Unión Internacional de Telecomunicaciones

# UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

# X.1602

(03/2016)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad de la computación en nube – Diseño de la seguridad de la computación en nube

## Requisitos de seguridad para el entorno de aplicación Software como servicio

Recomendación UIT-T X.1602

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

**REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD**

| | |
|---|---|
| REDES PÚBLICAS DE DATOS | X.1–X.199 |
| INTERCONEXIÓN DE SISTEMAS ABIERTOS | X.200–X.299 |
| INTERFUNCIONAMIENTO ENTRE REDES | X.300–X.399 |
| SISTEMAS DE TRATAMIENTO DE MENSAJES | X.400–X.499 |
| DIRECTORIO | X.500–X.599 |
| GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS | X.600–X.699 |
| GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS | X.700–X.799 |
| SEGURIDAD | X.800–X.849 |
| APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS | X.850–X.899 |
| PROCESAMIENTO DISTRIBUIDO ABIERTO | X.900–X.999 |
| SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES | |
| Aspectos generales de la seguridad | X.1000–X.1029 |
| Seguridad de las redes | X.1030–X.1049 |
| Gestión de la seguridad | X.1050–X.1069 |
| Telebiometría | X.1080–X.1099 |
| APLICACIONES Y SERVICIOS CON SEGURIDAD | |
| Seguridad en la multidifusión | X.1100–X.1109 |
| Seguridad en la red residencial | X.1110–X.1119 |
| Seguridad en las redes móviles | X.1120–X.1139 |
| Seguridad en la web | X.1140–X.1149 |
| Protocolos de seguridad | X.1150–X.1159 |
| Seguridad en las comunicaciones punto a punto | X.1160–X.1169 |
| Seguridad de la identidad en las redes | X.1170–X.1179 |
| Seguridad en la TVIP | X.1180–X.1199 |
| SEGURIDAD EN EL CIBERESPACIO | |
| Ciberseguridad | X.1200–X.1229 |
| Lucha contra el correo basura | X.1230–X.1249 |
| Gestión de identidades | X.1250–X.1279 |
| APLICACIONES Y SERVICIOS CON SEGURIDAD | |
| Comunicaciones de emergencia | X.1300–X.1309 |
| Seguridad en las redes de sensores ubicuos | X.1310–X.1339 |
| INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD | |
| Aspectos generales de la ciberseguridad | X.1500–X.1519 |
| Intercambio de estados/vulnerabilidad | X.1520–X.1539 |
| Intercambio de eventos/incidentes/heurística | X.1540–X.1549 |
| Intercambio de políticas | X.1550–X.1559 |
| Petición de heurística e información | X.1560–X.1569 |
| Identificación y descubrimiento | X.1570–X.1579 |
| Intercambio asegurado | X.1580–X.1589 |
| SEGURIDAD DE LA COMPUTACIÓN EN NUBE | |
| Visión general de la seguridad de la computación en nube | X.1600–X.1601 |
| **Diseño de la seguridad de la computación en nube** | **X.1602–X.1639** |
| Prácticas óptimas y directrices en materia de seguridad de la computación en nube | X.1640–X.1659 |
| Aplicación práctica de la seguridad de la computación en nube | X.1660–X.1679 |
| Otras cuestiones de seguridad de la computación en nube | X.1680–X.1699 |

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

# Recomendación UIT-T X.1602

## Requisitos de seguridad para el entorno de aplicación Software como servicio


### Resumen

La Recomendación UIT-T X.1602 analiza el nivel de madurez de la aplicación Software como servicio (SaaS) y propone requisitos de seguridad que ofrezcan un entorno de ejecución del servicio que sea coherente y seguro para las aplicaciones SaaS. Los requisitos propuestos tienen su origen en los proveedores de servicios en la nube (CSP) y los asociados a los servicios en la nube (CSN) que necesitan un entorno de aplicaciones SaaS que satisfaga sus exigencias en materia de seguridad. Los requisitos son generales e independientes de cualquier servicio o modelo específico de algún escenario (por ejemplo, servicios web o transferencia del estado representacional (REST)), hipótesis o soluciones.



### Historia

| Edición | Recomendación | Aprobación | Comisión de Estudio | ID único* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1602 | 2016-03-23 | 17 | 11.1002/1000/12615 |

### Palabras clave

Entorno de aplicación Software como servicio (SaaS), requisito de seguridad, nivel de madurez del SaaS.


* 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 propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

## ÍNDICE

# Recomendación UIT-T X.1602

## Requisitos de seguridad para el entorno de aplicación Software como servicio

### 1 Alcance

Esta Recomendación se centra principalmente en los requisitos de seguridad del entorno de aplicación Software como servicio (SaaS) tomando como base el nivel de madurez de la aplicación SaaS. Esta Recomendación se dirige a los proveedores de servicios en la nube (CSP) y a asociados a los servicios en la nube (CSN) tales como los desarrolladores de aplicaciones.

### 2 Referencias

Ninguna.

### 3 Definiciones

#### 3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

**3.1.1 servicio en la nube** [b-UIT-T Y.3500]: Una o varias capacidades que se ofrecen mediante computación en la nube a la que se accede con una interfaz declarada.

**3.1.2 categoría del servicio en la nube** [b-UIT-T Y.3500]: Grupo de servicios en la nube que poseen un conjunto de cualidades en común.

**3.1.3 cliente del servicio en la nube** [b-UIT-T Y.3500]: Parte que mantiene una relación comercial a los efectos de servicios en la nube.

**3.1.4 asociado al servicio en la nube** [b-UIT-T Y.3500]: Entidad que colabora o asiste en actividades del proveedor de servicios en la nube o del cliente del servicio en la nube.

**3.1.5 proveedor del servicio en la nube** [b-UIT-T Y.3500]: Parte que ofrece servicios en la nube.

**3.1.6 usuario del servicio en la nube** [b-UIT-T Y.3500]: Persona física, o entidad que la represente, asociada a un cliente del servicio en la nube, que utilice servicios en la nube.

**3.1.7 escritorio como servicio** [b-UIT-T Y.3500]: Las capacidades proporcionadas al cliente del servicio en la nube son la posibilidad de construir, configurar, gestionar, almacenar, ejecutar y desempeñar las funciones del escritorio del usuario en remoto.

**3.1.8 infraestructura como servicio (IaaS)** [b-UIT-T Y.3500]: Categoría de servicio en la nube en la que el tipo de capacidades de la nube proporcionado al cliente del servicio en la nube es un tipo de capacidades de infraestructura.

**3.1.9 software como servicio (SaaS)** [b-UIT-T Y.3500]: Categoría de servicio en la nube en la que el tipo de capacidades de la nube es un tipo de capacidades de aplicación.

#### 3.2 Términos en esta Recomendación

Ninguno.

## 4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas y acrónimos:

ASP Proveedor de servicios de aplicación (*application service provider*)

CaaS Comunicaciones como servicio (*communications as a service*)

CRM Gestión de las relaciones con los clientes (*customer relationship management*)

CSC Cliente del servicio en la nube (*cloud service customer*)

CSN Asociado al servicio en la nube (*cloud service partner*)

CSP Proveedor de servicios en la nube (*cloud service provider*)

DaaS Escritorio como servicio (*desktop as a service*)

IaaS Infraestructura como servicio (*infrastructure as a service*)

IAM Gestión de identidades y accesos (*identity and access management*)

IdM Gestión de identidades (*identity management*)

OLAP Procesamiento analítico en línea (*OnLine analytical processing*)

OS Sistema operativo (*operating system*)

PaaS Plataforma como servicio (*platform as a service*)

PKI Infraestructura de claves públicas (*public key infrastructure*)

REST Transferencia del estado de la representación (*representational state transfer*)

SaaS Software como servicio (*software as a service*)

SAP Punto de acceso al servicio (*service access point*)

SLA Acuerdo de nivel de servicio (*service level agreement*)

## 5 Convenios

Ninguno.

## 6 Generalidades

Un entorno de aplicación de software como servicio (SaaS) es un entorno de desarrollo, despliegue y ejecución multidivisión (*multi-tenant*) orientado al servicio en el que el software y los datos asociados se alojan en un servidor central y normalmente se accede a ellos a petición de los usuarios que utilizan un cliente, por ejemplo, un navegador web, por Internet.

Aunque esta Recomendación se refiere principalmente al SaaS, algunos de los conceptos que figuran en ella también pueden ser de aplicación a otras categorías de servicios en la nube que también incluyan este tipo de capacidades de aplicación, por ejemplo las comunicaciones como servicio (CaaS).

En la Figura 1 se representa un modelo conceptual del entorno de aplicación SaaS. Las capacidades subyacentes de la infraestructura como servicio (IaaS), la plataforma como servicio (PaaS) y el escritorio como servicio (DaaS) se encapsularán en servicios y proporcionarán un acceso coherente y seguro utilizando el punto de acceso al servicio exportado (SAP). En la presente Recomendación, el IaaS podría prestar servicios de computación, servicios de almacenamiento y servicios de red; el PaaS podría prestar el servicio de plataforma y el DaaS podría prestar el servicio de escritorio para un entorno de aplicación SaaS. Todos estos servicios constituyen los elementos constructivos básicos del desarrollo de una aplicación.

Este entorno proporciona además ciertas funciones de gestión del servicio necesarias, entre ellas la inscripción en el servicio, la configuración del servicio, la orquestación del servicio, la verificación de la dependencia del servicio, el control de acceso al servicio, el aislamiento del servicio, la supervisión del servicio y otras funciones de control del servicio.

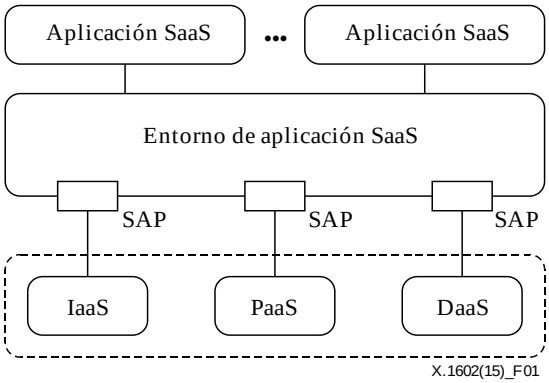
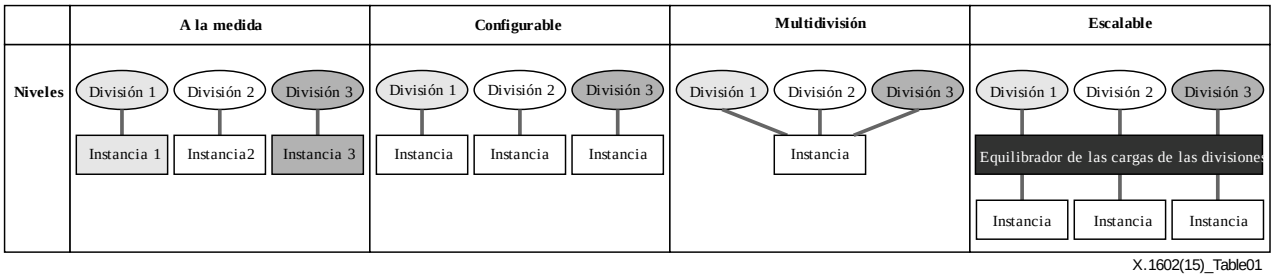



**Figura 1 – Modelo conceptual del entorno de aplicación SaaS**

## 7 Niveles de madurez de la aplicación SaaS

En la industria, la madurez del SaaS se clasifica en cuatro niveles que pueden denominarse abreviadamente nivel a la medida, nivel configurable, nivel multidivisión y nivel escalable. Cada uno de los niveles cubre características del anterior y proporciona características ampliadas. El diagrama que representa las características de los diferentes modelos de madurez del SaaS se muestra en el Cuadro 1.

**Cuadro 1 – Diagrama de los niveles de madurez de la aplicación SaaS**




Los distintos niveles de madurez de la aplicación SaaS tienen requisitos de seguridad diferentes para los entornos de aplicación SaaS. En la cláusula 8 se presentan los distintos requisitos desde la perspectiva de los CSP y CSN.

### 7.1 Nivel 1: Aplicación SaaS a la medida

La aplicación SaaS a la medida es semejante al clásico modelo de distribución de software del proveedor de servicios de aplicación (ASP). Cada cliente dispone de su solución personalizada para la aplicación SaaS y ejecuta su instancia personal de aplicación en el servidor en la nube. Como se representa en la Figura 2, la instancia de la aplicación a la medida comprende todo el entorno de ejecución, incluido el sistema operativo (OS), el sistema de gestión de datos y el software intermedio, específico de cada división (*tenant*), y el proveedor del entorno SaaS tiene que mantener varias instancias. Este modelo es difícil de escalar para satisfacer la creciente demanda de los clientes y su explotación puede resultar bastante costosa.

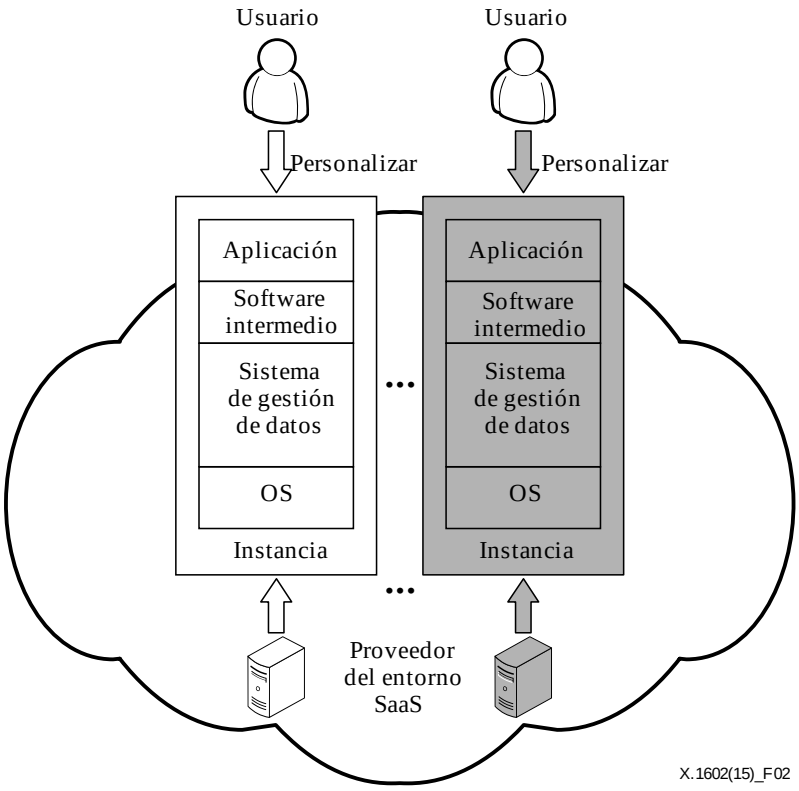



**Figura 2 – Arquitectura de la aplicación SaaS a la medida**

Las aplicaciones del modelo cliente-servidor normales pueden transformarse fácilmente en aplicaciones SaaS a la medida trasladando los servidores a la nube con un número relativamente pequeño de modificaciones. Las aplicaciones adecuadas para este escenario suelen desarrollarse cumpliendo requisitos especiales de la empresa u organización. Se prestará la máxima atención a la seguridad en el propio sistema, por ello la forma habitual consiste en agrupar un conjunto de máquinas físicas en una zona privada y desplegar un sistema de gestión de datos (que proporcione métodos abstraídos de persistencia y operaciones para diferentes tipos de datos) y el software asociado en el mismo. El sistema sólo se utiliza internamente y dispone de un estricto control de acceso. La plantilla de la instancia de aplicación es la misma para todos los clientes y proporciona una capacidad de configuración limitada. Sin embargo, la instancia de cada cliente es totalmente independiente de las demás.

### 7.2 Nivel 2: Aplicación SaaS configurable

Para algunas aplicaciones comúnmente utilizadas que no están personalizadas, tales como el sistema de creación de sitios web de autoservicio, los proveedores de aplicaciones SaaS ofrecen plantillas comunes para estas aplicaciones y varios conjuntos de entornos en tiempo de ejecución para las instancias de estas aplicaciones. Tomando como base la misma plantilla, los clientes pueden crear varias instancias de la aplicación independientes configurando la apariencia y el comportamiento de la aplicación, que se despliegan y ejecutan en máquinas individuales, físicas o virtuales, para satisfacer sus necesidades personales. Las instancias de la aplicación están aisladas entre sí. Esta arquitectura se muestra en la Figura 3.

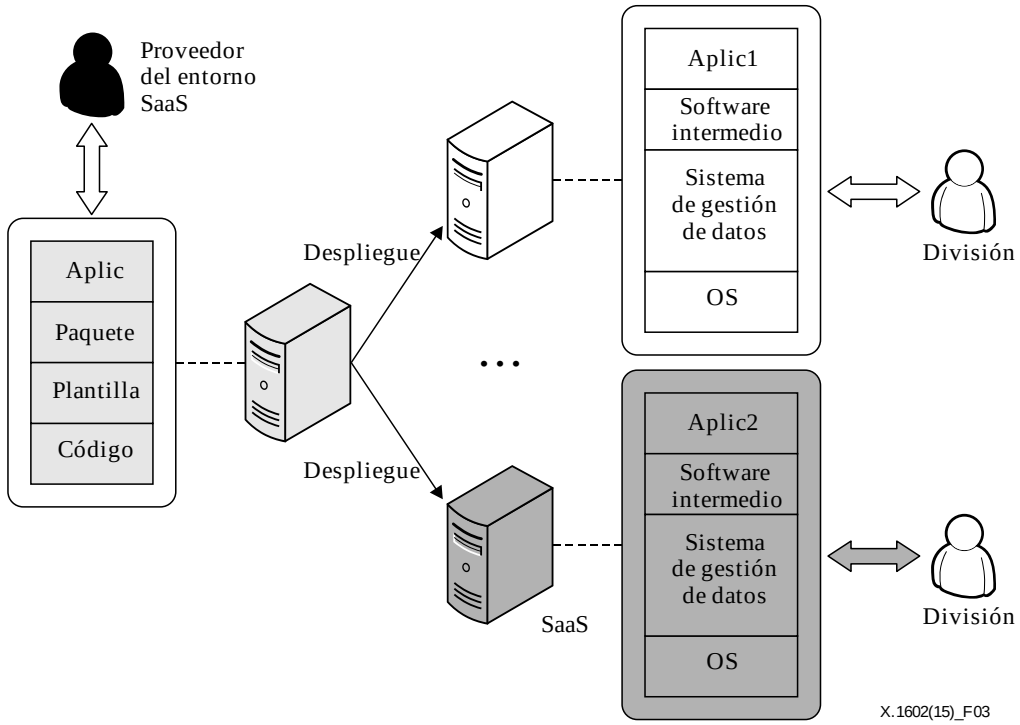



**Figura 3 – Arquitectura de la aplicación SaaS configurable**

La aplicación SaaS configurable tiene las características siguientes:

1) La aplicación en el despliegue inicial es copia de un producto estándar y las divisiones configuran la aplicación para adaptarla a sus propias necesidades. Sin embargo, las alternativas de configuración del producto son limitadas.

2) Para los proveedores de aplicaciones SaaS, las modificaciones de los códigos de producto pueden aplicarse inmediatamente a todas las divisiones con facilidad. Sin embargo, sólo una pequeña actualización u optimización de los códigos de producto es adecuada para cada instancia debido al problema de compatibilidad con las versiones posteriores a que puede dar lugar la actualización u optimización.

3) Las divisiones almacenan sus datos en sus propias máquinas, virtuales o físicas, aisladas entre sí. Esto supone que el proveedor del entorno SaaS tiene que habilitar los recursos suficientes tales como el almacenamiento, para soportar la ejecución simultánea de un número potencialmente grande de instancias de aplicación.

Dado el desarrollo y la mejora de la tecnología del software, la aplicación se proporcionará con las suficientes alternativas de configuración como para satisfacer las necesidades personales de los clientes. Tanto la configuración como el proceso de utilización deben ser más inteligentes y estar más automatizados. Los proveedores de aplicaciones SaaS clasificarán los productos en versiones diferentes para ajustarse a los diversos niveles de divisiones.

### 7.3 Nivel 3: Aplicación SaaS multidivisión

En este nivel, con ayuda de metadatos configurables, un proveedor de aplicaciones SaaS puede proporcionar una sola instancia que atienda a varias divisiones simultáneamente. La funcionalidad multidivisión puede activarse en varias capas entre ellas la del OS, la del sistema de gestión de base de datos, la del software intermedio y la de la aplicación. Se introduce un identificador de división para distinguir a los diferentes clientes. Cuando se utilice una base de datos en un sistema de gestión de base de datos, el esquema de la base de datos se ampliará para incluir el parámetro de identidad de la división a fin de almacenar todos los datos de los clientes en el mismo conjunto de cuadros.

La identidad de una división también es necesaria en las consultas de la base de datos para recuperar datos para un cliente específico. En la Figura 4 se representa la arquitectura general de la aplicación SaaS multidivisión.

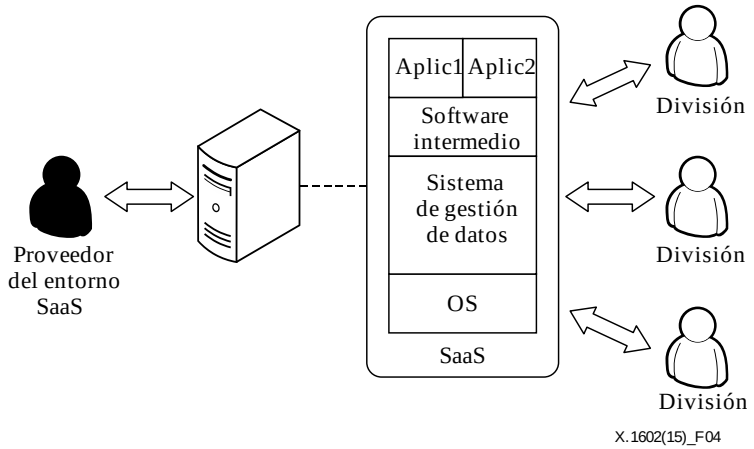



**Figura 4 – Arquitectura de la aplicación SaaS multidivisión**

El SaaS de inteligencia empresarial, por ejemplo la gestión de las relaciones con el cliente (CRM, *customer relationship management*), se considera una implementación característica a este nivel. Hasta ahora, se han realizado más intentos de combinar el almacenamiento de datos y la computación en la nube con el SaaS para proporcionar aplicaciones de inteligencia empresarial en línea. El almacenamiento de datos se aloja en el centro de datos, mientras que las aplicaciones de inteligencia empresarial y los modelos de datos están diseñados para utilizarse con muy poca personalización. Todo lo que tienen que hacer las divisiones es seleccionar los datos que necesitan las aplicaciones de inteligencia empresarial y definir la correspondencia de datos entre las fuentes de datos, el almacenamiento de datos y el modelo de datos. El sistema integrará los datos de varios sistemas fuente en el almacenamiento de datos para dar soporte a las aplicaciones de procesamiento analítico en línea (OLAP) utilizando guiones (*scripts*) generados automáticamente. En tiempo de ejecución, una única instancia de la aplicación de inteligencia empresarial suele atender a varias divisiones simultáneamente gracias a la utilización de técnicas de metadatos. Las autorizaciones y las políticas de seguridad garantizan que cada uno de los accesos a los datos del cliente y a la aplicación quede aislado de los correspondientes a los otros clientes.

Este nivel proporciona mucha más eficiencia en la utilización de los recursos de computación y almacenamiento y, por consiguiente, puede acomodar a más divisiones. También se pueden lograr un rendimiento, escalabilidad y elasticidad similares con ayuda de la partición de datos y técnicas paralelas.

La configurabilidad y la eficiencia multidivisión son las características distintivas de este nivel de la aplicación SaaS.

### 7.4 Nivel 4: Aplicación SaaS escalable

La mayor parte de los proveedores de servicios públicos atienden a un número arbitrariamente grande de clientes como varias divisiones. Por este motivo, se requiere que cada capa de la arquitectura de la plataforma subyacente, desde el hardware a la aplicación sea fácilmente escalable para las aplicaciones y los servicios como se muestra en la Figura 5. De aquí que puedan añadirse cada vez más divisiones y más usuarios por división sin necesidad de modificar la arquitectura de las aplicaciones.

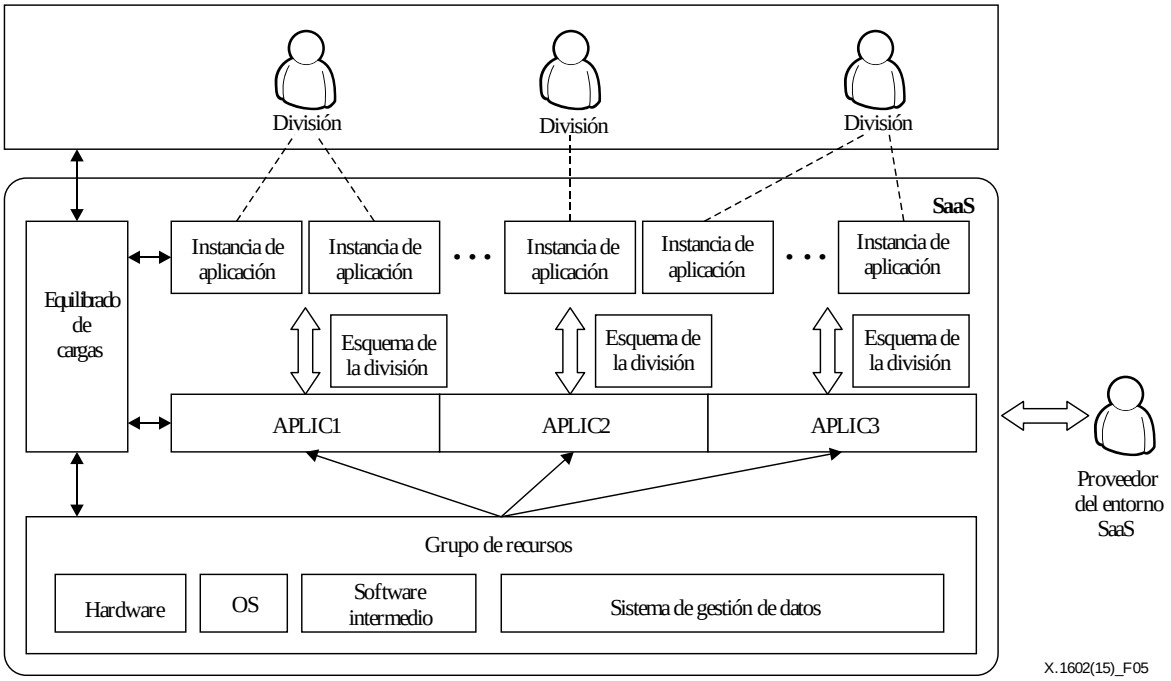



**Figura 5 – Arquitectura de la aplicación SaaS escalable**

Para la capa de aplicación, cuando hay una nueva división se generan una o varias instancias según las necesidades específicas de los usuarios, o se elige una instancia existente según las necesidades que determine el mecanismo de equilibrado de cargas. Es necesario que todas las instancias de la aplicación en un entorno como éste se creen dinámicamente.

Los recursos subyacentes de las aplicaciones SaaS escalables también soportan el escalado elástico. Todo el hardware, el software intermedio, el software propiamente dicho y los datos tienen que gestionarse en el grupo de recursos. Las aplicaciones obtienen dinámicamente todos los recursos que necesitan del grupo de recursos. Cuando es necesario, pueden añadirse nuevos recursos sin necesidad de recombinación ni de modificación de la arquitectura.

Deben tenerse en cuenta varias consideraciones relativas a las tecnologías de escalado dinámico, tales como las alternativas de escalado, la asignación de recursos, el acuerdo de nivel de servicio (SLA), etc. Una nueva división puede ejecutarse como una instancia aislada o puede coexistir con otras divisiones en una instancia compartida. Las diferentes instancias que ejecutan distintos tipos de divisiones pueden asignarse a varios recursos. El proveedor del entorno SaaS debe considerar diversos SLA para las diferentes divisiones cuando equilibre las cargas y los recursos compartidos.

## 8 Requisitos de seguridad para el entorno de aplicación SaaS

En la Figura 6 se muestra la relación entre el cliente del servicio en la nube (CSC), el CSP y el CSN con respecto al entorno de aplicación SaaS, en el que el CSP y el CSN desempeñan cometidos distintos cuando ejecutan funciones diferentes. El CSN puede servir al CSP como proveedor de contenidos, proveedor de software, integrador de sistemas o auditor, mientras que tanto el CSN como el CSP pueden desarrollar aplicaciones para el CSC. El CSP y el CSN tienen interfaces con el entorno de aplicación SaaS, pero el CSC sólo interacciona con las aplicaciones construidas sobre aquél. Por ello, la presente Recomendación está dedicada especialmente a los requisitos de seguridad del entorno de aplicación SaaS para el CSP y el CSN en un modelo de madurez diferente. Los requisitos de seguridad para el entorno de aplicación SaaS tienen su origen en el CSP y el CSN ya que necesitan que el entorno de aplicación SaaS tenga la capacidad de satisfacer sus exigencias en materia de seguridad.

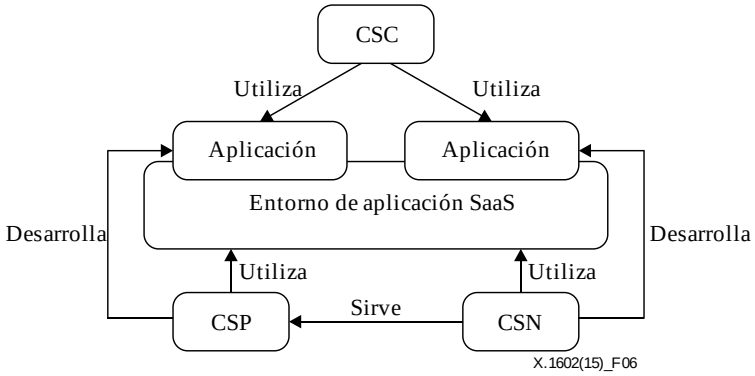



**Figura 6 – Relación entre el CSC, el CSP y el CSN**

El CSP y el CSN tienen sus propios requisitos de seguridad con respecto al entorno a diferentes niveles del SaaS. El Cuadro 2 muestra los requisitos de seguridad del CSP y el CSN en el entorno de aplicación SaaS. Los requisitos aplicables tanto al CSP como al CSN se denominan requisitos comunes.

**Cuadro 2 – Requisitos de Seguridad para el CSP y el CSN en el entorno de aplicación SaaS**

| | **Entorno de aplicación SaaS** |
|---|---|
| **Requisitos comunes** | Gestión de identidades y accesos, seguridad de los datos, evaluación y auditoría de la seguridad, seguridad de la interfaz, refuerzo de la seguridad |
| **CSP** | Disponibilidad, garantía de interoperabilidad/portabilidad del servicio, protección de los activos de software, cumplimiento de la ley, verificación de la seguridad de los códigos fuente |
| **CSN** | Seguridad de la auditoría, seguridad del software, posibilidad de mantenimiento del software |

### 8.1 Requisitos de seguridad comunes

El CSP y el CSN tienen varios requisitos de seguridad comunes en el entorno de aplicación SaaS.

#### 8.1.1 Gestión de identidades y accesos (IAM, *identity and access management*)

##### 8.1.1.1 Gestión de identidades (IdM, *identity management*)

En el entorno de aplicación SaaS entran en juego varios administradores y usuarios a los que se puede tener acceso para utilizarlos tanto internamente (CSP) como externamente (CSN). La gestión de identidades (IdM) es necesaria no sólo para proteger las identidades sino también para facilitar la gestión, autenticación y autorización de los accesos y los procesos de auditoría de las transacciones en el entorno de aplicación SaaS que se distingue por su apertura y dinamismo.

Para todos los modelos de madurez, la IdM debe facilitar la implementación del inicio de sesión individual y/o la federación de identidades para el entorno de aplicación SaaS utilizando diversos mecanismos de autenticación en los diferentes dominios de seguridad.

##### 8.1.1.2 Modelo de confianza

Se exige al entorno de aplicación SaaS que incorpore un modelo de confianza global tanto para el nivel multidivisión como para el nivel escalable. Este modelo de confianza permitirá que se creen islas y/o federaciones de entidades de confianza. Por consiguiente, el sistema de gestión del entorno de aplicación SaaS, los recursos subyacentes, los hipervisores, las máquinas virtuales y las aplicaciones construidas sobre el entorno de aplicación SaaS podrán autenticar las identidades y derechos autorizados de otras entidades y componentes. Cada una de las islas o federaciones de confianza se basará en una o varias autoridades de confianza (por ejemplo, una autoridad de certificación de la infraestructura de claves públicas (PKI)).

#### 8.1.1.3 Gestión de accesos

Es necesario que los administradores del entorno de aplicación SaaS proporcionen mecanismos que deleguen la autorización en los administradores de las divisiones. Los administradores de las divisiones otorgan derechos de acceso a sus recursos correspondientes. La gestión de accesos de un entorno de aplicación SaaS tal como éste debe soportar varios modelos de control de acceso tales como el modelo basado en identidades, el modelo basado en estrategias, el modelo basado en misiones, el modelo basado en tareas, etc.

Para las aplicaciones SaaS de los niveles a la medida y configurable, el modelo de control de acceso basado en misiones es un requisito básico. Por ejemplo, el CSN, que soporta la construcción de un servicio del CSP, puede encargarse de algunas aplicaciones pero no tiene los derechos de administración de todo el sistema del servicio en la nube. Además, puede permitirse que el CSN tenga acceso a sólo una parte de los recursos a los que se ha otorgado derechos de acceso. No obstante, el CSN puede compartir su recurso proporcionando interfaces de aplicación a otros CSN.

Para los niveles multidivisión y escalable, la integración del modelo de control de accesos para cada individuo y grupo es imprescindible. Para el control de accesos basado en misiones, debe utilizarse la compartición de recursos entre varias divisiones, dependiendo de los grupos de tareas del flujo de trabajo y de los derechos otorgados a dichas tareas. Así pues, cuando se ejecuten estos grupos de tareas, el entorno de aplicación SaaS deberá definir el mecanismo de soporte del control de accesos basado en tareas. Este mecanismo se utilizará para conseguir que el derecho de acceso de las divisiones a los recursos subyacentes se pueda otorgar y revocar a tiempo, y para evitar que los recursos subyacentes se utilicen sin autorización.

### 8.1.2 Seguridad de la interfaz

Se requiere que el entorno de aplicación SaaS asegure la apertura de interfaces a los CSP o los CSN para que presten o desarrollen diversos tipos de servicios de computación, y también se requiere que asegure las comunicaciones que utilizan dichas interfaces. Entre los mecanismos que están disponibles para garantizar la seguridad de la interfaz se encuentran, entre otros, los siguientes: autenticación unilateral/mutua, verificación de la integridad por suma de control, firma digital, etc.

### 8.1.3 Seguridad de los datos

#### 8.1.3.1 Aislamiento de los datos

Los datos pueden aislarse física o lógicamente. El aislamiento físico de los datos puede efectuarse mediante el control de acceso del almacenamiento físico. Esto exige que el entorno de aplicación SaaS almacene los datos de las diversas divisiones en zonas de almacenamiento físico distintas, o que se implemente el control de acceso para las diferentes divisiones mediante permisos de acceso, dominios de datos o cualquier otro método. El aislamiento lógico de los datos consiste en evitar que unas divisiones accedan a los datos de otras por medio de técnicas tales como la virtualización, aunque todos los datos se almacenen juntos.

Para las aplicaciones SaaS de los niveles a la medida y configurable, los datos de cada división se almacenarán por separado y aisladamente de los de otras a nivel físico.

Para las aplicaciones SaaS de los niveles multidivisión y escalable, todos los datos de las divisiones se almacenarán en la nube. Por consiguiente, se requiere que el entorno de aplicación SaaS sea lo suficientemente inteligente como para segregar los datos de las distintas divisiones y mantener el aislamiento entre los datos de las diversas divisiones, ya sea en reposo, durante su procesamiento o con ocasión de su transmisión. La frontera entre cada división debe garantizarse a nivel físico o a nivel lógico, dependiendo de la granularidad de aislamiento necesaria y el despliegue específico del software y hardware de computación en la nube.

#### 8.1.3.2 Confidencialidad de los datos

En la mayor parte de los casos, los datos de las divisiones se almacenan y utilizan fuera de las instalaciones del cliente y están sujetas a cierto grado de exposición. Por ello, se requiere que el entorno de aplicación SaaS soporte mecanismos de encriptación que garanticen la confidencialidad de los datos durante su transmisión, su procesamiento o cuando están desocupados, y que se eviten las fugas de datos debidas a las vulnerabilidades de seguridad de la aplicación.

El servicio de encriptación de datos se exige en todos los niveles del SaaS. Se exige la encriptación de los datos críticos para evitar su exposición.

Para los niveles multidivisión y escalable, dado que los datos de las divisiones deben almacenarse en una base de datos o incluso en un gran cuadro, se requiere que el entorno de división proporcione un mecanismo de gestión de claves adecuado que garantice que los datos no puedan ser objeto de intromisión dolosa por otras divisiones.

#### 8.1.3.3 Integridad de los datos

Los datos, y en particular los datos del sistema y los datos de los usuarios tales como los registros de anotaciones y los datos de configuración, requieren que el entorno de aplicación SaaS soporte mecanismos de integridad para evitar que sean manipulados sin autorización durante la transmisión, el procesamiento o en estado de reposo.

El registro de anotaciones del sistema y el de la aplicación no deben modificarse. Esto evita que, cuando se produzca una avería o una utilización indebida, el CSP o el software malintencionado borren sus pistas modificando los registros de anotaciones.

Es posible que la aplicación SaaS exija a los CSC su configuración a petición. Se exigirá también que los datos de configuración, tales como el fichero de configuración, no puedan modificarse sin autorización.

En el entorno de aplicación SaaS, los datos de los usuarios se almacenan en la nube que gestiona el CSP. En este caso, la verificación de la integridad de los datos se convierte en un requisito de seguridad primordial. Además, es necesario verificar la integridad de un gran volumen de datos.

#### 8.1.3.4 Fiabilidad de los datos

En apoyo de la fiabilidad de los datos, se exige al entorno de aplicación SaaS que soporte la copia de seguridad de datos o mecanismos de redundancia que garanticen el acceso de las divisiones a los datos aunque una parte de los nodos del almacenamiento en la nube haya perdido eficacia.

Se requiere de los datos alojados que implementen una copia de seguridad con varios emplazamientos; de lo contrario los datos resultarán totalmente ineficaces. Se requiere del entorno de aplicación SaaS que tenga la capacidad de recuperar datos por completo y restaurar los datos a tiempo así como la de mantener el sincronismo de los datos para garantizar la coherencia de las diversas copias.

#### 8.1.3.5 Rastreo y control de los datos

Se requiere que el entorno de aplicación SaaS garantice que el emplazamiento físico de los datos cumpla la legislación aplicable y los reglamentos locales, y que respete las posibles restricciones en los acuerdos con validez jurídica. Se requiere que el entorno de aplicación SaaS proporcione métodos para que los CSC especifiquen el emplazamiento de los lugares de almacenamiento de sus datos y verifiquen si sus datos se encuentran adecuadamente colocados.

Entre los posibles problemas de importancia de las infraestructuras compartidas y virtualizadas se encuentran no sólo la pérdida del control por los usuarios de sus propios datos, sino también la localización de los datos y el control de toda su vida útil. En un instante determinado, se exige al entorno de aplicación SaaS que conozca exactamente dónde se almacenan y se procesan los datos, ya sean del sistema o de los usuarios, y que se ofrezca la posibilidad de que los CSC verifiquen el

emplazamiento de los datos. Tanto durante la utilización de los datos como tras ella, no debe de permitirse el rastreo del movimiento de los datos por parte de terceros (entre ellos, otros CSP) sin autorización.

### 8.1.4 Evaluación y auditoría de seguridad

Cuando se modifican o manipulan inadecuadamente los recursos subyacentes o son objeto de intromisión indebida, se requiere que el entorno de aplicación SaaS inicie un procedimiento de evaluación de la seguridad para determinar si han quedado afectados, o no, servicios de seguridad específicos o las políticas de seguridad a ellos aplicadas, y se ofrecerán indicaciones o se propondrán instrucciones en el caso de que no se satisfagan unas condiciones preestablecidas. Se delegará en un tercero autorizado la verificación de que el entorno de aplicación SaaS cumpla los requisitos de seguridad aplicables. La evaluación de seguridad o la auditoría de seguridad podrán llevarla a cabo el CSC, el CSP o un tercero (CSN), y la certificación de seguridad podrá expedirla un tercero (CSN) con autorización.

Debe recurrirse a terceros independientes de confianza para que efectúen las evaluaciones de seguridad o auditorías de seguridad con fiabilidad, independencia y neutralidad.

### 8.1.5 Refuerzo de la seguridad

El entorno de aplicación SaaS pretende sobre todo ofrecer un entorno multidivisión de desarrollo, despliegue y ejecución, orientado a un servicio seguro para las aplicaciones SaaS. En algunos casos, las características de seguridad de las aplicaciones SaaS son insuficientes o no están bien desarrolladas. Se requiere que el entorno de aplicación SaaS recupere y verifique dichas características de seguridad deficientes de las aplicaciones SaaS y proporcione mecanismos diferenciados de refuerzo de la seguridad para mejorar las aplicaciones dependiendo de esas características de seguridad deficientes, a fin de cumplir los requisitos de seguridad de las diversas divisiones en diferentes contextos. Las características de seguridad de las aplicaciones se clasifican en características de seguridad estáticas cuando las aplicaciones se encuentran en un estado de reposo, y características de seguridad dinámicas, cuando las aplicaciones están ejecutándose.

## 8.2 Requisitos de seguridad del CSP

Además de los requisitos de seguridad comunes, el CSP tiene requisitos de seguridad específicos en el entorno de aplicación SaaS.

### 8.2.1 Disponibilidad

Para el CSP, se exige al entorno de aplicación SaaS que garantice que los CSC estén en servicio permanentemente, lo que a su vez requiere la resolución de los fallos del software/hardware, los ataques de denegación de servicio, etc. Es esencial garantizar un tiempo de parada mínimo para los CSC.

### 8.2.2 Garantía de interoperabilidad/portabilidad del servicio

Cuando el CSC quiera migrar todo su sistema o parte del mismo a otro CSP, el CSP de partida exigirá al entorno de aplicación SaaS que ofrezca garantías de la interoperabilidad y portabilidad del servicio para minimizar el perjuicio a las actividades del CSC. Por otra parte, se requiere del entorno de aplicación CSC que garantice que los datos afectados se borrarán permanentemente del CSP de partida y no podrá recuperarlos un tercero.

### 8.2.3 Protección de los activos de software

Se requiere que los activos de software (tales como aplicaciones, datos internos de las aplicaciones, guiones, macros, la biblioteca de códigos de funciones, las licencias de software, etc.) queden protegidos en el entorno de aplicación SaaS.

El CSP exigirá al entorno de aplicación SaaS que proteja la confidencialidad e integridad de cualquier activo de software proporcionado por el CSP o el CSN, lo que supone que dichos activos de software no podrán copiarse, utilizarse indebidamente, manipularse, enajenarse ni utilizarse de cualquier modo sin autorización.

### 8.2.4 Cumplimiento de la ley

Aunque el CSP pueda utilizar mecanismos de copia de seguridad y de redundancia de datos para garantizar la fiabilidad de los datos del CSC, se requiere que el entorno de aplicación SaaS garantice que las copias de los datos no se conservarán por más tiempo que el periodo de retención permitido en virtud de la ley de protección de datos aplicable.

### 8.2.5 Verificación de seguridad del código fuente

Dado que en el entorno de aplicación SaaS, el CSN puede proporcionar al CSP códigos, contenidos o software de las aplicaciones, se requiere del entorno de aplicación SaaS que proporcione mecanismos que ayuden al CSP a verificar los códigos y evitar códigos malintencionados.

## 8.3 Requisitos de seguridad del CSN

En el entorno de aplicación SaaS, el CSN puede ser un desarrollador de aplicaciones, un proveedor de contenidos, un proveedor de software, un integrador de sistemas o un auditor. Además de los requisitos de seguridad comunes, el CSN tiene sus propios requisitos de seguridad en el entorno de aplicación SaaS.

### 8.3.1 Seguridad de auditoría

Cuando el CSN sea un auditor, se requerirá que el entorno de aplicación SaaS proporcione mecanismos que ayuden al CSN a recopilar los eventos de auditoría, efectuando anotaciones en el histórico y comunicando la información con la granularidad de la división y la aplicación. Esta información se utilizará para asegurar que el servicio del CSP cumpla los requisitos reglamentarios del gobierno y los acuerdos legales establecidos con las divisiones. También se requerirá que el entorno de aplicación SaaS proporcione mecanismos que ayuden al CSN a garantizar que la información que recopilan y comunican los componentes de auditoría del sistema CSP sea correcta y no se haya alterado ni manipulado.

Además, se requerirá que el entorno de aplicación SaaS proporcione la capacidad de que el CSN registre los cambios de los datos importantes y supervise la disponibilidad de los datos en línea, a fin de emitir una alarma de seguridad a tiempo, reduciendo de este modo las pérdidas.

### 8.3.2 Seguridad del software

Cuando el CSN es un desarrollador de software o de contenidos en la nube, se requiere que el entorno de aplicación SaaS ayude al CSN a lograr que su código u otros componentes suministrados al CSP cumplan los posibles requisitos de programación que exija el CSP. Además, los códigos y componentes no deben contener software malintencionado ni violar la integridad de los servicios del CSP en la nube.

### 8.3.3 Mantenibilidad del software

Cuando el CSN sea un desarrollador de software, se requerirá que el entorno de aplicación SaaS soporte mecanismos que ayuden al CSN a proporcionar el código fuente u otra funcionalidad para el sistema del CSP. Se requerirá que el código fuente o la funcionalidad contengan un sistema de gestión de versiones y otros métodos adecuados a fin de garantizar el mantenimiento durante la vida útil del servicio. Estos métodos incluyen, entre otros, el suministro de actualizaciones para arreglar vulnerabilidades conocidas, la supresión de la independencia de los otros componentes con vulnerabilidades conocidas y el aumento de la seguridad global del sistema.

# Bibliografía


[b-UIT-T X.1601] Recomendación UIT-T X.1601 (2014), *Marco de seguridad para la computación en la nube*.

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

## 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 |

Impreso en Suiza
Ginebra, 2017