Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1641

(09/2016)

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

Seguridad de la computación en nube – Prácticas óptimas y directrices en materia de seguridad de la computación en nube

Directrices para la seguridad de los datos de cliente de los servicios en la nube

Recomendación UIT-T X.1641

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Recomendaciones relacionadas con la PKI	
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/eurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de eurística 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.1641

Directrices para la seguridad de los datos de cliente de los servicios en la nube

Resumen

La Recomendación UIT-T X.1641 proporciona directrices genéricas para la seguridad de los datos de clientes de servicios en la nube (CSC) en la computación en la nube. Se analiza el ciclo de vida de la seguridad de los datos del CSC y se proponen requisitos de seguridad para cada fase del ciclo de vida de los datos. La Recomendación también proporciona directrices acerca del momento en que debe utilizarse cada uno de los controles para lograr una práctica óptima en materia de seguridad.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1641	2016-09-07	17	11.1002/1000/12853

Términos

Datos de cliente de servicio en la nube, controles de la seguridad de los datos, ciclo de vida de la 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-es.

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/.

© UIT 2017

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

ÍNDICE

Página

1 Alcance 1
2 Referencias 1
3 Definiciones 1
3.1 Términos definidos en otros documentos 1
3.2 Términos definidos en esta Recomendación 3
4 Siglas y acrónimos 3
5 Convenios 3
6 Introducción 3
6.1 Especificación de los datos en esta Recomendación 3
6.2 Amenazas para la seguridad de los datos de clientes de servicios en la nube 4
6.3 Requisitos existentes relativos a la seguridad de los datos 4
6.4 Ciclo de vida de la seguridad de los datos 5
7 Directrices para los controles de seguridad relativos a la seguridad de los datos 6
7.1 Controles de seguridad en la fase de creación 6
7.2 Controles de seguridad en la fase de transmisión 6
7.3 Controles de seguridad en la fase de almacenamiento 6
7.4 Controles de seguridad en la fase de utilización 7
7.5 Controles de seguridad en la fase de migración 7
7.6 Controles de seguridad en la fase de destrucción 7
7.7 Controles de seguridad en la fase de copia de seguridad y recuperación 8
Apéndice I – Directrices para la utilización de controles de seguridad 9
Bibliografía 10

Recomendación UIT-T X.1641

Directrices para la seguridad de los datos de cliente de los servicios en la nube

1 Alcance

En la presente Recomendación se proporcionan directrices para la seguridad de los datos de clientes de servicios en la nube (CSC) en la computación en la nube, en los casos en que el proveedor de servicios en la nube (CSP) es responsable de velar para que el tratamiento de datos se realice con la seguridad adecuada. No siempre es el caso, pues para algunos servicios en la nube, la seguridad de los datos es responsabilidad de los propios CSC. En otros casos, puede existir una responsabilidad compartida.

En algunos casos, por ejemplo, el CSP puede ser responsable de la limitación del acceso a los datos, mientras que el CSC es responsable de decidir qué usuarios del servicio en la nube (CSU) pueden acceder a ellos, y el comportamiento de cada guion o aplicación con los cuales el CSU procesa los datos.

En esta Recomendación se identifican controles de seguridad para los datos de CSC que pueden utilizarse en diferentes fases del ciclo de vida completo de los datos. Estos controles de seguridad pueden diferir cuando cambia el nivel de seguridad de los datos del CSC. La presente Recomendación proporciona, por lo tanto, directrices acerca del momento en que debe utilizarse cada uno de los controles para lograr una práctica óptima de seguridad.

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 X.1631] Recomendación UIT-T X.1631 (2015) | ISO/CEI 27017:2015, *Tecnologías de la información – Técnicas de seguridad – Código de conducta para los controles de seguridad de la información de servicios de computación en la nube basados en ISO ISO/CEI 27002*.

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 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 – Los ejemplos de recursos incluyen: servidores, sistemas operativos, redes, software, aplicaciones y equipos de almacenamiento.

3.1.3 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.

3.1.4 cliente de servicios en la nube [b-UIT-T Y.3500]: parte que mantiene una relación empresarial a los efectos de utilizar servicios en la nube.

NOTA – Una relación empresarial no implica acuerdos económicos.

3.1.5 datos de cliente de servicios en la nube [b-UIT-T Y.3500]: clase de objetos de datos que se controlan por motivos jurídicos o de otra índole, del cliente de servicios en la nube que se registraron en el servicio en la nube, o que son el resultado del ejercicio de las capacidades del servicio en la nube por el cliente de servicios en la nube o en su nombre, por medio de la interfaz publicada del servicio en la nube

NOTA 1 – Un ejemplo de control legal es el derecho de autor.

NOTA 2 – Puede ocurrir que el servicio en la nube contenga u opere sobre datos que no son datos de cliente del servicio en la nube; estos datos pueden ser datos suministrados por el proveedor del servicio en la nube, obtenidos de otra fuente o pueden ser datos de acceso público. Sin embargo, cualquier dato generado por la actuación del cliente en la utilización de las capacidades del servicio en la nube sobre los datos pueden ser datos del cliente del servicio en la nube, según los principios de los derechos de autor, salvo que existan disposiciones específicas contrarias en el acuerdo de servicio en la nube.

3.1.6 datos derivados del servicio en la nube [b-UIT-T Y.3500]: clase de objetos de datos, controlados por el proveedor de servicios en la nube, creados como resultado de la interacción del cliente de servicios en la nube con este servicio en la nube.

3.1.7 proveedor de servicios en la nube [b-UIT-T Y.3500]: parte que ofrece servicios en la nube.

3.1.8 usuario de servicios en la nube [b-UIT-T Y.3500]: persona natural o entidad que actúa en su nombre, relacionado con un cliente de servicios en la nube que utiliza servicios en la nube

NOTA – Ejemplos de estas entidades pueden ser dispositivos o aplicaciones.

3.1.9 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.

3.1.10 multiarrendamiento [b-UIT-T Y.3500]: atribución de recursos físicos y virtuales mediante los cuales varios arrendatarios y sus cálculos y datos están aislados y son inaccesibles por los demás.

3.1.11 plataforma como servicio (PaaS) [b-UIT-T Y.3500]: categoría de servicios en la nube en la que el tipo de capacidades en la nube ofrecidas al cliente de servicios en la nube son capacidades de tipo plataforma.

3.1.12 parte [b-UIT-T Y.3500]: persona física o jurídica, organizada o no, o una agrupación de éstas.

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

3.1.14 titular de la PII [b-ISO/CEI 29100]: persona física con quien está relacionada la información de identificación personal (PII).

NOTA – En función de la jurisdicción y de la legislación sobre privacidad y protección de datos concreta, también puede utilizarse el sinónimo "sujeto de los datos" en vez del término "titular de la PII".

3.1.15 software como servicio (SaaS) [b-UIT-T Y.3500]: categoría de servicio en la nube en la que las capacidades de tipo nube que se ofrecen al cliente de servicios en la nube son capacidades de tipo aplicación

3.1.16 arrendatario [b-UIT-T Y.3500]: uno o varios usuarios de servicios en la nube que comparten acceso a un conjunto de recursos físicos o virtuales

3.1.17 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 esta Recomendación

Ninguno.

4 Siglas y acrónimos

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

CSC Cliente de servicios en la nube

CSP Proveedor de servicios en la nube

CSU Usuario de servicios en la nube

IaaS Infraestructura como servicio

PaaS Plataforma como servicio

PII Información de identificación personal

SaaS Software como servicio

5 Convenios

Ninguno.

6 Introducción

6.1 Especificación de los datos en esta Recomendación

Los datos de CSC incluyen los datos privados de los clientes almacenados en una plataforma en la nube y los datos relacionados con los CSC por servicios en la nube tales como información de la cuenta, registro de entrada y registro de operación.

La diferencia entre los términos CSC (véase 3.1.4) y CSU definido en el párrafo 3 (véase 3.1.8) se amplía tal como se indica a continuación.

El CSC es la persona u organización con quien el CSP establece un acuerdo legal. El CSC puede, por lo tanto, ser una empresa, una subsidiaria, un departamento del gobierno o un consumidor individual.

El CSU es la persona, dispositivo o aplicación que utiliza el servicio en la nube que ha sido contratado. El CSU puede ser un empleado del gobierno, una aplicación que funciona en un teléfono inteligente, un consumidor individual o un miembro de un hogar como un niño. El CSC nombra habitualmente a un CSU para que actúe de administrador y gestione la relación entre el CSC y el CSP. Un CSU siempre actúa en nombre de un CSC. La mayoría de los empleados CSU necesitan poca o ninguna visibilidad sobre las operaciones del CSC y sobre los servicios que el CSC ha contratado, salvo que el CSC decida que deben saberlo (por ejemplo, administradores y auditores internos).

Un CSC puede disponer de múltiples arrendatarios en la nube. Un arrendatario puede contener varios CSU.

6.2 Amenazas para la seguridad de los datos de clientes de servicios en la nube

Como el entorno de servicios en la nube es normalmente de multiarrendamiento, la pérdida o la filtración de datos son una grave amenaza para el CSC. La falta de una gestión adecuada de la información criptográfica como las claves de encriptación, los códigos de autentificación y los privilegios de acceso puede provocar un daño considerable, como la pérdida de datos o su imprevista filtración al exterior. Por ejemplo, los controles insuficientes de autentificación, autorización y auditoría; la utilización arbitraria de claves de encriptación o autentificación; los fallos operativos; los problemas de eliminación; las cuestiones políticas y de jurisdicción; la fiabilidad del centro de datos; y la recuperación en caso de catástrofe pueden identificarse como las principales fuentes de esta amenaza y pueden incluirse en los retos.

Como en el caso de la seguridad de los datos almacenados, como todos los datos de CSC están almacenados en equipos de CSP y los recursos de almacenamiento están compartidos entre varios CSC, pueden existir varios riesgos como, entre otros:

1) alguien interno del propio CSP con privilegios puede acceder sin autorización y dar lugar a una filtración de datos de CSC;
2) usuarios malintencionados o piratas informáticos, pueden también obtener un acceso no autorizado y una filtración de datos de CSC;
3) el flujo de datos transfronterizos puede llevar a filtraciones de datos, en especial de los datos más sensibles;
4) los fallos de software y de hardware, las caídas de alimentación y los desastres naturales pueden también llevar a pérdidas de datos.

La seguridad de los datos reside también en el proceso de transmisión. Los datos pueden ser robados o manipulados durante la transmisión, y provocar una filtración de información privada o confidencial cuando los datos no están adecuadamente encriptados. Si los CSC no adopta mecanismos de encriptación adecuados, los CSP deben verificar la integridad de los datos y adoptar las medidas correspondientes de encriptación.

Otra de las amenazas es la filtración de datos residuales. Cuando un CSC finaliza su servicio, se suprimen sus datos y el espacio de almacenamiento se atribuye o reasigna a otro CSC. Es la responsabilidad del CSP asegurar que los datos residuales de un CSC o arrendatario no pueden ser recuperados por otro.

6.3 Requisitos existentes relativos a la seguridad de los datos

El "marco de seguridad para la computación en la nube" en [UIT-T X.1601] proporciona los requisitos relativos a la seguridad de los datos, incluido el aislamiento de los datos y la protección de la privacidad.

1) Aislamiento de los datos

   En un entorno de computación en la nube, se impide el acceso de un arrendatario a los datos pertenecientes a otro arrendatario, incluso cuando los datos están encriptados, y excepto cuando está autorizado explícitamente. El aislamiento de los datos puede realizarse de manera lógica o física, dependiendo de la granularidad del aislamiento necesario y el despliegue específico de software y hardware de la computación en la nube.

   NOTA – En la computación en la nube, el asilamiento se realiza a nivel de arrendatario. Un CSC en concreto puede tener múltiples arrendatarios en la nube, para poder separar diferentes filiales, divisiones o unidades de negocio.

2) Protección de los datos

   La protección de los datos asegura la adecuada protección de los datos de CSC y los datos derivados del servicio en la nube y que sólo pueden accederse o cambiarse en función de las autorizaciones del CSC (o de acuerdo con la legislación aplicable). Esta protección puede

también incluir una combinación de listas de control de acceso, comprobaciones de integridad, corrección de errores y recuperación de datos, encriptación y otros mecanismos apropiados. Cuando el CSP facilita una encriptación de los datos almacenados a los CSC, esta funcionalidad puede ser una encriptación realizada en el lado del cliente (es decir, en una aplicación del CSP) o una encriptación en el lado del servidor.

3) Protección de la privacidad

La información privada puede contener información de identificación personal (PII) y datos empresariales confidenciales. La recogida, utilización, transferencia, manipulación, almacenamiento y destrucción de información privada pueden estar sujetas a la reglamentación o la legislación. Esta restricción es aplicable a los CSP y sus CSC, es decir, un CSC debe poder ser capaz de suprimir de manera permanente un cuadro de datos que contenga información personal, aunque el CSP no esté al corriente de su contenido. También puede ser necesario que los CSP soporten el tratamiento de la información, por ejemplo, búsquedas de datos del CSC en su forma transformada o encriptada.

La protección de la privacidad se extiende a la información privada que puede observarse y derivarse de las actividades del CSC, tales como tendencias de negocio, relaciones y comunicaciones con otras partes y niveles de actividad o patrones de comportamiento, etc.

La protección de la privacidad también se encarga de asegurar que toda la información privada (incluidos los datos observados y derivados) se utiliza sólo para los fines acordados entre un CSC y un CSP.

Un análisis de los riesgos relativos a la información privada (denominado "análisis de riesgo de la privacidad") puede ayudar a un CSP a identificar los riesgos específicos de vulneración de la privacidad en una operación prevista. El CSP debe identificar y tomar las medidas adecuadas para abordar los riesgos de privacidad identificados en el análisis de riesgo y el tratamiento de información privada.

NOTA – En algunas jurisdicciones, las personas físicas (es decir, seres humanos) se consideran separadamente de sus empleadores a los efectos de la privacidad. En tales circunstancias, la privacidad del CSU se deberá proteger adecuadamente además de proteger al CSC o al arrendatario del servicio en la nube.

6.4 Ciclo de vida de la seguridad de los datos

Sobre la base de la situación real de los servicios en la nube, el ciclo de vida de la seguridad de los datos CSC incluye:

1) Creación: Posiblemente sería mejor utilizar los términos creación/actualización porque se aplica a la creación o la actualización de un elemento de datos o de contenido, no sólo de un documento o una base de datos. La creación es la generación de un nuevo contenido digital o la modificación/actualización de un contenido existente.

2) Transmisión: Proceso de comunicación que transfiere los datos de un emplazamiento a otro.

3) Almacenamiento: Almacenamiento es el acto de introducir los datos digitales en algún tipo de repositorio, y normalmente ocurre simultáneamente con la creación.

4) Utilización: Los datos son examinados, compartidos o utilizados en algún tipo de actividad.

5) Migración: La migración de los datos es el proceso de transferir los datos entre tipos de almacenamiento, formatos o sistemas informáticos. Es un elemento fundamental de cualquier implementación, actualización o combinación de sistema. La migración de los datos ocurre por múltiples razones que incluyen: la sustitución o mejora de los equipos servidores o de almacenamiento, la combinación de sitios web, el mantenimiento de servidores y la reubicación de centros de datos.

6) Destrucción: Se destruyen los datos permanentemente utilizando medios físicos o digitales (como criptotrituradoras).

7) Copia de seguridad y recuperación: Los usuarios pueden crear copias de seguridad de los datos y recuperar los datos a partir de las copias de seguridad.

7 Directrices para los controles de seguridad relativos a la seguridad de los datos

En este apartado se describen directrices para los controles de seguridad relativos a las fases del ciclo de vida descritas en el punto 6.4.

7.1 Controles de seguridad en la fase de creación

Las directrices para los controles de seguridad en la fase de creación incluyen lo siguiente:

a) Los CSP deben definir los niveles de sensibilidad de los datos. El marcado de los datos por el usuario puede utilizarse para ayudar a clasificar los datos.

b) Los datos deben clasificarse de acuerdo con su sensibilidad cuando se crean.

c) Los CSP deben considerar la utilización de mecanismos de derechos digitales de empresa o de encriptación para la protección de los accesos no autorizados.

7.2 Controles de seguridad en la fase de transmisión

Las directrices para los controles de seguridad en la fase de transmisión incluyen lo siguiente:

a) Los CSP deben utilizar métodos tecnológicos para asegurar la seguridad de los datos de autentificación.

b) Los CSP deben soportar a los usuarios para asegurar que se mantiene una transmisión segura de datos críticos de la operación y de datos de gestión.

c) Los daños a la integridad de los datos deben detectarse con prontitud durante la transmisión, y deben adoptarse las medidas necesarias para restaurar la integridad de los datos tras la detección de errores.

7.3 Controles de seguridad en la fase de almacenamiento

Las directrices para los controles de seguridad en la fase de almacenamiento incluyen:

a) Los CSP deben identificar controles de acceso, como los definidos en [UIT-T X.1631], para su utilización por los CSC con los datos de usuario de los repositorios de almacenamientos.

b) Los CSP deben utilizar tecnología de encriptación u otras medidas de protección para velar por la privacidad del almacenamiento de los datos de autentificación.

c) Los CSP deben soportar a los usuarios para mantener la privacidad del almacenamiento de los datos de operación críticos y datos de gestión.

d) Los CSP deben proporcionar métodos eficaces de protección de los discos duros o adoptar mecanismos de almacenamiento fragmentado para prevenir que usuarios no autorizados consigan datos válidos del disco duro incluso en caso de robo.

e) Los daños a la integridad de los datos deben detectarse con prontitud y deben adoptarse las medidas necesarias para restaurar la integridad de los datos después de la detección de errores.

f) Debe soportarse la configuración opcional por el usuario de parámetros de encriptación, como algoritmos, intensidad y esquemas.

g) Los CSP deben soportar a los usuarios en la elección de un mecanismo de encriptación de terceros para encriptar los datos de la clave.

h) Los CSP deben soportar la encriptación de datos mediante claves seguras, así como el almacenamiento y el mantenimiento local de las claves seguras.

i) Los CSP deben proporcionar métodos eficaces de protección contra la descarga de archivos imagen de las máquinas virtuales para prevenir que usuarios no autorizados puedan ejecutarlas en sus propios recursos de computación desde el disco duro incluso en caso de robo.

7.4 Controles de seguridad en la fase de utilización

Las directrices para los controles de seguridad en la fase de utilización incluyen lo siguiente:

a) Los CSP deben autorizar y verificar la utilización de los datos.

b) Debe controlarse la utilización de los datos sensibles y generarse registros de auditoria.

c) Los CSP deben supervisar la actividad maliciosa y utilizar mecanismos de vigilancia, de acuerdo con su responsabilidad y derechos, para descubrir las amenazas y controlar la utilización de los datos.

7.5 Controles de seguridad en la fase de migración

Las directrices para los controles de seguridad en la fase de migración incluyen lo siguiente:

a) Se debe evaluar la conectividad de la red antes de la migración de los datos para asegurar la seguridad del proceso de migración.

b) Los CSP deben asegurar que la integridad y la privacidad de los datos no se ve afectada durante una migración.

c) Los CSP deben asegurar que la migración de los datos no afecta a la continuidad de los servicios y las aplicaciones.

d) Los CSP deben realizar copias de seguridad y efectuar el trabajo correspondiente de recuperación de manera adecuada durante la migración de los datos.

e) Como preparación para la migración de datos, los CSP deben establecer un esquema de migración, evaluar su viabilidad y riesgos conexos y desarrollar, en consecuencia, las medidas de control de riesgos.

7.6 Controles de seguridad en la fase de destrucción

Las directrices para los controles de seguridad en la fase de destrucción incluyen lo siguiente:

a) Los CSP deben ser capaces de borrar todo el material de las claves utilizadas para la encriptación de los datos.

b) Los CSP deben utilizar la destrucción física, como la desmagnetización de los medios físicos, cuando desmantela hardware de almacenamiento.

c) Los CSP deben utilizar técnicas de recuperación de datos para confirmar los procesos de destrucción.

d) Los CSP deben poder proporcionar los medios adecuados para ayudar a eliminar datos preexistentes tras la migración de los datos entre diferentes plataformas de computación en la nube, la terminación del servicio y del contrato, y en caso de catástrofe natural.

e) Los CSP deben proporcionar los medios para eliminar todas las copias de los datos.

f) Los CSP deben asegurar que el espacio de almacenamiento de la información de autentificación como la identificación de la cuenta de usuario y contraseña no va a liberarse o reasignarse a otros usuarios antes de borrar totalmente la información.

g) Los CSP deben asegurar que el espacio de almacenamiento de recursos como archivos, directorios, y registros de bases de datos no va a liberarse o a reasignarse a otros usuarios antes de borrar totalmente la información.

h) Los CSP deben proporcionar medios para impedir la recuperación de datos destruidos.

7.7 Controles de seguridad en la fase de copia de seguridad y recuperación

Las directrices para los controles de seguridad en la fase de copia de seguridad y recuperación incluyen lo siguiente:

a) Los CSP deben utilizar mecanismos de recuperación de contenidos, como los de prevención de la pérdida de datos para ayudar a identificar y auditar los datos que necesitan una copia de seguridad.

b) Los CSP deben soportar un algoritmo de encriptación adecuado para la copia de seguridad de larga duración de los medios de almacenamiento (archivado), como la utilización de claves de encriptación largas y la planificación de su sustitución por un algoritmo de encriptación mejorado.

c) Los CSP deben proporcionar funciones de copia de seguridad local y de recuperación de datos. Deben realizarse copias de seguridad completas al menos una vez por semana y la copia de seguridad incremental al menos una vez al día.

d) El centro remoto de recuperación de catástrofes debe establecerse con todas las funcionalidades como líneas de comunicaciones, equipos de red y equipos de procesamiento de datos necesarios para la recuperación en caso de catástrofe, incorporadas.

e) Puede establecerse un centro de recuperación redundante para casos de catástrofe. Debe proporcionar la capacidad equivalente básica de operación del negocio y sincronizar los datos en tiempo real mediante un enlace de alta velocidad. Debería poder compartir las operaciones de los sistemas de negocio y de gestión. Así como mantener la continuidad del negocio con un equipo de conmutación de emergencia. en caso de catástrofe.

f) Para los datos clasificados como importantes o sensibles, los CSP debe proporcionar las funcionalidades de copia de seguridad remota junto con la capacidad de recuperación rápida de datos. Un enfoque para proporcionar este servicio podría ser una red que utilice un centro de recuperación en caso de catástrofe.

Apéndice I

Directrices para la utilización de controles de seguridad

(Este apéndice no forma parte integrante de la presente Recomendación.)

El Cuadro I.1 proporciona ejemplos de conjuntos de controles que pueden utilizarse para seguir las directrices para algunos casos ejemplo de datos, en función de la clasificación de los datos y de la fase del ciclo de vida.

Cuadro I.1 - Ejemplos de conjuntos de controles

Ciclo de vida de los datos / Tipo	**Creación**	**Transmisión**	**Almacena-miento**	**Utilización**	**Migración**	**Destrucción**	**Copia de seguridad y recuperación**
IaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e), h), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), c), d), e), f)
PaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e), f), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), b), c), d), e), f)
SaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e),f), g), h), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), b), c), d), e), f)

Bibliografía

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

[b-ISO/CEI 27000] ISO/CEI 27000:2014, *Information technology – Security techniques - Information security management systems – Overview and vocabular* .

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

[b-NIST-SP-800-53] Publicación especial 800-53 Revisión 4 del NIST (2015), *Security and privacy controls for Federal information systems and organizations*. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

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 de otros 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	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
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 los sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2017