servicios en la nube a través del **componente funcional** función usuario, que invoca el **servicio en la nube** mediante el **componente funcional** acceso al servicio. El **componente funcional** acceso al servicio procede a la autenticación del CSC:usuario de servicios en la nube y otorga las autorizaciones para utilizar determinadas capacidades del **servicio en la nube**. De obtenerse la autorización, el **componente funcional** acceso al servicio invoca la implementación del **servicio en la nube**, que responde a la solicitud formulada.

En la Figura A.1 se ilustran las relaciones entre **componentes funcionales** implicados en la **actividad** utilizar **servicios en la nube** del CSC:usuario de servicios en la nube.



Y.3502(14)_FA.1

Figura A.1 – Relaciones del CSC:usuario de servicios en la nube para la actividad "utilizar servicios en la nube"

A.1.2 Relación comercial

El CSC:gestor comercial de servicios en la nube realiza las **actividades de computación en la nube** seleccionar y adquirir servicios, administración comercial y solicitar informe de auditoría a través del **componente funcional** función comercial de la capa de usuario. El **componente funcional** función comercial invoca las capacidades comerciales del **proveedor de servicios en la nube** a través de un punto extremo y una interfaz facilitada por el **componente funcional** acceso comercial.

El **componente funcional** acceso comercial procede a la autenticación del CSP:gestor comercial de servicios en la nube y otorga la autorización necesaria para utilizar determinadas funciones de las capacidades comerciales. El **componente funcional** capacidades comerciales interactúa con el **componente funcional** sistemas de soporte comercial para responder a las solicitudes formuladas por el CSC:gestor comercial de servicios en la nube, incluidos los **componentes funcionales catálogo de productos**, gestión de cuentas y gestión de abonos.

La información relacionada con las capacidades comerciales suele ser la siguiente:

- entradas de **servicios en la nube** disponibles del **catálogo de productos**, junto con su información técnica, precio, términos y condiciones;
- información sobre abonos relativa a los servicios a que está abonado el cliente, junto con la información cuantitativa correspondiente, si procede (por ejemplo, número de usuarios, volumen de datos, cantidad de procesamiento, etc.);
- información de facturación, que puede incluir información sobre las tarifas, los pagos y el estado de las cuentas.

En la Figura A.2 se ilustran las relaciones entre los **componentes funcionales** implicados en la **actividad** seleccionar y adquirir servicios del CSC:gestor comercial de servicios en la nube.

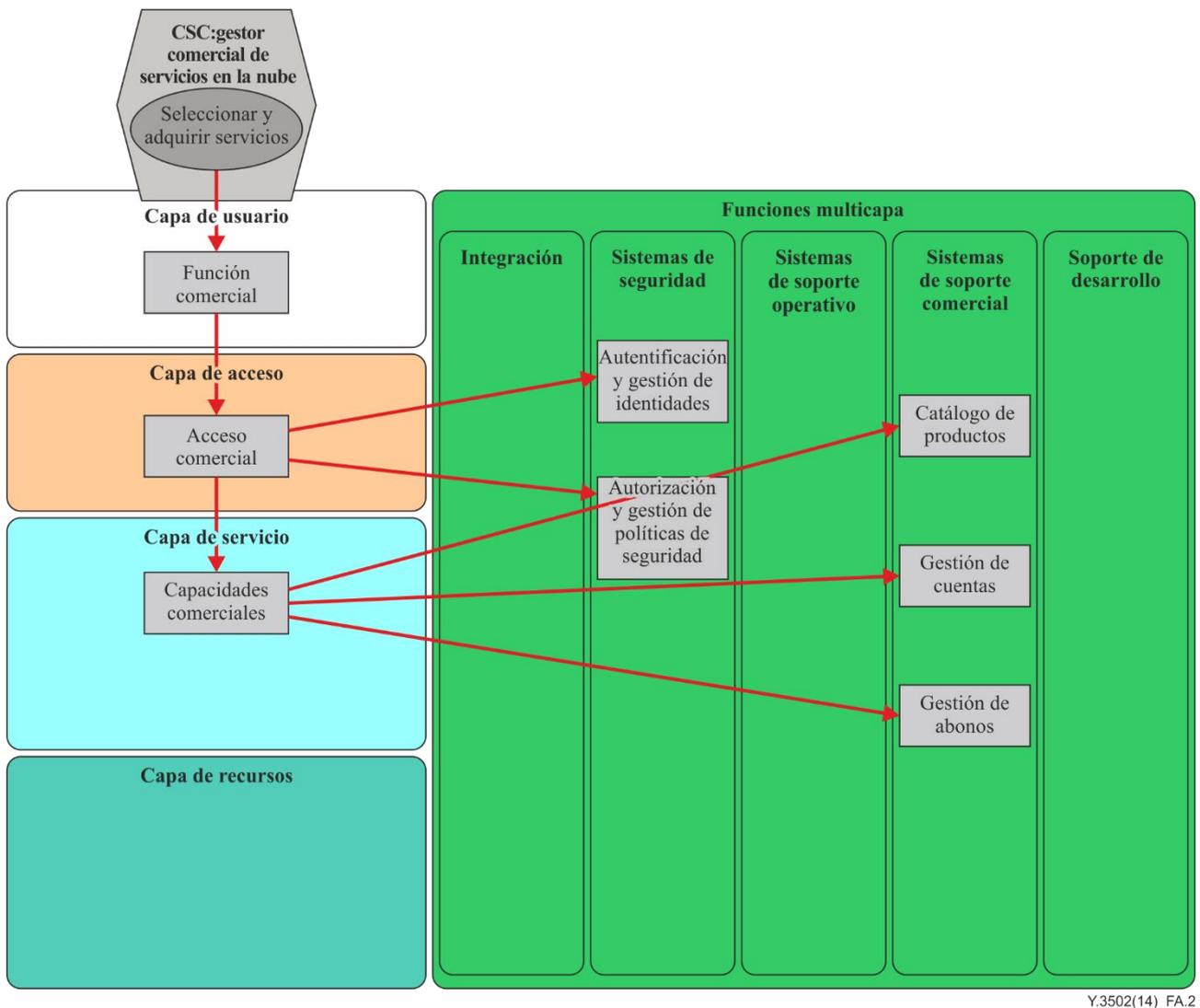


Figura A.2 – Relaciones del CSC:gestor comercial de servicios en la nube para la actividad "seleccionar y adquirir servicios"

A.1.3 Relación administrativa

El CSC:administrador de servicios en la nube realiza las siguientes **actividades de computación en la nube** a través del **componente funcional** función administrador:

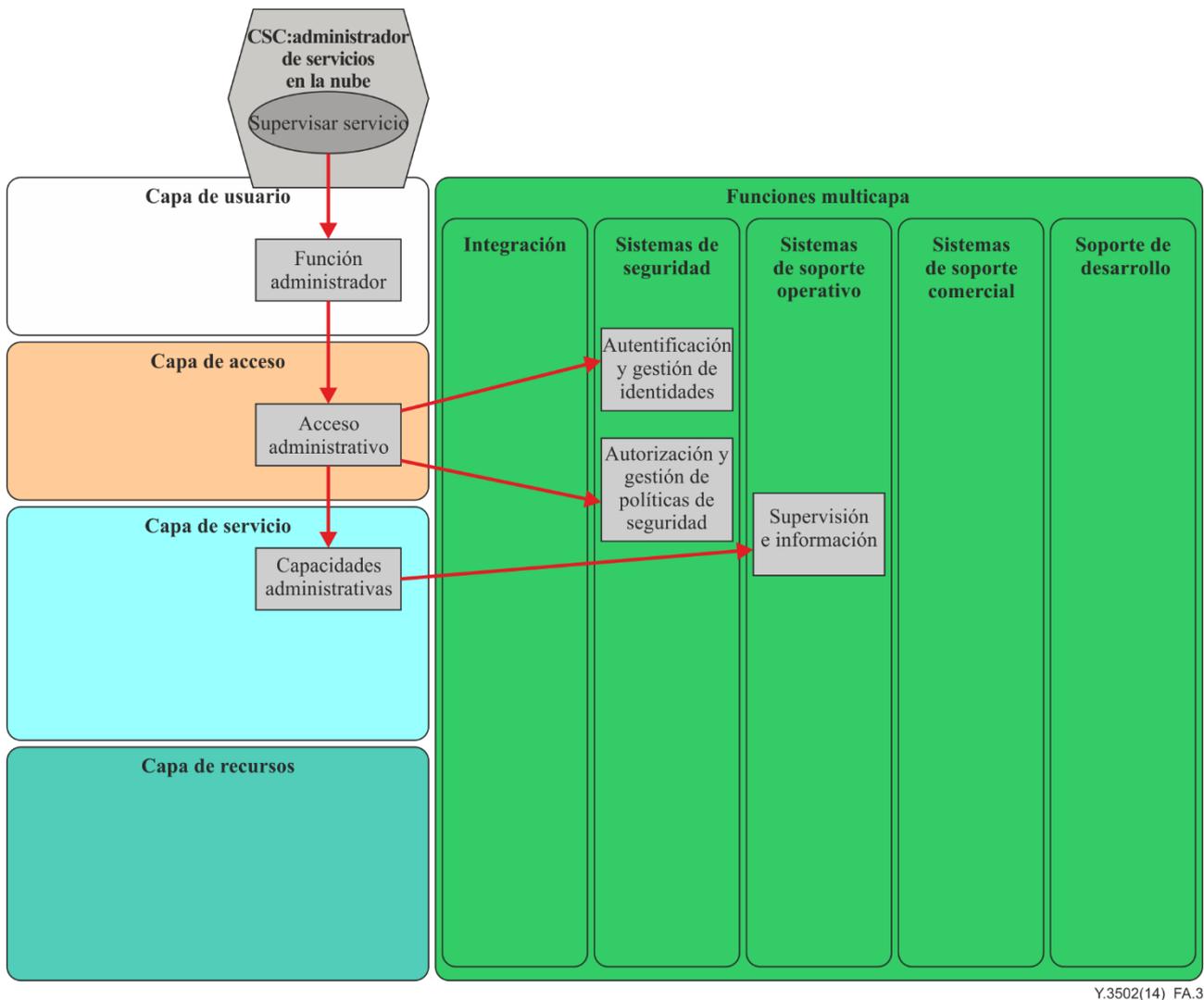
- supervisar servicio;
- facturación y comunicación de informes de utilización;
- administrar divisiones;
- administrar seguridad de servicio;
- tramitar informes de problemas. El **componente funcional** función administrador invoca el **componente funcional** capacidades administrativas del **proveedor de servicios en la nube** a través de un punto extremo y una interfaz facilitada por el **componente funcional** acceso administrativo.

El **componente funcional** acceso administrativo procede a la autenticación del CSC:administrador de servicios en la nube y otorga la autorización necesaria para utilizar funciones concretas del **componente funcional** capacidades administrativas. El **componente funcional** capacidades administrativas interactúa con los **componentes funcionales** sistemas de soporte operativo para responder a las solicitudes formuladas por el CSC:administrador de servicios en la nube, por ejemplo, el **componente funcional** supervisión e información.

La información relacionada con las capacidades administrativas comprende:

- información de seguridad, como la creación de cuentas de usuario y datos de autorización, la encriptación de datos;
- notificaciones relativas a la utilización de los servicios, incluidas las estadísticas de utilización, los registros cronológicos (por ejemplo, con fines de seguridad);
- informes/eventos de excepción (por ejemplo, cuando se incumple un objetivo del **SLA** de un servicio o hay un incidente de seguridad).

En la Figura A.3 se ilustran las relaciones entre los **componentes funcionales** implicados en la **actividad** supervisar servicio del CSC:administrador de servicios en la nube.



Y.3502(14)_FA.3

Figura A.3 – Relaciones del CSC:administrador de servicios en la nube para la actividad "supervisar servicio"

Otros elementos pertinentes en la relación **cliente de servicios en la nube-proveedor de servicios en la nube** pueden ser los acuerdos entre el cliente y el proveedor, incluido el **SLA**, las cuestiones de propiedad intelectual y otros asuntos reglamentados, como la adecuada protección de los datos personales.

A.2 Relación entre el proveedor y el proveedor par (o "entre nubes")

Un **proveedor de servicios en la nube** puede utilizar uno o más **servicios en la nube** prestados por otros **proveedores de servicios en la nube**, estableciendo una relación **proveedor de servicios en la nube-proveedor de servicios en la nube par**, o relación "entre nubes", donde el proveedor que utiliza los servicios se denomina **proveedor de servicios en la nube** primario y el proveedor cuyos servicios se utilizan se denomina **proveedor de servicios en la nube** secundario.

Como ocurre en la relación **cliente de servicios en la nube-proveedor de servicios en la nube**, hay dos componentes funcionales que participan en la relación entre dos **proveedores de servicios en la nube**:

- la utilización de los **servicios en la nube** del proveedor secundario por el proveedor primario;
- la utilización de las capacidades comerciales y administrativas del proveedor secundario por el CSP:gestor operativo de servicios en la nube y el CSP:gestor de servicios en la nube del proveedor primario para establecer y controlar la utilización de los **servicios en la nube** del proveedor secundario.

Desde el punto de vista del proveedor secundario, el proveedor primario asume la función de **cliente de servicios en la nube**. los clientes del **proveedor de servicios en la nube** primario utilizan los servicios que ofrece el **proveedor de servicios en la nube** secundario. En el marco de la relación entre el **proveedor de servicios en la nube** secundario y el **cliente de servicios en la nube** del proveedor primario se ha de prestar especial atención a asuntos como la seguridad, la protección de la **IIP** y la propiedad de los datos.

Es fundamental que el proveedor primario se asegure de que el **SLA** aplicable a los servicios del proveedor secundario se ajusta a los requisitos de los servicios del proveedor primario y que todo incumplimiento del **SLA** se gestiona adecuadamente.

Hay tres interfaces implicadas en la relación proveedor-proveedor par: la interfaz administrativa, la interfaz comercial y la(s) interfaz(es) de servicio, que ofrecen en general las mismas capacidades que las interfaces equivalentes en la relación **cliente de servicios en la nube-proveedor de servicios en la nube**. En la Figura A.4 se muestra cómo se utiliza la interfaz administrativa. La utilización de la interfaz de servicio se ilustra en la Figura A.5 y la utilización de la interfaz comercial se muestra en la Figura A.6.

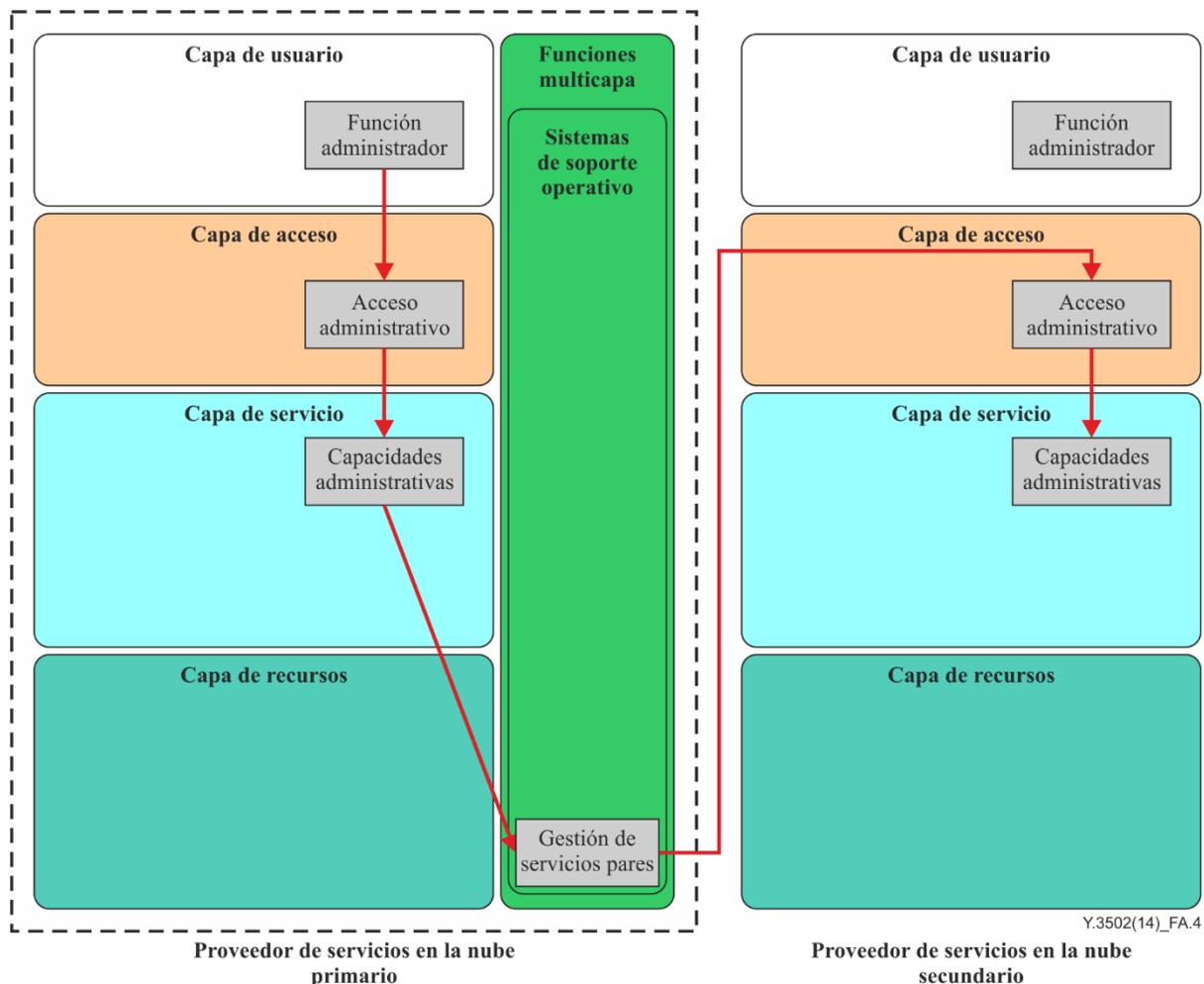


Figura A.4 – Relación proveedor-proveedor par para la actividad administrar

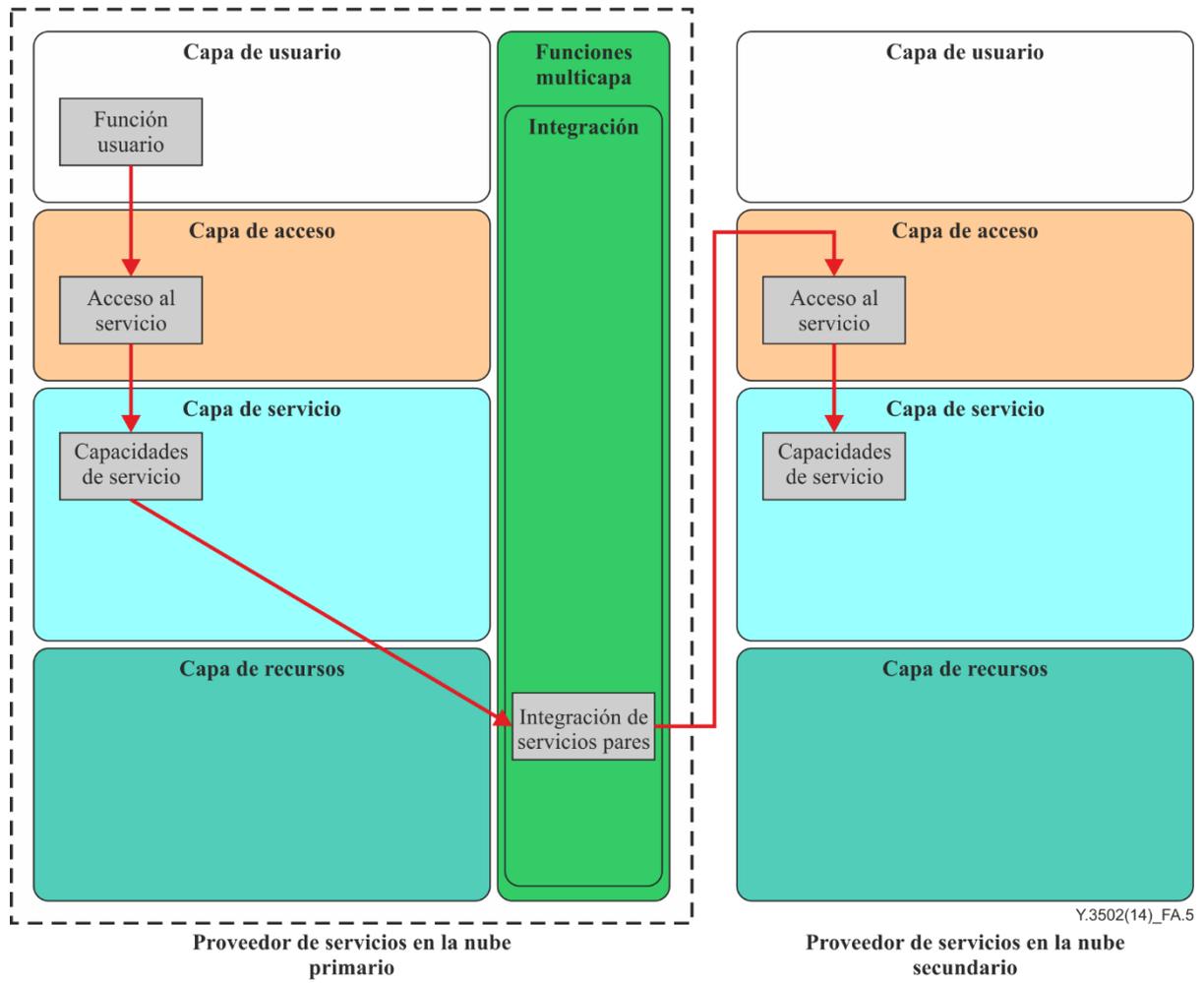


Figura A.5 – Relación proveedor-proveedor par para la actividad utilizar servicio

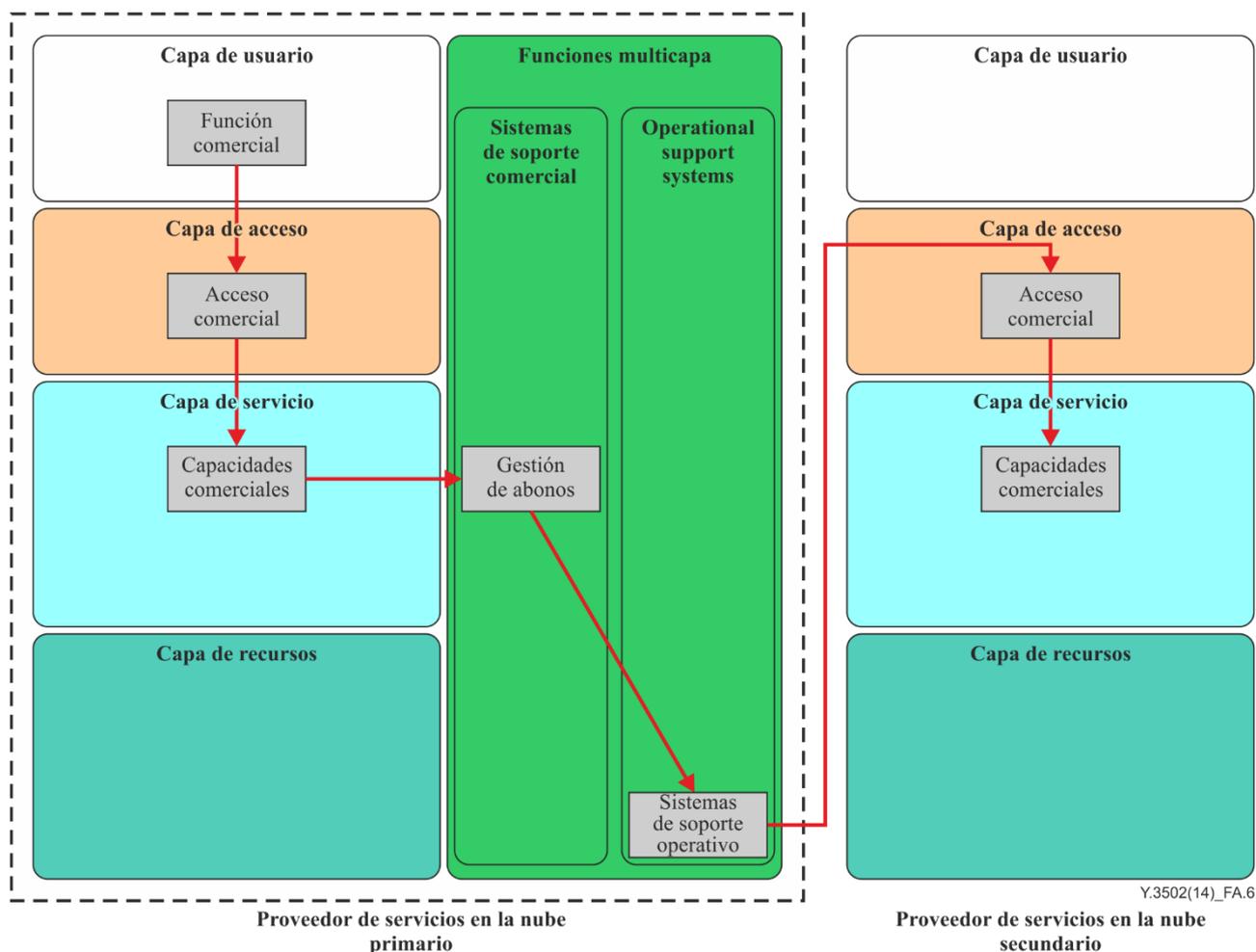


Figura A.6 – Relación proveedor-proveedor par para la interfaz comercial

A.3 Relación entre el creador de servicios en la nube y el proveedor de servicios en la nube

Los creadores de servicios en la nube crean y empaquetan implementaciones de servicio y las entregan a los **proveedores de servicios en la nube** para su despliegue y explotación. Por consiguiente, el creador de servicios en la nube interactúa con el **proveedor de servicios en la nube** para:

- 1) inspeccionar el entorno de ejecución del servicio del **proveedor de servicios en la nube**;
- 2) probar las implementaciones de servicio;
- 3) entregar paquetes de implementaciones de servicio.

El **componente funcional** soporte de desarrollo soporta las **actividades de computación en la nube** del creador de servicios en la nube, incluidas las **actividades de computación en la nube** crear servicio, probar servicio y mantener servicio. Esas **actividades de computación en la nube** dependen de los **componentes funcionales** entorno de creación, gestión de construcción y gestión de pruebas.

Las líneas que salen del componente entorno de creación en la Figura A.7 muestran que el creador de servicios en la nube crea la implementación de un **servicio en la nube** y compone el servicio gracias al **componente funcional** entorno de creación para posteriormente utilizar el sistema de gestión de construcción a fin de construir el servicio y sus artefactos conexos en un paquete desplegable. Las flechas desde/hacia el **componente funcional** gestión de pruebas indica que el sistema de gestión de pruebas efectúa las pruebas correspondientes del paquete construido, obteniéndolo del sistema de gestión de construcción e interactuando con el entorno del proveedor a través del **componente funcional** acceso al desarrollo para desplegar una versión de prueba del servicio y realizar las pruebas.

En la Figura A.7 las líneas que salen del entorno de creación muestran que éste y el sistema de gestión de construcción se utilizan para crear el software y los artefactos correspondientes de la implementación de servicio que ofrece la interfaz de servicio. El creador de servicios en la nube también puede crear la implementación de acceso de servicio.

Para que la implementación de servicio y el acceso de servicio se ejecuten en el entorno de ejecución previsto, es necesario activar adecuadamente la seguridad, la supervisión, la gestión y la automatización, así como la integración en el entorno

de ejecución de servicio. El creador de servicios en la nube descubre la activación adecuada de la integración de supervisión, la integración de seguridad y la integración de servicio empleando las capacidades de acceso al desarrollo. Además, a través del **componente funcional** acceso al desarrollo se extraen la información y los requisitos que permiten la autenticación y la gestión de identidades, así como la autorización y la gestión de políticas de seguridad.

La activación de la implementación del **servicio en la nube** para su despliegue y configuración también se efectúa mediante el entorno de creación y el sistema de gestión de construcción (por ejemplo, con guiones y ficheros de metadatos de configuración). El creador de servicios en la nube utiliza el **componente funcional** acceso al desarrollo para descubrir cuáles son los requisitos de configuración y despliegue.

La implementación de servicio se empaqueta con la información de despliegue y configuración y se transmite al CSP:gestor de servicios en la nube para que éste realice la **actividad** desplegar servicios, tras lo cual el servicio estará disponible para su utilización por los clientes en la **actividad** prestar servicios.

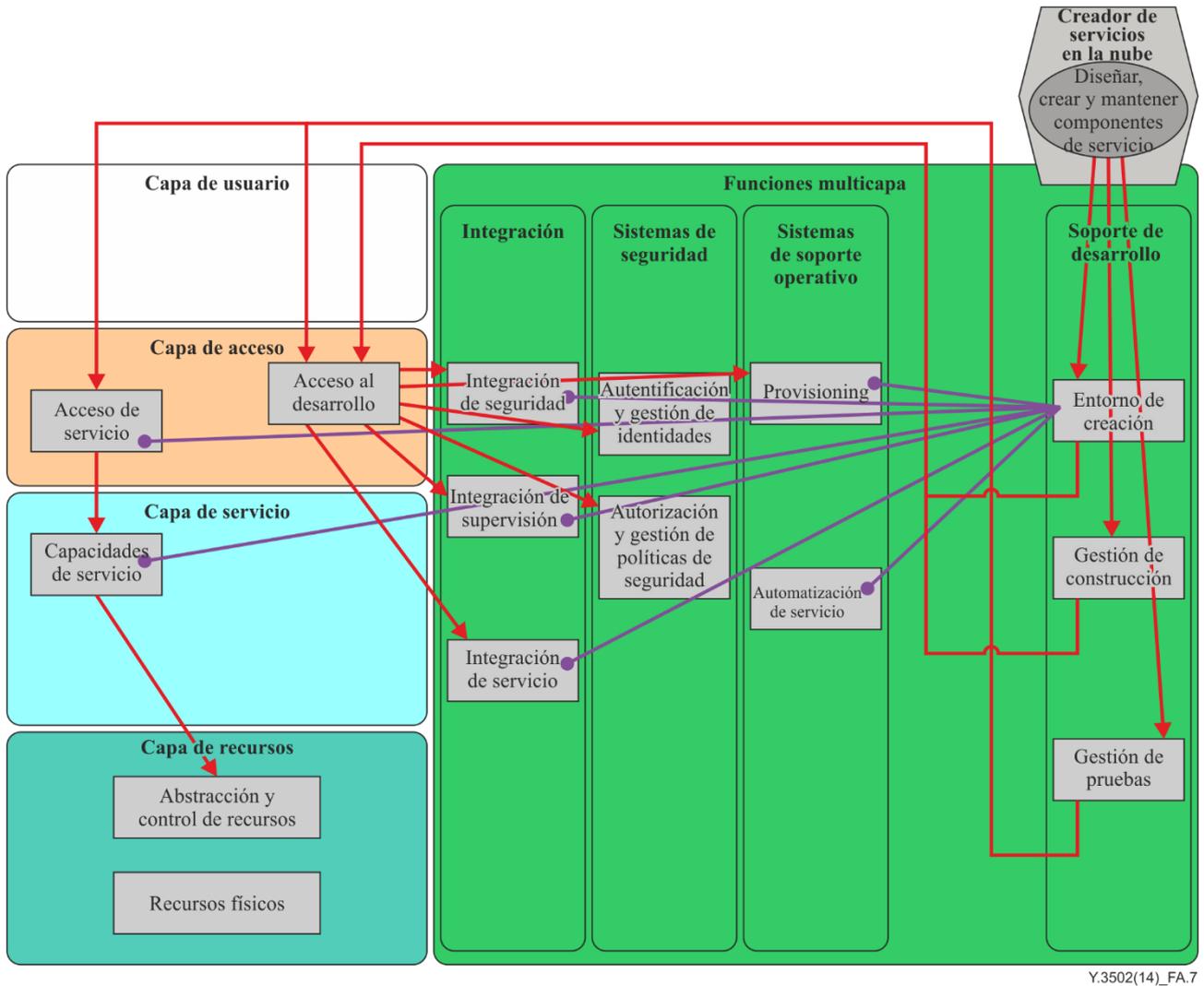


Figura A.7 – Relación creador de servicios en la nube-proveedor de servicios en la nube

A.4 Relación entre el proveedor de servicios en la nube y el auditor

Un **auditor de la nube** debe realizar auditorías de las especificaciones, políticas y acuerdos adoptados.

Las especificaciones de auditoría pueden ser normas fijadas por el **proveedor de servicios en la nube**, el auditor o una entidad independiente, posiblemente de conformidad con la legislación vigente. La norma utilizada dependerá de a quién estén dirigidos los resultados de la auditoría. Si los resultados de la auditoría están destinados a un **cliente de servicios en la nube** que desea obtener una garantía independiente, la auditoría deberá conformarse a las normas fijadas por una entidad independiente.

El proveedor fija las políticas de auditoría de sus infraestructuras y servicios. Esas políticas las define la empresa siguiendo los procesos de gobernanza.

El acuerdo de **servicios en la nube** puede comprender términos relativos a la auditoría del **proveedor de servicios en la nube** y posiblemente también del **cliente de servicios en la nube**. Acuerdos semejantes pueden concluirse entre el **proveedor de servicios en la nube** primario y los **proveedores de servicios en la nube** secundarios. Las responsabilidades del auditor son las mismas en ambos casos.

Las **actividades de computación en la nube** del **auditor de la nube** son la auditoría de seguridad, la auditoría de consecuencias para la privacidad y la auditoría de calidad de funcionamiento. Para todas esas **actividades de computación en la nube** el **auditor de la nube** puede obtener pruebas del **proveedor de servicios en la nube**. La forma que adopten esas pruebas de auditoría dependerá del tipo de auditoría que se realice y de las normas de auditoría que se empleen. Las pruebas pueden ser documentos procesales o registros cronológicos. En cualquier caso, el **proveedor de servicios en la nube** debe disponer de un medio a través del cual el **auditor de la nube** pueda obtener las pruebas necesarias.

En la Figura 10-2, la **actividad** auditar del **auditor de la nube** solicita pruebas de auditoría al **proveedor de servicios en la nube** a través del **componente funcional** acceso administrativo del **proveedor de servicios en la nube**, que invoca las capacidades administrativas necesarias.

A.4.1 Auditoría de seguridad

Existen diversas normas sobre auditoría de la seguridad de los sistemas. Una de ellas es ISO/CEI 27001, que abarca la gestión de la **seguridad de la información**. Hay otras muchas organizaciones que han definido normas sobre auditoría de la seguridad de la nube.

A.4.2 Auditoría de consecuencias para la privacidad

Las diversas autoridades en materia de protección de datos (por ejemplo, el *Privacy Commissioner* de Canadá y el *Information Commissioner* de Reino Unido) publican directrices sobre la evaluación y/o auditoría de las consecuencias para la privacidad de los programas, políticas o sistemas. La **protección de la IIP** suele estar sujeta a reglamentos y/o leyes, pero uno de los problemas que plantean los **servicios en la nube** es que el **cliente de servicios en la nube** puede estar en una jurisdicción distinta de aquella por la que se rige el **proveedor de servicios en la nube**. La situación puede ganar en complejidad si el **proveedor de servicios en la nube** explota múltiples centros de datos en jurisdicciones distintas y traslada los datos o la ejecución de los servicios de uno a otro (por ejemplo, en pro de la continuidad del servicio o para utilizar eficazmente los recursos).

ISO/CEI 27018 es una norma que define los controles de **seguridad de la información** aplicables al **proveedor de servicios en la nube** cuando ejerce de procesador de datos. La ISO/CEI también considera la privacidad en su definición más amplia (véase, por ejemplo, la serie de normas ISO/CEI 29100).

Un **auditor de la nube** debe evaluar la protección de la **información de identificación personal** de un **servicio en la nube**, así como las operaciones del **proveedor de servicios en la nube**, de acuerdo con la reglamentación de protección de datos de la jurisdicción pertinente, siguiendo las directrices publicadas por las autoridades en materia de protección de datos y las normas pertinentes.

A.4.3 Auditoría de calidad de funcionamiento

La auditoría de calidad de funcionamiento evalúa la capacidad del **proveedor de servicios en la nube** para cumplir los objetivos de calidad de funcionamiento especificados para sus **servicios en la nube**, que suelen estipularse en el **SLA**.

Bibliografía

- ISO/CEI 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*
- ISO/CEI 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements.*
- ISO/CEI 27002:2013, *Information technology – Security techniques – Information security management systems – Code of practice for information security management.*
- ISO/CEI 27018:2014, *Information technology – Security techniques – Information security management systems – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.*
- ISO/CEI/IEEE 24765:2010, *Systems and software engineering – Vocabulary.*
- ISO/CEI/IEEE 42010:2011, *Systems and software engineering – Architecture description.*

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación