Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1603

(03/2018)

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 los datos para el servicio de control de la computación en la nube

Recomendación UIT-T X.1603

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	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.1319
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.1603

Requisitos de seguridad de los datos para el servicio de control de la computación en la nube

Resumen

La Recomendación UIT-T X.1603 analiza los requisitos de seguridad de los datos para el servicio de control de la computación en la nube, que incluyen los requisitos de alcance de datos de control, la vida útil de los datos de control, los requisitos de seguridad de la adquisición de datos de control y los requisitos de seguridad del almacenamiento de datos de control. Los requisitos de alcance de los datos de control incluyen el alcance de control necesario que los proveedores de servicios en la nube (CSP) deben suministrar para mantener la seguridad de la nube y el mayor alcance de control de los CSP. La vida útil de los datos de control consta de la creación, el almacenamiento, la utilización, la migración, la presentación, la destrucción y la copia de seguridad de los datos. La adquisición del control determina los requisitos de seguridad de la técnica de adquisición del servicio de control. El almacenamiento de datos de control determina los requisitos de seguridad para que los CSP almacenen los datos de control.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1603	2018-03-29	17	11.1002/1000/13406

Palabras clave

Control, nube, seguridad de los datos.

* 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.1603

Requisitos de seguridad de los datos para el servicio de control de la computación en la nube

1 Alcance

En esta Recomendación se describen los requisitos de seguridad de los datos para el servicio de control de la computación en la nube. También se analizan los problemas y amenazas para la seguridad de los datos, relativos al servicio de control en un entorno de computación en la nube, y se describen los requisitos de seguridad de los datos del servicio de control, incluidos alcance, ciclo de vida, adquisición y almacenamiento de datos. Además, la Recomendación puede utilizarse por proveedores de servicios en la nube (CSP) que ofrecen servicios de control a clientes del servicio en la nube (CSC).

2 Referencias

Ninguna.

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 autentificación [b-NIST-SP-800-53]: Verificación de la identidad de un usuario, proceso o dispositivo, que suele ser condición necesaria para acceder a recursos de un sistema de información.

3.1.2 capacidad [b-ISO/CEI 19440]: Cualidad de poder realizar una determinada actividad.

3.1.3 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 compartibles con administración y configuración en autoservicio previa solicitud.

NOTA – Como ejemplos de recursos pueden citarse servidores, sistemas operativos, redes, software, aplicaciones y equipos de almacenamiento, entre otros.

3.1.4 servicio en la nube [b-UIT-T Y.3500]: Una o varias capacidades que se ofrecen mediante computación en la nube (véase la cláusula 3.1.3) a las que se accede con una interfaz declarada.

3.1.5 cliente de servicio en la nube [b-UIT-T Y.3500]: Parte (véase la cláusula 3.1.15) que mantiene una relación comercial a los efectos de utilizar servicios en la nube (véase la cláusula 3.1.4).

NOTA – Una relación comercial no implica necesariamente un acuerdo financiero.

3.1.6 asociado del servicio en la nube [b-UIT-T Y.3500]: Parte (véase la cláusula 3.1.15) que colabora o asiste en actividades del proveedor de servicios en la nube (véase la cláusula 3.1.7) o del cliente del servicio en la nube (véase la cláusula 3.1.5), o en ambas.

3.1.7 proveedor de servicios en la nube [b-UIT-T Y.3500]: Parte (véase la cláusula 3.1.15) que ofrece servicios en la nube (véase la cláusula 3.1.4).

3.1.8 usuario de servicios en la nube [b-UIT-T Y.3500]: Persona física, o entidad que la represente, asociada a un cliente del servicio en la nube (véase la cláusula 3.1.5), que utilice servicios en la nube (véase la cláusula 3.1.4).

NOTA – Como ejemplos de tales entidades pueden citarse los dispositivos y aplicaciones, entre otros.

3.1.9 comunicaciones como servicio (CaaS) [b-UIT-T Y.3500]: Categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube (véase la cláusula 3.1.5) una capacidad de comunicación y colaboración en tiempo real.

NOTA – CaaS puede ofrecer los tipos de capacidad de plataforma y de aplicación.

3.1.10 nube comunitaria [b-UIT-T Y.3500]: Modelo de implantación en la nube donde los servicios en la nube (véase la cláusula 3.1.4) están compartidos y destinados exclusivamente a un grupo específico de clientes del servicio en la nube (véase la cláusula 3.1.5), que comparten requisitos y están relacionados unos con otros, y donde los recursos están controlados al menos por un miembro de ese grupo.

3.1.11 hipervisor [b-NIST-SP-800-125]: Componente de virtualización que gestiona el sistema operativo (SO) huésped en el anfitrión y controla el flujo de instrucciones entre el SO cliente y el soporte físico.

3.1.12 infraestructura como servicio (IaaS) [b-UIT-T Y.3500]: Categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube (véase la cláusula 3.1.5) un tipo de capacidades de infraestructura.

NOTA – El cliente de servicio en la nube (véase la cláusula 3.1.5) no gestiona o controla los recursos virtuales y físicos subyacentes, pero sí el sistema operativo, el almacenamiento y las aplicaciones instaladas que utilizan dichos recursos físicos y virtuales. El cliente del servicio en la nube (véase la cláusula 3.1.5) también puede tener limitaciones para controlar ciertos componentes de red (por ejemplo, cortafuegos centrales).

3.1.13 multidivisión [b-UIT-T Y.3500]: Atribución de recursos físicos y virtuales mediante los cuales varios arrendatarios (véase la cláusula 3.1.24) y sus cálculos y datos están aislados y son inaccesibles para terceros.

3.1.14 red como servicio (NaaS) [b-UIT-T Y.3500]: Categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube (véase la cláusula 3.1.5) conectividad de transporte y sus correspondientes capacidades de red.

NOTA – NaaS puede ofrecer cualquiera de los tres tipos de capacidades en la nube.

3.1.15 parte [b-ISO/CEI 27729]: Persona física o jurídica, organizada o no, o una agrupación de éstas.

3.1.16 información de identificación personal [b-ISO/CEI 29100]: Toda información que a) puede utilizarse para identificar el titular de la PII con quien está relacionada esa información, o b) está o puede estar relacionada directa o indirectamente con el titular de la PII.

3.1.17 plataforma como servicio (PaaS) [b-UIT-T Y.3500]: Categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube (véase la cláusula 3.1.5) un tipo de capacidades de plataforma.

3.1.18 nube privada [b-UIT-T Y.3500]: Modelo de implantación en la nube donde los servicios en la nube (véase la cláusula 3.1.4) están destinados exclusivamente a un solo cliente del servicio en la nube (véase la cláusula 3.1.5) y donde los recursos están controlados por dicho cliente (véase la cláusula 3.1.5).

3.1.19 nube pública [b-UIT-T Y.3500]: Modelo de implantación en la nube donde los servicios en la nube (véase la cláusula 3.1.4) están potencialmente disponibles para cualquier cliente del servicio en la nube (véase la cláusula 3.1.5) y donde los recursos están controlados por el proveedor de servicio en la nube (véase la cláusula 3.1.7).

3.1.20 dominio de seguridad [b-UIT-T X.810]: Conjunto de elementos, política de seguridad, autoridad de seguridad y conjunto de actividades relativas a la seguridad, donde el conjunto de elementos ha de cumplir la política de seguridad para las actividades especificadas y cuya política administra la autoridad de seguridad encargada del dominio de seguridad.

3.1.21 incidente de seguridad [b-UIT-T E.409]: Cualquier evento adverso que podría amenazar algún aspecto relacionado con la seguridad.

3.1.22 acuerdo de nivel de servicio (SLA) [b-ISO/CEI 20000-1]: Acuerdo por escrito entre el proveedor de servicios y el cliente en el que se estipulan los servicios y los objetivos de los mismos.

NOTA 1 – También es posible concertar un acuerdo de nivel de servicio entre el proveedor de servicios y un suministrador, grupo interno o cliente que actúa de suministrador.

NOTA 2 – El acuerdo de nivel de servicio puede incluirse en un contrato u otro tipo de documento.

3.1.23 software como servicio (SaaS) [b-UIT-T Y.3500]: Categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube (véase la cláusula 3.1.5) un tipo de capacidades de aplicación.

3.1.24 división [b-UIT-T Y.3500]: Usuario o grupo de usuarios del servicio en la nube (véase la cláusula 3.1.8) que comparten acceso a un conjunto de recursos físicos y virtuales.

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

3.1.26 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 amenaza.

3.2 Términos definidos en la presente Recomendación

En esta Recomendación se definen los términos siguientes:

3.2.1 datos de control: Los datos de control son el resultado del servicio de control en la nube que ayuda al proveedor de servicios en la nube (CSP) y a los clientes del servicio en la nube (CSC) a gestionar recursos y plataformas en la nube.

3.2.2 servicio de control: Con el servicio de control se controla la calidad de servicio proporcionado con respecto a los niveles de servicio como se definen en el acuerdo de nivel de servicio (SLA) entre el cliente del servicio en la nube y el proveedor de servicios en la nube.

3.2.3 datos de control necesarios: Los datos de control necesarios se utilizan para mantener acuerdos de nivel de servicio (SLA). También podrían ayudar al proveedor de servicios en la nube (CSP) a mantener la seguridad y estabilidad de las plataformas de computación en la nube. En los datos de control necesarios podrían figurar, entre otros, datos de control de sistema de gestión, datos de control de recursos físicos, datos de control de red, etc. Los datos de control necesarios se suelen utilizar principalmente por el CSP pero también podrían compartirse con clientes del servicio en la nube (CSC).

3.2.4 datos de control opcionales: Los datos de control opcionales se proporcionan por solicitud de los clientes del servicio en la nube (CSC) y para ofrecer un servicio de control en la nube. En los datos de control opcionales podrían figurar, entre otros, datos de control de máquina virtual, datos de control de servicio de almacenamiento de datos, aplicaciones CSC sobre datos de control en la nube, etc.

3.2.5 máquina virtual (VM): Duplicado lógico, aislado y eficiente de una máquina real.

4 Abreviaturas y acrónimos

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

API Interfaz de programación de aplicaciones (*application programming interface*)

BCP Plan de continuidad administrativa (*business continuity plan*)

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

CPU Unidad central de procesamiento (*central processing unit*)

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

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

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

CSU Usuario del servicio en la nube (*cloud service user*)

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

DNS Sistema de nombres de dominio (*domain name system*)

DOS Denegación de servicio (*denial of service*)

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

IAM Gestión de identidad y de acceso (*identity and access management*)

IIP Información de identificación personal

IP Protocolo Internet (*Internet protocol*)

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

OS Sistema operativo (*operating system*)

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

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

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

SIM Módulo de identificación del abonado (*subscriber identity module*)

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

TI Tecnología de la información

TIC Tecnología de la información y la comunicación

VM Máquina virtual (*virtual machine*)

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

En la presente Recomendación se analizan requisitos de seguridad de los datos para el servicio de control de la computación en la nube, incluidos alcance de datos de control, ciclo de vida de datos de control, problemas y amenazas de seguridad, y requisitos de seguridad de los datos de control de la computación en la nube.

El control del alcance de los datos describe dos tipos de datos de control en la nube: los necesarios y los opcionales, y también explica los casos de utilización.

El ciclo de vida de los datos de control y los problemas y amenazas de seguridad describen el contenido y los problemas y amenazas de seguridad de la recopilación, almacenamiento, uso, migración, análisis, presentación, destrucción y copia de seguridad de los datos de control en la nube.

Los requisitos de seguridad de los datos de control describen los requisitos detallados para cada etapa del ciclo de vida de los datos de control en la nube.

7 Alcance de los datos de control para la computación en la nube

En un entorno de computación en la nube hay dos tipos de datos de control: datos de control necesarios y datos de control opcionales.

Los datos de control necesarios se utilizan para mantener acuerdos de nivel de servicio (SLA). Pueden ayudar al CSP a gestionar la plataforma de computación en la nube de forma segura y estable. En los datos de control necesarios podrían figurar, entre otros, datos de control de sistema de gestión, datos de control de recursos físicos y datos de control de red. Los datos de control necesarios los utilizan principalmente los CSP pero también pueden compartirse con los CSC.

Los datos de control opcionales se proporcionan por solicitud de los CSC para que el CSP preste el servicio de control. En los datos de control opcionales pueden figurar, entre otros, datos de control de máquina virtual, datos de control de servicio de almacenamiento de datos y datos de los CSC asociados con el control de sus propias aplicaciones en la nube.

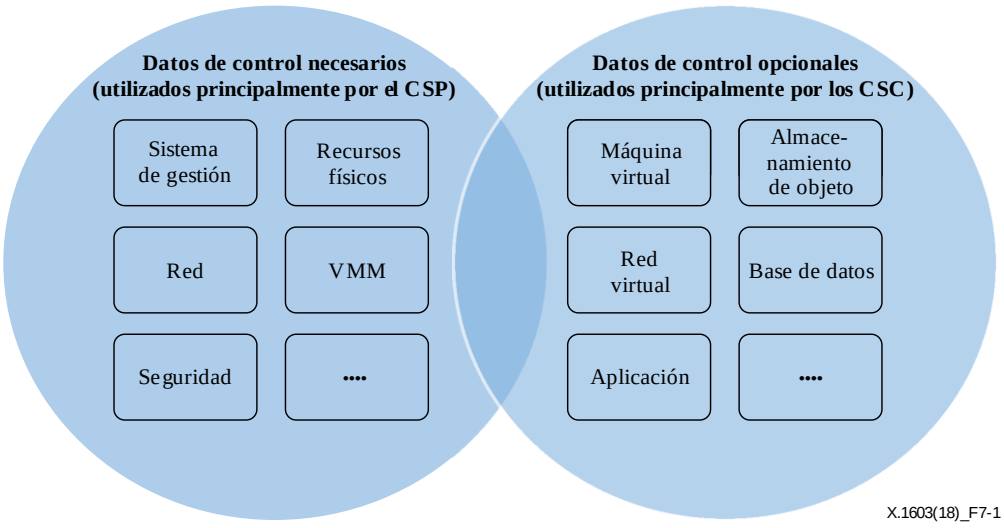

Figura 7-1 – Casos de utilización de dos tipos de datos de control

Los datos de control necesarios se utilizan principalmente por el CSP pero también podrían compartirse con los CSC. Por ejemplo, los datos de control de recursos físicos en la nube los utilizan principalmente los CSP para mantener la estabilidad de la plataforma en la nube pero también podrían utilizarlos los CSC si se proporcionaron al cliente recursos físicos afines a la nube como servicio.

Los datos de control opcionales se proporcionan por solicitud de los CSC y los utilizan también principalmente los CSC. Los CSP también podrían utilizar datos de control opcionales para mantener SLA. Por ejemplo, los CSC podrían solicitar los datos de los CSC asociados al control de sus propias aplicaciones en la nube. Esos datos los proporcionan los CSP y se utilizan para gestionar mejor sus aplicaciones en la nube. Por ejemplo, un CSP podría utilizar la base de datos como datos de control de servicio (DBaas) para mantener la seguridad y estabilidad de los recursos de bases de datos y servicios en la nube.

La relación entre esos dos tipos de datos de control se ilustra en la Figura 7-1.

8 Ciclo de vida de datos de control en computación en la nube

Esa cláusula describe el ciclo de vida de datos de control en computación en la nube y clarifica las diferencias principales entre él y el ciclo de vida de otros datos en computación en la nube.

8.1 Recopilación de datos de control

La recopilación de datos de control resulta de la adquisición de datos de control y la transmisión de esos datos a un servidor de almacenamiento. La mayoría de los datos de control se crea cuando los CSC utilizan el servicio en la nube. Los datos de control necesarios también se crean mediante otras actividades de control de servicios en la nube.

8.2 Almacenamiento de datos de control

Tras crear una recopilación de datos de control, los datos de control en la nube pueden almacenarse en los recursos en la nube de los CSC localmente o en servidores de almacenamiento de datos de control del CSP.

8.3 Uso de datos de control

Los datos de control pueden utilizarse para mantener el rendimiento y la seguridad de la plataforma en la nube y el servicio en la nube por el CSP; también pueden utilizarse para mantener la seguridad y el rendimiento de los recursos en la nube por los CSC.

8.4 Migración de datos de control

Cuando se migran recursos en la nube, los datos de control pueden migrar con los recursos en la nube.

8.5 Análisis de datos de control

Los datos de control pueden analizarlos el CSP y los CSC para comprender el estado de los recursos de plataforma en la nube para gestionarlos y asegurarlos mejor.

8.6 Presentación de datos de control

Se recomienda que los datos de control puedan presentarse de forma coherente para que puedan utilizarse para gestionar mejor los SLA y la seguridad en la nube. Como el volumen de datos de control en la nube puede ser muy grande, se recomienda que esos datos se resuman de forma gestionable y comprensible.

8.7 Destrucción de datos de control

Para mantener la seguridad de datos de control, el CSP debe destruir los datos de control si así lo solicitan los CSC.

Los CSP tienen la opción de destruir datos de control tras un periodo adecuado de tiempo tras la creación de datos de control.

8.8 Copia de seguridad de datos de control

Se requiere crear copias de seguridad de datos de control y recuperar datos a partir de esas copias.

9 Problemas y amenazas de seguridad para los datos de control de la computación en la nube

Las amenazas y problemas de seguridad para la computación en la nube, cláusulas 7 y 8 en [b-UIT-T X.1601] respectivamente, son las amenazas y problemas de seguridad para los CSC y CSP en la computación en la nube; los datos de control en la nube también se enfrentan a amenazas y problemas de seguridad similares (definidos en [b-UIT-T X.1601]). Algunos de esos problemas y amenazas de seguridad para los datos de control en la nube son, entre otros, los siguientes:

a) pérdida y filtración de datos;

b) acceso inseguro al servicio;

c) acceso con derechos de administración no autorizado;

d) amenazas internas;

e) pérdida de confianza;

f) pérdida de gobernanza;

g) pérdida de confidencialidad;

h) indisponibilidad del servicio;

i) apropiación indebida de propiedad intelectual;

j) contexto compartido;

k) conflictos jurisdiccionales;

l) migración e integración deficientes.

Para cada fase de ciclo de vida de datos de control, los datos de control en la nube se enfrentan a algunos problemas y amenazas de seguridad concretos.

9.1 Problemas y amenazas de seguridad en la fase de recopilación de datos de control

a) Recopilación de datos sin autorización: Un CSP o un atacante puede recopilar datos de control de los CSC sin autorización.

b) Vulnerabilidad en interfaz de adquisición: Los atacantes podrían utilizar la vulnerabilidad en una interfaz de adquisición de datos de control.

c) Robo de identidad: Los atacantes podrían robar la identidad del sistema de gestión o del servidor de almacenamiento de datos del servicio de control en la nube y ocasionar la pérdida de datos de control.

d) Manipulación e intercepción: Los atacantes podrían utilizar un ataque por intermediario u otros ataques de red para manipular o interceptar datos de control.

e) Acceso inseguro al servicio: En la fase de recopilación de datos de control, un acceso inseguro a las interfaces de recopilación de datos podría ocasionar la pérdida de datos de control.

f) Acceso con derechos de administración no autorizado: El acceso de administración no autorizado al sistema de recopilación de datos de control del CSP o al sistema de los CSC podría ocasionar una pérdida de datos de control. Por ejemplo, los atacantes pueden utilizar una vulnerabilidad en el sistema para obtener acceso de administración no autorizado al sistema de los CSC y cambiar la dirección IP de destino de la recopilación de control por la del atacante.

9.2 Problemas y amenazas de seguridad en la fase de almacenamiento de datos de control

a) Pérdida y filtración de datos: Dado que el entorno del servicio en la nube suele ser de multidivisión, la pérdida o filtración de datos es una grave amenaza para los CSC y CSP. Una falta de gestión adecuada de información criptográfica, como claves de encriptación, códigos de autentificación y privilegios de acceso, podría entrañar daños considerables, como la pérdida de datos o su imprevista filtración al exterior. Las principales fuentes de esta amenaza son, por ejemplo, controles insuficientes de autentificación, autorización y auditoría; utilización arbitraria de claves de encriptación y/o autentificación; fallos operativos; problemas de eliminación; cuestiones políticas y de jurisdicción; fiabilidad del centro de datos; y recuperación en caso de catástrofe.

b) Indisponibilidad del servicio: Un servidor de almacenamiento de datos puede ser atacado por un ataque de denegación de servicio (DoS) o de denegación de servicio distribuida (DDoS); además, el soporte físico para el almacenamiento de datos de control puede fallar y ocasionar la pérdida o destrucción de datos.

9.3 Problemas y amenazas de seguridad en la fase de uso de datos de control

a) Utilización indebida de datos: Los datos de control de los CSC podría utilizarlos indebidamente el CSP. Los datos de control podría utilizarlos un CSP para mantener SLA y la operación de recursos y plataforma de computación en la nube; ahora bien, los datos de control de los CSC también podría utilizarlos para otros fines el CSP sin permiso de los CSC.

b) Amenazas internas: Un empleado de un CSP o CSC podría utilizar indebidamente los datos de control de los CSC para otros fines diferentes a los previstos.

c) Vulnerabilidad en sistema: Los datos de control podrían perderse durante el uso de datos debido a vulnerabilidades en el sistema.

d) Escuchas clandestinas: Los datos de control podrían escucharlos clandestinamente atacantes.

9.4 Problemas y amenazas de seguridad en la fase de migración de datos de control

a) Utilización indebida de datos: Los datos de control podrían migrar entre diferentes ubicaciones físicas. Es muy importante no permitir que se utilicen indebidamente datos cuando se transmiten datos de control a diferentes ubicaciones.

b) Robo de identidad: Los atacantes podrían robar la identidad del sistema de gestión o del servidor de almacenamiento de datos del servicio de control en la nube y ocasionar la pérdida o el uso indebido de datos de control.

c) Manipulación e intercepción: Los atacantes podrían utilizar un ataque por intermediario u otros ataques de red para manipular e interceptar datos de control.

9.5 Problemas y amenazas de seguridad en la fase de análisis de datos de control

a) Utilización indebida de datos: Los datos de control de los CSC podría utilizarlos indebidamente el CSP durante el análisis de datos.

b) Vulnerabilidad en sistema: Los datos de control podrían perderse debido a una vulnerabilidad en el sistema de análisis de datos.

c) Ataque DoS: Un servidor de análisis de datos de control podría ser atacado por un ataque DoS o DDoS.

9.6 Problemas y amenazas de seguridad en la fase de presentación de datos de control

a) Utilización indebida de datos: Los datos de control de los CSC podría utilizarlos indebidamente (o presentarlos sin permiso de los CSC) el CSP durante la presentación de datos.

b) Vulnerabilidad de sistema: Los datos de análisis y de elaboración de informes podrían perderse debido a una vulnerabilidad en el sistema de presentación de datos.

c) Interpretación inadecuada: Los datos de control de los CSC podrían ser interpretados inadecuadamente durante una presentación de datos.

9.7 Problemas y amenazas de seguridad en la fase de destrucción de datos de control

a) Robo de identidad: Los atacantes pueden robar la identidad del sistema de gestión del servicio de control en la nube y ocasionar la pérdida de datos de control.

b) Vulnerabilidad en sistema operativo: Los datos de control podrían perderse durante el uso de datos debido a una vulnerabilidad en el sistema.

9.8 Problemas y amenazas de seguridad en la fase de copia de seguridad de datos de control

a) Vulnerabilidad en sistema operativo: Los datos de control también pueden perderse durante la copia de seguridad de datos e impedir su recuperación debido a una vulnerabilidad en el sistema.

10 Requisitos de seguridad para los datos de control de la computación en la nube

En esta cláusula se describen los requisitos de seguridad de los datos para el servicio de control de la computación en la nube.

10.1 Requisitos de seguridad para recopilación de datos de control

Entre los requisitos de seguridad de los datos para la recopilación de datos de control figuran los siguientes:

a) se requiere que los datos de recopilación opcionales sean creados únicamente por solicitud de los CSC;

b) se recomienda ofrecer notificaciones a los CSC cuando se creen datos de control necesarios;

c) se recomienda notificar a los CSC el alcance de los datos de control;

d) se requiere mantener la integridad y exactitud de los datos de control;

e) se recomienda utilizar técnicas de adquisición de datos estándar;

f) se recomienda proporcionar métodos de control de acceso a interferencias de adquisición de datos de control, como listas blancas, listas negras, etc.;

g) se recomienda proporcionar métodos criptográficos para velar por que la interfaz de adquisición de datos de control sea segura;

h) se recomienda utilizar protocolos de red estándar entre los recursos en la nube y los servidores de almacenamiento de datos de control.

En el Cuadro 10-1 se proporciona un resumen de las amenazas de seguridad en la recopilación de datos de control para los requisitos de seguridad.

Cuadro 10-1 – Recopilación de datos de control: cuadro de amenazas de seguridad para requisitos de seguridad

Amenazas de seguridad	Requisitos de seguridad
Recopilación de datos sin autorización	a), b), c)
Vulnerabilidades en interfaz de adquisición	d), e), f), g)
Robo de identidad	d), e), f), g), h)
Manipulación e intercepción	h)
Acceso inseguro al servicio	b), d), e), f), g), h)
Acceso con derechos de administración no autorizado	d), e), f), g), h)

10.2 Requisitos de seguridad para almacenamiento de datos de control

Entre los requisitos de seguridad de los datos para el almacenamiento de datos de control figuran los siguientes:

a) se recomienda que el CSP proporcione los métodos de control de acceso adecuados a los servidores de almacenamiento de datos de control;

b) se recomienda que el CSP determine el periodo máximo de tiempo para la retención de datos de control;

c) se recomienda que el CSP proporcione métodos de encriptación adecuados para datos de control.

En el Cuadro 10-2 se proporciona un resumen de las amenazas de seguridad en el almacenamiento de datos de control para los requisitos de seguridad.

Cuadro 10-2 – Almacenamiento de datos de control: cuadro de amenazas de seguridad para requisitos de seguridad

Amenazas de seguridad	Requisitos de seguridad
Pérdida y filtración de datos	a), b), c)
Indisponibilidad de servicio	a), c)

10.3 Requisitos de seguridad para uso de datos de control

Entre los requisitos de seguridad de los datos para el uso de datos de control figuran los siguientes:

a) se requiere que el CSP defina claramente cómo se van a utilizar los datos de control para los CSC;

b) se recomienda que el CSP proporcione una declaración de uso de datos de control formal a los CSC, como se ilustra en el Cuadro 10-1;

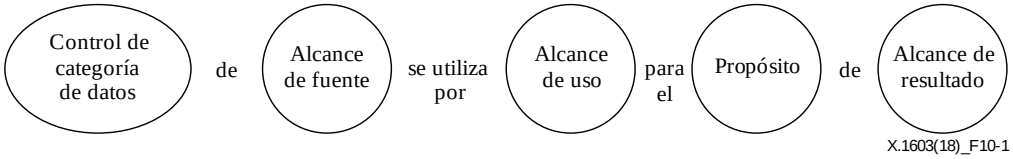

Figura 10-1 – Declaración de uso de datos de control recomendado

c) se requiere que el CSP proporcione una notificación y obtenga un permiso de los CSC antes de utilizar los datos de control para otros fines diferentes a los previstos;

d) se requiere que el CSP soporte el registro y la auditoría del uso de datos de control.

En el Cuadro 10-3 se proporciona un resumen de las amenazas de seguridad en el uso de datos de control para los requisitos de seguridad.

Cuadro 10-3 – Uso de datos de control: cuadro de amenazas de seguridad para requisitos de seguridad

Amenazas de seguridad	Requisitos de seguridad
Utilización indebida de datos	a), b), c), d)
Amenazas internas	a), b), c), d)
Vulnerabilidad en sistema	d)
Escuchas clandestinas	d)

10.4 Requisitos de seguridad para migración de datos de control

Entre los requisitos de seguridad de los datos para la migración de datos de control figuran los siguientes:

a) se recomienda que el CSP proporcione una notificación a los CSC de migración de datos de control;

b) se requiere que el CSP vele por una transmisión segura en la migración de datos de control;

c) se requiere que el CSP soporte el registro y la auditoría de las operaciones de migración de datos de control.

En el Cuadro 10-4 se proporciona un resumen de las amenazas de seguridad en la migración de datos de control para los requisitos de seguridad.

Cuadro 10-4 – Migración de datos de control: cuadro de amenazas de seguridad para requisitos de seguridad

Amenazas de seguridad	Requisitos de seguridad
Utilización indebida de datos	a), c)
Robo de identidad	b), c)
Manipulación e intercepción	b), c)

10.5 Requisitos de seguridad para análisis de datos de control

Entre los requisitos de seguridad de los datos para el análisis de datos de control figuran los siguientes:

a) se requiere que el CSP proporcione una notificación sobre el propósito del análisis de datos de control a los CSC;

b) se requiere que el CSP implemente defensas contra las vulnerabilidades del sistema de análisis de datos de control, por ejemplo, el CSP debería evitar la pérdida y filtrado de datos en el sistema de análisis de datos de control.

En el Cuadro 10-5 se proporciona un resumen de las amenazas de seguridad en el análisis de datos de control para los requisitos de seguridad.

Cuadro 10-5 – Análisis de datos de control: cuadro de amenazas de seguridad para requisitos de seguridad

Amenazas de seguridad	Requisitos de seguridad
Utilización indebida de datos	a)
Vulnerabilidad en sistema	b)
Ataque DoS	b)

10.6 Requisitos de seguridad para presentación de datos de control

Entre los requisitos de seguridad de los datos para la presentación de datos de control figuran los siguientes:

a) se requiere que el CSP mantenga la integridad y precisión de datos de control presentados;

b) se requiere que el CSP aplique métodos de autenticación para proteger el acceso a la presentación de datos de control;

b) se requiere que el CSP soporte defensas contra las vulnerabilidades del sistema de presentación de datos de control, por ejemplo, el CSP podría utilizar métodos de prueba de penetración para evitar vulnerabilidades del sistema de presentación de datos de control.

En el Cuadro 10-6 se proporciona un resumen de las amenazas de seguridad en la presentación de datos de control para los requisitos de seguridad.

Cuadro 10-6 – Presentación de datos de control: cuadro de amenazas de seguridad para requisitos de seguridad

Amenazas de seguridad	Requisitos de seguridad
Utilización indebida de datos	a), b)
Vulnerabilidad en sistema	b), c)
Interpretación inadecuada	a), b), c)

10.7 Requisitos de seguridad para destrucción de datos de control

Entre los requisitos de seguridad de los datos para la destrucción de datos de control figuran los siguientes:

a) se requiere que el CSP proporcione métodos de destrucción adecuados para datos de control;

b) se requiere que el CSP evite la destrucción no intencionada de datos de control;

c) se requiere que el CSP evite la destrucción incompleta de datos de control;

d) se requiere que el CSP borre cualquier clave específica de los CSC para datos encriptados;

e) se requiere que el CSP destruya copias de datos de control;

f) se requiere que el CSP proporcione una notificación de destrucción de datos de control a los CSC.

En el Cuadro 10-7 se proporciona un resumen de las amenazas de seguridad en la destrucción de datos de control para los requisitos de seguridad.

Cuadro 10-7 – Destrucción de datos de control: cuadro de amenazas de seguridad para requisitos de seguridad

Amenazas de seguridad	Requisitos de seguridad
Robo de identidad	a), b), c), d), e), f)
Vulnerabilidad en sistema operativo	b), c), d), e), f)

10.8 Requisitos de seguridad para copia de seguridad de datos de control

Entre los requisitos de seguridad de los datos para la copia de seguridad de datos de control figuran los siguientes:

a) se requiere que el CSP proporcione métodos de copia de seguridad para evitar la pérdida de datos de control;

b) se requiere que el CSP mantenga la integridad y precisión de datos de control recuperados;

c) se requiere que el CSP soporte el registro y la auditoría de la restauración de datos de control.

En el Cuadro 10-8 se proporciona un resumen de las amenazas de seguridad en la copia de seguridad de datos de control para los requisitos de seguridad.

Cuadro 10-8 – Copia de seguridad de datos de control: cuadro de amenazas de seguridad para requisitos de seguridad

Amenazas de seguridad	Requisitos de seguridad
Vulnerabilidad en sistema operativo	a), b), c)

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.810] Recomendación UIT-T X.810 (1995), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general*.

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

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

[b-UIT-T Y.3502] Recomendación UIT-T Y.3502 (2014), *Tecnología de la información – Computación en la nube – Arquitectura de referencia*.

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

[b-ISO/CEI 19944] ISO/CEI 19944 (2016), *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 – Part 1: Service management system requirements*.

[b-ISO/CEI 27000] ISO/CEI 27000 (2016), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[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*.

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

[b-NIST-SP-800-53] NIST Special Publication 800-53 Rev.3 (2013), *Recommended Security Controls for Federal Information Systems and Organizations*.

[b-NIST-SP-800-125] NIST Special Publication 800-125 (2011), *Guide to Security for Full Virtualization Technologies*.

[b-NIST-SP-800-145] NIST Special Publication 800-145 (2011), *The NIST Definition of Cloud Computing*.

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, 2019