|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | **Unión Internacional de Telecomunicaciones**  **Oficina de Normalización de las Telecomunicaciones** | |  |
|  | |  | |

Ginebra, 21 de octubre de 2015

|  |  |  |  |
| --- | --- | --- | --- |
| Ref.:  Tel.: Fax: Correo-e: | | **Circular TSB 174**  COM 17/MEU  +41 22 730 5866 +41 22 730 5853 [tsbsg17@itu.int](mailto:tsbsg17@itu.int) | - A las Administraciones de los Estados Miembros de la Unión |
|  | |  | **Copia**:  - A los Miembros del Sector UIT-T;  - A los Asociados del UIT-T;  - A las Instituciones Académicas de la UIT;  - 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: | **Reunión de la Comisión de Estudio 17 para la aprobación de los proyectos de nuevas Recomendaciones UIT‑T X.1247, X.1256, X.1257, X.1602, X.1642 y el proyecto de revisión de la Recomendación UIT‑T X.1521, de acuerdo con las disposiciones de la Sección 9 de la Resolución 1, de la AMNT (Dubái, 2012), Ginebra, 23 de marzo de 2016** | | |

Muy Señora mía/Muy Señor mío:‎

1 A petición del Presidente de la Comisión de Estudio 17, *Seguridad*, tengo el honor de informarle que esta Comisión de Estudio, que se reunirá del 14 al 23 de marzo de 2016, se propone aplicar el procedimiento descrito en la Sección 9 de la Resolución 1 de la AMNT (Dubái, 2012) para la aprobación del proyecto de Recomendación revisada y de los proyectos de nueva Recomendación arriba mencionados.

2 El **Anexo 1** contiene los títulos y los resúmenes del proyecto de Recomendación UIT-T revisada y de los proyectos de nueva Recomendación UIT‑T propuestos para aprobación, con indicación de los documentos en que figuran.

3 Todo Estado Miembro, Miembro de Sector, Asociado o Institución Académica de la UIT consciente de la titularidad de una patente propia o ajena que pueda cubrir total o parcialmente los elementos de los proyectos de Recomendación propuestos para aprobación debe poner esa información en conocimiento de la TSB, de conformidad con la política común sobre patentes del UIT‑T/UIT-R/ISO/CEI.

Puede accederse en línea a la información disponible sobre patentes a través del sitio web del UIT‑T ([www.itu.int/ITU-T/ipr/](http://www.itu.int/ITU-T/ipr/)).

4 Teniendo en cuenta las disposiciones de la Resolución 1, Sección 9, le agradecería que me comunicase antes de las 24.00 horas UTC del **2 de marzo de 2016** si su Administración otorga a la Comisión de Estudio 17 la autoridad necesaria para que durante su reunión puedan considerar la aprobación de estos proyectos de Recomendación nueva y revisada.

Si algunos Estados Miembros opinan que no puede procederse a considerar la aprobación, deben indicar sus razones de desaprobación así como los posibles cambios que facilitarían el nuevo examen y la aprobación de los proyectos de revisión.

5 Si el 70% como mínimo de las respuestas de los Estados Miembros están a favor de que se considere la aprobación de estos proyectos de Recomendación nueva y revisada en la reunión de la Comisión de Estudio, el **23 de marzo de 2016** se dedicará una Sesión Plenaria a la aplicación del procedimiento de aprobación.

Invito pues a su Administración a que envíe un representante a dicha reunión. Se invita a las **Administraciones de los Estados Miembros de la Unión** a precisar el nombre de su Jefe de delegación. Si su Administración desea estar representada en esa reunión por una empresa de explotación reconocida, un organismo científico o industrial u otra entidad que se ocupe de cuestiones de telecomunicaciones, habrá de comunicarlo al Director de conformidad con lo dispuesto en el Artículo 19, número 239, del Convenio de la UIT.

6 El orden del día y toda la información pertinente sobre la reunión de la Comisión de Estudio 17 figurarán en la Carta Colectiva 7/17.

7 Después de la reunión, el Director de la TSB notificará por Circular la decisión tomada sobre estas Recomendaciones. Esta información se publicará también en el Boletín de Explotación de la UIT.

Atentamente,

Chaesub Lee  
Director de la Oficina de   
Normalización de las Telecomunicaciones

**Anexo:** 1

Anexo 1  
(a la Circular TSB ‎174‎)

Resumen y ubicación de los textos

Proyecto de nueva Recomendación UIT-T X.1247 (X.tfcmm), Marco técnico para luchar contra el correo basura en la mensajería móvil  
COM 17 – R 50

Resumen

El correo basura en la mensajería móvil está aumentando considerablemente con el rápido desarrollo de los servicios de mensajería móvil. Desgraciadamente, ninguna medida ha resultado infalible contra el correo basura en la mensajería móvil. Es por lo tanto necesario establecer un marco práctico para luchar contra el correo basura en la mensajería móvil. La Recomendación UIT‑T X.1247 ofrece una visión general de los procesos necesarios en la lucha contra‎ el correo basura en la mensajería móvil, y propone un marco técnico para luchar contra el mismo. En este marco se especifican las funciones de la entidad y los procedimientos de procesamiento. Además, esta Recomendación ofrece mecanismos de compartición de la información contra el correo basura en la mensajería móvil dentro del dominio de lucha contra el correo basura y entre dominios de lucha contra el correo basura.

Proyecto de nueva Recomendación ‎UIT-T X.1256 (X.authi), Directrices y marco para la compartición de los resultados de la autentificación de la red con las aplicaciones de los servicios  
COM 17 – R 54

Resumen

Con la explosión de los dispositivos y las aplicaciones móviles que acceden a internet, la red y el entorno de servicio están adquiriendo una complejidad creciente. En consecuencia, existe una presión para simplificar el mecanismo de autentificación del usuario para mejorar la experiencia del mismo y la calidad del servicio.

Varias organizaciones de normalización, incluida la UIT han realizado muchas actividades de investigación sobre el mecanismo de autentificación unificado (por ejemplo, el inicio de sesión único). Sin embargo, todo el trabajo actual se centra en la autentificación unificada entre las aplicaciones de los servicios, sin considerar la relación con la autentificación de la red.

Desde el punto de vista del operador de red, los usuarios rellenan algún formulario de autentificación de red cuando acceden a ella, aunque cuando vuelven a acceder para solicitar un acceso a un servicio no se vuelve a reutilizar su autentificación inicial de la red. Cuando se adopta un mecanismo de compartición los resultados de la autentificación entre el servicio y la red, las aplicaciones del servicio pueden identificar un usuario utilizando los resultados de la autentificación de la red. Un mecanismo de este tipo permite al usuario autentificarse una vez con la red y acceder directamente al servicio.

La Recomendación UIT-T X.1256 desarrolla las directrices para que los operadores de red y los proveedores de servicios compartan los resultados de la autentificación de la red, y ofrece un marco para compartir los atributos mínimos entre múltiples servicios dentro de una relación establecida de confianza.

Proyecto de nueva Recomendación ‎UIT-T X.1257 (X.iamt), Taxonomía de la gestión del acceso y de la identidad  
COM 17 – R 55

Resumen

La Recomendación UIT-T X.1257 ‎desarrolla una especificación para asegurar que se asigna el necesario significado de negocio a los roles y autorizaciones del IAM (Gestión de la Identidad y el Acceso) y que se puede comprobar y hacer referencia a este significado de negocio a lo largo del ciclo del proceso IAM para que las autorizaciones puedan asignarse de manera eficaz a los usuarios, se realicen con éxito los controles de separación de responsabilidades (SoD) entre aplicaciones, y los procesos de revisión del acceso y de reconciliación puedan realizarse de manera eficaz.

Proyecto de revisión de la Recomendación ‎UIT-T X.1521 (X.cvss), Sistema común de puntuación de vulnerabilidades 3.0  
COM 17 – R 49

Resumen

La Recomendación ‎UIT-T X.1521 ‎relativa al sistema común de puntuación de vulnerabilidades (CVSS, *common vulnerabilities scoring system*) describe un marco abierto para la comunicación de las características y repercusiones de las vulnerabilidades de las tecnologías de la información y la comunicación (TIC), en particular en el software comercial o de código fuente abierto utilizado en redes de telecomunicaciones, en los dispositivos de usuario final o en cualquier otro tipo de dispositivo TIC capaz de ejecutar software. El objetivo de esta Recomendación es permitir a los gestores de las TIC, proveedores de boletines de vulnerabilidades, vendedores de productos de seguridad, vendedores de aplicaciones e investigadores, utilizar un lenguaje común para la asignación de una valoración numérica a las vulnerabilidades de las TIC.

Proyecto de nueva Recomendación ‎UIT-T X.1602 (X.sfcse), Requisitos de seguridad para los entornos de aplicación del software como servicio   
COM 17 – R 52

Resumen

La Recomendación ‎UIT-T X.1602 analiza los niveles de madurez de la aplicación de software como servicio (SaaS) y propone requisitos de seguridad para ofrecer un entorno de ejecución del servicio consistente y seguro para las aplicaciones SaaS. Estos requisitos propuestos provienen de los Proveedores de servicios en la nube (CSP) y Asociados del servicio en la nube (CSN) pues necesitan un entorno de aplicación SaaS que cumpla con sus necesidades de seguridad. Los requisitos son generales e independientes de cualquier modelo de servicio o de caso específico (por ejemplo, servicios web, Transferencia de Estado Representacional (REST)), suposición o soluciones.

‎Proyecto de nueva Recomendación ‎UIT-T X.1642 (X.goscc), Directrices para la seguridad operativa de la computación en la nube   
COM 17 – R 53

Resumen

La Recomendación ‎UIT-T X.1642 ‎ofrece una 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. Se ofrece un conjunto de medidas de seguridad y de actividades detalladas de seguridad relativas al funcionamiento diario y al mantenimiento, para ayudar a los CSP a reducir los riesgos de seguridad y abordar los retos de la seguridad en el funcionamiento de la computación en la nube.

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