Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1605

(03/2020)

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 de la infraestructura pública como servicio (IaaS) en la computación en la nube

Recomendación UIT-T X.1605

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 (1)	
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 (1)	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 (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
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
COMUNICACIÓN CUÁNTICA	X.1700–X.1729

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

Recomendación UIT-T X.1605

Requisitos de seguridad de la infraestructura pública como servicio (IaaS) en la computación en la nube

Resumen

Las plataformas de infraestructura como servicio (IaaS) y los servicios virtualizados se enfrentan a distintos y quizá más numerosos problemas y amenazas que las infraestructuras y aplicaciones de tecnologías de la información tradicionales. Las plataformas IaaS que comparten servicios de computación, almacenamiento e interconexión de redes necesitan de una protección específica a las amenazas que acechan en el entorno IaaS. En esta Recomendación se pretende documentar los requisitos de seguridad de la IaaS pública a fin de ayudar a los proveedores de IaaS a mejorar la seguridad de la plataforma IaaS a lo largo de las fases de planificación, construcción y explotación.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1605	2020-03-26	17	11.1002/1000/14094

Palabras clave

Computación en la nube, IaaS, recursos virtuales, requisito de seguridad.

* 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

Página

1 Alcance 1
2 Referencias 1
3 Definiciones 1
3.1 Términos definidos en otros documentos 1
3.2 Términos definidos en la presente Recomendación 2
4 Abreviaturas y acrónimos 2
5 Convenios 3
6 Resumen 3
7 Retos de seguridad en el entorno IaaS 5
8 Requisitos de seguridad de la capa de acceso de IaaS 6
8.1 Requisitos de seguridad para el acceso web 6
8.2 Requisitos de seguridad para el acceso API 7
9 Requisitos de seguridad de la capa de servicio de IaaS 7
9.1 Requisitos de seguridad del servicio de computación 7
9.2 Requisitos de seguridad del servicio de almacenamiento 8
9.3 Requisitos de seguridad para el servicio de interconexión de redes 8
10 Requisitos de seguridad de la capa de recursos de IaaS 8
10.1 Requisitos de seguridad de abstracción y control de recursos 8
10.2 Requisitos de seguridad de recursos físicos 10
11 Requisitos de gestión de la seguridad 11
11.1 Gestión de identidad y control de acceso 11
11.2 Auditoría de seguridad 12
11.3 Gestión de vulnerabilidades 12
11.4 Respuesta de emergencia 13
11.5 Recuperación en caso de catástrofe 13
11.6 Copias de seguridad 14
Bibliografía 15

Recomendación UIT-T X.1605

Requisitos de seguridad de la infraestructura pública como servicio (IaaS) en la computación en la nube

1 Alcance

En esta Recomendación se analizan los problemas de seguridad que afrontan los proveedores de infraestructura como servicio (IaaS, *infrastructure as a service*) en el entorno IaaS y se especifican los requisitos de seguridad de la IaaS pública en la computación en la nube. Esta Recomendación es aplicable a los proveedores de IaaS pública.

Se da aquí una descripción detallada de los requisitos de seguridad. Quedan fuera del alcance de este documento las orientaciones de aplicación concretas.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T X.1642] Recomendación UIT-T X.1642 (2016), *Directrices para la seguridad operativa de la computación en la nube*.

[UIT-T Y.3502] Recomendación UIT-T Y.3502 (2014) | ISO/CEI 17789:2014, *Tecnología de la información – Computación en la nube – Arquitectura de referencia*.

[UIT-T Y.3513] Recomendación UIT-T Y.3513 (2014), *Computación en la nube – Requisitos funcionales de la infraestructura como servicio*.

[ISO/CEI 27002] ISO/CEI 27002:2013, *Tecnología de la información – Técnicas de seguridad – Código de prácticas relativo a los controles para la seguridad de la información*.

[ISO/IEC 27031] ISO/IEC 27031:2011, *Information technology –Security techniques– Guidelines for information and communication technology readiness for business continuity*.

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 computación en la nube [b-UIT-T Y.3500]: Paradigma para dar acceso a la red a un conjunto elástico y ampliable de recursos físicos o virtuales con administración y configuración en autoservicio previa solicitud.

3.1.2 servicio en la nube [b-UIT-T Y.3500]: Una o varias capacidades que se ofrecen en la computación en la nube que se invoca a través de una interfaz definida.

3.1.3 cliente de servicios en la nube (CSC) [b-UIT-T Y.3500]: Parte que mantiene una relación empresarial a los efectos de utilizar servicios en la nube.

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

3.1.5 proveedor de servicios en la nube (CSP) [b-UIT-T Y.3500]: Parte que ofrece servicios en la nube.

3.1.6 infraestructura como servicio (IaaS) [b-UIT-T Y.3500]: Categoría de servicio en la nube según la cual el tipo de capacidades en la nube suministrado al cliente de servicios en la nube consiste en capacidades de tipo infraestructura.

3.1.7 problema de seguridad [b-UIT-T X.1601]: "Dificultad" de seguridad diferente a una amenaza de seguridad directa que se debe a la naturaleza y al entorno de funcionamiento de los servicios en la nube, incluidas las amenazas "indirectas".

3.1.8 vulnerabilidad [b-NIST-SP-800-30]: Punto débil de un sistema de información, de procedimientos de seguridad, de controles internos o de una implementación que podría explotar una fuente de una amenaza.

3.2 Términos definidos en la presente Recomendación

Ninguno.

4 Abreviaturas y acrónimos

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

ACL Lista de control de acceso (*access control list*)
API Interfaz de programación de aplicaciones (*application programming interface*)
BIA Análisis del impacto en las operaciones (*business impact analysis*)
CPU Unidad central de procesamiento (*central processing unit*)
CSC Cliente del servicio en la nube (*cloud service customer*)
CSP Proveedor de servicios en la nube (*cloud service provider*)
DDoS Ataque distribuido de denegación de servicio (*distributed denial of service*)
DRO Objeto recuperación en caso de catástrofe (*disaster recovery object*)
DSP Proveedor de servicios digitales (*digital service provider*)
IAM Gestión de identidad y de acceso (*identity and access management*)
IaaS Infraestructura como servicio (*infrastructure as a service*)
IdM Gestión de identidad (*identity management*)
I/O Entrada/salida (*input/output*)
NIC Tarjeta de interfaz de red (*network interface card*)
OS Sistema operativo (*operating system*)
OTT Servicios superpuestos (*over the top*)
PaaS Plataforma como servicio (*platform as a service*)
RPO Objetivo de punto de recuperación (*recovery point objectives*)
RTO Objetivos de tiempo de recuperación (*recovery time objectives*)
SaaS *Software* como servicio (*software as a service*)
SLA Acuerdo de nivel de servicio (*service level agreement*)
SQL Lenguaje de búsqueda estructurado (*structured query language*)

TIC	Tecnología de la información y la comunicación
VDC	Centro de datos virtual (*virtual data centre*)
VLAN	Red virtual de área local (*virtual local area network*)
VM	Máquina virtual (*virtual machine*)
VXLAN	Red virtual extensible de área local (*virtual extensible local area network*)
XSS	Secuencias de comandos en sitios cruzados (*cross site script*)

5 Convenios

La expresión "se requiere" indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con esta Recomendación.

La expresión "se recomienda" indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. Su cumplimiento no es indispensable para poder declarar la conformidad.

La expresión "se tiene la opción de" indica que el requisito se permite, sin que ello signifique que se recomienda. No se pretende implicar que el fabricante deba ofrecer esta opción y que el operador de red/proveedor de servicio tenga la posibilidad de activarla. Significa, más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

En el cuerpo de la presente Recomendación y en sus apéndices aparecen algunas veces verbos que expresan obligación, prohibición, recomendación y posibilidad, en cuyo caso deben interpretarse en dicho sentido. Cuando estas expresiones o términos aparecen en apéndices o en partes incluidas explícitamente a título informativo no deben interpretarse en su sentido normativo.

6 Resumen

La infraestructura como servicio (IaaS, *infrastructure as a service*) es una categoría de servicios en la nube en la que el tipo de capacidades de nube que se ofrece al cliente de servicios en la nube (CSC, *cloud service customer*) es un tipo de capacidades infraestructura [b-UIT-T Y.3500]. La IaaS permite al CSC utilizar recursos de infraestructura de la nube (computación, almacenamiento o interconexión de redes) que pueden configurarse rápidamente y liberarse con un esfuerzo de gestión mínimo. Los servicios IaaS públicos permiten a los CSC lanzar rápida y fácilmente sus negocios sin necesidad de crear una nueva infraestructura de tecnologías de la información y la comunicación (TIC); y los CSC pueden emplear esos recursos para desarrollar, albergar y ejecutar servicios y aplicaciones a la demanda de manera flexible y elástica, según sus necesidades.

Sobre la base del marco de capas elaborado junto con la ISO/CEI, que se define en [UIT-T Y.3502] y el concepto IaaS de alto nivel definido en [UIT-T Y.3513], en la Figura 6-1 se muestra el concepto de alto nivel de los requisitos de seguridad de la IaaS.

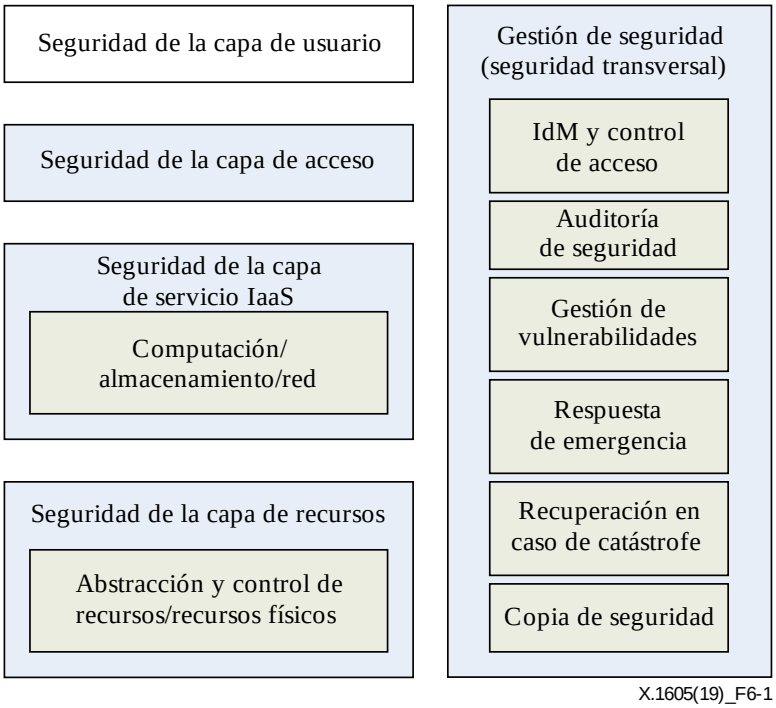

Figura 6-1 – Concepto de alto nivel de los requisitos de seguridad de la IaaS

La capa de usuario es la interfaz de usuario a través de la cual el CSC interactúa con el proveedor de servicios en la nube (CSP, *cloud service provider*). Entre los componentes funcionales de la capa de usuario se cuentan la función usuario, la función negocio y la función administrador, que interactúan con los servicios en la nube del CSP, realizan actividades administrativas relacionadas con el CSC y supervisan los servicios en la nube. De acuerdo con las responsabilidades entre el CSP y el CSC, éstos últimos deben asumir el control de los mecanismos de seguridad de la capa usuario, pues suelen utilizar sus propias herramientas o sistemas para acceder al servicio IaaS. En caso contrario, es decir, cuando el CSP facilita las herramientas o sistemas de la capa de usuario, éste debe facilitar herramientas o sistemas que se ajustan a las prácticas idóneas en materia de seguridad a nivel industrial. Los requisitos de seguridad de la capa de usuario quedan fuera del alcance de esta Recomendación.

La capa de acceso ofrece una interfaz común para el acceso tanto manual como automático a las capacidades disponibles en la capa de servicio. Los componentes funcionales de la capa de acceso comprenden el control de acceso y la gestión de la conexión. La capa de acceso es responsable de presentar las capacidades de servicio IaaS a través de uno o más mecanismos, como la web y las interfaces de programas de aplicación (API, *application programming interfaces*). Los requisitos de seguridad de la capa de acceso se definen en la cláusula 8.

La capa de servicio contiene la implementación de los servicios IaaS que ofrece el CSP. Contiene y controla los componentes de *software* que implementan los servicios IaaS y dispone la oferta de los servicios al CSC a través de la capa de acceso. Los requisitos de seguridad de la capa de servicio se definen en la cláusula 9.

Entre los componentes de la capa de recursos se cuentan la abstracción y el control de recursos y los recursos físicos, como se define en [UIT-T Y.3502]. Los recursos virtualizados se generan y controlan mediante la abstracción de *software*. Los requisitos de seguridad de la capa de recursos se definen en la cláusula 10.

La gestión de seguridad ofrece capacidades de gestión de seguridad transversales fundamentales, que se implementan en la capa de usuario, la capa de acceso, la capa de servicio y la capa de recursos, como se indica anteriormente. Los requisitos de gestión de seguridad de gestión de identidad, control de acceso, auditoria de seguridad, gestión de vulnerabilidades, respuesta de emergencia, recuperación en caso de catástrofe y copia de seguridad se definen en la cláusula 11.

7 Retos de seguridad en el entorno IaaS

Gracias a las enormes ventajas que ofrece, la IaaS se ha convertido en uno de los servicios más importantes de los CSP, en particular para los operadores de telecomunicaciones tradicionales, los servicios superpuestos (OTT, *over the top*) y los proveedores de servicios digitales (DSP, *digital service providers*), y su expansión ha sido muy rápida. En paralelo al rápido desarrollo de la IaaS, los problemas de seguridad siguen siendo graves y de una importancia que no se puede ignorar. Las plataformas y servicios de IaaS afrontan más retos y amenazas que las infraestructuras y las aplicaciones de tecnologías de la información tradicionales, sobre todo debido a la amplia implementación de las tecnologías de virtualización, entre otras la compartición de recursos entre múltiples titulares.

Dado que la IaaS pública puede tener muchos CSC de diversas organizaciones coexistiendo unos con otros, la seguridad y la protección de los datos personales son los factores más importantes que evalúan los CSC a la hora de escoger un servicio IaaS público.

Resumiendo, los problemas de seguridad que afronta la IaaS pública pueden tener los siguientes orígenes:

1) Virtualización: en tanto que característica técnica capital de la computación en la nube, la tecnología de virtualización permite la ejecución de distintas máquinas virtuales (VM, *virtual machines*) en el mismo hipervisor, pero también hace que los ficheros de las VM sean vulnerables a la modificación ilegal. Además, una vez explotadas las vulnerabilidades del hipervisor, todas las VM que se ejecutan en él se verán expuestas a los mismos riesgos de seguridad. Esos riesgos pueden estar causados por:
   - Configuración inadecuada y aislamiento de la red de los anfitriones físicos. Los atacantes pueden utilizar directamente las vulnerabilidades del hipervisor.
   - Vulnerabilidades de las interfaces entre las VM y el hipervisor. Los atacantes pueden explotar las vulnerabilidades para controlar el hipervisor. Esto se denomina escape VM.
2) API abiertas: como premisa de la gestión automática de las VM, las API abiertas pueden ampliar la superficie de ataque abusando o explotando vulnerabilidades como la falta de autentificación, autorización o verificación de integridad, lo que puede destruir numerosas aplicaciones.
3) Conectividad de red e Internet: las amenazas a la red, como los ataques de denegación de servicio distribuidos (DDoS, *distributed denial of service*), los ataques por intermediario, los ataques de falsificación de IP, etc. pueden lanzarse no sólo desde la red tradicional, sino también desde las VM alojadas en la misma máquina, cuya defensa es más difícil dada la vaguedad de las fronteras en la red virtualizada.
4) Alto grado de compartición de recursos: esta característica técnica puede ofrecer un objetivo más específico, pues, si se destruyen el anfitrión físico o la red física, todas sus VM se verían perjudicadas. La destrucción de dispositivos de almacenamiento obsoletos o sustituidos afecta a la confidencialidad de los datos de todos los CSC. También dificultaría el aislamiento entre CSC. Si no se configura adecuadamente el aislamiento entre distintas VM, la posibilidad de que haya fugas de datos o incluso ataques de red entre distintas VM puede aumentar notablemente. Cualquier accidente de este tipo conllevará graves riesgos y consecuencias para la seguridad.

5) Adaptabilidad de los recursos virtuales. La expansión elástica de los recursos virtuales y el ajuste dinámico del perímetro de seguridad de la red virtual genera un rápido crecimiento del flujo de red este-oeste y nuevas demandas de seguridad complejas. Las instalaciones de seguridad deben ser ágiles y trabajar en colaboración, pero la mayoría de equipos y sistemas de seguridad funcionan individualmente y carecen de un mecanismo de cooperación efectivo.

6) Gestión de configuración: el entorno de computación en la nube contiene grandes cantidades de activos de distintos tipos, así como diferentes tipos de servicios, lo que genera una elevada demanda de configuración, incluso del control de acceso, el aislamiento, la copia de seguridad de datos, etc. Una configuración deficiente puede abrir nuevas superficies de ataque o directamente causar fugas de información sensible.

7) Problemas de registro: los datos de registro de los sistemas operativos, las aplicaciones y los equipos de seguridad pueden ayudar a los operadores a evitar catástrofes e incluso detectar la causa última de los incidentes de seguridad. En el entorno de computación en la nube, la adquisición, la protección y la sincronización de los registros son más complejas. Por ejemplo, si se omite la protección de los registros, se corre el riesgo de que éstos puedan ser manipulados, mientras que una falta de sincronización dificultará la correlación de registros heterogéneos.

8 Requisitos de seguridad de la capa de acceso de IaaS

La capa de acceso de IaaS es responsable de la presentación de las capacidades de servicio IaaS para que los CSC puedan acceder a ellas y gestionarlas a través de uno o más mecanismos de acceso. Entre los mecanismos de acceso pueden contarse, entre otros, los siguientes:

– acceso web;

– acceso API.

Otra de las responsabilidades de la capa de acceso es implementar los mecanismos de gestión de la conexión adecuados para la aplicación de las políticas de calidad de servicio, el equilibrio de la carga y la transmisión segura del tráfico y las conexiones desde y/o hacia los componentes funcionales de la capa de usuario.

8.1 Requisitos de seguridad para el acceso web

1) El CSP IaaS debe aplicar medidas de autentificación y autorización a los CSC que acceden al servicio IaaS por la web, por ejemplo, mediante la autentificación de la petición con las credenciales del CSC y la validación de la autorización del CSC.

2) El CSP IaaS debe aplicar un mecanismo de control de acceso para que el CSC utilice las capacidades de servicio conexas.

3) Se recomienda que el CSP IaaS ofrezca un túnel de comunicación seguro para los CSC que utilicen el acceso web.

4) Se recomienda que el CSP IaaS ofrezca protección del acceso web para los CSC, por ejemplo, mediante la verificación de la validez de entradas y salidas, la verificación de la integridad de la petición, las capacidades de defensa contra comportamientos intrusivos en la web (inyección de lenguaje de búsqueda estructurado (SQL, *structured query language*), secuencias de comandos en sitios cruzados (XSS, *cross site script*), ejecución de comandos a distancia, etc.).

5) El CSP IaaS debe soportar capacidades de registro sin manipulación, análisis y auditoria de seguridad para el acceso web.

8.2 Requisitos de seguridad para el acceso API

1) El CSP IaaS debe soportar la autentificación y autorización de las credenciales de usuario de los CSC en el servicio API de llamadas, por ejemplo, al registrarse en la API, para garantizar que sólo se utilizan llamantes legítimos.
2) El CSP IaaS CSP debe ofrecer un mecanismo de control de acceso para los CSC en el servicio API de llamadas.
3) Se recomienda que los CSP IaaS ofrezcan un túnel de comunicación seguro para los CSC que accedan por API.
4) Se recomienda que los CSP IaaS ofrezcan la protección de interfaz API para los CSC, por ejemplo, mediante la verificación de la integridad de la petición, las capacidades de defensa contra comportamientos de ataque, ataques de reproducción, inyección de código, etc.
5) El CSP IaaS debe soportar capacidades de registro, análisis y auditoria de seguridad para el acceso API.

9 Requisitos de seguridad de la capa de servicio de IaaS

La capa de servicio de IaaS contiene la implementación de los servicios ofrecidos por el CSP. La capa de servicio contiene y controla los componentes de *software* que implementan los servicios IaaS (como el servicio de computación, el servicio de interconexión de redes, el servicio de almacenamiento, etc.) y dispone la oferta de esos servicios IaaS a los CSC por la capa de acceso.

9.1 Requisitos de seguridad del servicio de computación

1) El CSP IaaS debe ofrecer mecanismos de aislamiento de los recursos virtuales, incluido el aislamiento de la unidad central de procesamiento (CPU, *central processing unit*), la red interna, la memoria y el almacenamiento, etc., y permitir únicamente las comunicaciones que se ajustan a la política de seguridad entre distintas unidades de recursos virtuales, como las VM.
2) El CSP IaaS debe soportar la configuración de un límite superior de recursos para una única unidad de recursos virtuales en un anfitrión físico para evitar la degradación de la calidad de funcionamiento causada por la ocupación excesiva de una unidad de recursos virtuales específica.
3) Se recomienda que los CSP IaaS soporten la migración automática de la unidad de recursos virtuales una vez entre en fallo el servidor albergado a fin de evitar la interrupción de los servicios que se ejecutan en el recurso virtual.
4) El CSP IaaS debe soportar la verificación de la integridad de la unidad de recursos virtuales para evitar la manipulación maligna y garantizar que un volumen lógico sólo se ocupe por una unidad de recursos virtuales a la vez.
5) El CSP IaaS debe soportar la migración de la política de seguridad, que se sincronizará simultáneamente con la unidad de recursos virtuales, según proceda.
6) El CSP IaaS debe facilitar al administrador de CSC la capacidad de personalizar la política de seguridad de cada unidad de recursos virtuales.
7) El CSP IaaS debe ofrecer al CSC la capacidad de borrar completamente sus propios datos. Cuando el CSC elimine una unidad de recursos virtuales, simultáneamente se borrarán los archivos de imagen, las instantáneas y las copias de seguridad.

9.2 Requisitos de seguridad del servicio de almacenamiento

1) Se recomienda que los CSP IaaS soporten un mecanismo de redundancia de datos. Se deberán garantizar, como mínimo dos copias de seguridad de los datos del CSC en dos emplazamientos físicos distintos y el mecanismo deberá ser transparente para el CSC.

2) Se recomienda que los CSP IaaS soporten simultáneamente el control entrada/salida (I/O, *input/output*) y el acceso paralelo seguro para múltiples VM que utilicen el mismo sistema de almacenamiento.

3) El CSP IaaS debe garantizar la ejecución del control del acceso a los datos almacenados tanto en entidades de almacenamiento físicas como lógicas, y que ese control no pueda evitarse mediante un cambio del emplazamiento físico del almacenamiento.

4) El CSP IaaS debe garantizar que se puedan borrar íntegramente los datos del CSC y:
   - que la eliminación completa de los datos se realice antes de que se reasigne el recurso de almacenamiento a un nuevo CSC;
   - que, una vez borrados los ficheros/objetos de un CSC, la zona de almacenamiento correspondiente en el volumen físico se sobreescriba adecuadamente o se etiquete como de sólo escritura para evitar la recuperación no autorizada;
   - que, una vez migrados los datos de un CSC, se borren inmediata y completamente los metadatos del CSC.

9.3 Requisitos de seguridad para el servicio de interconexión de redes

1) Se recomienda que los CSP IaaS ofrezcan al CSC la capacidad de supervisar el tráfico de red norte-sur y este-oeste de sus propios recursos virtuales.

2) Se recomienda que los CSP IaaS ofrezcan al CSC la capacidad de implementar la interfaz de red control de ancho de banda de recursos virtuales.

3) El CSP IaaS debe ofrecer medidas de aislamiento entre la red virtualizada del CSC y la plataforma IaaS y la red de gestión, prohibiendo, por ejemplo, que el CSC acceda al anfitrión o al nodo de gestión.

4) El CSP IaaS debe implementar un mecanismo de lista de control de acceso (ACL, *access control list*) a la red para lograr el aislamiento de seguridad y controlar el acceso en las redes virtualizadas.

5) Se recomienda que los CSP IaaS puedan defenderse contra ataques a la red como el desplazamiento sucesivo de red virtual de área local (VLAN, *virtual local area network*) o red virtual de área local extensible (VXLAN, *virtual extensible local área network*).

10 Requisitos de seguridad de la capa de recursos de IaaS

De acuerdo con los componentes funcionales de la capa de recursos de IaaS, los requisitos de seguridad de la capa de recursos de IaaS son los siguientes:

- requisitos de seguridad de la abstracción y el control de recursos; y
- requisitos de seguridad de recursos físicos.

10.1 Requisitos de seguridad de abstracción y control de recursos

El componente funcional abstracción y control de recursos permite al CSP ofrecer cualidades como la elasticidad rápida, la puesta en común de recursos y el autoservicio a la demanda. Comprende el conjunto de recursos virtuales (como el recurso de computación virtual, el recurso de red virtual, etc.) y la plataforma de gestión de recursos virtuales. Los requisitos de seguridad de abstracción y control de recursos se ilustran desde la perspectiva de la configuración y gestión de recursos virtuales.

10.1.1 Requisitos de seguridad del conjunto de recursos virtuales

10.1.1.1 Requisitos de seguridad de los recursos de computación virtual

1) Las unidades de recursos de computación virtual (como las máquinas virtuales, los contenedores, etc.) deben estar aislados lógicamente unas de otras.
2) Es necesario que las unidades de recursos de computación virtual no puedan verse influidas por otras unidades o anfitriones en caso de accidente anormal o fallo.
3) Es necesario que las unidades de recursos de computación virtual no puedan superar su cuota de utilización.
4) Se recomienda prohibir instrucciones como "copiar", "pegar" y similares entre distintas unidades de recursos de computación virtual o anfitriones.
5) Se recomienda que los CSP IaaS soporten la supervisión en tiempo real de los recursos virtuales en modo en banda o fuera de banda y que se envíen alarmas cuando se detecten anormalidades. Para cada unidad de recursos virtuales se supervisará el estado de ejecución, el consumo de recursos y el estado de migración, entre otras cosas.

10.1.1.2 Requisitos de seguridad de recursos de red virtual

1) Las redes virtuales de los CSC deben estar aisladas lógicamente unas de otras mediante la implementación de medidas de VLAN, VXLAN, ACL, etc.
2) Se ha de ofrecer una capacidad de supervisión del tráfico de red entre distintas unidades de recursos virtuales.
3) Debe ofrecerse la capacidad de control de velocidad binaria en los puertos virtuales.
4) Se recomienda que se puedan detectar e impedir comportamientos de ataque a la red (como la falsificación de IP, los gusanos, etc.) con origen dentro de los recursos virtuales.
5) Para evitar el rastreo del tráfico de red, se ha de prohibir el modo promiscuo en los puertos de tarjeta de interfaz de red (NIC, *network interface card*) virtual.

10.1.1.3 Requisitos de seguridad de recursos de almacenamiento virtual

1) El conjunto de recursos de almacenamiento virtual debe estar aislado entre un CSC y otro.
2) Es necesario aplicar medidas de seguridad a los datos almacenados en las entidades de almacenamiento lógicas y físicas.
3) Se ha de prohibir el acceso directo a los recursos de almacenamiento físicos.
4) La capacidad de control I/O simultáneo y acceso paralelo seguro debe soportar que múltiples unidades de recursos virtuales utilicen las mismas entidades de almacenamiento.
5) Se recomienda que los recursos de almacenamiento virtual soporten la expansión elástica sin interrupción de los servicios de almacenamiento normales.

10.1.2 Requisitos de seguridad de la plataforma de gestión de recursos virtuales

1) Las medidas de control de acceso se han de implementar adecuadamente para evitar el acceso ilegal a la plataforma de gestión de recursos virtuales.
2) Se recomienda instalar sólo los componentes y las aplicaciones necesarios y cerrar los puertos de servicio irrelevantes siguiendo el principio de la minimización de riesgos.
3) Es necesario detectar los comportamientos de ataque a la plataforma de gestión de recursos virtuales, y emitir puntualmente alarmas, y en los registros ha de incluirse la dirección IP de origen, el tipo de ataque, el sello de tiempo, etc.
4) Es necesario ofrecer una capacidad de supervisión en tiempo real de los recursos virtuales, incluidos el estado de ejecución, la ocupación de recursos, la migración, etc.
5) Se recomienda desactivar los recursos virtuales innecesarios y desocupados.

6) Las instrucciones de gestión a la plataforma de gestión de recursos virtuales se han de transmitir por un túnel seguro.

7) Se recomienda poder limitar las instrucciones con privilegios cuando se ejecutan a distancia.

8) Es necesario poder aislar y destruir adecuadamente las unidades de recursos virtuales ilegales para minimizar su influencia sobre todos los recursos virtuales.

9) Se ha de ofrecer la capacidad de detección y destrucción de código maligno.

10) Se recomienda que la política de seguridad pueda migrar tras la migración simultánea de las unidades de recursos virtuales.

11) Una vez detectadas las vulnerabilidades de seguridad de los componentes de gestión de recursos virtuales (como el hipervisor, el motor contenedor, los componentes de gestión, etc.), se han de aplicar puntualmente y mantener al día los parches de seguridad o la configuración de seguridad reforzada.

12) Se ha de facilitar la gestión de fallos para mantener la continuidad de servicio superior, es decir, que las unidades de recursos virtuales de un anfitrión en fallo puedan migrar a otro anfitrión a tiempo.

13) Todas las operaciones y eventos de la plataforma de gestión de recursos virtuales han de registrarse para su posterior rastreo y auditoría.

10.2 Requisitos de seguridad de recursos físicos

Entre los recursos físicos se cuentan los recursos de *hardware*, como las computadoras, equipos de red, componentes de almacenamiento y demás elementos de la infraestructura de computación física, que necesita el CSP para ejecutar y gestionar los servicios IaaS que ofrece a los CSC.

10.2.1 Requisitos de seguridad del entorno físico

Los requisitos de seguridad del entorno físico de IaaS se definen en [ISO/CEI 27002].

10.2.1.1 Requisitos de seguridad de recursos físicos

Los recursos físicos incluyen los recursos de *hardware*, como la infraestructura de interconexión de redes física, los dispositivos de almacenamiento, los anfitriones, los terminales de gestión y demás elementos de infraestructura física.

1) Es necesario facilitar la capacidad de detección de fallos y posicionamiento en los recursos físicos (como equipos de interconexión de redes, anfitriones, dispositivos de almacenamiento, etc.) para mantener la disponibilidad y fiabilidad de la infraestructura física subyacente.

2) Se recomienda poder detectar y marcar a tiempo la alteración de los recursos físicos.

3) Se recomienda ofrecer la capacidad de recuperación de datos cuando fallen algunos componentes físicos.

4) Se ha de facilitar la capacidad de defensa de la plataforma IaaS contra DDoS.

5) La red de infraestructura se debe dividir en distintos dominios de seguridad de red, aislados lógicamente unos de otros.

6) Se han de implementar mecanismos de detección de la supervisión del tráfico de red y del comportamiento intrusivo con dispositivos de protección desplegados en la frontera de la red, incluidos la gestión de identidad y acceso (IAM, *identity and access management*), IPS, cortafuegos, etc.

7) Se recomienda poder detectar y evitar comportamientos de ataque de red salientes iniciados en los recursos IaaS.

8) Se ha de facilitar la capacidad de detección y destrucción de código maligno, sobre todo en los terminales de gestión, los anfitriones y demás servidores de aplicación.

9) Se ha de implementar una política de seguridad básica y que sólo los terminales y servidores que hayan satisfecho las políticas de seguridad puedan acceder a la plataforma IaaS.

10) Todas las operaciones y eventos de los recursos físicos han de registrarse para su posterior rastreo y auditoría.

11 Requisitos de gestión de la seguridad

La gestión de la seguridad es responsable de aplicar los controles de seguridad necesarios para mitigar las amenazas de seguridad en el entorno de la computación en la nube. Los componentes funcionales de la gestión de seguridad comprenden todas las instalaciones de seguridad necesarias para soportar los servicios en la nube.

Los componentes funcionales de gestión de la seguridad son:

- gestión de identidad y control de acceso;
- auditoria de seguridad;
- gestión de vulnerabilidades;
- respuesta de emergencia;
- recuperación en caso de catástrofe; y
- copias de seguridad.

11.1 Gestión de identidad y control de acceso

La plataforma IaaS debe ofrecer a CSC y los administradores de la plataforma IaaS las funciones de gestión de identidad (IdM, *identity management*) unificada y control de acceso.

1) La identidad del CSC durante la vida útil debe ser única en cada servicio IaaS y estar asociada a una auditoría de seguridad. La identidad del CSC debe gestionarse, mantenerse y protegerse contra el acceso no autorizado, la modificación o la eliminación.

2) La plataforma IaaS ha de facilitar la gestión de la política de contraseñas a los CSC y, entre otras cosas:
   - Es necesario aplicar una política de complejidad de contraseñas.
   - Es necesario utilizar un mecanismo de periodo de reconfiguración de la contraseña.
   - Es necesario emplear la generación aleatoria de la clave inicial de CSC y ésta debe modificarse al registrarse por primera vez.

3) Se recomienda que la plataforma IaaS soporte la detección de anormalidades en la identidad de CSC y en envío de alarmas al CSC concernido.

4) La plataforma IaaS debe soportar la autentificación multifactorial de CSC, además de técnicas de autentificación como las contraseñas, los certificados digitales, las tarjetas IC o la validación biométrica, entre otras.

5) Es necesario soportar una estrategia de autorización de granularidad fina acorde con los CSC y con la definición grupal de los recursos a los que se va a acceder. Es necesario que la plataforma IaaS proteja la confidencialidad e integridad de las credenciales de autentificación de los CSC.

6) Se han de almacenar para su ulterior auditoria los registros detallados de la autentificación, la autorización y demás operaciones de IdM de los CSC.

7) Se recomienda que la plataforma IaaS soporte la anexión al sistema IdM del CSC.

8) La función y los privilegios conexos del administrador de la plataforma IaaS se han de conceder utilizando una cuenta diferente.

9) La plataforma IaaS debe utilizar la autentificación multifactorial para los administradores.

10) La plataforma IaaS debe utilizar el principio de minimización de la autoridad para los administradores.

11) En el procedimiento de almacenamiento y transferencia, los datos sensibles, como los datos de autentificación, datos de autorización, etc., deben estar encriptados.

11.2 Auditoría de seguridad

1) La plataforma IaaS debe utilizar varios registros para la auditoria de seguridad, entre ellos, los siguientes:
   - Información de registro, autentificación de identidad y autorización de los CSC y los administradores de la plataforma IaaS.
   - Registros de funcionamiento y mantenimiento de la infraestructura IaaS realizados por los administradores de la plataforma IaaS.
   - Registros de funcionamiento de los recursos de los CSC realizados por los administradores de la plataforma IaaS.
   - Registros de funcionamiento de los recursos de los CSC realizados por los propios CSC.
   - Registros de funcionamiento y mantenimiento durante el proceso de ejecución de la plataforma IaaS.

2) La plataforma IaaS debe implementar mecanismos de seguridad para proteger los diversos registros contra la manipulación.

3) Todos los relojes de red se han de mantener sincronizados dentro de la plataforma IaaS a fin de registrar sistemáticamente los accesos y operaciones.

4) Los registros de la auditoria de seguridad comprenderán los sujetos, los objetos, el tiempo, los tipos y los resultados de los eventos de seguridad.

5) Los registros de auditoria entre CSC han de mantenerse aislados unos de otros.

6) Es necesario que los CSC puedan obtener y consultar los registros de auditoria relacionados con sus propios recursos.

7) Los registros de auditoria han de estar protegidos, por ejemplo, mediante la prohibición del acceso no autorizado a los registros de auditoría, la prevención de la supresión imprevista, la modificación, la toma de control y la pérdida.

8) El periodo de retención de los registros de auditoria ha de ajustarse a la legislación vigente y a los requisitos de retención específicos de los CSC.

9) Se recomienda que la plataforma IaaS soporte que los CSC empleen sistemas de auditoria terceros e interfaces para lograr los objetivos de auditoría bajo su responsabilidad.

11.3 Gestión de vulnerabilidades

La plataforma IaaS puede tener vulnerabilidades en sus procesos, gestión, configuración, *hardware*, *software*, etc.

1) Es necesario registrar la información de todos los activos y las versiones de la plataforma IaaS y actualizar esa información periódicamente.

2) Es necesario crear un mecanismo de evaluación de las vulnerabilidades en el que se aclaren los objetos, la frecuencia y la estrategia de la evaluación de las vulnerabilidades.

3) Es necesario realizar periódicamente una evaluación de las vulnerabilidades de todos los activos de la plataforma IaaS, generar informes de evaluación de las vulnerabilidades y formular recomendaciones para su reparación.

4) Es necesario gestionar el proceso de reparación y parcheo:
   - Es necesario hacer un seguimiento de las amenazas de seguridad y de los parches de seguridad emitidos por los distintos fabricantes y determinar qué parches se han de instalar en la plataforma IaaS.
   - Es necesario probar los parches de seguridad antes de su instalación a fin de garantizar que son compatibles con los sistemas y aplicaciones existentes.
   - Es necesario crear un plan de actualización de parches para todos los componentes de la plataforma IaaS, llevar a cabo la instalación de los parches de acuerdo con ese plan y crear registros de esa instalación.
5) Es necesario formular la configuración de seguridad básica de la plataforma IaaS y configurar los componentes de la plataforma IaaS de acuerdo con ella.
6) Es necesario realizar periódicamente una inspección de seguridad básica de todos los activos de la plataforma IaaS, realizar un informe de inspección básica y formular recomendaciones de rectificación.
7) Es necesario auditar las modificaciones de la estrategia de configuración de la plataforma IaaS para verificar la corrección, coherencia, integridad y eficacia de cada elemento de configuración y garantizar que la modificación de la configuración no crea defectos de seguridad nuevos.

11.4 Respuesta de emergencia

Las consideraciones sobre la respuesta de emergencia en la IaaS son conformes con la cláusula 8.9 de [UIT-T X.1642].

11.5 Recuperación en caso de catástrofe

Las consideraciones de recuperación en caso de catástrofe de la IaaS deben ajustarse a la reglamentación común de la tecnología TI, como la norma [ISO/CEI 27031]. Sin embargo, al ser una tecnología de rápida evolución, para la recuperación en caso de catástrofe también se ha de considerar lo siguiente:

1) Definir los objetos de recuperación en caso de catástrofe para cada CSC. Es necesario realizar un análisis del impacto en las operaciones (BIA, *business impact analysis*) para determinar los objetos de recuperación en caso de catástrofe de las distintas operaciones, basándose en el reconocimiento de los componentes clave y los principales riesgos de seguridad de la plataforma IaaS. Los objetos de recuperación en caso de catástrofe pueden definirse por prioridades, RPO/RTO, etc. Cada DRO determina el correspondiente SLA y la arquitectura de servicio, incluida la tecnología de alta disponibilidad en los centros de datos virtuales (VDC, *virtual data center*) remotos, las copias de seguridad transregionales, etc.
2) Copia de seguridad periódica de los sistemas y los datos. Es necesario soportar la capacidad de almacenamiento de datos transregional y la tolerancia a las catástrofes. Además, se han de ofrecer a los titulares de la plataforma IaaS copias de seguridad a nivel de sistema y a nivel de datos, además de la correspondiente capacidad de recuperación en caso de catástrofe, lo que puede ayudar a los CSP y CSC a implementar la resistencia a fallos. Los CSC pueden incluso hacer copias de seguridad con distintos CSP periódicamente para evitar el riesgo de interrupción prolongada de un único CSP.
3) Validación periódica del plan de recuperación en caso de catástrofe. Aunque los sistemas y datos de los CSC pueden mantenerse relativamente constantes, es posible que se introduzcan nuevos riesgos de seguridad con la actualización de la infraestructura por el CSP. Por ese motivo han de realizarse periódicamente simulacros de recuperación en caso de catástrofe y se ha de registrar la información clave, incluida la disponibilidad, la integridad y la validez

de los planes de recuperación en caso de catástrofe, los problemas encontrados en el proceso y sus correspondientes soluciones, etc.

4) Evaluación periódica del riesgo. Para soportar la continuidad de las operaciones del CSC, el CSP debe evaluar los riesgos de seguridad que pueden afectar al plan de continuidad de las operaciones del CSC, lo que incluye el fallo del servicio IaaS, la interrupción de la red entre el CSP y el CSC, la terminación de los servicios en la nube, etc., y comunicar diligentemente los resultados al CSC. Además, se han de notificar por adelantado, e incluso ajustarse a los requisitos del CSC, los planes y actividades de respuesta de emergencia y recuperación en caso de catástrofe en pro de la continuidad de las operaciones del CSC.

11.6 Copias de seguridad

Las consideraciones sobre las copias de seguridad en la IaaS son conformes a la cláusula 8.10 de [UIT-T X.1642].

Bibliografía

[b-UIT-T X.1601] Recomendación UIT-T X.1601(2015), *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 la nube – Descripción general y vocabulario*.

[b-NIST 500-291] NIST SP 500-291,2011, NIST *Cloud Computing Standards Roadmap*.

[b-NIST-SP-800-30] NIST Special Publication 800-30 Rev.1 (2012), *Guide for Conducting Risk Assessments.*

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, 2020