Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1604

(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 red como servicio (NaaS) en la computación en la nube

Recomendación UIT-T X.1604

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 (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.1604

Requisitos de seguridad de la red como servicio (NaaS) en la computación en la nube

Resumen

En la Recomendación UIT-T X.1604 se analizan las amenazas y los problemas de seguridad para la red como servicio (NaaS) en la computación en la nube, y se especifican los requisitos de seguridad de la NaaS en los aspectos de la aplicación NaaS, la plataforma NaaS y la conectividad NaaS basados en los correspondientes tipos de capacidad en la nube.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1604	2020-03-26	17	11.1002/1000/14093

Palabras clave

Nube, red como servicio, requisitos 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

Recomendación UIT-T X.1604

Requisitos de seguridad de la red como servicio (NaaS) en la computación en la nube

1 Alcance

En la presente Recomendación se analizan las amenazas y los problemas de seguridad para la red como servicio (NaaS) en la computación en la nube, y se especifican los requisitos de seguridad de la NaaS en los aspectos de la aplicación NaaS, la plataforma NaaS y la conectividad NaaS basados en los correspondientes tipos de capacidad en la nube.

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.1601] Recomendación UIT-T X.1601 (2015), *Marco de seguridad para la computación en la nube*

[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*

[UIT-T Y.3512] Recomendación UIT-T Y.3512 (2014), *Computación en la nube – Requisitos funcionales de la red como servicio*

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 control de acceso [b-UIT-T X.800]: Prevención del uso no autorizado de un recurso, incluida la prevención del uso de un recurso de una manera no autorizada.

3.1.2 autenticación [b-ISO/CEI 18014-2]: Acción de garantizar la identidad de una entidad.

3.1.3 autorización [b-UIT-T X.1251]: El servicio de autorización está diseñado para la toma de decisiones relativas a los derechos de acceso del usuario y para hacer cumplir las decisiones de autorización correspondientes a los privilegios del usuario. La autorización es un servicio opcional. Sólo se suministra cuando hay que controlar el acceso a los recursos en función de los derechos del usuario.

3.1.4 confidencialidad [b-UIT-T X.800]: Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.

3.1.5 integridad de los datos [b-UIT-T X.800]: Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada.

3.1.6 cortafuegos [b-ISO/CEI 27033-1]: Tipo de barrera de seguridad colocada entre entornos de red – que consiste en un dispositivo especial o una combinación de diversos componentes y técnicas – a través de la cual pasa todo el tráfico de un entorno de red a otro, y viceversa, y solo se permite el tráfico autorizado que se defina en la política de seguridad local.

3.1.7 sistema de detección de intrusión [b-ISO/CEI 27039]: Sistemas de información utilizados para detectar que se ha producido una intrusión, se está produciendo o ha habido un intento.

3.1.8 clave [b-UIT-T X.800]: Secuencia de símbolos que controla las operaciones de cifrado y descifrado.

3.1.9 gestión de claves [b-UIT-T X.800]: Generación, almacenamiento, distribución, supresión, archivo y aplicación de claves de acuerdo con una política de seguridad.

3.1.10 certificado de clave pública (PKC, *public-key certificate*) [b-UIT-T X.509]: Clave pública de una entidad, junto con alguna otra información, hecha infalsificable por firma digital con la clave privada de la autoridad de certificación que la emitió.

3.1.11 amenaza [b-ISO/CEI 27000]: Posible causa de un incidente no deseado, que puede dañar un sistema o perjudicar a una organización.

3.2 Términos definidos en la presente Recomendación

Ninguno.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

BoD Ancho de banda a la demanda (*bandwidth on demand*)

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

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

DDoS Denegación de servicio distribuida (*distributed denial of service*)

DoS Denegación de servicio (*denial of service*)

NaaS Red como servicio (*network as a service*)

SNMP Protocolo de gestión simple de red (*simple network management protocol*)

vCDN Red de entrega de contenido virtual (*virtual content delivery network*)

vEPC Red medular de paquetes evolutiva virtualizada (*virtualised evolved packet core*)

vFW Cortafuegos virtual (*virtual firewall*)

VPN Red privada virtual (*virtual private network*)

5 Convenios

En esta Recomendación:

La expresión "**se le exige que**" indica un requisito que debe cumplirse estrictamente, no permitiéndose desviación alguna si la Recomendación pretende reclamar su conformidad.

La expresión "**se recomienda**" indica un requisito recomendado pero que no se exige con carácter taxativo. Por ello no es necesario cumplir este requisito para reclamar su conformidad.

La expresión "**se le prohíbe**" indica un requisito que debe cumplirse estrictamente, sin permitirse desviación alguna si la Recomendación pretende ser conforme.

La expresión "**puede opcionalmente**" indica un requisito opcional admisible que no reviste en absoluto el carácter de recomendación. Esta expresión no pretende dar a entender que la implementación del fabricante deba suministrar una opción o característica que puedan ser activadas opcionalmente por el operador de red o proveedor del servicio. Más bien significa que el fabricante puede proporcionar opcionalmente esta característica sin menoscabo de su derecho de reclamar la conformidad con la Recomendación.

6 Resumen

Según [UIT-T Y.3500], una categoría de servicio en la nube es un grupo de servicio en la nube que propone un conjunto común de cantidades. La red como servicio (NaaS) es una categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube (CSC) conectividad de transporte y sus correspondientes capacidades de red.

Como se define en [UIT-T Y.3512], los servicios NaaS pueden ofrecer cualquiera de las tres capacidades en la nube siguientes: aplicación NaaS, plataforma NaaS y conectividad NaaS.

- **El servicio de aplicación NaaS** ofrece al CSC una aplicación de red en la nube como el encaminador virtual, la red de entrega de contenido virtual (vCDN), la red medular de paquetes evolutiva virtualizada (vEPC) y el cortafuegos virtual (vFW).
- **El servicio de plataforma NaaS** ofrece al CSC un entorno programable para las funcionalidades de red.
- **El servicio de conectividad NaaS** ofrece configuración al CSC y utiliza recursos de conectividad de redes como redes privadas virtuales flexibles y ampliadas (VPN), ancho de banda a la demanda (BoD), etc.

El concepto de NaaS de alto nivel puede describirse como se muestra en la Figura 1:

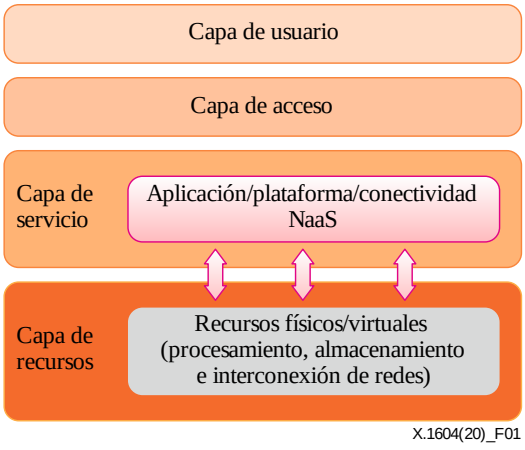

Figura 1 – Concepto de NaaS de alto nivel

Al utilizar estos tres tipos de servicios de interconexión de redes, la NaaS puede prestar funciones de red en la computación en la nube, a saber: coordinación de la virtualización de la computación y el almacenamiento con las capacidades de red, control armonizado de tecnologías de red heterogéneas y reconfiguración a la demanda.

Por otra parte, la NaaS también hace frente a varios problemas de seguridad:

- **Amenazas y problemas de seguridad en la aplicación NaaS:** Un servicio de aplicación NaaS consiste en que un CSP proporciona al CSC aplicaciones de red virtual, como cortafuegos virtual (vFW), encaminador virtual, red de entrega de contenido virtual (vCDN), etc. El servicio de aplicación NaaS hace frente a problemas de seguridad, como las vulnerabilidades de seguridad de la aplicación, los riesgos de seguridad de la virtualización de la red, la utilización compartida de dispositivos físicos de red, etc.
- **Amenazas y problemas de seguridad en la plataforma NaaS:** Un servicio de plataforma NaaS consiste en que un CSP proporciona al CSC entornos de software y una plataforma con el fin de gestionar, implantar y ejecutar aplicaciones de red. Los problemas de seguridad en el caso de la plataforma NaaS son, entre otros, los ataques de DoS a plataformas de red, las vulnerabilidades de seguridad de los sistemas operativos, el acceso al control de acceso, etc.
- **Amenazas y problemas de seguridad en la conectividad NaaS:** Un servicio de conectividad NaaS consiste en que un CSP proporciona al CSC conexión de red, como red privada virtual (VPN), ancho de banda a la demanda (BoD), etc. Un problema de seguridad ligado a la conectividad provoca riesgos no solo para los servicios NaaS, sino también para otros recursos en la nube y los datos del CSC. Los problemas de seguridad ligados al servicio de conectividad NaaS son, entre otros, las escuchas clandestinas, los ataques de intermediarios, etc.

En la presente Recomendación se analizan los requisitos de seguridad para la NaaS en la computación en la nube, incluidas la aplicación NaaS, la plataforma NaaS y la conectividad NaaS.

7 Amenazas y problemas de seguridad de la red como servicio en la computación en la nube

En las cláusulas 7 y 8 de [UIT-T X.1601] se abordan las amenazas y los problemas de seguridad para el CSC y el CSP en la computación en la nube, respectivamente. La NaaS en la nube también hace frente a amenazas y problemas de seguridad similares a los que se definen en [UIT-T X.1601], como se indica a continuación:

a) vulnerabilidades del sistema;

b) pérdida y filtración de datos;

c) acceso inseguro al servicio;

d) acceso con derechos de administración no autorizado;

e) amenazas internas;

f) pérdida de confianza;

g) pérdida de gobernanza;

h) pérdida de confidencialidad;

i) indisponibilidad del servicio; y

j) contexto compartido.

Para cada capacidad en la nube, la NaaS en la computación en la nube hace frente a amenazas y problemas de seguridad particulares.

7.1 Amenazas y problemas de seguridad de la aplicación NaaS

a) Vulnerabilidades de red y del sistema: Los atacantes podrían explotar las posibles vulnerabilidades de seguridad de la aplicación NaaS. Los defectos técnicos de la virtualización de la aplicación NaaS podrían provocar diversos riesgos para la seguridad; además, una tecnología de ejecución y mantenimiento inmadura podría provocar riesgos más graves.

b) Utilización compartida de los dispositivos físicos de red: En la medida en que se comparten los dispositivos físicos de red, los datos de un dispositivo compartido podrían perderse, filtrarse o utilizarse indebidamente.

c) Acceso inseguro: El acceso inseguro a la aplicación NaaS podría dar lugar a la pérdida, filtración o utilización indebida de los datos de la aplicación.

d) Acceso con derechos de administración no autorizado: El acceso con derechos de administración no autorizado a la aplicación NaaS puede dar lugar a que se pierdan datos.

e) Indisponibilidad de la aplicación: Una aplicación NaaS puede recibir ataques como consecuencia de una denegación de servicio (DoS) o una denegación de servicio distribuida (DDoS); además, el ataque puede causar daños en el equipo de hardware y pérdida o destrucción de datos.

7.2 Amenazas y problemas de seguridad de la plataforma NaaS

a) Ataques de DoS a plataformas de red: Cuando una o más plataformas han sido objeto de ataques como consecuencia de una DoS, la plataforma u otras plataformas virtualizadas no pueden responder debido al consumo de CPU y de transición de memoria.

b) Vulnerabilidades de seguridad del sistema operativo: Se pueden perder datos en las plataformas NaaS; por otra parte, las vulnerabilidades de seguridad de los sistemas operativos podrían provocar la propagación de virus y otros riesgos graves para la seguridad.

c) Acceso al control de acceso: El acceso al control de acceso podría provocar la pérdida, la filtración o la utilización indebida de datos.

d) Indisponibilidad de la plataforma de red: La indisponibilidad de una plataforma NaaS podría provocar la indisponibilidad de servicios NaaS, por lo que la aplicación NaaS y la conectividad NaaS conexas podrían no funcionar tampoco.

e) Acceso con derechos de administración no autorizado: El acceso con derechos de administración no autorizado a la plataforma NaaS podría provocar la pérdida, la filtración o la utilización indebida de datos. Por ejemplo, los atacantes podrían aprovechar una vulnerabilidad del sistema para obtener acceso con derechos de administración no autorizado a la plataforma NaaS y cambiar la dirección IP de destino de la recopilación de datos por la de los atacantes.

f) Amenazas internas de empleados: Cuando el cliente de un servicio NaaS es una empresa u organización, no una persona física, los empleados de la organización comparten las contraseñas "de administración", al igual que el proveedor de servicios NaaS. Los usuarios descuidados o que carecen de la formación adecuada (o miembros de una familia en el caso de un hogar), o los empleados descontentos que actúan de mala fe, siempre representan una amenaza considerable.

7.3 Amenazas y problemas de seguridad de la conectividad NaaS

a) Escuchas clandestinas: Los datos de conexión y de transmisión pueden ser objeto de escuchas clandestinas por atacantes.

b) Ataque a la conexión de red: Los ataques a la red pueden producirse durante la conexión a la red, como los ataques de intermediarios, los ataques de DoS, etc.

c) Pérdida y filtración de datos: Cuando se utilizan servicios NaaS, los clientes NaaS suelen utilizar la red proporcionada por los proveedores de NaaS para transportar datos. Estos datos pueden incluir datos personales, secretos comerciales y cuestiones políticas, de modo que cualquier filtración de datos es una grave amenaza para los usuarios NaaS.

d) Robo de identidad: Los atacantes podrían robar la identidad del sistema de gestión o del servidor de almacenamiento de datos de la NaaS de la computación en la nube, y ocasionar la pérdida de datos de conexión o de transmisión.

e) Manipulación e intercepción: Los equipos de red dañados, la intrusión de ciberdelincuentes y la quiebra de un proveedor de servicios NaaS pueden provocar la pérdida de datos imposibles de recuperar. Además, los ciberdelincuentes también pueden manipular datos si acceden a la red.

f) Acceso inseguro a la red: El acceso inseguro a la red puede provocar la pérdida, la filtración o la utilización indebida de los datos de conexión o de transmisión.

g) Autenticación insegura de la identidad: La autenticación insegura de la identidad puede provocar la pérdida, la filtración o la utilización indebida de los datos de conexión o de transmisión.

h) Indisponibilidad de la red: La conectividad a la red NaaS podría recibir ataques como consecuencia de una DoS o de una DDoS; además, esos ataques DoS o DDoS pueden provocar la caída de los servidores NaaS en la computación en la nube.

i) Vulnerabilidad en interfaz de adquisición: Los atacantes pueden utilizar la adquisición de datos de control para explotar la vulnerabilidad en interfaz.

j) Acceso con derechos de administración no autorizado: El acceso con derechos de administración no autorizado a un sistema de conectividad NaaS puede provocar la pérdida de datos de transmisión.

8 Requisitos de seguridad para la aplicación NaaS

En esta cláusula se identifican los requisitos de seguridad para la NaaS de la computación en la nube.

8.1 Requisitos de seguridad para la aplicación NaaS

Los requisitos de seguridad para la aplicación NaaS son, entre otros, los siguientes:

a) Se exige mantener la integridad y exactitud de los datos de la aplicación NaaS.

b) Se recomienda proporcionar métodos de control de acceso a los datos de la aplicación NaaS, como listas blancas, listas negras, etc.

c) Se recomienda que el CSP proporcione los métodos de control de acceso adecuados al CSC, como una lista blanca/negra, una cuenta y una contraseña, etc., para evitar que usuarios no autorizados accedan al sistema o a datos. En [UIT-T X.1601] se indican soluciones comunes de control de acceso para la computación en la nube.

d) Se exige que el CSP respalde el registro y la auditoría de la utilización de la aplicación NaaS.

e) Se exige que el CSP implemente defensas contra las vulnerabilidades del sistema de aplicación NaaS; por ejemplo, el CSP podría utilizar métodos de prueba de penetración del sistema de aplicación NaaS.

f) Se exige que el CSP proporcione métodos de copia de seguridad para evitar la pérdida de datos de aplicación NaaS, como copias de seguridad mediante la utilización de discos físicos, métodos de almacenamiento de datos distribuidos, etc. En [UIT-T X.1601] se indican métodos habituales para efectuar copias de seguridad.

En el Cuadro 8-1 se resume la relación entre amenazas de seguridad de la aplicación NaaS y sus correspondientes requisitos de seguridad.

Cuadro 8-1 – Aplicación NaaS: Relación de amenazas de seguridad y requisitos de seguridad

Amenazas de seguridad	Requisitos de seguridad
Vulnerabilidades de seguridad de la aplicación	b), d), e), f)
Riesgos de seguridad de la virtualización de la red	a), b), c), d), f)
Utilización compartida de dispositivos físicos de red	a), b), c), d), f)
Acceso inseguro	b), c), d), e), f)
Acceso con derechos de administración no autorizado	b), c), d), f)
Indisponibilidad de la aplicación	d), e), f)

8.2 Requisitos de seguridad para la plataforma NaaS

Los requisitos de seguridad para la plataforma NaaS son, entre otros, los siguientes:

a) Se exige para mantener la integridad y exactitud de los datos de la plataforma NaaS.

b) Se recomienda proporcionar métodos de control de acceso a los datos de la plataforma NaaS, como listas blancas, listas negras, etc.

c) Se recomienda que el CSP proporcione los métodos de control de acceso adecuados al CSC, como una lista blanca/negra, una cuenta y una contraseña, etc., para evitar que usuarios no autorizados accedan al sistema o a datos. En [UIT-T X.1601] se indican soluciones comunes de control de acceso para la computación en la nube.

d) Se exige que el CSP respalde el registro y la auditoría de la utilización de la plataforma NaaS.

e) Se exige que el CSP implemente defensas contra las vulnerabilidades del sistema de plataforma NaaS; por ejemplo, el CSP podría evitar la pérdida y filtración de datos en la plataforma NaaS.

f) Se exige que el CSP proporcione métodos de copia de seguridad para evitar la pérdida de datos de plataforma NaaS, como copias de seguridad mediante la utilización de discos físicos, métodos de almacenamiento de datos distribuidos, etc. En [UIT-T X.1601] se indican métodos habituales para efectuar copias de seguridad.

En el Cuadro 8-2 se resume la relación entre amenazas de seguridad de la plataforma NaaS y sus correspondientes requisitos de seguridad.

Cuadro 8-2 – Plataforma NaaS: Relación de amenazas de seguridad y requisitos de seguridad

Amenazas de seguridad	Requisitos de seguridad
Ataques de DoS a plataformas de red	a), b), c), d), e), f)
Vulnerabilidades de seguridad del sistema operativo	a), b), d), e), f)
Acceso al control de acceso	a), b), c), d), e), f)
Indisponibilidad de plataforma de red	a), d), e), f)
Acceso con derechos de administración no autorizado	b), c), d), f)
Amenazas internas de empleados	b), d), f)

8.3 Requisitos de seguridad para la conectividad NaaS

Los requisitos de seguridad para la conectividad NaaS son, entre otros, los siguientes:

a) Se exige para mantener la integridad y exactitud de los datos de la conectividad NaaS.

b) Se recomienda proporcionar métodos de control de acceso a los datos de la conectividad NaaS, como listas blancas, listas negras, etc.

c) Se recomienda proporcionar métodos criptográficos para garantizar la seguridad de los datos de conexión y de transmisión.

d) Se recomienda utilizar protocolos de red normalizados entre los recursos de la nube y los servidores de conectividad NaaS, como el protocolo de gestión simple de red (SNMP, *Simple Network Management Protocol*) u otros protocolos de red normalizados.

e) Se recomienda que el CSP proporcione los métodos de control de acceso adecuados al CSC, como una lista blanca/negra, una cuenta y una contraseña, etc., para evitar que usuarios no autorizados accedan al sistema o a datos. En [UIT-T X.1601] se indican soluciones habituales de control de acceso para la computación en la nube.

f) Se exige que el CSP respalde el registro y la auditoría de la utilización de la conectividad NaaS.

g) Se exige que el CSP implemente métodos de autenticación para proteger el acceso a los datos de conectividad NaaS, como los métodos de autenticación de dos factores u otros tipos. En [UIT-T X.1601] se indican métodos habituales de autenticación para la computación en la nube.

h) Se exige que el CSP implemente defensas contra las vulnerabilidades del sistema de conectividad NaaS; por ejemplo, el CSP podría recurrir a métodos de prueba de penetración para evitar vulnerabilidades del sistema de conectividad NaaS.

En el Cuadro 8-3 se resume la relación entre amenazas de seguridad de la plataforma NaaS y sus correspondientes requisitos de seguridad.

Cuadro 8-3 – Conectividad NaaS: Relación de amenazas de seguridad y requisitos de seguridad

Amenazas de seguridad	Requisitos de seguridad
Escuchas clandestinas	b), c), d), e), f), g) h)
Ataque a la conexión de red	d), f), h)
Pérdida y filtración de datos	a), b), c), d), e), f), g) h)
Robo de identidad	a), b), d), e), f), g) h)
Manipulación e intercepción	a), b), c), d), e), f), g) h)
Acceso inseguro a la red	b), c), d), e), f), g) h)
Autenticación insegura de la identidad	b), c) , e), f), g) h)
Indisponibilidad de la red	d), f), h)
Vulnerabilidad en interfaz de adquisición	a), b), c), d), f), h)
Acceso con derechos de administración no autorizado	c), f), g)

Bibliografía

[b-UIT-T E.409] Recomendación UIT-T E.409 (2004), *Estructura para organizar los incidentes y solucionar los incidentes de seguridad: Directrices para las organizaciones de telecomunicaciones*.

[b-UIT-T X.509] Recomendación UIT-T X.509 (2019) | ISO/CEI 9594-8:2020, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*.

[b-UIT-T X.800] Recomendación UIT-T X.800 (1991) | ISO/CEI 7498-2:1989, *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT.*

[b-UIT-T X.810] Recomendación UIT-T X.810 | ISO/CEI 10181-1 :1995, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general*.

[b-UIT-T X.1251] Recomendación UIT-T X.1251 (2019), *Expresión estructurada de información sobre amenazas: casos de uso*

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

[b-ISO/CEI 18014-2] ISO/CEI 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens.*

[b-ISO/CEI 19440] ISO/CEI 19440: 2007, *Enterprise integration – Constructs for enterprise modelling*.

[b-ISO/CEI 19944] ISO/CEI 19944:2017, *Information technology – Cloud services and devices: data flow, data categories and data use*.

[b-ISO/CEI 20000-1] ISO/CEI 20000-1:2011, *Information technology –Service management – Part1: Service management system requirements.*

[b-ISO/CEI 27000] ISO/CEI 27000:2018, *Information technology –Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/CEI 27033-1] ISO/CEI 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-ISO/CEI 27039] ISO/CEI 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS).*

[b-ISO/CEI 27729] ISO/CEI 27729:2012, *Information and documentation – International standard name identifier (ISNI).*

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

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