|  |  |
| --- | --- |
| **Oficina de Normalización de las Telecomunicaciones** | **logo_S_** |
|  |  |

Ginebra, 6 de marzo de 2012

|  |  |  |
| --- | --- | --- |
| Ref.:  Tel.: Fax: | **Circular TSB 266**  COM 17/MEU  +41 22 730 5866 +41 22 730 5853 | - A las Administraciones de los Estados Miembros de la Unión |
| Correo-e: | [tsbsg17@itu.int](mailto:tsbsg17@itu.int) | **Copia**:  - A los Miembros del Sector UIT‑T;  - A los Asociados del UIT‑T;  - A las Instituciones Académicas del UIT-T;  - Al Presidente y a los Vicepresidentes de la Comisión de Estudio 17;  - Al Director de la Oficina de Desarrollo de las Telecomunicaciones;  - Al Director de la Oficina de Radiocomunicaciones |

|  |  |
| --- | --- |
| Asunto: | **Aprobación de la Cuestión 8/17 revisada** |

Muy Señora mía/Muy Señor mío:

1 A petición del Presidente de la Comisión de Estudio 17, *Seguridad*, tengo el honor de informarle que, de conformidad con las disposiciones de la Resolución 1, Sección 7, § 7.2.2, de la AMNT (Johannesburgo, 2008), los Estados Miembros y los Miembros del Sector presentes en la última reunión de dicha Comisión que tuvo lugar en Ginebra del 20 de febrero al 2 de marzo de 2012, acordaron por consenso aprobar la Cuestión revisada siguiente:

*Cuestión 8/17 Seguridad de la computación en nube* (véase el anexo 1)

2 **Queda por tanto aprobada la Cuestión 8/17.**

3 Se supone que las Recomendaciones resultantes se someterán al proceso de aprobación tradicional (TAP).

Le saluda muy atentamente.

Malcolm Johnson  
Director de la Oficina de  
Normalización de las Telecomunicaciones

**Anexo: 1**

ANEXO 1  
(a la Circular TSB 266)

Cuestión 8/17 – Seguridad de la computación en nube

(Cuestión revisada)

Motivos

La computación en nube es un modelo que permite ofrecer al usuario de servicio un acceso ubicuo, práctico, por demanda y a través de la red a un conjunto compartido de recursos informáticos configurables (como, por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser suministrados y liberados rápidamente con una labor de gestión mínima o una interacción mínima con el proveedor de servicio. El modelo de computación en nube tiene cinco características esenciales (por demanda, acceso universal a la red, agrupación de recursos, elasticidad rápida, autoservicio y servicios medidos), cinco categorías de servicios de computación en nube, a saber, software como servicio (SaaS, *Software as a Service*), comunicación como servicio (CaaS, *Communication as a Service*), plataforma como servicio (PaaS, *Platform as a Service*), infraestructura como servicio (IaaS, *Infrastructure as a Service*) y red como servicio (NaaS, *Network as a Service*), y de diferentes modelos de implantación (pública, privada, híbrida...). El hecho de que la computación en nube se haya convertido en la opción preferida para el descubrimiento, la externalización, la composición y la reutilización del servicio en los flujos de trabajo, las aplicaciones y las aplicaciones de comunicaciones pone de manifiesto la necesidad de que sea segura.

Entre los beneficios que se prevé reportará la computación en nube se cuentan la configuración flexible y dinámica de recursos y la administración más simple y automatizada de la infraestructura de TI. La virtualización permite compartir recursos prácticamente ilimitados con mejoras progresivas y una reducción masiva de los costos de gestión de la infraestructura. Sin embargo, los sistemas abiertos y los recursos compartidos de la computación en nube suscitan inquietudes en torno a la seguridad, probablemente el más importante obstáculo a la adopción de la computación en nube. Pasar a la nube implica dejar atrás los sistemas de TI propios, tradicionales y seguros para pasar a infraestructuras abiertas de tipo nube y no seguras. Es, por tanto, necesario un replanteamiento total de la seguridad.

Durante años la computación en nube fue considerada una tecnología de la información centrada en el servicio y controlada por los actores de Internet. Sin embargo, los actores de telecomunicaciones cumplen una importante función en el mercado y ecosistema emergentes de la computación en nube. Dado que los servicios en nube se entregan a través de las redes de telecomunicaciones, los actores de telecomunicaciones deben garantizar un alto nivel de seguridad. Una protección de seguridad fuerte, pero flexible, será fundamental para habilitar todo el ecosistema y el mercado de la nube.

Además, la utilización flexible de grandes recursos en el entorno de computación en nube hará posibles nuevos servicios de seguridad que las actuales defensas no pueden ofrecer (por ejemplo, servicios anti-malware como servicio en nube). Por tanto, es necesario estudiar qué tipo de medidas de seguridad la computación en nube podrá ofrecer en un futuro próximo.

En los proyectos de Recomendación UIT-T X.ccsec, X.srfcts y X.sfcse se formulan una serie de Recomendaciones relativas al servicio de seguridad en el marco general de la seguridad en nube, la arquitectura y el marco general, la seguridad en nube entre capas y la seguridad específica de los servicios de red. Hoy en día resulta fundamental dar seguridad a los servicios de voz, multimedios e identidad, los servicios de garantía de la información, los servicios de identidad y datos y los servicios de emergencia disponibles en la computación en nube. Con esta Cuestión se pretenden elaborar nuevas Recomendaciones, basadas en la parte 5 del Informe Técnico del Grupo Temático sobre computación en nube, sobre:

• elaboración de directrices y prácticas idóneas sobre cómo proporcionar seguridad en un entorno de computación en nube;

• definición de amenazas y requisitos de seguridad, y aclaración de las responsabilidades que incumben a cada uno de los actores principales y sus correspondientes funciones en el ecosistema de la computación en nube;

• arquitectura de seguridad basada en la arquitectura de referencia definida por la C27/13;

• gestión de seguridad y tecnologías de auditoria para la gestión de confianza.

La C8/17 colaborará con las Cuestiones afines, como C2/17, C3/17, C4/17, C7/17, C10/17 y C11/17, para elaborar Recomendaciones sobre la computación en nube.

Las Recomendaciones y Suplementos bajo responsabilidad de esta Cuestión al 2 de marzo de 2012 son UIT-T X.ccsec, X.sfcse y X.fssvpn.

Cuestión

Los temas de estudio son, aunque no exclusivamente, los siguientes:

a) Qué nuevas Recomendaciones o documentos de otro tipo conviene elaborar para los principales actores, como proveedores de servicio, usuarios de servicio y socios de servicio, así como otras partes interesadas de la industria, para avanzar en la seguridad de la computación en nube.

b) Qué nuevas Recomendaciones se han de elaborar sobre la arquitectura de seguridad y la organización de las funcionalidades de seguridad de acuerdo con la arquitectura de referencia.

c) Qué nuevas Recomendaciones se han de elaborar sobre la gestión de la seguridad, los mecanismos de garantía, las tecnologías de auditoría y la evaluación de riesgos conexos para crear confianza entre los diferentes actores.

d) Bajo los auspicios de la Actividad de Coordinación Conjunta sobre computación en nube (JCA-Nube), con qué otras Cuestiones, Comisiones de Estudio y organismos de normalización será necesario colaborar para minimizar la duplicación de esfuerzos.

e) Cómo se debe desarrollar la seguridad como servicio para proteger los sistemas de TIC.

Tareas

Las tareas que se han de realizar son, aunque no exclusivamente, las siguientes:

a) Elaborar Recomendaciones o documentos de otro tipo para avanzar en la seguridad de la computación en nube.

b) Elaborar Recomendaciones para identificar las amenazas y requisitos de seguridad para los servicios de computación en nube basándose en los requisitos generales de la computación en nube especificados por la Comisión de Estudio 13 del UIT-T.

c) Elaborar Recomendaciones para definir la arquitectura de seguridad y organizar las funciones de seguridad de acuerdo con la arquitectura de referencia especificada por la Comisión de Estudio 13 del UIT-T.

d) Elaborar Recomendaciones para definir una arquitectura de seguridad fuerte, flexible y elástica y su aplicación a los sistemas de computación en nube.

e) Elaborar Recomendaciones para identificar los mecanismos de garantía, las tecnologías de auditoria, la evaluación de riesgos a fin de lograr relaciones de confianza en el ecosistema de la computación en nube.

f) Asumir todas las actividades sobre seguridad de la computación en nube de la Comisión de Estudio 17.

g) Representar el trabajo de la Comisión de Estudio 17 en relación con la seguridad de la computación en nube dentro de la Actividad de Coordinación Conjunta sobre computación en nube (JCA-Nube).

Relaciones

Recomendaciones:

• Serie Y de Recomendaciones sobre computación en nube

Cuestiones:

• Cuestiones 1/17, 2/17, 3/17, 4/17, 7/17, 10/17 y 11/17 del UIT-T

Comisiones de Estudio:

• CE 2, 13 y 16 del UIT-T

Organismos de normalización:

• JTC 1/SC 27 y SC 38 de la ISO/CEI; OASIS; IETF y otros organismos pertinentes que se puedan identificar

Otros organismos:

• DMTF; CSA (*Cloud Security Alliance*).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_