Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1642

(03/2016)

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 operativa de la computación en la nube

Recomendación UIT-T X.1642

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
Recomendaciones relacionadas con la PKI	X.1340–X.1349

Recomendación UIT-T X.1642

Directrices para la seguridad operativa de la computación en la nube

Resumen

La Recomendación UIT-T X.1642 proporciona directrices operativas genéricas de seguridad para la computación en la nube desde la perspectiva de los Proveedores de servicios en la nube (CSP). Analiza los requisitos de seguridad y las métricas para el funcionamiento de la computación en la nube. Define un conjunto de medidas y actividades detalladas de seguridad relativas al funcionamiento diario y al mantenimiento a fin de ayudar a los CSP a reducir los riesgos de seguridad y abordar los retos de seguridad relativos al funcionamiento de la computación en la nube.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1642	2016-03-23	17	11.1002/1000/12616

Palabras clave

Cláusula de seguridad del acuerdo de nivel de servicio (SLA), computación en la nube, , seguridad operativa

* 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.1642

Directrices para la seguridad operativa de la computación en la nube

1 Alcance

En la presente Recomendación se aclaran las responsabilidades en materia de seguridad entre los proveedores de servicios en la nube (CSP) y los clientes del servicio en la nube (CSC) y se analizan los requisitos y las categorías de las métricas de seguridad de la seguridad operativa de la computación en la nube. Se definen conjuntos de medidas detalladas de seguridad y de actividades de seguridad para el funcionamiento diario y el mantenimiento de los servicios en la nube y la infraestructura desde la perspectiva de los CSP, a fin de dar respuesta a los requisitos de seguridad operativa para la computación en la nube.

La presente Recomendación permitirá a los CSP reducir los riesgos operativos. Se dirige a distintos tipos de CSP, como los operadores de telecomunicaciones tradicionales o los proveedores de servicios de Internet (PSI).

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

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

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

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

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

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

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

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

3.1.7 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.

3.1.8 red como servicio (NaaS) [b-UIT-T Y.3500]: categoría de servicio en la nube que consiste en ofrecer al cliente de servicios en la nube conectividad de transporte y sus correspondientes capacidades de red.

3.1.9 parte [b-ISO 27729]: persona física o jurídica, organizada o no, o una agrupación de éstas.

3.1.10 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.

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

3.1.12 dominio de seguridad [b-UIT-T X.810]: conjunto de elementos, política de seguridad, autoridad de seguridad y actividades sobre seguridad, cuyos elementos deben cumplir la política de seguridad para las actividades especificadas y cuya política está administrada por la autoridad de seguridad encargada del dominio de seguridad.

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

3.1.14 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 sus objetivos.

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/IEC 27000]: posible causa de un incidente no deseado, que puede dañar un sistema o perjudicar a una organización.

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

3.2 Términos definidos en la presente Recomendación

Ninguno.

4 Abreviaturas y acrónimos

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

ACL Lista de control de acceso (*access control list*)

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

BIA Análisis del impacto en las operaciones (*business impact analysis*)

CCTV Televisión en circuito cerrado (*closed circuit television*)

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)*

DB Base de datos (*database*)

DDoS Ataque distribuido de denegación de servicio (*distributed denial of service*)

DLP Prevención de fuga de datos (*data leakage prevention*)

DoS Denegación de servicio (*denial of service*)

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

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

IdM Gestión de identidad (*identity management*)

IP Protocolo Internet (*Internet protocol)*

IPS Sistema de prevención de intrusiones (*intrusion prevention system*)

ISP Proveedor de servicios de Internet (*Internet service provider*)

JAT Justo a tiempo (*just in time*)

LDAP Protocolo ligero de acceso al directorio (*lightweight directory access protocol*)

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

OS Sistema operativo (*operating system)*

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

RPO Objetivo de punto de recuperación (*recovery point objective*)

RTO Objetivos de tiempo de recuperación (*recovery time objectives*)

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

SDI Sistema de detección de intrusión (*intrusion detection system*)

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

SMS Servicio de mensajes breves (*short message service*)

SSO Inicio de sesión con registro único (*single sign-on*)

TI Tecnología de la información

TIC Tecnología de la información y la comunicación

VDC Centro de datos virtual (*virtual data centre*)

VM Máquina virtual (*virtual machine)*

5 Convenios

Ninguno.

6 Generalidades

Como consecuencia de la rápida expansión del mercado de la computación en la nube y el establecimiento de cadenas industriales, la seguridad sigue siendo un tema capital que no puede pasarse por alto. Los sistemas de computación en la nube se enfrentan a más desafíos que los que afectan a los sistemas tradicionales de tecnologías de la información (TI), ya que son más complejos y almacenan en la nube una cantidad de datos privados de los usuarios enorme. La seguridad y la protección de la privacidad son los factores principales que los usuarios tienen en cuenta al considerar la posibilidad de utilizar servicios de computación en la nube.

El número de estos servicios irá en aumento, motivo por el cual es urgente dotarse de métodos para garantizar su fiabilidad. Por lo tanto, es necesario investigar a fondo la seguridad operativa de la computación en la nube, a fin de suministrar directrices a los proveedores de servicios en la nube (CSP) que podrían ser de utilidad para reducir el riesgo en materia de seguridad provocado por un funcionamiento indebido, un diseño de negocio irracional, etc., así como para mejorar el nivel general de seguridad de funcionamiento de los servicios de computación en la nube.

A continuación se describen los principales desafíos en materia de seguridad operativa desde la perspectiva de los CSP:

1) Desafíos para el mantenimiento de la infraestructura de computación en la nube: cuando la computación en la nube proporciona a los usuarios infraestructura de TI, una plataforma o software como servicio, toda operación requiere unos servicios en la nube estables, fiables y seguros. Con el objetivo de que no se interrumpa el servicio a los clientes, habría que garantizar la fiabilidad y la estabilidad de la infraestructura del sistema en la nube y adoptar las precauciones necesarias para proteger la seguridad y la privacidad de la información del usuario. Incluso en caso de un pequeño fallo, muchos CSC pueden experimentar dificultades tales como la interrupción de las operaciones o la pérdida de datos. Los CSP deberían estudiar detenidamente maneras de localizar rápidamente los errores y de conectarse automáticamente y sin interrupciones al sistema auxiliar para proteger la disponibilidad del servicio para los clientes.
2) Desafíos relativos a la gestión de la computación en la nube: las características de la computación en la nube, tales como los servicios interregionales, una elevada potencia de cálculo y la separación de la titularidad y la gestión de los datos los diferencian de los servicios tradicionales de las TI. Estos desafíos requieren una gestión efectiva y la cooperación entre los nodos para que los CSP puedan resolver los problemas de seguridad. Los CSP tendrán que adoptar algunas medidas técnicas necesarias, como la gestión de la configuración de seguridad, etc., así como diseñar una distribución razonable de la autoridad de gestión y un conjunto de reglas y de procesos de gestión efectivos a fin de evitar la fuga de datos de los usuarios. Por ejemplo, los CSP deberían adoptar medidas para impedir que los administradores internos se extralimiten en sus funciones en su afán por evitar que los usuarios utilicen de manera indebida los recursos de la computación en la nube.

En general, y con miras a garantizar la total seguridad de las aplicaciones que están en la infraestructura en la nube, los CSP deberían adoptar distintos métodos tecnológicos y mecanismos de gestión, no sólo para mantener la seguridad, estabilidad y disponibilidad de la infraestructura en la nube, sino también para proteger la continuidad de las operaciones y los datos de los usuarios de los servicios en la nube bajo su responsabilidad.

7 Requisitos de la cláusula de seguridad del acuerdo de nivel de servicio

La cláusula de seguridad del acuerdo de nivel de servicio (SLA) es el factor clave para que los CSP se ganen la confianza de los usuarios. La cláusula de seguridad del SLA debería describir claramente la relación entre los CSC y los CSP, por ejemplo sobre quién recae la responsabilidad en materia de seguridad. Los CSP deben centrar sus medidas de seguridad operativa en el cumplimiento de los requisitos estipulados en la cláusula de seguridad del SLA.

7.1 Responsabilidad en materia de seguridad entre los CSP y los CSC

Habría que definir la responsabilidad tanto de los CSP como de los CSC en lo que respecta a la seguridad de la computación en la nube, atendiendo a su respectiva capacidad de control sobre la infraestructura y los recursos de la computación en la nube.

Las responsabilidades en materia de seguridad están estrechamente relacionadas con el modo de servicio en la nube, por cuanto éste refleja la capacidad de control del recurso en el entorno de la nube tanto para los CSP como para los CSC. Por ejemplo, en comparación con la plataforma como servicio (PaaS) o la infraestructura como servicio (IaaS), en el software como servicio (SaaS) los CSP deberían asumir más responsabilidades en materia de seguridad, así como una mayor capacidad de control sobre los recursos.

En el caso del modo de servicio de IaaS, los CSP proporcionan los servicios de infraestructuras, como el centro de datos virtual (VDC), que incluye los servidores alojados, el recurso de almacenamiento,

la red y las herramientas de gestión. Las responsabilidades fundamentales en materia de seguridad de los CSP incluyen la seguridad física, la seguridad de la red, la seguridad del sistema subyacente y la fiabilidad del conjunto de la infraestructura de la nube. Los CSC deberían encargarse de todas las cuestiones relacionadas con la seguridad que no pertenecen a la infraestructura de la nube que adquieren, como la seguridad del sistema operativo (OS), los programas de aplicación, etc.

En el caso del modo de servicio de PaaS, los CSP proporcionan un entorno simplificado y distribuido para el desarrollo, la comprobación y la instalación de programas. Los CSP deberían encargarse de la seguridad de la interfaz de programación de aplicaciones (API) del entorno de aplicación, la seguridad de los programas intermedios, la disponibilidad de la plataforma en la nube, etc., así como de la seguridad de la infraestructura subyacente. Por otra parte, los CSC deberían encargarse de la seguridad de los servicios de aplicación que funcionan sobre el entorno de la plataforma en la nube.

En el caso del modo de servicio de SaaS, los CSP deberían garantizar la seguridad general, desde la capa de infraestructura hasta la capa de aplicación, y los CSC deberían ocuparse del mantenimiento de la seguridad de la información conexa, por ejemplo la seguridad de la gestión de identidad (IdM) o la detección de fugas de contraseñas.

Además, los CSC deberían tener en cuenta las cuestiones de seguridad relacionadas con los terminales utilizados para acceder a la nube.

7.2 Requisitos de la cláusula de seguridad del SLA

7.2.1 Requisitos generales

La cláusula de seguridad del SLA debería especificar las condiciones de seguridad de los servicios en la nube, así como las obligaciones y las responsabilidades de los CSP y los CSC.

Desde la perspectiva del CSC, los CSC deberían poder enunciar sus requisitos en relación con la cláusula de seguridad del SLA. Esta cláusula puede ayudarles a garantizar que sus CSP den una protección adecuada a los activos, los recursos y los servicios informativos adaptados, tanto cuando están en pausa como cuando están en uso o en movimiento, así como que se han adoptado medidas correctoras para cumplir las normas sobre privacidad de datos de la jurisdicción pertinente.

Desde la perspectiva del CSP, la cláusula de seguridad del SLA establece los requisitos y las condiciones cuantificables de la seguridad del servicio en la nube proporcionado, que los CSC pueden evaluar, comparar y adaptar. Los CSP deberían aplicar mecanismos de gestión y tecnológicos adecuados para mejorar la fiabilidad y la seguridad de los servicios en la nube, y satisfacer los requisitos de la cláusula de seguridad del SLA, hecho que, en última instancia, puede servir para ganarse la confianza de los CSC. Los servicios en la nube pueden tener distintos tipos de SLA en función del contenido de los servicios, el grado de servicio e incluso la región en la que se prestan; con todo, los requisitos mínimos de la cláusula de seguridad del SLA deberían atenerse a los requisitos jurídicos y reglamentarios, así como a los relacionados con las normas públicas del sector.

Los CSP y los CSC podrían negociar los requisitos específicos de la cláusula de seguridad del SLA basándose en los requisitos adaptados de los CSC y en su capacidad de control sobre los recursos. En el caso de los CSP, los contratos comerciales o las descripciones de producto deberían estipular claramente los descargos de responsabilidad a fin de evitar riesgos de seguridad o disputas innecesarias, de modo que no se responsabilice al CSP en caso de fuerza mayor.

7.2.2 Elementos de la cláusula de seguridad del SLA

Las cláusulas de seguridad del SLA incluyen, entre otros, los elementos siguientes.

7.2.2.1 Continuidad de las operaciones

Los CSP deberían dotarse de unos mecanismos de protección adecuados en caso de catástrofe natural o artificial a fin de garantizar la disponibilidad del servicio y la continuidad de las operaciones. A continuación se detallan los elementos o los requisitos a este respecto:

1) Disponibilidad del servicio

Porcentaje de tiempo durante el cual el servicio puede utilizarse a lo largo de un periodo determinado. Para un servicio en la nube concreto, los términos de su capacidad de servicio no deberían ser inferiores, en general, a los del servicio de tecnologías de la información y la comunicación (TIC) tradicional.

2) Tiempo de recuperación medio

Tiempo necesario para recuperar los datos perdidos o reanudar el servicio tras un fallo o cualquier catástrofe.

7.2.2.2 Protección de la seguridad de los datos

Los CSP deberían disponer de un programa amplio de protección a fin de salvaguardar los datos del CSC y demás información sobre privacidad, y los CSP y los CSC deberían llegar a un acuerdo detallado sobre mecanismos y requisitos.

1) Seguridad del almacenamiento físico

Los CSP deberían adoptar medidas para garantizar la seguridad del almacenamiento físico, como la presencia de vigilantes de seguridad en la entrada, sistemas de protección contra incendios, sistemas auxiliares de alimentación eléctrica, etc.

2) Protección del medio de almacenamiento de datos

Los CSP deberían adoptar medidas de protección, como el fortalecimiento de los dispositivos o la actualización de los parches, entre otras, para mejorar la seguridad del medio en el que están almacenados los datos.

3) Encriptación de datos

Habría que estipular qué datos se encriptan en el proceso de almacenamiento o de transmisión, así como los detalles de los algoritmos de encriptación.

4) Control de acceso a los datos

Habría que especificar qué medidas se han adoptado para controlar el acceso a los datos con miras a evitar el acceso ilegal.

5) Aislamiento de los datos

Habría que especificar si se han aislado lógica o físicamente los datos de distintos CSC.

6) Borrado de datos

Incluye la garantía del borrado de datos. Habría que garantizar el borrado permanente de los datos antes de atribuir los recursos a otros CSC.

7) Copias de seguridad de datos

Incluye las condiciones relativas al objetivo de punto de recuperación (RPO) y al objetivo de tiempo de recuperación (RTO), la política de retención, la combinación de las copias de seguridad internas y externas, etc.

8) Auditoría del funcionamiento de los datos

Los CSP deberían auditar el funcionamiento de los datos del CSC y ser capaces de detectar operaciones anormales; la auditoría debería realizarla un auditor certificado.

9) Cumplimiento normativo de los datos

La recopilación, transferencia, manejo, almacenamiento y destrucción de los datos debería ajustarse a los reglamentos y a la legislación aplicables de la jurisdicción por la que se rige el CSC. Del mismo modo, los requisitos para la retención de datos también deberían respetar el tiempo de retención permitido por las distintas restricciones legales.

7.2.2.3 Respuesta en situaciones de emergencia

Los CSP deberían facilitar un número telefónico de atención gratuita para ofrecer un servicio de comunicación de fallos disponible en horario laboral o las 24 horas del día los siete días de la semana (24/7). Asimismo, los indicadores de servicio deberían incluir el tiempo de aceptación del fallo, el tiempo de solución de problemas, etc.

7.2.2.4 Medidas de seguridad

Los CSP deberían ofrecer a toda la infraestructura de computación en la nube unas medidas de seguridad adecuadas.

1) Medidas sobre virtualización informática

   Los CSP deberían aplicar las medidas disponibles para que sea posible inspeccionar el flujo y ofrecer cortafuegos virtuales y otras características de seguridad en la capa del hipervisor que permitan a los administradores observar y controlar el comportamiento de las máquinas virtuales (VM).

2) Aislamiento de la red y de los dominios

   Los CSP deberían aplicar medidas de aislamiento de la red y de los dominios, como cortafuegos o políticas relativas a la lista de control de acceso (ACL) en enrutadores y controladores de dominio, a fin de mantener estrictamente aislados los distintos CSC.

3) Acceso privilegiado

   Los CSP deberían aplicar medidas para garantizar el acceso privilegiado, como el acceso justo a tiempo (JAT).

4) Autenticación

   Los CSP deberían implementar métodos fiables de autenticación, como la autenticación por múltiples factores o la autenticación a partir de las huellas dactilares, entre otros, a fin de reforzar la seguridad de la autenticación.

5) Medidas para asegurar el tráfico de la red

   Los CSP deberían aplicar las medidas disponibles para defenderse de los ataques de denegación de servicio (DoS)/ataque distribuido de denegación de servicio (DDoS) y evitar la congestión de la red y desplegar sistemas de prevención o de detección de las intrusiones para hacer frente a éstas.

6) Medidas contra el software maligno

   Los CSP deberían implementar las medidas disponibles para evitar infecciones por software maligno o por virus.

7) Mejora de los parches

   Los CSP deberían actualizar periódicamente los parches y las versiones de los programas de virtualización, el sistema operativo y la base de datos (DB) a fin de disponer de las versiones más recientes.

7.2.2.5 Auditoría de seguridad

Los CSP deberían realizar periódicamente auditorías de seguridad en todo el sistema de computación en la nube. Estas auditorías puede realizarlas un equipo de auditoría independiente interno o un auditor externo (que actuará en calidad de asociado del servicio en la nube (CSN)). Los CSC deberían poder acceder a los resultados de la auditoría.

7.2.2.6 Vigilancia de la seguridad para mejorar el SLA

Los CSP deberían proporcionar mecanismos para vigilar los parámetros cuantitativos de los servicios con miras a mejorar el SLA.

1) Objetos de la vigilancia

Definir los objetos de la vigilancia, como la utilización de la unidad central de procesamiento (CPU) o las alertas de seguridad. Asimismo, deberían indicarse expresamente la condición que desencadenará el mecanismo.

2) Notificación del incidente de seguridad

Deberían estipularse la manera y el tiempo en que se notifican los incidentes de seguridad. El canal de notificación incluye correo electrónico, teléfono, mensajes breves o cualquier otro medio acordado por los CSP y los CSC. Se entiende por tiempo de notificación el tiempo medio desde que se produce el incidente hasta que se notifica al CSC.

Los CSP pueden proporcionar a los CSC unas capacidades adecuadas, como la autovigilancia y la supervisión automática a nivel de servicio de los recursos que le han sido atribuidos.

7.2.2.7 Certificación de seguridad

Los CSP deberían encargarse de adquirir los certificados de seguridad correspondientes y actualizarlos periódicamente para responder a los requisitos de los CSC.

Los ingenieros y demás personal del CSP deberían asistir a cursos de formación en materia de seguridad y poseer las calificaciones para operar la plataforma de computación en la nube.

7.2.2.8 Documentación de la actividad de seguridad

Los CSP pueden facilitar los documentos de seguridad que muestren las iniciativas que se han puesto en marcha para mejorar la seguridad de su servicio de computación en la nube, como las medidas de seguridad adoptadas, los procedimientos de gestión de la seguridad y demás. Estos documentos deberían ser fácilmente accesibles y poderse consultar o descargar desde el portal web de los CSP.

8 Directrices para la seguridad del funcionamiento diario

Los CSP deberían aplicar medidas de seguridad y organizar actividades de seguridad para administradores y arrendatarios que tengan relación con el funcionamiento diario. Las medidas y las actividades de seguridad de los CSP deberían garantizar la cláusula de seguridad del SLA y asegurar su cumplimiento. Estas medidas y actividades de seguridad incluyen, entre otras, las siguientes:

1) **Medidas de seguridad**: los CSP deben aplicar conjuntos de medidas de seguridad para ofrecer las capacidades y las instalaciones básicas para vigilar el cumplimiento de la seguridad operativa de la computación en la nube.
   a) La gestión de la identidad y el control de acceso se detallan en la cláusula 8.1.
   b) El encriptado de los datos y la gestión de claves se detallan en la cláusula 8.2.
   c) La vigilancia de la seguridad del sistema se detalla en la cláusula 8.3.
   d) La recuperación tras una catástrofe se detalla en la cláusula 8.4.
   e) La gestión de la configuración de seguridad se detalla en la cláusula 8.5.
2) **Actividades de seguridad**: los CSP deben llevar a cabo actividades de seguridad rutinarias para abordar problemas de seguridad, a fin de garantizar el funcionamiento de la computación en la nube.
   a) El tratamiento de los incidentes de seguridad se detalla en la cláusula 8.6.
   b) La actualización de los parches se detalla en la cláusula 8.7.
   c) La gestión de la configuración de seguridad se detalla en la cláusula 8.8.
   d) La respuesta ante situaciones de emergencia se detalla en la cláusula 8.9.
   e) Las copias de seguridad se detallan en la cláusula 8.10.
   f) La auditoría de seguridad interna se detalla en la cláusula 8.11.

8.1 Gestión de la identidad y del control de acceso

8.1.1 Gestión de la identidad

Los CSP deberían ofrecer una gestión de la identidad unificada a administradores internos y arrendatarios externos, que pueden proporcionar los datos brutos para un control, autorización y auditoría de acceso unificadas.

1) Este mecanismo debería apoyar la federación de identidades, a fin de permitir el intercambio de información, y la sincronización entre distintas aplicaciones en la nube en la misma zona de confianza.

2) Debería promover la gestión de la vida útil de la identidad, que incluye el control de la identidad durante toda la vida útil, es decir el registro de la identidad, la asignación de la función y de los privilegios, la modificación de éstos, la supresión de la identidad, etc. Además, el registro y la modificación de la identidad deberían incluir un procedimiento de aprobación por los administradores.

3) Las políticas de gestión de la identidad incluyen la política de denominación de la cuenta de la identidad, la política de aplicación de la cuenta de la identidad, entre otras. Estos conjuntos de políticas de seguridad deberían incluir:

   - El nombre de la cuenta de la identidad debería ser único en una misma zona de confianza.
   - La cuenta de la identidad debería bloquearse si se introduce reiteradamente una contraseña errónea.
   - La cuenta de la identidad debería desactivarse si no se utiliza durante un periodo prolongado de tiempo.
   - La cuenta de la identidad debería bloquearse si se intenta acceder a ella repetidamente en un espacio de tiempo muy breve.

4) En el marco de la gestión unificada de cuentas de usuarios, la asociación de la cuenta a un individuo concreto o a un arrendatario debería estar expresada con precisión. La cuenta principal debería identificar a los usuarios, y cada uno de ellos (administrador o arrendatario) debería tener solamente una cuenta principal. En la cuenta principal pueden crearse subcuentas, en las que pueden autorizarse determinados privilegios, como la gestión de las células de la red, los servidores de la base de datos, los servidores de la aplicación, etc.

5) La auditoría unificada de la cuenta debería centrarse principalmente en la asignación de la cuenta de la identidad, así como en el comportamiento de la conexión y la desconexión en función de los módulos de control de acceso, hecho que puede permitir identificar cuentas ilegales y cuentas atrasadas, detectar aquellas cuentas con una autorización excesiva o no autorizadas y evitar los intentos de conexión a cuentas abandonadas o falsas. Debería presentar una relación de los incidentes de seguridad relacionados con las cuentas al módulo o a los sistemas de auditoría de seguridad a fin de poder realizar muchas más tareas de auditoría, como la detección de intromisiones, la auditoría de fallos de control, etc.

6) Debería soportar la gestión de las contraseñas de usuario, que incluye los conjuntos unificados de políticas de contraseñas de usuarios basadas en la política de seguridad de la plataforma en la nube, como los algoritmos criptográficos, la longitud de la contraseña, su complejidad o su ciclo de actualización. Debería soportar distintos tipos de contraseñas, como las contraseñas gráficas o sonoras, entre otras. Además, debería soportar las funciones de sincronización y de renovación de las contraseñas.

7) Debería ofrecer a los arrendatarios la posibilidad de gestionar sus cuentas. Los propios arrendatarios pueden llevar a cabo determinadas tareas de gestión, como la modificación de algunas propiedades sencillas de usuario y la actualización de las contraseñas, lo que puede aligerar las tareas de mantenimiento que recaen en el personal de gestión.

8.1.2 Gestión del control del acceso

Los CSP deberían establecer un sistema unificado y centralizado de autenticación y autorización a fin de mejorar el control de acceso en las actividades cotidianas. Los registros operativos del control del acceso a los sistemas de computación en la nube deberían almacenarse para su posterior auditoría.

1) La autenticación unificada debería soportar las siguientes funciones:
   - Debería soportar el inicio de sesión con registro único (SSO): debería soportar los parámetros que establecen el SSO, como el tiempo máximo de sesión, el tiempo máximo de reposo y el tiempo máximo de caché.
   - Debería soportar las principales tecnologías de autenticación, como la autenticación LDAP, la autenticación de la certificación digital, la autenticación por testigo, la autenticación biométrica o la autenticación a partir de múltiples factores, entre otros.
   - Debería proporcionar unos registros de autenticación detallados que incluyan las identificaciones del sistema, los usuarios activos, la hora de conexión y de desconexión, la dirección del protocolo Internet (IP) de conexión, el terminal desde el que se ha realizado la conexión, los registros del resultado de la conexión (éxito o fracaso).
   - Debería proporcionar métodos de autenticación optativos y diferenciados, en función de los distintos sistemas y servicios. Esta medida puede servir para encontrar un punto de equilibrio entre el nivel de seguridad, la facilidad de uso e incluso el coste.
2) La autorización unificada debería soportar las funciones siguientes:
   - Debería proporcionar autorización para acceder a los recursos en la nube, según la definición previa de usuarios, grupos de usuarios y nivel de privilegio de éstos.
   - Debería soportar tanto los mecanismos de autorización centralizada como los de autorización jerárquica; asimismo, el administrador de las autorizaciones debería restringir el nivel de autorización de los administradores jerárquicos autorizados.
   - Debería soportar una política específica de autorización, así como una política general de autorización.
   - Debería proporcionar registros detallados de las autorizaciones, incluidas las direcciones IP, el operador y el tiempo de autorización, así como de los permisos otorgados y cancelados.
3) Otros requisitos:
   - Control en los registros de acceso. Los CSP deberían velar por que los administradores dispongan de los privilegios correspondientes para acceder a los registros. Los administradores deberían conceder a los arrendatarios los privilegios necesarios para consultar sus registros mediante un portal de autoservicio u otras herramientas de cliente.
   - Mecanismos de encriptación. Los datos sensibles, como los datos de autenticación o de autorización, entre otros, deberían estar encriptados durante el procedimiento de almacenamiento y de transmisión.
   - Todos los registros operativos relativos al CSC deberían ser convenientemente visibles.

8.2 Encriptado de datos y gestión de claves

El encriptado y la gestión de claves son los mecanismos principales para proteger los datos en los sistemas de computación en la nube. El encriptado permite la protección de los recursos, mientras que la gestión de claves proporciona el control de las claves criptográficas que se utilizan para proteger los recursos.

La cláusula de seguridad del SLA debería definir claramente la aplicación específica del encriptado. Además, el encriptado debería seguir las normas gubernamentales y del sector pertinentes. Los CSP y los CSC deberían considerar los elementos siguientes:

1) Encriptado de la transmisión de datos en la red. Es especialmente importante proteger credenciales como la información financiera, las contraseñas, etc.

2) Encriptado de datos estáticos en el disco o en la base de datos. Podría servir para evitar CSP maliciosos o arrendatarios vecinos maliciosos.

3) Encriptado de datos en los medios para la copias de seguridad. Podría servir para evitar la fuga de datos en caso de que se perdieran los medios para las copias de seguridad o fueran sustraídos.

Si el CSP es el principal responsable de garantizar el encriptado de los datos, la gestión de las claves es un aspecto fundamental de las operaciones cotidianas. El CSP debería definir y aplicar una gestión integrada de las claves durante toda su vida útil, incluida su generación, utilización, almacenamiento, copia de seguridad, recuperación, actualización y destrucción. Los CSP también deberían tener en cuenta las cuestiones siguientes:

1) Protección del almacenamiento de claves: el almacenamiento de claves debe protegerse, al igual que se hace con otros datos sensibles, e incluso el nivel de seguridad en este caso debe ser mayor que el que se aplica a otros elementos. Solamente una entidad específica puede acceder al almacenamiento de claves. También se necesitan políticas conexas, como la separación de funciones, para velar por un control de acceso más estricto.

2) Copias de seguridad y recuperación: dado que la pérdida imprevista de una clave concreta puede provocar la destrucción de un servicio, es necesario disponer de una solución para la realización de copias de seguridad de las claves y su recuperación.

3) Introducción de un tercero para la gestión de claves: la separación de funciones podría ayudar a los CSP a evitar conflictos de índole legal cuando exista la certeza de que se han facilitado los datos disponibles en sistemas de computación en la nube.

8.3 Vigilancia de la seguridad del sistema

En las operaciones cotidianas, los CSP deberían llevar a cabo una vigilancia centralizada de la seguridad en tiempo real tanto en la plataforma y en la infraestructura de la nube que incluya vigilar el estado de distintos recursos físicos y virtuales activos. Al considerar los términos principales del SLA (como el rendimiento de la red, la utilización de los recursos del sistema anfitrión y del almacenamiento, etc.) y analizar todo tipo de registros, los CSP pueden llevar a cabo la gestión de los fallos, del desempeño y de la inspección automática a fin de alcanzar el objetivo de vigilancia de la situación de los recursos en la nube en tiempo real o casi en tiempo real.

En general, los CSP son gestionados y estrictamente protegidos por los CSP. No obstante, si los CSC lo necesitan, los CSP podrían facilitarles los registros de vigilancia que soliciten, por ejemplo, un CSC puede necesitar registros de supervisión para la resolución de problemas en respuesta a situaciones de emergencia.

Los CSP también pueden detectar proactivamente posibles riesgos operativos y resolverlos oportunamente. Además, los CSP deberían ofrecer la posibilidad de realizar un análisis de la correlación entre los CSC y los servicios ofrecidos por los CSP que puede contribuir a evaluar la calidad y la situación de seguridad de los servicios en la nube.

Existen dos tipos de modos de vigilancia de la seguridad: la vigilancia automática y la inspección manual, basados en los medios técnicos y en la gestión de cada CSP. La finalidad de la vigilancia de la seguridad implica distintos elementos:

1) Vigilancia del estado de la infraestructura de la computación en la nube: los CSP deberían ofrecer la capacidad para recopilar y vigilar los registros de los incidentes de seguridad, la información sobre vulnerabilidad, la alteración de la configuración de los dispositivos de seguridad, la situación de respuesta y funcionamiento de todos los objetos de la infraestructura de computación en la nube, lo que incluye los recursos de máquina virtual (VM), la plataforma de gestión de la computación en la nube, los dispositivos de seguridad,

las bases de datos y demás. Esta vigilancia puede servir para que los CSP se hagan una idea del estado general y operativo de la infraestructura en la nube.

2) Detección de un comportamiento anormal: el comportamiento anormal incluye la conexión ilegal, el acceso ilegal a la plataforma de gestión en la nube y el acceso ilegal a otros recursos, las modificaciones anormales de la configuración del equipo de red y de las máquinas virtuales u otras intromisiones que pueden llevarse a cabo por medios técnicos, como las herramientas integradas de auditoría, los programas de DLP y otras herramientas de seguridad.

3) Vigilancia de un tráfico anormal en la red: los CSP deberían disponer de la capacidad para detectar y analizar el tráfico anormal en la red física y en la red virtual, especialmente el tráfico intra-VM. Es necesario conocer el tráfico de la red y su rendimiento, pues esos detalles pueden ayudar a los CSP a mejorar la capacidad de defensa contra gusanos, ataques por tráfico anormal y otras posibles amenazas para la seguridad en el entorno de la computación en la nube.

4) Vigilancia de la seguridad física: los objetos de la vigilancia de la seguridad física incluyen el sistema de control de la temperatura y la humedad, la televisión en circuito cerrado (CCTV), la vigilancia de los accesos a las instalaciones, un sistema de protección contra incendios, sistemas de aire acondicionado, sistema de alimentación, vigilancia, verjas de protección, etc., que pueden inspeccionarse a diario.

Ante todo, los CSP deberían comprobar exhaustivamente el entorno de la computación en la nube a fin de conocer la situación de estos servicios durante las tareas de funcionamiento diario y mantenimiento. Esta medida puede permitir a los CSP detectar rápidamente indicadores como la calidad de rendimiento de la red, el comportamiento de la VM o la calidad de servicio orientada a los CSC, entre otros. Además, este proceso de comprobación puede adaptarse para soportar alertas relativas a los valores umbral o incluso de referencia. La información recopilada debería permitir a los CSP detectar rápidamente problemas en la red, de almacenamiento, de las máquinas físicas o de las plataformas virtuales cuando se produzcan fallos.

Los CSP también deberían ser capaces de poder ubicar otros CSC potencialmente afectados a partir de un análisis de correlación sobre cada fallo específico, partiendo de la hipótesis de que los CSC comparten las mismas debilidades, aplicaciones y la misma versión del sistema operativo, etc.

8.4 Recuperación tras una catástrofe

Los CSP deberían adoptar medidas de seguridad para que, tras una catástrofe, los sistemas recuperen el nivel de seguridad anterior. La tecnología empleada en las medidas de seguridad incluye la aglomeración de servidores o la duplicación remota sincrónica y asincrónica para dotarse de unos mecanismos que permitan la recuperación tras una catástrofe sin necesidad de inicializar el sistema.

1) Agrupación de servidores

   La agrupación de servidores permite coordinar y gestionar los errores y los fallos de los distintos componentes y añadir componentes a la aglomeración de manera transparente, elástica y progresiva a fin de alcanzar un rendimiento suficiente.

2) Duplicación a distancia síncrona

   A través de programas de duplicación a distancia, los datos del sitio primario se replican de manera síncrona y se transmiten a un sitio distante. Cuando falla el sitio primario, los programas en funcionamiento se dirigirán hacia el sitio distante. La duplicación síncrona permite garantizar la continuidad de las operaciones sin que haya pérdida de datos. Este método tiene un coste elevado, ya que depende de un programa de duplicación cuidadosamente diseñado y requiere un ancho de banda de red suficiente. La duplicación a distancia síncrona se lleva a cabo periódicamente en sistemas con un nivel de seguridad alto.

3) Duplicación a distancia asíncrona

Existe otro método de duplicación remota que suele tener un coste menor que la duplicación a distancia síncrona. Los datos del sitio primario se replican periódicamente y se transmiten a un sitio distante. Si no hay problemas, este método puede garantizar una copia completa en el sitio distante sin que el rendimiento del sitio primario se vea afectado. No obstante, si hay problemas durante la duplicación, la pérdida de datos es inevitable. Puede optarse por la duplicación a distancia asíncrona tras una evaluación exhaustiva de los riesgos.

8.5 Gestión de la configuración de seguridad

La configuración de seguridad incluye las reglas de seguridad configuradas en la plataforma en la nube, la red, las máquinas virtuales y distintos componentes de aplicación. Es distinta de una política de seguridad de alto nivel, que establece el enfoque de la organización para alcanzar los objetivos en materia de seguridad de la información.

Los CSP deberían encargarse de la gestión integrada de la configuración de seguridad a fin de garantizar una aplicación efectiva y un despliegue rápido de la configuración de seguridad.

En términos de gestión de la configuración de seguridad, se recomienda que los CSP elaboren unos modelos de configuración de la política de seguridad y unos criterios de referencia de la política de configuración de seguridad. Además, los CSP deberían adoptar medidas para velar por la coherencia y la efectividad de la configuración de seguridad cuando se produzcan cambios en el entorno en la nube, así como para aislar la configuración de seguridad entre los CSC en un entorno de multiarrendamiento.

Los modelos de la configuración de seguridad incluyen los modelos principales de configuración de seguridad que necesita el entorno actual de computación en la nube, como la gestión de cuentas, la autenticación, las políticas de control de acceso, las políticas de auditoría, las políticas de respuesta dinámica, las políticas de aplicación y actualización de los programas, las políticas de copias de seguridad y recuperación, etc.

Los criterios de referencia en materia de configuración de seguridad permiten orientar los requisitos para la configuración de seguridad en todo el entorno de la computación en la nube, hecho que puede ayudar a los CSP a evaluar si la configuración vigente reúne o no el nivel de seguridad fundamental y proporcionar orientaciones adicionales sobre el cumplimiento. Las categorías de los criterios de referencia sobre configuración de seguridad deberían incluir, entre otras, las siguientes: criterios de referencia sobre configuración de seguridad del sistema operativo, criterios de referencia sobre configuración de seguridad de la base de datos, criterios de referencia sobre configuración de seguridad del cortafuegos, criterios de referencia sobre configuración de seguridad del centro de conmutación, criterios de referencia sobre configuración de seguridad del enrutador, etc.

La gestión de la configuración de seguridad implica las siguientes medidas:

1) Gestión del modelo de configuración de seguridad

   Los CSP deberían fijar los principales modelos de seguridad para los requisitos del entorno en la nube a fin de agilizar y adecuar el despliegue de la configuración de seguridad. La gestión del modelo de configuración de seguridad debería soportar modelos adaptados y actualizarlos y optimizarlos continuamente basándose en los cambios que se produzcan en la plataforma en la nube, la situación de la red o las necesidades del servicio, entre otras.

   Además, los CSP deberían facilitar a los CSC las herramientas para adaptar los nuevos modelos de configuración de seguridad a partir de sus propios requisitos. Adicionalmente, los CSC deberían responsabilizarse de la eficacia de la configuración de seguridad que ellos mismos han adaptado.

2) Gestión del proceso de configuración de seguridad

   Los CSP deberían dar fe de la eficacia de la configuración de seguridad. Ésta puede configurarse en función de las necesidades de los CSC y de los servicios en la nube. El

proceso principal de gestión de la configuración de seguridad implica distintas etapas: solicitud de configuración, aprobación, comprobación y validación técnica, aplicación, archivo de la configuración e informe final.

3) Gestión de los criterios de referencia en materia de configuración de seguridad

Los CSP deberían desarrollar unos criterios de referencia en materia de configuración de seguridad a partir de un examen exhaustivo de los requisitos de seguridad de la plataforma de la computación en la nube, los servicios en la nube, los CSC, la cláusula de seguridad del SLA etc.

Principalmente, la gestión de los criterios de referencia en materia de configuración de seguridad implica la solicitud y el registro de los controles de la configuración de seguridad, la aprobación y aplicación de estos controles, el informe final al respecto, la aplicación de medidas de refuerzo y el informe sobre el resultado de estas medidas de refuerzo. El control de la configuración de seguridad debería llevarse a cabo periódicamente durante el funcionamiento diario y puede efectuarse recopilando información sobre la configuración y analizando los criterios de referencia en materia de seguridad.

4) Gestión de los conflictos derivados de la configuración de seguridad

En un entorno en la nube con compartición de recursos, como consecuencia de los fallos causados por el administrador de seguridad o a causa de otros motivos, la configuración de seguridad podría verse amenazada, hecho que puede provocar vulnerabilidades en el entorno de computación en la nube. Los CSP deberían adoptar medidas eficientes para detectar conflictos en la configuración de seguridad y establecer procesos de gestión de los conflictos derivados de la configuración de seguridad y mecanismos de recuperación.

El proceso de gestión de los conflictos derivados de la configuración de seguridad debería incluir alertas en caso de conflicto, el análisis de estos conflictos (que debería incluir un análisis de los motivos y de las consecuencias), su gestión y un informe de resultados.

5) Gestión de la migración de la configuración de seguridad

Cuando se produzcan cambios en los servicios o en el recurso de computación en la nube (por ejemplo, una ampliación de la capacidad de servicio, la migración de VM, etc.), los CSP deberían proporcionar medios dinámicos para ajustar la configuración de seguridad. Por ejemplo, durante la migración de VM, puede llevarse a cabo una migración automática de la configuración de seguridad mediante la detección de la situación de la migración, la concordancia automática y la instauración de nuevo de la política original de configuración de seguridad, que podría garantizar una coherencia de la política de configuración de seguridad y una rápida implantación en el entorno en la nube, además de mejorar la eficacia de la seguridad.

6) Gestión del aislamiento de la configuración de seguridad

En un entorno de multiarrendamiento de computación en la nube, los CSP deberían llevar a cabo una gestión estricta de la clasificación de la configuración de seguridad de los CSC y adoptar medidas tales como la autenticación o el control de acceso, etc., a fin de garantizar el aislamiento de la configuración de seguridad entre distintos CSC.

8.6 Tratamiento de los incidentes de seguridad

Los CSP deberían llevar a cabo determinadas actividades para gestionar los incidentes de seguridad en el entorno de computación en la nube, como las alertas por amenaza, las vulnerabilidades, las emergencias, etc. Los CSP deberían implementar además medidas técnicas para ayudar a detectar incidentes de seguridad, alertar sobre ellos y abordarlos.

En general, el procedimiento para el Tratamiento de los incidentes de seguridad en el entorno de la computación en la nube se compone de los pasos siguientes: detección, análisis, supresión,

comprobación, presentación de informes y registro. Los CSP deberían especificar explícitamente quiénes son las personas responsables en cada etapa.

8.6.1 Detección

Los CSP deberían adoptar medidas para vigilar la situación de seguridad de la plataforma en la nube, cuestión que se menciona en la cláusula 8.3, disponer de los medios para enviar a tiempo alertas cuando se produzcan incidentes de seguridad. Deberían velar porque esas alertas puedan enviarse a la persona designada, por ejemplo el responsable de seguridad de la plataforma de computación en la nube. Las alertas pueden enviarse por correo electrónico, mediante una llamada telefónica, un mensaje breve de texto (SMS), etc. Los CSP deberían asegurarse de que se supervisan todos los tipos de incidentes de seguridad señalados en la cláusula de seguridad del SLA.

8.6.2 Análisis

Los CSP deberían confirmar los incidentes de seguridad después de recibir las alertas y proceder posteriormente a su análisis y diagnóstico para determinar el tipo de incidente, sus causas y las medidas para su tratamiento. Los CSP pueden solicitar asistencia a los CSC en caso de que sea necesario.

8.6.3 Supresión

Los CSP deberían adoptar medidas de gestión, en función del tipo y el nivel de los incidentes de seguridad, a fin de minimizar sus consecuencias. Los CSP deberían hacer referencia a las actividades de seguridad mencionadas en las cláusulas 8.7, 8.8 y 8.9, que incluyen, entre otras:

1) En el caso de una emergencia de seguridad, los CSP deberían adoptar medidas de acuerdo con los planes de respuesta para situaciones de emergencia.
2) En el caso de una vulnerabilidad de seguridad, los CSP deberían adoptar medidas de acuerdo con la actualización del parche.
3) En el caso de una debilidad de la configuración, los CSP deberían adoptar medidas de acuerdo con la gestión de la configuración de seguridad.

Los CSP deberían vigilar y evaluar de manera dinámica los incidentes de seguridad, y comunicar a los CSC la información conexa y los progresos en la gestión de los incidentes.

8.6.4 Comprobación

Después de suprimir los incidentes de seguridad, los CSP deberían seguir analizando los motivos y las situaciones que pueden provocar esos incidentes y comprobar si otros sistemas de los CSC presentan vulnerabilidades similares que podrían provocar unos incidentes de seguridad idénticos. Si la vulnerabilidad persiste, los CSP deberían notificarlo inmediatamente a los CSC conexos y adoptar las medidas correspondientes. La notificación no debería afectar a la privacidad de otros CSC.

8.6.5 Presentación de informes y registro

Los CSP deberían elaborar informes sobre la gestión de los incidentes de seguridad en los que se detalle el comportamiento de los incidentes de seguridad, sus causas, las medidas de gestión, etc., y enviarlos a los CSC conexos dentro del plazo estipulado en la cláusula de seguridad del SLA. Los CSP deberían registrar la información de los incidentes de seguridad para su inspección y auditoría posterior. Los informes correspondientes pueden transmitirse a los CSC afectados y a los auditores externos (que ejercen de CSN).

8.7 Actualización de parches

8.7.1 Responsabilidades

Los CSP deberían optimizar el proceso de gestión de parches de la plataforma en la nube a fin de reducir los posibles riesgos causados por las vulnerabilidades y proteger un funcionamiento estable de las plataformas y de los servicios en la nube.

En la computación en la nube, los CSP y los CSC deberían encargarse conjuntamente de la gestión de los parches.

1) Responsabilidades de los CSP:
   - hacer un seguimiento de los informes de vulnerabilidades de los sistemas operativos duplicados y localizar oportunamente los parches más recientes;
   - comprobar la seguridad y la adaptabilidad de los parches;
   - actualizar el parche del sistema operativo duplicado y crear los archivos de imagen más recientes;
   - informar y ayudar a los CSC a concluir la actualización del parche y asegurarse de que no se repetirá la misma vulnerabilidad;
   - realizar la prueba de efecto de los últimos archivos de imagen mediante la creación de una nueva máquina virtual.
2) Responsabilidades del CSC:
   - ayudar a los CSP a hacer un seguimiento de las novedades sobre vulnerabilidades y localizar las actualizaciones más recientes;
   - actualizar de manera oportuna los parches de la máquina virtual, de acuerdo con la información suministrada por los CSP.

En función de cual sea el modo de servicio de la computación en la nube (IaaS, PaaS o SaaS), el CSP, al igual que el CSC, solamente es responsable del recurso que él mismo controla. En el caso de IaaS, los CSP deberían encargarse de la actualización de parches de la infraestructura de la computación en la nube y los CSC, del OS invitado, del programa de aplicación, etc., bajo su control.

8.7.2 Proceso de actualización de parches de seguridad

Los componentes de la plataforma en la nube que deben actualizarse mediante parches incluyen el programa de virtualización, los sistemas operativos, el equipo de red, el equipo de seguridad, los servidores de la base de datos o los terminales de gestión, entre otros. El proceso de bucle cerrado de la actualización de parches se compone de cuatro etapas, tal y como se muestra a continuación; estas etapas podrían ayudar a los CSP a garantizar los mejores plazos para actualizar la plataforma en la nube.

1) Recopilación del parche

Los CSP deberían recopilar información sobre el parche del sitio web oficial del vendedor y utilizar las herramientas de actualización automática del parche proporcionadas por éste o cualquier otro medio que garantice la integridad de los requisitos del parche. Los CSP deberían efectuar un análisis de los parches recopilados, detectar y registrar las vulnerabilidades de los sistemas y de las aplicaciones existentes, evaluar los efectos y los riesgos potenciales de la actualización y determinar la urgencia y la importancia de los parches.

2) Prueba del parche

Los CSP deberían realizar pruebas del parche para verificar su seguridad, compatibilidad y estabilidad. Deberían establecer un entorno de prueba que permita emular la plataforma o los sistemas objetivo antes de llevar a cabo la actualización. Tras la comprobación, habría que elaborar un informe que sugiera la conveniencia o no de publicar el parche. El informe contiene asimismo orientaciones

técnicas detalladas sobre los pasos de la actualización y su despliegue, y debería facilitar además una descripción exhaustiva de los parches a fin de que los ingenieros puedan entender las funciones del parche y su funcionamiento, sus efectos sobre los sistemas y aplicaciones (por ejemplo, los problemas que provoca), a qué sistemas y archivos afecta, si habría que volver a cargar el sistema o la aplicación, etc.

3) Actualización del parche

Los CSP deberían preparar un plan operativo para la actualización del parche que incluya los pasos detallados, de acuerdo con el informe resultante de la prueba. También habría que elaborar un plan de emergencia que incluya la copia de seguridad del sistema y de los datos, la conmutación de aplicaciones, el control del tiempo de publicación del parche, la desinstalación del parche y el despliegue del sistema en caso de fallo del parche. Para la publicación de parches a gran escala, los CSP deberían recurrir por anticipado al soporte técnico de los vendedores con miras a mejorar la capacidad de tratamiento de las emergencias ante situaciones inesperadas.

Los CSP también deberían poner en conocimiento de los CSC el momento de la publicación del parche en la plataforma en la nube y los intercambios de información con éstos antes de la instalación del parche deberían ser claros. Los CSP no deberían tratar de influir en modo alguno en los servicios de los CSC, motivo por el cual deberían adoptar las medidas oportunas junto con los CSC.

4) Verificación del parche

Una vez publicado el parche, los CSP deberían utilizar las herramientas de gestión de parches para comprobarlos periódicamente y asegurarse de que en todos los componentes de la plataforma en la nube se han instalado las versiones más recientes. El documento del registro de los parches debería actualizarse periódicamente y archivarse para ulteriores auditorías de seguridad.

El tiempo de espera entre la recopilación y la actualización del parche y el requisito de aprobación de los CSC respecto de su actualización debería estar claramente estipulado en el SLA, en función del tipo de prioridad del parche (p. ej., crítica, alta, media o baja).

A continuación se presenta un ejemplo de un proceso de actualización de parches de seguridad, incluida la actualización de la máquina virtual y sus archivos imagen. En este proceso, si se opta por la versión más reciente de algún parche, corresponde a los CSP comprobar su seguridad y adaptabilidad. Los CSC son los encargados de encontrar y recopilar las versiones más recientes de los parches. Una vez comprobadas con éxito las versiones más recientes de los parches, los CSP informarán a los CSC de la actualización de los parches. Al mismo tiempo, los CSP actualizarán los parches de los archivos de imagen actuales. Los CSP podrían crear una nueva máquina virtual a partir de estos nuevos archivos de imagen. Los CSP también llevarán a cabo un escaneado específico para asegurarse de que los CSC han actualizado con éxito los parches.

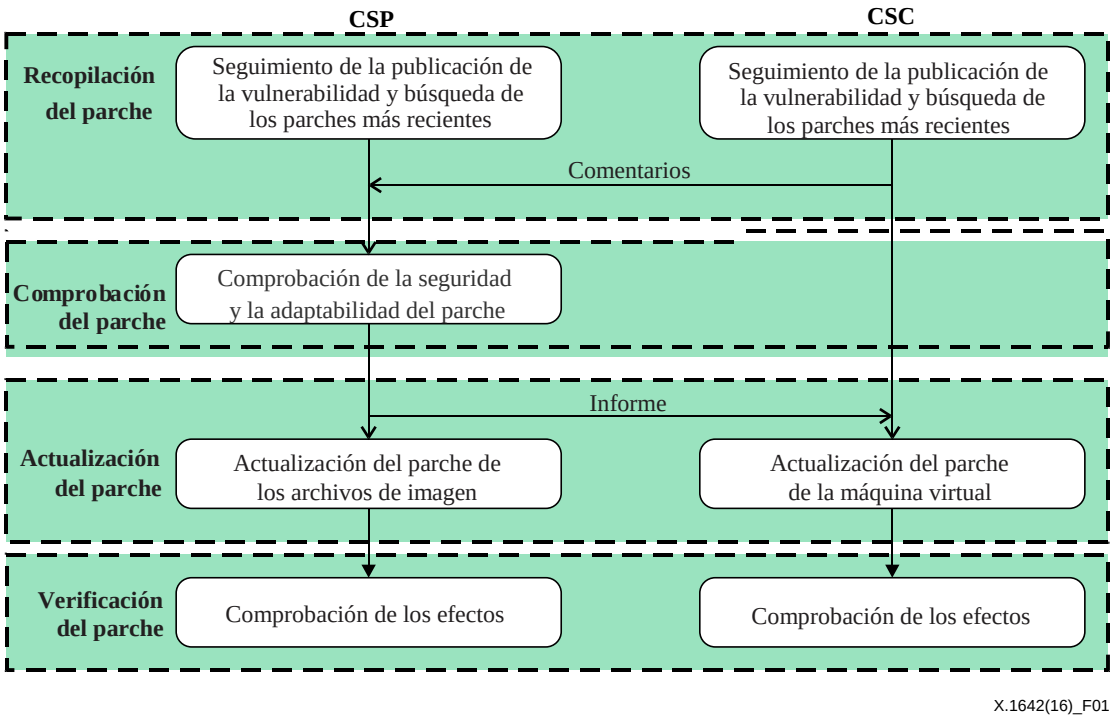

Figura 1 – Ejemplo de proceso de actualización de parches de seguridad

8.8 Seguridad de la gestión de la configuración

Los CSP deberían llevar a cabo controles de seguridad de la gestión de la configuración de la plataforma en la nube, la configuración de red y los parámetros de los distintos componentes de la aplicación; estas medidas podrían contribuir a reducir los riesgos operativos provocados por una mala configuración o una utilización indebida y a mejorar la seguridad y la estabilidad del entorno de computación en la nube.

La gestión de la configuración suele incluir la gestión de las modificaciones en la configuración y de la publicación. Los CSP deberían adoptar medidas para velar por que se hayan supervisado y registrado las modificaciones de la configuración y su publicación. A fin de facilitar la gestión de la configuración, suele crearse una base de datos integrada con información relativa a la configuración que incorpora los registros actuales e históricos de todos los archivos de configuración, la política de seguridad y los perfiles de aplicación de cada elemento y de cada componente de la computación en la nube. Los CSP deberían proteger esta base de datos respecto del acceso no autorizado, las fugas de información, etc.

La seguridad de la gestión de la configuración comporta las medidas siguientes:

1) Auditoría de gestión de la configuración

   La auditoría de gestión de la configuración tiene por fin garantizar que los requisitos de modificación y de publicación de la configuración se han aplicado de manera efectiva y eficiente. Puede ayudar a los CSP a verificar la exactitud, coherencia, exhaustividad, validez y trazabilidad de cada elemento de la configuración. La auditoría de gestión de la configuración debería realizarse periódicamente durante las operaciones cotidianas.

   Todos los registros de acceso de usuario, modificación, archivo y recuperación, deberían registrarse y archivarse para su auditoría en línea y fuera de línea.

   Además, los CSC deberían poder consultar el informe de la auditoría de gestión de la configuración relativo a ellos o a sus servicios, a fin de poder supervisar las medidas de seguridad y la efectividad de los CSP.

2) Vigilancia de la gestión de la configuración

Los CSP deberían vigilar todas las alteraciones y demás operaciones en los archivos de configuración de todo el entorno de computación en la nube a fin de evitar el acceso no autorizado, las filtraciones, las modificaciones ilegales o las configuraciones inadecuadas.

3) Protección de la base de datos de gestión de la configuración

Los CSP deberían llevar a cabo un mantenimiento y una gestión precisa de la base de datos de gestión de la configuración y ejecutar tareas como la asignación de competencias según las funciones, la eliminación de archivos basura, auditorías periódicas, la realización periódica de copias de seguridad, etc.

8.9 Planes de respuesta a situaciones de emergencia

Es vital garantizar que los CSP pueden operar de manera efectiva los sistemas de computación en la nube sin que haya interrupciones excesivas tras un incidente de seguridad. Los planes de respuesta para situaciones de emergencia soportan este requisito al definir un programa, procedimientos y medidas técnicas efectivas.

A fin de reducir las consecuencias de los incidentes de seguridad en las plataformas y los servicios de computación en la nube, el plan de respuesta para situaciones de emergencia de los CSP debería proporcionar unas orientaciones claras a los operadores y lograr un equilibrio entre el nivel de detalle necesario y el grado adecuado de flexibilidad. El desarrollo y la gestión de un plan de respuesta para situaciones de emergencia es un ciclo de mejora continuada que consta de tres fases: la fase de desarrollo, la fase de comprobación y aplicación y la fase de mantenimiento.

8.9.1 Fase de desarrollo

En primer lugar, habría que adoptar métodos de análisis cuantitativo y cualitativo para realizar una evaluación exhaustiva de los riesgos y un análisis del impacto de las actividades (BIA) de los sistemas de computación en la nube. De este modo, podrían conocerse las características y los componentes clave del sistema, así como los efectos de los distintos incidentes de seguridad. A partir de estos elementos, y de acuerdo con lo dispuesto en la cláusula de seguridad del SLA entre los CSP y los CSC, pueden formularse los requisitos reglamentarios y el objetivo de recuperación de la respuesta para situaciones de emergencia, entendidos como el alcance de RTO y de RPO. Además, al formular un plan de respuesta para situaciones de emergencia también habría que tener en cuenta las características del servicio en la nube y la clasificación de los incidentes.

El plan de respuesta para situaciones de emergencia incluye:

1) Notificación: habría que desarrollar un procedimiento de notificación para comunicar al equipo de respuesta, al personal directivo y a los CSC conexos que ha ocurrido un incidente de seguridad.

2) Clasificación y calificación de los incidentes de seguridad: el equipo de respuesta para situaciones de emergencia debería evaluar el incidente de seguridad a fin de determinar su categoría y su calificación.

3) Inicio: una vez calificados y clasificados los incidentes de seguridad, los CSP y los CSC deben activar, con carácter de urgencia, el correspondiente programa de respuesta preestablecido.

4) Actuación: una vez activado el programa de respuesta, habría que adoptar inmediatamente medidas para contrarrestar las consecuencias de los incidentes de seguridad. Adicionalmente, habría que poner en marcha las actividades de recuperación en cuanto se hayan logrado controlar de manera efectiva los incidentes.

5) Medidas posteriores: una vez concluida la actuación de emergencia, es importante analizar la respuesta de emergencia más reciente a fin de formular una conclusión al respecto que incluya las medidas adoptadas para analizar y resumir los motivos que provocaron el incidente y evaluar las pérdidas y la efectividad del plan de respuesta para situaciones de emergencia.

Existen otros elementos fundamentales, entre ellos:

1) Los miembros del equipo de respuesta para situaciones de emergencia, sus responsabilidades específicas y la información de contacto de cada uno de los miembros. En sentido general, el equipo de respuesta para situaciones de emergencia se compone de personal de gestión, operativo, técnico y administrativo.

2) Los resultados del BIA relativos a la relación entre las distintas partes del sistema de computación en la nube, el nivel de prioridad de los componentes clave, etc.

3) El criterio, los procedimientos y las listas de comprobación relativas a la recuperación del sistema de computación en la nube.

4) El inventario de los soportes físicos, los equipos lógicos y los microprogramas, así como de otros recursos para soportar el funcionamiento diario de los CSP; cada entrada debería incluir la versión, el número de éstos, etc.

5) La información de contacto de los CSC y los procedimientos de respuesta negociados por los CSP y los CSC, de acuerdo con lo dispuesto en la cláusula de seguridad del SLA, a fin de minimizar las pérdidas de los CSC durante un incidente de seguridad.

6) En sentido general, el CSP no puede acceder a los datos privados del CSC a menos que éste se lo haya autorizado. En el caso de una emergencia iniciada por el CSC, éste podría necesitar la ayuda del CSP para proporcionar una respuesta más efectiva, motivo por el cual autorizaría al CSP a acceder a los datos. En este contexto, el CSP no debería hacer un uso indebido de la autorización para acceder a los datos del CSC.

8.9.2 Fase de pruebas e implantación

A fin de poner a prueba la efectividad del plan de respuesta para situaciones de emergencia, los CSP deberían organizar pruebas y simulacros del plan de respuesta para situaciones de emergencia con la participación de aquellos miembros del personal familiarizados con los procedimientos de respuesta. Las pruebas y las simulaciones deberían cumplir los requisitos siguientes:

1) Habría que establecer previamente los programas de prueba, formación y simulación.

2) Habría que describir detalladamente el proceso de prueba, formación y simulación y redactar los correspondientes informes.

3) Se recomienda a los CSP y a los CSC que realicen conjuntamente a nivel corporativo pruebas planificadas siempre que puedan producirse cambios significativos dentro o fuera de las condiciones de la computación en la nube.

Cuando se produzcan incidentes de seguridad o una interrupción de las operaciones, habría que aplicar estrictamente el plan de respuesta para situaciones de emergencia en cuanto se den las condiciones para su puesta en marcha, y habría que anotar todas las operaciones que se realizan durante la situación de emergencia. Posteriormente, de acuerdo con lo dispuesto en la cláusula de seguridad del SLA, el CSP debería someter los informes de respuesta a los CSC.

El plan de respuesta a situaciones de emergencia debería revisarse sobre la base de los resultados de las pruebas, las simulaciones y su implantación a fin de mejorar su efectividad y su viabilidad.

8.9.3 Fase de mantenimiento

Para que siga siendo efectivo, el plan de respuesta para situaciones de emergencia debería poder, en todo momento, hacerse eco de los requisitos de los sistemas de computación en la nube, la

modificación del SLA, los cambios en la configuración y los cambios de personal. En sentido general, habría que revisar anualmente el plan para adaptarlo a los cambios en el entorno real de computación en la nube. La modificación del plan se basa en los elementos siguientes:

1) Los cambios en las instalaciones, los recursos y los servicios.

2) Los cambios en la cláusula de seguridad de los requisitos del SLA, en la configuración crítica de la seguridad, en una actualización importante del parche o en los miembros fundamentales del equipo.

3) La evaluación de la efectividad del plan a partir de los registros de su aplicación real durante la fase de comprobación y los incidentes de seguridad.

8.10 Copias de seguridad

La capacidad para realizar copias de seguridad es un aspecto importante para los CSC y los CSP en el entorno de la computación en la nube. Antes de llevar a cabo cualquier copia de seguridad, los CSP deben ocuparse de determinadas especificaciones, tales como:

– la estrategia para la realización de copias de seguridad de cada CSC o servicio específico en la nube;

– el método de almacenamiento, en particular si incluye o no encriptado;

– la ubicación del almacenamiento, en particular si es local y/o remoto;

– los periodos de retención para los datos de la copia de seguridad;

– los procedimientos para comprobar los datos de la copia de seguridad.

Antes de elegir un CSP, el CSC debería confirmar si el CSP puede cumplir la cláusula de seguridad del SLA, incluida la capacidad para copias de seguridad. Si el CSP no dispone de las herramientas para realizar copias de seguridad, el CSC debería plantearse seriamente diseñar una estrategia para realizar copias de seguridad y su aplicación. Si, por el contrario, el CSP ofrece la posibilidad de realizar copias de seguridad, el CSC debería colaborar con el CSP para llevar a cabo esas operaciones.

El CSP debería compartir los detalles esenciales del mecanismo de las copias de seguridad con los CSC. Al realizar las copias de seguridad, los CSP deberían tratar de respetar las especificaciones para intentar satisfacer cada uno de los siguientes requisitos del CSC:

1) Estrategia para la realización de copias de seguridad: dado que cada CSC tiene sus propias necesidades en materia de copias de seguridad, habría que considerar los factores conexos, que incluyen:
   – Un objetivo de punto de recuperación (RPO) y unos objetivos de tiempo de recuperación (RTO) razonables. El RPO indica el plazo de tiempo entre dos copias de seguridad consecutivas, mientras que el RTO refleja el tiempo necesario para desplegar una copia de seguridad.
   – Una política de retención razonable: la política debería especificar el número de copia de cada copia de seguridad.
   – Un equilibrio razonable entre copias de seguridad de archivos y copias de seguridad de máquinas virtuales: el coste de inversión de esta combinación debería ser óptimo, y basarse tanto en RPO como en RTO.
   – Un equilibrio razonable entre copias de seguridad *in situ* y copias de seguridad en ubicaciones externas: las copias de seguridad *in situ* se almacenan en el sitio local, hecho que debería permitir una rápida recuperación en caso de catástrofe. Las copias de seguridad externas se almacenan en una ubicación remota, una medida necesaria en caso de catástrofe de gran magnitud. El equilibrio depende del requisito de la cláusula de seguridad del SLA y del coste de inversión.

– Comprobación periódica de los procedimientos de recuperación: la prueba de recuperación es el método último para verificar la validez de una copia de seguridad.

2) Organización de la tarea: una vez determinada la estrategia para la copia de seguridad, los CSP deberían organizar adecuadamente las operaciones de realización de copias de seguridad. A fin de reducir sus efectos sobre el desempeño de la infraestructura de computación en la nube, la organización de la copia de seguridad debería depender de los requisitos del CSC en materia de copias de seguridad, la matriz del tráfico de red y la capacidad del CSP para realizar copias de seguridad.

3) Procedimientos para comprobar la validez de una copia de seguridad: se considera que la copia de seguridad es satisfactoria si los datos se han copiado de manera completa y correcta. Generalmente, cualquier procedimiento debería incluir los siguientes dos pasos principales:

   – Utilizar una función de troceo unidireccional para comprobar que la copia de seguridad se corresponde con los datos originales. Si la copia de seguridad es idéntica al original, se puede pasar al siguiente paso. Asimismo, podría emplearse un método de firma digital para verificar la identidad del operador que realiza la copia de seguridad, hecho que puede resultar positivo para la gestión de la operación de realización de la copia de seguridad.

   – Llevar a cabo una prueba de recuperación para comprobar la copia de seguridad. Dado que los cambios en el entorno de la computación en la nube son constantes, la realización periódica de pruebas de recuperación es fundamental.

4) Prudencia en relación con las muestras instantáneas de la máquina virtual: en una hipótesis de computación en la nube, el método de muestras permite un despliegue rápido y sencillo y, hasta cierto punto, podría servir como método para la realización de copias de seguridad. No obstante, el método de muestras instantáneas no debería utilizarse frecuentemente, por los motivos siguientes:

   – Las muestras permiten multiplicar los mismos datos e inscribirlos en distintos archivos de muestras, lo que podría fácilmente provocar una degradación grave de su comportamiento y aumentar rápidamente el espacio que ocupan en los sistemas de computación en la nube.

   – A fin de reducir el espacio que ocupan, a menudo se configura una cadena de muestras originales procedentes de máquinas virtuales que contienen únicamente las diferencias respecto de la primera muestra. En cuanto se haya destruido la primera muestra, las muestras sucesivas acabarán siendo inválidas. El riesgo de seguridad se ve acentuado conforme aumenta la velocidad de las muestras sucesivas.

8.11 Auditoría de seguridad interna

Dado el amplio espectro de actividades que conlleva una auditoría de seguridad, la presente Recomendación se centra únicamente en la auditoría de seguridad interna desde la perspectiva de la seguridad operativa. Una auditoría de seguridad objetiva y fiable puede ayudar a garantizar que se han comprobado y revisado de manera exhaustiva las actividades de gestión de riesgos operativos en aras de una mayor transparencia de los servicios de computación en la nube, e incluso dar respuesta a los requisitos reglamentarios.

8.11.1 Requisitos de la auditoría de seguridad

Para garantizar la objetividad y la fiabilidad de la auditoría de seguridad, los CSP y los CSC deberían acordar la utilización de un marco común de control de TI y de garantía de la certificación, así como los medios para recopilar, almacenar y compartir el registro de auditoría (como los registros del sistema, los informes de actividad o las configuraciones del sistema). De acuerdo con lo dispuesto en la cláusula de seguridad del SLA entre CSP y CSC, al planificar la auditoría de seguridad, habría que fijarse como objetivo dar respuesta a algunas necesidades:

1) Equipo de auditoría y función: en primer lugar, los equipos de auditoría deberían incluir a personal directivo superior y a empleados de los distintos departamentos (administrativos y técnicos) a fin de garantizar la objetividad y una planificación de los recursos durante el proceso de la auditoría. En segundo lugar, el objetivo de la auditoría debería incluir la verificación de la arquitectura de gestión de la seguridad de los CSP y/o los CSC y la validación de la efectividad y la corrección de las medidas de control de riesgos. En tercer lugar, el equipo de auditoría debería controlar el proceso de auditoría, que debería ajustarse al flujo de trabajo normalizado. Por último, la auditoría de seguridad debería llevarse a cabo repetidamente durante un periodo de tiempo adecuado.

2) Requisitos del proceso de auditoría: en primer lugar, y basándose en lo anterior, las actividades de auditoría deberían registrarse cabalmente y estar debidamente planificadas para evitar interrupciones en la actividad de los CSP o de los CSC. En segundo lugar, habría que definir claramente el alcance de los objetivos de la auditoría y de los recursos necesarios y garantizar su disponibilidad. Por último, todos los procedimientos y requisitos de la auditoría deberían documentarse, al igual que las responsabilidades de los miembros del equipo.

3) Protección de las herramientas de auditoría: la utilización de herramientas de auditoría debería estar restringida y normalizada para evitar la utilización indebida de los recursos de computación en la nube.

8.11.2 Requisitos específicos de la auditoría

En comparación con los procedimientos empleados en la auditoría de seguridad de los sistemas de información tradicionales, los miembros del equipo de auditoría deben estar especialmente familiarizados con los desafíos que plantea la virtualización y otras tecnologías de computación en la nube. Al mismo tiempo, las categorías de la auditoría deben ampliarse para pasar de los registros tradicionales de seguridad al funcionamiento y mantenimiento de los datos, los datos de la actividad e incluso la ubicación de los espacios en que se almacenan los datos de los usuarios. Los elementos de la auditoría incluyen, entre otros:

1) Virtualización de la auditoría de seguridad: los requisitos principales de la auditoría incluyen los medios de encriptado y de comprobación de la integridad de los archivos de imágenes virtuales, el aislamiento y el refuerzo de las distintas máquinas virtuales, el control del acceso y la migración de las máquinas virtuales, la vigilancia de los procesos de las máquinas virtuales, y la inspección de vulnerabilidades en las máquinas virtuales, la vigilancia del tráfico interno y las medidas sobre la red virtualizada.

2) Auditoría de la arquitectura de la plataforma en la nube de la seguridad de los componentes: es fundamental auditar la racionalidad y la efectividad de las contramedidas, incluidas la política de división del dominio de seguridad, la redundancia de la seguridad de la arquitectura de la red y de los componentes fundamentales, el escaneo de la vulnerabilidad y el refuerzo de la seguridad, el empaquetado y la distribución de parches, y las configuraciones del sistema de prevención de intrusiones (IPS)/sistema de detección de intrusión (SDI), los cortafuegos y los dispositivos de seguridad para la virtualización.

3) Auditoría del funcionamiento, mantenimiento y comportamiento de las operaciones: los requisitos de la auditoría se centran fundamentalmente en los registros de funcionamiento y mantenimiento, los registros de acceso a las operaciones, el acceso a los datos y la inspección del comportamiento de las operaciones.

4) Auditoría de la gestión de identidad y de acceso (IAM) y del control del acceso: los requisitos de la auditoría son fundamentales para garantizar un funcionamiento correcto en el entorno de la computación en la nube, que incluye el diseño y el despliegue de la autenticación a partir de múltiples factores, el control del acceso, el inicio de sesión con registro único (SSO), la segregación de las tareas y la gestión de usuarios privilegiados.

5) Auditoría de la gestión de claves y del encriptado de datos: dado que el encriptado constituye el mecanismo fundamental para la protección de los datos en el entorno de la computación en la nube, con independencia de que el modelo de servicio sea IaaS, PaaS o incluso SaaS, los requisitos de la auditoría deberían incluir la aplicación y el procesamiento de la gestión de claves y el encriptado de datos.

6) Auditoría de la gestión y de la respuesta en situaciones de emergencia: los requisitos de auditoría se centran principalmente en un plan para situaciones de emergencia, una gestión centralizada de los incidentes de seguridad y un análisis de la correlación entre los distintos incidentes de seguridad.

Bibliografía

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

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

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

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

[b-UIT-T Y.3510] Recomendación UIT-T Y.3510 (2016), *Requisitos de infraestructura para la computación en nube.*

[b-ISO/IEC DIS 19086-1] ISO/CEI DIS 19086-1:2016, *Information technology – Cloud computing – Service level agreement (SLA) framework and technology – Part 1: Overview and concepts*.

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

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

[b-ISO/IEC DIS 27017] ISO/CEI DIS 27017:2015, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud* services.

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

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

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2017