Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1601

(01/2014)

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

Seguridad de la computación en nube – Visión general de la seguridad de la computación en nube

Marco de seguridad para la computación en la nube

Recomendación UIT-T X.1601

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

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

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

Recomendación UIT-T X.1601

Marco de seguridad para la computación en la nube

Resumen

La Recomendación UIT-T X.1601 describe el marco de seguridad para la computación en la nube. Esta Recomendación analiza las amenazas y los problemas de seguridad en el contexto de la computación en la nube y describe las capacidades de seguridad que podrían mitigar estas amenazas y resolver los problemas de seguridad. Se facilita una metodología marco para determinar qué capacidades de seguridad se han de especificar para mitigar las amenazas y resolver los problemas de seguridad en la computación en la nube. En el Apéndice I se facilita una tabla de correspondencia entre cada amenaza o problema de seguridad y la capacidad o capacidades correspondientes que lo abordan.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1601	2014-01-24	17	11.1002/1000/12036

Palabras clave

Amenazas de seguridad, capacidades de seguridad, computación en la nube, marco de seguridad, problemas de seguridad, protección de la privacidad.

* 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.1601

Marco de seguridad para la computación en la nube

1 Ámbito de aplicación

Esta Recomendación analiza las amenazas y los problemas de seguridad en el contexto de la computación en la nube y describe las capacidades de seguridad que podrían mitigar estas amenazas y resolver los problemas de seguridad. Se facilita una metodología marco para determinar qué capacidades de seguridad se han de especificar para mitigar las amenazas y resolver los problemas de seguridad en la computación en la nube.

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/IEC 19440]: cualidad de poder realizar una determinada actividad.

3.1.3 controlador de datos [b-key definition]: persona que (sola o en colaboración con otras) determina la finalidad y la manera en que se procesan o se han de procesar los datos personales.

3.1.4 procesador de datos [b-key definition]: en relación con los datos personales, se refiere a cualquier persona (distinta del empleado del controlador de datos) que procesa los datos en nombre del controlador de datos.

3.1.5 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.

3.1.6 información de identificación personal [b-ISO/IEC 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.

3.1.7 dominio de seguridad [b-ITU-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.

3.1.8 incidente de seguridad [b-ITU-T E.409]: cualquier evento adverso que podría amenazar algún aspecto relacionado con la seguridad.

3.1.9 Acuerdo de nivel de servicio (SLA) [b-ISO/IEC 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.

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

3.1.11 máquina virtual (VM) [b-NIST-SP-800-145]: duplicado lógico, aislado y eficiente de una máquina real.

3.1.12 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 la presente Recomendación se definen los siguientes términos:

3.2.1 computación en la nube: paradigma para dar acceso a la red a un conjunto elástico y ampliable de recursos físicos o virtuales con administración y configuración autoservicio previa solicitud.

3.2.2 servicio en la nube: una o varias capacidades que se ofrecen mediante computación en la nube (cláusula 3.2.1) a la que se accede con una interfaz declarada.

3.2.3 cliente del servicio en la nube: parte (cláusula 3.2.12) que mantiene una relación comercial a los efectos de servicios en la nube (cláusula 3.2.2).

3.2.4 asociado del servicio en la nube: una entidad que colabora o asiste en actividades del proveedor de servicios en la nube (cláusula 3.2.5) o del cliente del servicio en la nube (cláusula 3.2.3).

3.2.5 proveedor de servicios en la nube: una parte (3.2.12) que ofrece servicios en la nube (cláusula 3.2.2).

3.2.6 usuario del servicio en la nube: una persona que es cliente del servicio en la nube (cláusula 3.2.3) que utiliza servicios en la nube (cláusula 3.2.2).

3.2.7 comunicaciones como servicio (CaaS): categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube (cláusula 3.2.3) una capacidad de comunicación y colaboración en tiempo real.

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

3.2.8 nube comunitaria: modelo de implantación en la nube compartido y destinado exclusivamente a un grupo específico de clientes del servicio en la nube (cláusula 3.2.3) y cuyos recursos controla al menos un miembro de ese grupo.

NOTA – Los requisitos de compartición comprenden consideraciones tales como el cometido, la seguridad de la información, la política y la observancia.

3.2.9 infraestructura como servicio (IaaS): categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube (cláusula 3.2.3) un tipo de capacidades de infraestructura.

NOTA – El cliente de servicio en la nube (cláusula 3.2.3) 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 (cláusula 3.2.3) también puede tener limitaciones para controlar ciertos componentes de red (por ejemplo, cortafuegos centrales).

3.2.10 multidivisión: atribución de recursos físicos y virtuales mediante los cuales varios arrendatarios (cláusula 3.2.18) y sus cálculos y datos están aislados y son inaccesibles por los demás.

3.2.11 red como servicio (NaaS): categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube (cláusula 3.2.3) conectividad de transporte y sus correspondientes capacidades de red.

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

3.2.12 parte: persona física u organización.

3.2.13 plataforma como servicio (PaaS): categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube (cláusula 3.2.3) un tipo de capacidades de plataforma.

3.2.14 nube privada: modelo de implantación en la nube destinado exclusivamente a un solo cliente del servicio en la nube (cláusula 3.2.3) y cuyos recursos controla dicho cliente.

3.2.15 nube pública: modelo de implantación en la nube que está potencialmente disponible para cualquier cliente del servicio en la nube (cláusula 3.2.3) y cuyos recursos controla el proveedor de servicio en la nube (cláusula 3.2.5).

3.2.16 problema de seguridad: "dificultad" de seguridad diferente a una amenaza de seguridad directa que se debe a la naturaleza y al entorno de funcionamiento de los servicios en la nube, incluidas las amenazas "indirectas". Véanse las cláusulas 7 y 8.

3.2.17 software como servicio (SaaS): categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube (cláusula 3.2.3) un tipo de capacidades de aplicación.

3.2.18 división: grupo de usuarios del servicio en la nube (cláusula 3.2.6) que comparten acceso a un conjunto de recursos físicos y virtuales.

NOTA – Por regla general, en un contexto multidivisión (cláusula 3.2.10), todos los integrantes del grupo de usuarios del servicio en la nube (cláusula 3.2.6) que constituye una división pertenecerán a la misma organización cliente del servicio en la nube (cláusula 3.2.3). Puede haber casos en los que el grupo de usuarios del servicio en la nube (cláusula 3.2.6) sean clientes diferentes, especialmente en el caso de una nube comunitaria (cláusula 3.2.8), pero se trata de excepciones especializadas. Sin embargo, una determinada organización cliente del servicio en la nube (cláusula 3.2.3) puede tener diferentes divisiones con un mismo proveedor de servicio en la nube (cláusula 3.2.5), que quizá representan diferentes grupos administrativos dentro de la organización (por ejemplo, ventas y contabilidad), dado que puede haber buenas razones para mantener separados los datos y las actividades que pertenecen a distintos grupos por motivos administrativos y comerciales.

4 Siglas y acrónimos

En la presente Recomendación se utilizan los siguientes siglas 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*)

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

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

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

TIC Tecnología de la información y la comunicación

IP Protocolo Internet (*Internet protocol*)

TI Tecnología de la información

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*)

IIP Información de identificación personal

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*)

VM Máquina virtual (*virtual machine*)

5 Convenios

Ninguno.

6 Generalidades

La computación en la nube es un paradigma que permite ofrecer acceso en red práctico y por demanda a un conjunto compartido de recursos configurables (como, por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios), acceso que se puede suministrar y liberar rápidamente con una mínima gestión o interacción con el proveedor de servicio. Los clientes de la computación en la nube pueden emplear estos recursos para desarrollar, albergar y ejecutar servicios y aplicaciones a la carta de manera flexible utilizando cualquier dispositivo, en todo momento y desde cualquier lugar en el contexto de la computación en la nube. Los servicios de computación en la nube se suelen suministrar en ciertas categorías de servicio, por ejemplo, infraestructura como servicio (IaaS), plataforma como servicio (PaaS), software como servicio (SaaS), red como servicio (NaaS), etc. Estas categorías de servicio permiten a los clientes de la computación en la nube lanzar o modificar su negocio fácil y rápidamente sin tener que crear nuevos sistemas ni infraestructura de tecnología de la información y la comunicación (TIC), y gestionar los recursos con arreglo a las necesidades. Por ejemplo, algunos proveedores de servicios en la nube (CSP) pueden ofrecer recursos hardware y software desvinculados en forma de servicio (por ejemplo, IaaS o NaaS). Otros proveedores de servicios ofrecen plataformas (PaaS) o aplicaciones (SaaS) específicas de la nube para que los clientes y asociados puedan desarrollar y ofrecer rápidamente nuevas aplicaciones que se pueden configurar y utilizar a distancia.

La adopción de computación en la nube conlleva amenazas y problemas de seguridad; los requisitos de seguridad varían sobremanera en función de los modelos y las categorías de servicio de computación en la nube. La computación en la nube es inherentemente más vulnerable a amenazas externas e internas que otros paradigmas, debido a su naturaleza distribuida y multipartita, al predominio del acceso a distancia a sus servicios y al número de entidades que intervienen en cada proceso. Es posible mitigar muchas de las amenazas de seguridad mediante la aplicación de procesos y mecanismos de seguridad tradicionales. La seguridad incide y repercute en muchas partes del servicio de computación en la nube. Por ese motivo, la gestión de la seguridad de los servicios de computación en la nube, así como de los recursos afines, es un aspecto fundamental.

Antes de realizar la transición del sistema TIC a la computación en la nube, es preciso determinar las amenazas (véase la cláusula 7 *infra*) y los problemas (cláusula 8) de seguridad del posible cliente del servicio en la nube (CSC).

A partir de dichos problemas y amenazas, se determina el conjunto de capacidades de seguridad de alto nivel (véase la cláusula 9). Los requisitos específicos de estas capacidades quedan fuera del alcance de la presente Recomendación, pero tendrán que determinarse en cada caso concreto de servicio de computación en la nube, de acuerdo con el análisis del riesgo que entrañan las amenazas y dificultades identificadas.

Basándose en el análisis del riesgo, un CSC puede determinar si adopta o no la computación en la nube y tomar una decisión informada acerca de los proveedores y la arquitectura. Este análisis del riesgo debe llevarse a cabo utilizando un margo de gestión de riesgos de seguridad de la información (por ejemplo, el definido en [b-ISO/IEC 27005]). En la cláusula 10 se sugiere una metodología marco.

En la presente Recomendación se distingue entre amenazas y problemas de seguridad. Las amenazas de seguridad son las que guardan relación con ataques (activos y pasivos) y fallos o catástrofes ambientales. Los problemas de seguridad son los que surgen debido a la naturaleza y el entorno de funcionamiento de los servicios en la nube. Cuando no se resuelven debidamente, los problemas de seguridad dejan puertas abiertas a las amenazas.

A tenor de estos problemas y amenazas de seguridad, se describen las capacidades de seguridad para mitigar las amenazas y resolver los problemas relacionados con la seguridad de la computación en la nube.

7 Amenazas de seguridad en la computación en la nube

Las amenazas pueden dañar activos tales como la información, los procesos y los sistemas y, por ende, perjudicar a las organizaciones. Pueden ser de origen natural o humano, ya sea accidental o deliberado. Su procedencia puede ser interna o externa a la organización. Así, las amenazas pueden clasificarse en accidentales o deliberadas y en activas o pasivas.

Los tipos de amenazas en concreto que pueden surgir dependen mucho del servicio en la nube específico. Por ejemplo, en el caso de una nube pública, las amenazas pueden ser consecuencia de la división de responsabilidades entre el CSC y el CSP: lo complejo que resulta especificar la jurisdicción sobre datos y procesos, lo coherente y adecuada que sea la protección de los datos, el mantenimiento de la privacidad, etc. Ahora bien, en el caso de una nube privada, las amenazas son más fáciles de controlar dado que el CSC controla todos las divisiones que aloja el CSP. Aun cuando algunas de las amenazas identificadas en la presente Recomendación ya se estudian en otros documentos de la industria (por ejemplo, la Recomendación UIT-T X.800), todas las amenazas atañen a la computación en la nube. La posibilidad de aplicar una determinada amenaza depende del servicio en la nube específico.

En la presente cláusula se describen las distintas amenazas de seguridad que pueden producirse en el contexto de la computación en la nube.

7.1 Amenazas de seguridad al cliente de computación en la nube (CSC)

Las amenazas que se indican a continuación son las que afectan directamente a los CSC, ya sea a sus intereses personales o comerciales, o a su privacidad, legalidad o seguridad. No todos los CSC correrán riesgo de todas las amenazas. El riesgo dependerá de la naturaleza del CSC y del servicio de computación en la nube empleado. Por ejemplo, un servicio en la nube dedicado a la transcodificación de ficheros de vídeo comerciales no tendrá necesidad de proteger la información de identificación personal (IIP), pero sí tendrá que cumplir requisitos muy estrictos de protección de activos digitales.

7.1.1 Pérdida y filtración de datos

Dado que el entorno del servicio en la nube suele ser multipartito, la pérdida o filtración de datos es una grave amenaza para los CSC. Una falta de gestión adecuada de información criptográfica, como

las claves de encriptación, los códigos de autentificación y los 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, y pueden estar relacionadas con los problemas descritos en las cláusulas 8.1.2 "Pérdida de confianza", 8.1.3 "Falta de gobernanza" y 8.1.4 "Pérdida de privacidad".

7.1.2 Acceso inseguro al servicio

Las credenciales de identidad, incluso las de los administradores del CSC, son especialmente vulnerables a los usuarios no autorizados en el entorno sumamente distribuido de la computación en la nube, puesto que a diferencia de las telecomunicaciones tradicionales resulta difícil basarse en la ubicación (por ejemplo, cable telefónico) o en la presencia de un equipo físico concreto (por ejemplo, un módulo de identificación del abonado móvil (SIM)) para reforzar la autentificación de la identidad. Dado que la mayoría de los servicios se ofrecen a distancia, las conexiones desprotegidas están expuestas a posibles vulnerabilidades. Aun cuando las conexiones estén protegidas o sean locales, pueden funcionar otros métodos de ataque (como la *peska*, el fraude, la ingeniería social y la explotación de vulnerabilidades del software). Si el que perpetra el ataque consigue obtener las credenciales del usuario o administrador, puede espiar actividades y transacciones, manipular datos, remitir información falsificada, y desviar a los clientes CSC a sitios ilegítimos. A menudo, las contraseñas se reutilizan para varios sitios web y servicios, lo que amplifica el impacto de tales ataques, ya que al ganar acceso a un servicio quedan expuestos varios. Por otra parte, las soluciones de computación en la nube añaden una nueva amenaza al panorama. La cuenta del CSC o las instancias del servicio pueden convertirse en una nueva brecha para el atacante. A partir de ese punto, el atacante puede aprovechar la reputación y los recursos del CSC para lanzar nuevos ataques.

7.1.3 Amenazas internas

Siempre que intervienen seres humanos existe el riesgo de que actúen de manera incompatible con la seguridad del servicio. Los empleados CSC que comparten contraseñas de "administrador" o que no protegen las credenciales (por ejemplo, dejan notas pegadas en la pantalla), son descuidados o 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.

7.2 Amenazas de seguridad al proveedor del servicio en la nube (CSP)

En esta cláusula se indican las amenazas que afectan directamente a los CSP. Éstas pueden afectar a la capacidad de un CSP de ofrecer servicios, hacer negocio, conservar a sus clientes o de evitar problemas jurídicos o reglamentarios. Las amenazas a un determinado CSP también dependen de su contexto y oferta de servicios concretos.

7.2.1 Acceso con derechos de administración no autorizado

El servicio de computación en la nube consta de interfaces y componentes software que permiten al propio personal del CSC administrar aquellos aspectos del servicio de computación en la nube que están bajo su control, además de crear y suprimir cuentas de empleados del CSC y conexiones al servidor del CSC, modificar la capacidad del servicio, actualizar las entradas al sistema de nombres de dominio (DNS) y los sitios web, etc. Los atacantes tienen predilección por esas interfaces de administración, que les permite hacerse pasar por administradores del CSC para atacar a un CSP. Como esos servicios de computación en la nube tienen que ser accesibles por el personal del CSC, la protección de estos servicios se ha convertido en un motivo de gran preocupación para la seguridad de la computación en la nube.

7.2.2 Amenazas internas

Siempre que intervienen seres humanos existe el riesgo de que se comporten de manera descuidada o de mala fe poniendo en peligro la seguridad del servicio.

Los empleados CSC que comparten contraseñas de "administrador" o que no protegen las credenciales (por ejemplo, dejan notas pegadas en la pantalla), son descuidados o carecen de la formación adecuada, o los empleados descontentos que actúan de mala fe, siempre representan una amenaza considerable para cualquier negocio.

Los CSP, en particular, tienen que tomarse muy en serio el tema de la confianza en sus empleados. Aun cuando se haya realizado un escrutinio de los empleados, siempre existe el riesgo de que un hábil intruso obtenga un puesto en el centro de datos del CSP. Este tipo de intrusos puede tener como objetivo perjudicar al CSP o quizá tratar de introducirse en sistemas CSC específicos a los que éste da servicio, especialmente si el CSC es una empresa muy conocida o un organismo gubernamental.

8 Problemas de seguridad en la computación en la nube

Además de las amenazas de seguridad debidas a la naturaleza y al entorno de funcionamiento de los servicios en la nube, existen otros problemas de seguridad, en particular las amenazas "indirectas". Por amenaza indirecta se entiende la amenaza a un participante que puede tener consecuencias negativas para otros.

Cuando no se resuelven debidamente, los problemas de seguridad identificados en esta Recomendación pueden dejar una puerta abierta a las amenazas. Es indispensable tener en cuenta estos problemas al examinar los servicios de computación en la nube.

8.1 Problemas de seguridad al cliente de computación en la nube (CSC)

En esta cláusula se describen los problemas de seguridad relacionados con las dificultades contextuales o amenazas indirectas que pueden surgir como consecuencia de amenazas directas a los intereses del CSC.

8.1.1 Ambigüedad en las responsabilidades

Los CSC utilizan recursos de diferentes categorías de servicio y modelos de instalación. Así, los sistemas TIC creados por el cliente se basan en estos servicios. Si las responsabilidades entre los CSC y los CSP no se definen claramente, pueden aparecer conflictos conceptuales y operativos. Toda incoherencia contractual de los servicios prestados podrá producir anomalías o incidentes. Por ejemplo, a escala internacional resulta difícil definir qué entidad actúa de controlador y cuál de procesador de datos, aun cuando si el carácter internacional se reduce a un tercero fuera de la región del caso, como en la Unión Europea.

Debido a los requisitos jurídicos y reglamentarios, cualquier duda a este respecto (por ejemplo, si un determinado CSC o CSP es el "controlador de datos" o el "procesador de datos") puede implicar que haya ambigüedad en lo que respecta a qué reglamento hay que aplicar. Si esta interpretación varía según la jurisdicción, puede suceder que el CSC o el CSP tengan que aplicar reglamentos divergentes al mismo servicio o tipo de datos.

8.1.2 Pérdida de confianza

A veces resulta difícil al CSC reconocer su nivel de confianza del CSP debido a la característica de caja negra de la computación en la nube. Si no hay forma de obtener y compartir el nivel de seguridad del proveedor de manera normalizada, los CSC no disponen de ningún mecanismo para evaluar el nivel de seguridad que ofrece el proveedor. Para algunos CSC el hecho de no poder compartir el nivel

de seguridad del CSP podría representar una grave amenaza de seguridad cuando utilizan los servicios de computación en la nube.

8.1.3 Pérdida de gobernanza

La decisión del CSC de migrar una parte de su sistema TIC a infraestructura de computación en la nube implica traspasar una parte del control a un CSP. Esto podría representar una grave amenaza a los datos del CSC, especialmente en lo que respecta al papel y privilegio asignados al proveedor. Si ello se suma a la falta de transparencia en las prácticas del proveedor del servicio de computación en la nube, el proceso podría derivar en una mala configuración e incluso en ataques internos malignos.

Al adoptar servicios de computación en la nube, algunos CSC puede preocuparse por la falta de control sobre su información y activos alojados en el CSP, el almacenamiento de datos, la fiabilidad de las copias de seguridad (problemas de retención de datos), las contramedidas para los planes de continuidad de actividades (BCP), la recuperación en caso de catástrofe, etc.

Por ejemplo:

- Un CSC desea suprimir un fichero por motivos legales, pero el CSP mantiene una copia sin que el primero lo sepa.
- Un CSP confiere privilegios de administrador del CSC que no son compatibles con la política de este último.
- Algunos CSC pueden inquietarse por los datos que un CSP expone a gobiernos extranjeros, que podría afectar al cumplimiento de la normativa en materia de privacidad del CSC, como en el caso de las directivas de protección de datos de la Unión Europea.

8.1.4 Pérdida de privacidad

Cuando un CSP procesa la información privada, puede suceder que infrinja la reglamentación o legislación en materia de privacidad. Por ejemplo, puede filtrar información privada o procesar dicha información para un fin que no está autorizado por el CSC y/o el propietario de los datos.

8.1.5 Indisponibilidad del servicio

La disponibilidad no es un aspecto específico de la computación en la nube. Sin embargo, dado el principio de diseño orientado al servicio, la prestación de éste puede verse afectada cuando los servicios de computación en la nube no están totalmente disponibles. Por otra parte, la dependencia dinámica de la computación en la nube ofrece más posibilidades para el atacante. Por ejemplo, un ataque de denegación de servicio a un servicio puede afectar a todos los servicios en la cadena descendente del mismo sistema de computación en la nube.

8.1.6 Dependencia del proveedor de servicios en la nube

Depender mucho de un mismo CSP hace que sea más difícil cambiar de CSP, sobre todo cuando dicho CSP utiliza funciones y formatos no normalizados y no ofrece un servicio de compatibilidad. Esta dependencia puede convertirse en una amenaza a la seguridad si el CSP no resuelve las vulnerabilidades de seguridad, por cuando el CSC será vulnerable y no podrá migrar a otro CSP.

8.1.7 Apropiación indebida de propiedad intelectual

Cuando se ejecuta código de un CSC o el CSP almacena otros activos, existe la posibilidad de que ese material se filtre a un tercero o se utilice indebidamente sin autorización. Dicha utilización podría implicar una infracción del derecho de autor o la revelación de secretos comerciales.

8.1.8 Pérdida de integridad del software

Una vez que el código del CSC se está ejecutando en el CSP, existe la posibilidad de que sea modificado o infectado cuando está fuera del control directo del CSC, lo que en cierto modo lo haría funcionar mal. Aunque esta posibilidad esté fuera de control del CSC, podría afectar gravemente a su reputación y, por ende, a su negocio.

8.2 Problemas de seguridad para los proveedores de servicio en la nube (CSP)

En esta cláusula se describen los problemas de seguridad relacionados con las dificultades contextuales o amenazas indirectas que pueden dar lugar a amenazas más directas a los intereses del CSP.

8.2.1 Ambigüedad en las responsabilidades

En el sistema de computación en la nube se pueden definir diferentes funciones (CSP, CSC y asociado en el servicio en la nube (CSN)). La ambigüedad en la definición de responsabilidades sobre asuntos tales como la propiedad de los datos, el control de acceso o el mantenimiento de infraestructura puede afectar al negocio o dar lugar a litigios legales (especialmente cuando se trata con terceros, o cuando el CSP es a su vez un CSC o un CSN). Este riesgo de ambigüedad aumenta cuando el CSP actúa y/o ofrece servicios en diversas jurisdicciones, donde los contratos y acuerdos están en idiomas y marcos jurídicos diferentes. Véase también la cláusula 8.2.4, "Conflictos jurisdiccionales".

8.2.2 Contexto compartido

La computación en la nube permite ahorrar costes gracias a la compartición masiva de recursos a escala muy grande. Esta situación conlleva muchas interfaces potencialmente vulnerables. Por ejemplo, varios CSC diferentes consumen simultáneamente servicios en la misma nube. Así, el CSC podría tener acceso autorizado a las máquinas virtuales de otras divisiones, o a su tráfico de red, datos reales/residuales, etc. Este acceso no autorizado o malintencionado a los activos de otro CSC puede poner en peligro la integridad, disponibilidad y confidencialidad.

Por ejemplo, varias máquinas virtuales alojadas en un mismo servidor comparten la CPU (unidad de procesamiento central) y los recursos de memoria, que están virtualizados por el hipervisor. En este ejemplo, si se produce un fallo en los mecanismos de aislamiento del hipervisor, se podrá obtener acceso no autorizado a la memoria o a los datos almacenados en otras máquinas virtuales.

8.2.3 Incoherencia y conflictos en los mecanismos de protección

Debido a la arquitectura descentralizada de la infraestructura de computación en la nube, los módulos de seguridad distribuidos pueden tener mecanismos de protección incoherentes. Por ejemplo, un módulo de seguridad puede negar el acceso y otro concederlo. Esta incoherencia puede causar problemas a un usuario autorizado, y puede explotarlas un atacante, comprometiendo así la confidencialidad, la integridad y la disponibilidad.

8.2.4 Conflictos jurisdiccionales

Los datos en la nube pueden trasladarse entre centros de datos o incluso a través de las fronteras internacionales. Los datos se regirán por las distintas jurisdicciones aplicables, dependiendo del país. Por ejemplo, en algunas jurisdicciones, como en la Unión Europea, se exige una gran protección de la información de identificación personal, que por lo general no pueden procesarse en lugares donde no se garantice un nivel de protección suficiente. Como segundo ejemplo puede citarse las jurisdicciones donde las comunicaciones como servicio (CaaS) se considera un servicio de información desregulado, mientras que en otras se regula como un servicio telefónico. Este conflicto jurisdiccional puede dar lugar a complicaciones jurídicas.

8.2.5 Evolución de los riesgos

Una de las ventajas de la computación en la nube es que al diseñar el sistema se pueden aplazar algunos aspectos hasta la fase de ejecución. Esto significa que algunos componentes de software dependientes se pueden seleccionar y utilizar sólo cuando la función que las necesita se haya ejecutado. Sin embargo, la metodología convencional de análisis de riesgos ya no puede adaptarse a este tipo de sistemas de evolución dinámica. Un sistema que haya pasado la evaluación de seguridad en la fase de diseño puede presentar nuevas vulnerabilidades que aparecen durante su vida útil debido a los cambios en los componentes de software.

8.2.6 Migración e integración deficientes

La migración a la nube implica a menudo mover grandes volúmenes de datos e introducir grandes cambios en la configuración (por ejemplo, direcciones de red). La migración de una parte del sistema TIC a un CSP externo puede requerir cambios sustanciales en el diseño del sistema (por ejemplo, en la red y en las políticas de seguridad). Una integración deficiente debido a interfaces incompatibles o una aplicación de políticas incoherente puede tener consecuencias funcionales y no funcionales. Por ejemplo, las máquinas virtuales que funcionan detrás del cortafuegos en un centro de datos privado pueden quedar accidentalmente expuestas a Internet abierta en la nube del CSP.

8.2.7 Discontinuidad de actividades

La computación en la nube asigna recursos y los ofrece como servicio. Todo el ecosistema de la computación en la nube está constituido por muchas partes interdependientes. La discontinuidad de una parte (por ejemplo, un apagón, un ataque de denegación del servicio o un retraso) puede afectar a la disponibilidad del servicio de computación en la nube, como se indica en la cláusula 8.1.5 "Indisponibilidad del servicio", y por tanto causar una discontinuidad de actividades.

8.2.8 Dependencia del asociado de servicios en la nube

La plataforma del CSP se basa en utilizar componentes software y hardware de varios proveedores. Algunos componentes pueden incluir funciones o extensiones patentadas que son útiles para el CSP. Ahora bien, confiar en estas funciones patentadas limita la capacidad del CSP de migrar a otro proveedor de componentes.

Si bien esta dependencia es un problema empresarial, no constituye propiamente dicho una amenaza a la seguridad. Ahora bien, a veces puede suscitar inquietudes de seguridad. Por ejemplo, si el CSN que suministra componentes esenciales abandona el mercado, es posible que ya no se disponga de más parches de seguridad. Cuando surge una vulnerabilidad en un componente, puede resultar difícil u oneroso reducir el riesgo.

8.2.9 Vulnerabilidad en la cadena de suministro

Un CSP puede estar en peligro si el hardware o software suministrado a la plataforma a través de su cadena de suministro menoscaba la seguridad del CSC o del CSP, por ejemplo mediante la introducción deliberada o accidental de software maligno o de vulnerabilidades explotables.

Un ejemplo sería un código maligno en el CSN. Este problema de seguridad se produce cuando el CSP ejecuta un código CSN, como una interfaz del cliente, un sistema operativo (SO) cliente en una máquina virtual (VM), aplicaciones, componentes de plataforma o software de auditoría/control (por ejemplo, para un asociado que efectúa la auditoría de un servicio).

Otro ejemplo es cuando un CSP ejecuta un código suministrado por un asociado; el CSP estará en peligro si el asociado no puede ofrecer las actualizaciones de seguridad necesarias de manera oportuna.

8.2.10 Dependencias del software

Cuando se detecta una vulnerabilidad, quizá no sea posible hacer una actualización inmediata porque, en tal caso, se dañarían otros componentes del software (aunque, de otro modo, esos componentes quizá no requieran actualización). Esto es particularmente cierto cuando existe dependencia entre componentes facilitados por uno o varios CSN, en lugar de entre los CSP.

8.3 Problemas de seguridad para los asociados del servicio en la nube (CSP)

En esta cláusula se indican las amenazas que afectan directamente a los CSN. Éstas pueden afectar a la capacidad de un CSN de hacer negocio, recibir pagos, proteger su propiedad intelectual y evitar problemas jurídicos o reglamentarios. Los problemas de seguridad de un determinado CSN dependerán de sus actividades y contextos específicos, como el desarrollo, la integración, la auditoría, etc.

8.3.1 Ambigüedad en las responsabilidades

Cuando en el servicio se ejecuta conjuntamente código del CSP y del CSN, el CSC quizá no sepa quién es el responsable de mitigar y gestionar los incidentes de seguridad. Puede resultar bastante difícil determinar la entidad responsable mediante un análisis técnico. Estas situaciones pueden dar lugar a acusaciones mutuas entre el CSP y el CSN sobre de quién es la culpa, lo que se puede traducir en nuevas irrupciones si no se encuentra la raíz del problema.

8.3.2 Apropiación indebida de propiedad intelectual

Cuando los asociados envían códigos u otros activos para su ejecución, uno de los problemas de seguridad es que dicho material se filtre a un tercero o se utilice indebidamente sin autorización. Dicha utilización podría implicar una infracción del derecho de autor o la revelación de secretos comerciales.

8.3.3 Pérdida de integridad del software

Una vez que el código del CSC se está ejecutando en el CSP, existe la posibilidad de que sea modificado o infectado cuando está fuera del control directo del CSN, lo que en cierto modo lo haría funcionar mal. Aunque esta posibilidad esté fuera de control del CSN, podría afectar gravemente a su reputación y, por ende, a su negocio.

9 Capacidades de seguridad en la computación en la nube

En esta Recomendación se identifican las siguientes capacidades de seguridad contra las amenazas o problemas de seguridad de la computación en la nube. Los parámetros de estas capacidades de seguridad pueden estipularse en el acuerdo de nivel de servicio (SLA) sobre seguridad, por ejemplo, el tiempo de respuesta a incidentes.

9.1 Modelo de confianza

Todo sistema en el que varios proveedores cooperan para ofrecer un servicio fiable requiere un modelo de confianza común.

Dada la naturaleza multipartita y muy distribuida de la computación en la nube exigen integrar en la misma un modelo de confianza general. Este modelo de confianza permitirá la creación de islas y/o federaciones de entidades fiables, de modo que los elementos dispersos del sistema podrá autentificar la identidad y autorizar los derechos de otras entidades y componentes. Cada isla o federación de confianza se basará en una o varias autoridades de confianza (por ejemplo, una autoridad de certificados de infraestructura de clave pública.

Hoy en día existen diversos modelos de confianza tanto para la computación en la nube como para otros fines. El modelo de confianza específico que se haya de adoptar queda fuera del alcance de la presente Recomendación.

9.2 Gestión de identidad y de acceso (IAM), autentificación, autorización y auditoría de transacciones

En los servicios de computación en la nube intervienen varios administradores y usuarios, y se utilizan y accede a los mismos interna (CSP) y externamente (CSC). La gestión de identidad es necesaria no sólo para proteger las identidades, sino también para facilitar la gestión del acceso, la autentificación, autorización y auditoría de transacciones en una infraestructura tan dinámica y abierta como la de computación en la nube.

La IAM requiere uno o varios modelos de confianza comunes (cláusula 9.1) para la autentificación de identidades, y los ingenieros, hipervisores y otros componentes del sistema necesitan dichos modelos para autentificar componentes del sistema, como módulos software, aplicaciones o datos descargados.

La IAM contribuye a la confidencialidad, integridad y disponibilidad de servicios y recursos y, por ende, se convierte en una pieza esencial de la computación en la nube.

Por otra parte, la IAM permite crear un inicio de sesión único y una federación de identidades para nubes utilizando mecanismos de autentificación diferentes o distribuidos en distintos dominios de seguridad.

La auditoría de transacciones protege contra el rechazo, permite el análisis forense tras un incidente de seguridad y sirve para disuadir los ataques (tanto por intrusión como internos). Además de mantener simple registro de eventos, la auditoría de transacciones exige un control activo para detectar actividades sospechosas.

9.3 Seguridad física

Es indispensable garantizar la seguridad física. El acceso a los locales donde se encuentra el equipo del CSP está restringido a las personas autorizadas y éstas sólo pueden entrar en las zonas necesarias para desempeñar su trabajo; esta restricción forma parte de la AIM. Ahora bien, el nivel de seguridad física dependerá del valor de los datos y del número de clientes con acceso autorizado.

9.4 Seguridad de las interfaces

Esta capacidad protege las interfaces abiertas a los CSC y otros CSP contratados a través de los cuales se ofrecen diversos tipos de servicios de computación en la nube, y protege las comunicaciones que circulan por dichas interfaces. Entre los mecanismos disponibles para garantizar la seguridad de las interfaces cabe citar la autentificación unilateral/recíproca, la suma de verificación de la integridad, la encriptación de extremo a extremo, la firma digital, etc.

9.5 Seguridad en la virtualización informática

Por seguridad de virtualización informática se entiende la seguridad de todo el entorno de virtualización informática. Sirve para proteger al hipervisor contra ataques y a la plataforma anfitrión contra amenazas con origen en el entorno de virtualización informática y, además, protege a las MV durante toda su vida útil. Concretamente, esta capacidad permite el aislamiento de MV y protege las instancias de MV suspendidas en disco y durante la migración.

Para el CSP, el hipervisor ofrece a menudo protección de las MV alojadas, por ejemplo, mediante procesado interno antivirus y antispam, de modo que las MV no tienen que integrar esas funciones por separado. Normalmente, el hipervisor se configura con un conjunto mínimo de servicios. Por lo

general, se cierran las interfaces innecesarias y las de programación de aplicaciones (API) y se desactivan los componentes de servicio irrelevantes.

Las MV dotadas de esta capacidad son, entre otras, creadas por el CSC en IaaS y toda MV creada por SaaS y PaaS. Las máquinas virtuales suelen estar bien aisladas cuando comparte memoria, una unidad central de procesamiento (CPU) y capacidades de almacenamiento. Las máquinas virtuales disponen a menudo de capacidades intrínsecas de seguridad y de política (por ejemplo, en el sistema operativo cliente).

9.6 Seguridad en la red

En el contexto de la computación en la nube, la seguridad en la red permite aislar física y virtualmente la red y proteger las comunicaciones entre todos los participantes. También permite dividir el dominio de seguridad en la red, los controles de acceso en el límite de la red (por ejemplo, cortafuegos), la detección y prevención de intrusiones, la segregación del tráfico de red con arreglo a políticas de seguridad, y proteger la red contra ataques al entorno de red físico y virtual.

9.7 Aislamiento de datos, protección y protección de la privacidad

Esta capacidad guarda relación con las cuestiones generales de protección de datos, que con frecuencia tienen repercusiones jurídicas.

- Aislamiento de datos

En el contexto de la computación en la nube, se impide a cada división acceder a datos que pertenecen a otra división, aun cuando estos datos esté encriptados, salvo cuando dicho acceso se haya autorizado explícitamente. El aislamiento de datos puede ser físico o lógico, en función de la granularidad de aislamiento necesario y la instalación específica de software y hardware de computación en la nube.

NOTA 1 – En la computación en la nube, el aislamiento se efectúa a nivel de división. Un determinado CSC puede tener múltiples divisiones en la nube para, por ejemplo, separar diferentes filiales, divisiones o unidades administrativas.

- Protección de datos

La protección de datos garantiza que los datos del CSC y datos derivados almacenados en la computación en la nube están debidamente protegidos, de forma que sólo pueden modificarse o accederse a los mismos previa autorización del CSC (o de acuerdo con la legislación aplicables). Esta protección podría incluir algún tipo de combinación de listas de control de acceso, verificación de integridad, corrección de errores/recuperación de datos, y otros mecanismos adecuados.

Cuando un CSP ofrece a los CSC almacenamiento encriptado, la encriptación puede realizarse en el lado cliente (por ejemplo, en la aplicación del CSP) o en el lado servidor.

- Protección de la privacidad

La información privada comprende la PII y los datos confidenciales de la empresa. La recopilación, utilización, transferencia, manipulación, almacenamiento y destrucción de información privada puede estar contemplada en la legislación o reglamentación en materia de privacidad. Esta restricción se aplica tanto a los CSP como a sus CSC, por ejemplo, un CSC debe ser capaz de suprimir de manera permanente un cuadro de datos que contenga información privada, aun cuando el CSP no esté al corriente del contenido de dicho cuadro. Los CSP quizá también deban dar soporte a la manipulación, por ejemplo, búsqueda de datos de un CSC en forma encriptada o transformada.

La protección de la privacidad comprende la información privada que puede observarse o derivarse de las actividades del CSC, como las tendencias comerciales, las relaciones o comunicaciones con otras partes, los niveles y pautas de actividad, etc.

La protección de la privacidad también se encarga de velar por que toda la información privada (en particular los datos observados o derivados) se utiliza exclusivamente para los fines acordados entre un CSC y un CSP.

El análisis de riesgos de la información privada (denominado "análisis de riesgos de privacidad") puede ayudar a un CSP a determinar los riesgos específicos de violación de la privacidad que conlleva una operación prevista. El CSP debería identificar y aplicar capacidades para resolver los riesgos de privacidad determinados mediante el análisis de riesgos y el tratamiento de la información privada.

NOTA 2 – 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 usuario del servicio en la nube (CSU) se deberá proteger adecuadamente además de proteger al cliente de servicio en la nube (CSC) o a la división del servicio en la nube.

9.8 Coordinación de la seguridad

Dado que cada servicio de computación en la nube aplica diferentes controles de seguridad, esta capacidad de seguridad se encarga de coordinar los mecanismos de seguridad heterogéneos para evitar conflictos de protección.

Las partes que desempeñan distintos papeles en el ecosistema de computación en la nube -a saber, el CSP, el CSC, el CSN- tienen diferentes grados de control sobre los servicios y los recursos físicos o virtuales, en particular el control de seguridad.

Cada parte dispondrá de diversos mecanismos de seguridad, como aislamiento del hipervisor, IAM, protección de red, etc.

Uno de los fines de la computación en la nube es permitir que estas distintas partes colaboren en el diseño, construcción, instalación y explotación de diversos recursos físicos y virtuales. Por consiguiente, un CSP debe ser capaz de coordinar los diferentes mecanismos de seguridad entre las distintas partes. La coordinación de la seguridad depende de la compatibilidad y armonización de los diversos mecanismos de seguridad.

9.9 Seguridad operativa

Esta capacidad ofrece protección de seguridad en la explotación y mantenimiento cotidiano de los servicios e infraestructura de computación en la nube.

Esta capacidad de seguridad operativa comprende:

- definir un conjunto de políticas y actividades en materia de seguridad, como gestión de la configuración, parches de actualización, evaluación de la seguridad, respuesta a incidentes (véase también la cláusula 9.10 "gestión de incidentes") y velar por que estas medidas de seguridad se apliquen correctamente para cumplir los requisitos de la legislación y contratos aplicables, incluido todo eventual SLA sobre seguridad;
- supervisar las medidas de seguridad del CSP y su eficacia, con las debidas notificaciones a los CSC afectados y a los auditores del caso (que actúan como CSN), lo que permite al CSC cuantificar si un CSP está cumpliendo los compromisos de seguridad del SLA.

En caso de que varíen las medidas de seguridad del CSP o su eficacia, habrá que avisar de estos cambios a todos los CSP y CSC dependientes.

Estos informes y alertas permiten a los CSC autorizados a estar al corriente de los incidentes, la información de auditoría y los datos de configuración relacionados con sus servicios de computación en la nube.

9.10 Gestión de incidentes

La gestión de incidentes consiste en la supervisión, predicción, alerta y respuesta en caso de incidente. Para saber si el servicio de computación en la nube funciona según lo previsto en toda la infraestructura, es necesario realizar una supervisión continua (por ejemplo, supervisar en tiempo real la calidad de funcionamiento de la plataforma o máquina virtualizada). Así, el sistema capta el estado de la seguridad del servicio, identifica condiciones anormales y alerta en cuanto se produce una sobrecarga, brecha, discontinuidad, etc., del sistema de seguridad. Cuando se produce un incidente de seguridad, se determina el problema y se reacciona con celeridad, ya sea de manera automática o con la intervención de la persona que ejerce de administrador. Los incidentes resueltos se registran en un fichero y se analizan con el fin de descubrir patrones subyacentes para poder reaccionar proactivamente.

9.11 Recuperación en caso de catástrofe

La recuperación en caso de catástrofe es la capacidad de responder a este tipo de situaciones, restablecer el sistema a un estado seguro y reanudar las operaciones normales lo más pronto posible. Sirve para ofrecer continuidad del servicio prestado con una mínima interrupción.

9.12 Evaluación y auditoría de la seguridad del servicio

Esta capacidad permite evaluar la seguridad de la computación en la nube. La parte autorizada puede verificar que el servicio en la nube cumple los requisitos de seguridad aplicables. La evaluación o auditoría de seguridad puede realizarla el CSC, el CSP o un tercero (CSN), y la certificación de seguridad podría realizarla un tercero (CSN) autorizado.

Deben adoptarse unos criterios de seguridad adecuados para que el CSC y el CSP se entiendan en lo que respecta al nivel de seguridad.

Cada CSP y servicio que éste ofrezca puede tener un nivel de seguridad distinto en lo que respecta a los controles de seguridad y su eficacia. La publicación de los niveles de seguridad de los CSP y sus servicios contribuye a facilitar la comparación y selección de los CSP y servicios de computación en la nube adecuados. Puede recurrirse a terceros de confianza para efectuar una evaluación fiable, independiente y neutral del nivel de seguridad.

Para evitar que un CSP lleve a cabo una auditoría de seguridad para cada CSC, los resultados de la auditoría común del servicio pueden reutilizarse debidamente. A fin de que un CSP pueda ofrecer una gran variedad de servicios de computación en la nube, se podrían realizar auditorías de seguridad de cada uno de esos servicios. El CSP puede facilitar los resultados de auditoría de una parte o la totalidad de los servicios de computación en la nube a un CSC autorizado (por ejemplo, un potencial cliente) y a ciertos otros CSP o CSN (por ejemplo, un tercero auditor).

En una cadena de computación en la nube, los resultados de la auditoría de seguridad de un proveedor de servicio situado más abajo integrarán los resultados pertinentes de la auditoría de seguridad de los proveedores de servicios situados más arriba.

9.13 Interoperatividad, portabilidad y reversibilidad

Esta capacidad permite la coexistencia y cooperación de componentes heterogéneos (compatibilidad), permite a los CSC sustituir un CSP por otro si lo estiman conveniente (portabilidad) y permite a los CSC transferir sus sistemas TIC de un entorno de computación en la nube a una infraestructura TIC de computación fuera de la nube. Esta reversibilidad también permite el "derecho al olvido", si así lo exige la legislación o reglamentación local.

NOTA 1 – Esta capacidad sólo se refiere a la compatibilidad y portabilidad de las funciones de seguridad de la computación en la nube, y no a los datos reales, metadatos o formatos de mensaje, que son responsabilidad de otras funciones de la plataforma de computación en la nube. Por ejemplo, esta capacidad podría ofrecer encriptación provisional, gestión de claves e información sobre la identidad, de modo que se puedan desplazar datos y otro contenido entre dos sistemas de encriptación diferentes sin exponer el sistema ni los datos en tránsito.

NOTA 2 – El "derecho al olvido" no está claramente definido y en algunos casos puede verse restringido por los requisitos reglamentarios de mantener ciertos datos durante un periodo mínimo, como los registros de llamadas o la información sobre la conexión. Por consiguiente, también sería necesario mantener las correspondientes claves u otra información de seguridad durante ese mismo periodo.

9.14 Evaluación y auditoría de la seguridad del servicio

Un CSP utiliza diversos proveedores para crear sus servicios. Algunos de éstos serán participantes en la industria de la nube -por ejemplo, un CSN- mientras que otros serán proveedores tradicionales de equipos o servicios de tecnología de la información (TI), por ejemplo fabricantes de hardware que no tienen relación directa con la computación en la nube. Esta capacidad permite establecer una relación de confianza entre el CSP y todos los que intervienen en la cadena de suministro mediante actividades de seguridad. Estas actividades de seguridad en la cadena de suministro consisten en identificar y recabar información acerca de los componentes y servicios adquiridos por el CSP y que éste utiliza para prestar servicios de computación en la nube, así como en aplicar las políticas de seguridad a la cadena de suministro.

Por ejemplo, algunas actividades características de seguridad en la cadena de suministro son:

- confirmación de la información histórica acerca de los participantes en la cadena de suministro;
- validación del hardware, software y de los servicios empleados por el CSP;
- inspección del hardware y software adquirido por el CSP para garantizar que no haya sido alterado cuando estuvo en tránsito;
- proporcionar mecanismos para verificar el origen del software del servicio en la nube, por ejemplo, el código facilitado por un CSN. En su caso, el CSN y sus CSP anfitriones ofrecen un mecanismo para verificar la integridad del componente de software del CSN con el fin de garantizar que está exactamente igual a cuando se envió y que no ha sido modificado o alterado. Algunos CSN podrían solicitar mecanismos para verificarlo directamente ellos mismos.

Esta capacidad debe permitir seguir la evolución del sistema y sus actualizaciones.

10 Metodología marco

Crear un marco de seguridad para la computación en la nube significa comprender qué amenazas y problemas existen, como se analizó en las cláusulas 7 y 8, para un determinado servicio en la nube, junto con los requisitos comerciales, tecnológicos y reglamentarios que hay que tomar en consideración para determinar los controles, las políticas y los procedimientos de seguridad necesarios para dicho servicio. Las capacidades descritas en la cláusula 9 para resolver y reducir dichas amenazas y problemas se utilizan luego para crear controles, políticas y procedimientos de seguridad para ese determinado servicio de computación en la nube. Esta Recomendación se ciñe a cuáles son las necesidades de seguridad en un entorno de computación en la nube, qué amenazas y problemas de computación tradicional siguen existiendo en la nube y, en tal caso, qué normas y prácticas idóneas definidas por la industria deberían aplicarse, además de las estipuladas en la presente Recomendación.

La metodología aquí descrita se debería aplicar al crear el marco que determinará los controles, políticas y procedimientos de seguridad que serán necesarios para un determinado servicio de computación en la nube. Resulta imposible definir un solo marco normativo para todos los servicios de computación en la nube, por cuanto el modelo administrativo, los servicios ofrecidos y las opciones de realización varían sobremanera de uno a otro:

- Etapa 1: Utilizar las cláusulas 7 y 8 para determinar las amenazas y repercusiones de seguridad de los problemas en el servicio de computación en la nube del caso.
- Etapa 2: Utilizar la cláusula 9 para determinar las capacidades de seguridad de alto nivel que podrían mitigar amenazas y problemas de seguridad identificados.
- Etapa 3: Obtener los controles, políticas y procedimientos de seguridad que podrían proporcionar la seguridad necesaria de acuerdo con las capacidades de seguridad identificadas.

NOTA – El CSC y el CSP han de determinar el conjunto de requisitos pertinentes de las capacidades de seguridad, utilizando las normas correspondientes. Para ello se basarán en el análisis de riesgos.

A fin de determinar qué amenazas y problemas de seguridad atañen al servicio en la nube en cuestión, debería examinarse cada una de estas amenazas y problemas. Un procedimiento sería crear un simple cuadro con un "Sí" en la casilla correspondiente a la amenaza o problema.

Un ejemplo sería cuando el CSP ofrece un servicio de almacenamiento de ficheros a usuarios particulares, y el CSP desea saber qué amenazas y problemas de seguridad preocupan más a los usuarios y analizar cuáles deben resolver principalmente. En el Cuadro 1 se muestra un ejemplo de este procedimiento.

Una vez identificados los problemas y amenazas de seguridad, es posible determinar las capacidades de seguridad que podrían mitigar dichas amenazas y resolver los problemas identificados. En el Cuadro I.1 se muestra un ejemplo de correspondencia entre amenazas y problemas de seguridad en la computación en la nube y las capacidades de seguridad correspondientes. Por "Sí" en una casilla del cuadro se entiende que la amenaza o problema de seguridad indicado en la fila se resuelve con la capacidad de seguridad de la columna correspondiente. En el cuadro se muestran todas las amenazas y problemas y las capacidades de seguridad correspondientes.

Una vez identificadas las capacidades requeridas, podrán determinarse los controles, políticas y procedimientos de seguridad que son necesarios. Como ejemplos de controles puede citarse la "seguridad en las operaciones" (cláusula 12 en [b-ISO/IEC 27002]) y "gestión de incidentes de seguridad de la información" en [b-ISO/IEC 27002]), que puede derivarse de las capacidades identificadas en las cláusulas 9.9 y 9.10, respectivamente.

Un servicio en la nube puede tener una cadena de suministro formada por varios CSP. Las empresas que intervienen en dicha cadena pueden remitirse a las normas de la UIT y de la industria sobre el tema de seguridad en la cadena de suministro (por ejemplo, [b-ISO/IEC 28000]). Cada CSP tendrá de delimitar su responsabilidad en la cadena de servicio de la computación en la nube y crear sus propios controles, políticas y procedimientos de seguridad con arreglo a las capacidades de seguridad obtenidas con este procedimiento de tres etapas. Para ofrecer seguridad coherente a los CSC, el CSP situado más arriba quizá tenga que negociar con los CSP de más abajo acerca de estas capacidades de seguridad con arreglo a sus responsabilidades. En caso necesario, los CSC también deberían aplicar este procedimiento de tres etapas.

Por otra parte, el procedimiento descrito debería llevarse a cabo periódicamente o siempre que se estime necesario (por ejemplo, cuando se produce una brecha de seguridad importante, o cuando un CSP cambia su CSP más arriba).

Cuadro 1 – Ejemplo de la etapa 1 de análisis del marco de seguridad para un servicio de almacenamiento de ficheros

Ámbito de análisis	Amenaza o problema específico		¿Aplicable a este servicio?
Cláusula 7.1 Amenazas de seguridad al cliente de computación en la nube (CSC)	Cláusula 7.1.1	Pérdida y filtración de datos	Sí
	Cláusula 7.1.2	Acceso inseguro al servicio	Sí
	Cláusula 7.1.3	Amenazas internas	
Cláusula 7.2 Amenazas de seguridad al proveedor del servicio en la nube (CSP)	Cláusula 7.2.1	Acceso con derechos de administración no autorizado	Sí
	Cláusula 7.2.2	Amenazas internas	Sí
Cláusula 8.1 Problemas de seguridad al cliente de computación en la nube (CSC)	Cláusula 8.1.1	Ambigüedad en las responsabilidades	Sí
	Cláusula 8.1.2	Pérdida de confianza	Sí
	Cláusula 8.1.3	Pérdida de gobernanza	Sí
	Cláusula 8.1.4	Pérdida de privacidad	Sí
	Cláusula 8.1.5	Indisponibilidad del servicio	Sí
	Cláusula 8.1.6	Dependencia del proveedor de servicios en la nube	Sí
	Cláusula 8.1.7	Apropiación indebida de propiedad intelectual	
	Cláusula 8.1.8	Pérdida de integridad del software	
Cláusula 8.2 Problemas de seguridad para los proveedores de servicio en la nube (CSP)	Cláusula 8.2.1	Ambigüedad en las responsabilidades	Sí
	Cláusula 8.2.2	Contexto compartido	Sí
	Cláusula 8.2.3	Incoherencia y conflictos en los mecanismos de protección	Sí
	Cláusula 8.2.4	Conflictos jurisdiccionales	Sí
	Cláusula 8.2.5	Evolución de los riesgos	
	Cláusula 8.2.6	Migración e integración deficientes	Sí
	Cláusula 8.2.7	Discontinuidad de actividades	Sí
	Cláusula 8.2.8	Dependencia del asociado de servicios en la nube	
	Cláusula 8.2.9	Vulnerabilidad en la cadena de suministro	Sí
	Cláusula 8.2.10	Dependencias del software	
Cláusula 8.3 Problemas de seguridad para los asociados del servicio en la nube (CSP)	Cláusula 8.3.1	Ambigüedad en las responsabilidades	
	Cláusula 8.3.2	Apropiación indebida de propiedad intelectual	
	Cláusula 8.3.3	Pérdida de integridad del software	

Apéndice I

Correspondencia entre amenazas y problemas de seguridad en la computación en la nube y las capacidades de seguridad

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

En el Cuadro I.1 se muestra la correspondencia entre amenazas y problemas de seguridad en la computación en la nube y las capacidades de seguridad.

Por "Sí" en una casilla del cuadro se entiende que la amenaza o problema de seguridad indicado en la fila se resuelve con la capacidad de seguridad de la columna correspondiente.

Cuadro I.1 – Correspondencia entre amenazas y problemas de seguridad en la computación en la nube y las capacidades de seguridad

			Cláusula 9 Capacidades de seguridad en la computación en la nube													
			Cláusula 9.1 Modelo de confianza	**Cláusula 9.2 Gestión de identidad y de acceso (IAM), autentificación, autorización y auditoría de transacciones**	**Cláusula 9.3 Seguridad física**	**Cláusula 9.4 Seguridad de las interfaces**	**Cláusula 9.5 Seguridad en la virtualización informática**	**Cláusula 9.6 Seguridad en la red**	**Cláusula 9.7 Aislamiento de datos, protección y protección de la privacidad**	**Cláusula 9.8 Coordinación de la seguridad**	**Cláusula 9.9 Seguridad operativa**	**Cláusula 9.10 Gestión de incidentes**	**Cláusula 9.11 Recuperación en caso de catástrofe**	**Cláusula 9.12 Evaluación y auditoría de la seguridad del servicio**	**Cláusula 9.13 Compatibilidad, portabilidad y reversibilidad**	**Cláusula 9.14 Seguridad en la cadena de suministro**
Cláusula 7 Amenazas de seguridad en la computación en la nube	Cláusula 7.1 Amenazas de seguridad al cliente de computación en la nube (CSC)	Cláusula 7.1.1 Pérdida y filtración de datos	Sí	Sí	Sí				Sí				Sí			
		Cláusula 7.1.2 Acceso inseguro al servicio	Sí	Sí		Sí	Sí	Sí								
		Cláusula 7.1.3 Amenazas internas		Sí	Sí									Sí		

Cuadro I.1 – Correspondencia entre amenazas y problemas de seguridad en la computación en la nube y las capacidades de seguridad

			Cláusula 9 Capacidades de seguridad en la computación en la nube													
			Cláusula 9.1 Modelo de confianza	**Cláusula 9.2 Gestión de identidad y de acceso (IAM), autentificación, autorización y auditoría de transacciones**	**Cláusula 9.3 Seguridad física**	**Cláusula 9.4 Seguridad de las interfaces**	**Cláusula 9.5 Seguridad en la virtualización informática**	**Cláusula 9.6 Seguridad en la red**	**Cláusula 9.7 Aislamiento de datos, protección y protección de la privacidad**	**Cláusula 9.8 Coordinación de la seguridad**	**Cláusula 9.9 Seguridad operativa**	**Cláusula 9.10 Gestión de incidentes**	**Cláusula 9.11 Recuperación en caso de catástrofe**	**Cláusula 9.12 Evaluación y auditoría de la seguridad del servicio**	**Cláusula 9.13 Compatibilidad, portabilidad y reversibilidad**	**Cláusula 9.14 Seguridad en la cadena de suministro**
	Cláusula 7.2 Amenazas de seguridad al proveedor del servicio en la nube (CSP)	Cláusula 7.2.1 Acceso con derechos de administración no autorizado	Sí	Sí	Sí											
		Cláusula 7.2.2 Amenazas internas		Sí	Sí									Sí		
Cláusula 8 Problemas de seguridad en la computación en la nube	Cláusula 8.1 Problemas de seguridad al cliente de computación en la nube (CSC)	Cláusula 8.1.1 Ambigüedad en las responsabilidades		Sí												
		Cláusula 8.1.2 Pérdida de confianza												Sí		
		Cláusula 8.1.3 Pérdida de gobernanza		Sí	Sí				Sí		Sí	Sí	Sí	Sí		
		Cláusula 8.1.4 Pérdida de privacidad		Sí					Sí					Sí		
		Cláusula 8.1.5 Indisponibilidad del servicio								Sí	Sí	Sí	Sí			Sí

Cuadro I.1 – Correspondencia entre amenazas y problemas de seguridad en la computación en la nube y las capacidades de seguridad

			Cláusula 9 Capacidades de seguridad en la computación en la nube													
			Cláusula 9.1 Modelo de confianza	**Cláusula 9.2 Gestión de identidad y de acceso (IAM), autentificación, autorización y auditoría de transacciones**	**Cláusula 9.3 Seguridad física**	**Cláusula 9.4 Seguridad de las interfaces**	**Cláusula 9.5 Seguridad en la virtualización informática**	**Cláusula 9.6 Seguridad en la red**	**Cláusula 9.7 Aislamiento de datos, protección y protección de la privacidad**	**Cláusula 9.8 Coordinación de la seguridad**	**Cláusula 9.9 Seguridad operativa**	**Cláusula 9.10 Gestión de incidentes**	**Cláusula 9.11 Recuperación en caso de catástrofe**	**Cláusula 9.12 Evaluación y auditoría de la seguridad del servicio**	**Cláusula 9.13 Compatibilidad, portabilidad y reversibilidad**	**Cláusula 9.14 Seguridad en la cadena de suministro**
		Cláusula 8.1.6 Dependencia del proveedor de servicios en la nube													Sí	
		Cláusula 8.1.7 Apropiación indebida de propiedad intelectual		Sí	Sí				Sí							
		Cláusula 8.1.8 Pérdida de integridad del software		Sí			Sí		Sí							
	Cláusula 8.2 Problemas de seguridad para los proveedores de servicio en la nube (CSP)	Cláusula 8.2.1 Ambigüedad en las responsabi-lidades		Sí												
		Cláusula 8.2.2 Contexto compartido					Sí	Sí	Sí							
		Cláusula 8.2.3 Incoherencia y conflictos en los mecanismos de protección								Sí					Sí	

Cuadro I.1 – Correspondencia entre amenazas y problemas de seguridad en la computación en la nube y las capacidades de seguridad

			Cláusula 9 Capacidades de seguridad en la computación en la nube													
			Cláusula 9.1 Modelo de confianza	**Cláusula 9.2 Gestión de identidad y de acceso (IAM), autentificación, autorización y auditoría de transacciones**	**Cláusula 9.3 Seguridad física**	**Cláusula 9.4 Seguridad de las interfaces**	**Cláusula 9.5 Seguridad en la virtualización informática**	**Cláusula 9.6 Seguridad en la red**	**Cláusula 9.7 Aislamiento de datos, protección y protección de la privacidad**	**Cláusula 9.8 Coordinación de la seguridad**	**Cláusula 9.9 Seguridad operativa**	**Cláusula 9.10 Gestión de incidentes**	**Cláusula 9.11 Recuperación en caso de catástrofe**	**Cláusula 9.12 Evaluación y auditoría de la seguridad del servicio**	**Cláusula 9.13 Compatibilidad, portabilidad y reversibilidad**	**Cláusula 9.14 Seguridad en la cadena de suministro**
		Cláusula 8.2.4 Conflictos jurisdiccio-nales							Sí		Sí					
		Cláusula 8.2.5 Evolución de los riesgos									Sí				Sí	Sí
		Cláusula 8.2.6 Migración e integración deficientes				Sí	Sí	Sí	Sí	Sí	Sí					
		Cláusula 8.2.7 Discontinuidad de actividades										Sí	Sí			
		Cláusula 8.2.8 Dependencia del asociado de servicios en la nube														Sí
		Cláusula 8.2.9 Vulnerabilidad en la cadena de suministro														Sí
		Cláusula 8.2.10 Dependencias del software														Sí

Cuadro I.1 – Correspondencia entre amenazas y problemas de seguridad en la computación en la nube y las capacidades de seguridad

			Cláusula 9 Capacidades de seguridad en la computación en la nube													
			Cláusula 9.1 Modelo de confianza	**Cláusula 9.2 Gestión de identidad y de acceso (IAM), autentificación, autorización y auditoría de transacciones**	**Cláusula 9.3 Seguridad física**	**Cláusula 9.4 Seguridad de las interfaces**	**Cláusula 9.5 Seguridad en la virtualización informática**	**Cláusula 9.6 Seguridad en la red**	**Cláusula 9.7 Aislamiento de datos, protección y protección de la privacidad**	**Cláusula 9.8 Coordinación de la seguridad**	**Cláusula 9.9 Seguridad operativa**	**Cláusula 9.10 Gestión de incidentes**	**Cláusula 9.11 Recuperación en caso de catástrofe**	**Cláusula 9.12 Evaluación y auditoría de la seguridad del servicio**	**Cláusula 9.13 Compatibilidad, portabilidad y reversibilidad**	**Cláusula 9.14 Seguridad en la cadena de suministro**
	Cláusula 8.3 Problemas de seguridad para los asociados del servicio en la nube (CSP)	Cláusula 8.3.1 Ambigüedad en las responsabi-lidades		Sí												
		Cláusula 8.3.2 Apropiación indebida de propiedad intelectual		Sí	Sí				Sí							
		Cláusula 8.3.3 Pérdida de integridad del software		Sí			Sí		Sí							

Bibliografía

[b-ITU-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-ITU-T X.810] Recomendación UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general*.

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

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

[b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology –Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

[b-ISO/IEC 27005] ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management*.

[b-ISO/IEC 28000] ISO/IEC 28000:2007, *Specification for security management systems for the supply chain*.

[b-ISO/IEC 29100] ISO/IEC 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 (2009), *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*.

[b-CSA Matrix] CSA (2013), *Cloud Controls Matrix*, Cloud Security Alliance.

[b-key definition] Key definitions of the Data Protection Act, Information Commissioners Office <http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx>

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
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	Construcción, instalación y protección de los cables y 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 y redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2014