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

Ginebra, 7 de enero de 2011

|  |  |  |
| --- | --- | --- |
| Ref.:  Tel.: Fax: | **Circular TSB 158**  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;  - 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 nueva Recomendación UIT-T X.1261, X.1500, X.1520 y X.1521****de conformidad con las disposiciones de la Resolución 1, Sección 9, de la AMNT (Johannesburgo, 2008) Ginebra, 20 de abril de 2011** |

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 11 al 20 de abril de 2011, se propone aplicar el procedimiento descrito en la Resolución 1, Sección 9, de la AMNT (Johannesburgo, 2008) para la aprobación de los proyectos de nueva Recomendación mencionados arriba.

2 El **anexo 1** contiene el título y el resumen de los proyectos de nueva Recomendación UIT‑T, con indicación de los documentos en que figuran.

3 Todo Estado Miembro, Miembro de Sector o Asociado 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 Recomendaciones propuestos para aprobación debe poner esa información en conocimiento de la TSB, de conformidad con la política 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 30 de marzo de 2011** 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 nuevas Recomendaciones.

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 nuevas Recomendaciones.

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 nuevas Recomendaciones en la reunión de la Comisión de Estudio, **el 20 de abril de 2011** 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 5/17.

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.

Le saluda muy atentamente.

Malcolm Johnson  
Director de la Oficina de  
Normalización de las Telecomunicaciones

**Anexo**: 1

ANEXO 1  
(a la Circular TSB 158)

**Resumen y ubicación de los textos**

**Proyecto de nueva Recomendación UIT-T X.1500 (X.cybex), Técnicas para el intercambio de información en materia de ciberseguridad  
COM 17 – R 25** *(disponible en breve en la web)*

**Resumen**

En esta Recomendación se describen técnicas para el intercambio de información en materia de ciberseguridad. Dichas técnicas pueden utilizarse aisladamente o en diversas combinaciones, según se desee o convenga, a fin de mejorar la ciberseguridad a través de un intercambio de información coherente, exhaustivo, global, oportuno y seguro. Esta Recomendación no implica obligaciones de intercambio de información, como tampoco los medios de adquisición o el uso final que se dé a la información tratada.

**Proyecto de nueva Recomendación UIT-T X.1520 (X.cve), Vulnerabilidades y riesgos corrientes (CVE)  
COM 17 – R 26**

**Resumen**

En esta Recomendación se plantea un mecanismo estructurado para intercambiar vulnerabilidades y riesgos conocidos en materia de seguridad de la información (CVE) destinado a proporcionar denominaciones comunes para los problemas conocidos públicamente que se plantean en los programas informáticos comerciales o de fuente abierta utilizados en las redes de comunicación, los dispositivos de usuario o cualquiera de los demás tipos de tecnologías de la información y la comunicación (TIC) aptos para utilizar programas informáticos. El objetivo de esta Recomendación es, gracias a esta denominación común, facilitar el intercambio de datos para distintos tipos de vulnerabilidad (herramientas, depósitos y servicios). La Recomendación está destinada a permitir la vinculación de bases de datos de vulnerabilidad y otras capacidades, y facilitar la comparación de las herramientas y servicios de seguridad. Como tal, la Recomendación no recoge datos tales como el riesgo, las repercusiones, la información sobre la solución de problemas, o información técnica detallada. Sólo se recogen el número identificador habitual y el indicador de estado, una breve descripción, y referencias a los informes y consejos en materia de vulnerabilidad conexos.

Esta Recomendación pretende ser exhaustiva en lo que respecta a todas las vulnerabilidades y los riesgos conocidos. Aunque se ha concebido para recoger información contrastada, su finalidad principal es la identificación de vulnerabilidades y riesgos que son detectados por las herramientas de seguridad y cualquier nuevo problema que se haga público, y en segundo lugar tratar cualquier problema de seguridad más antiguo que requiera validación.

**Proyecto de nueva Recomendación UIT-T X.1521 (X.cvss), Sistema de puntuación para las vulnerabilidades corrientes (CVSS)  
COM 17 – R 27** *(disponible en breve en la web)*

**Resumen**

En esta Recomendación se facilita un marco abierto para comunicar las características y efectos de las vulnerabilidades de las tecnologías de la información y la comunicación (TIC) en los programas informáticos comerciales o de fuente abierta utilizados en las redes de comunicaciones y los dispositivos de usuario, usuario o cualquiera de los demás tipos de TIC aptos para utilizar programas informáticos. Esta Recomendación abarca el sistema de puntuación para las vulnerabilidades corrientes (CVSS), cuyo objetivo es permitir que los directores de TIC, proveedores de boletines sobre vulnerabilidad, vendedores de seguridad, vendedores de aplicaciones e investigadores utilicen un lenguaje común para atribuir puntuaciones a las vulnerabilidades de las TIC.

**Proyecto de nueva Recomendación UIT-T X.1261 (X.EVcert), Marco ampliado para la validación de certificados (EVcert)  
COM 17 – R 30**

Resumen

Esta Recomendación trata del marco ampliado para la validación de certificados y constituye una combinación integrada de tecnologías, protocolos, prácticas de demostración de identidad (*identity proofing*), de gestión del ciclo de vida y de auditoría con la que se describen los requisitos mínimos que deben cumplirse para emitir y mantener los certificados de validación ampliados ("Certificados EV") que se refieren a una organización. Así la información de los "Certificados EV" de la organización en cuestión puede presentarse de cierta manera mediante ciertas aplicaciones informáticas de las partes confiantes (por ejemplo un navegador web) a fin de ofrecer al usuario una confirmación fiable acerca de la identidad de la entidad que controla el sitio web u otros servicios a los que esté accediendo. Aunque inicialmente destinadas al establecimiento de conductos de transmisión de datos por la web a través de los protocolos de seguridad de la capa de transporte – o de capa de zócalo segura (TLS/SSL), las extensiones se han contemplado para extensiones del correo Internet multipropósito/seguro (S/MIME), de indicación del tiempo, de protocolo de voz por Internet (VoIP), de mensajería instantánea (IM), de servicios web, etc.

Los objetivos básicos de esta Recomendación son los siguientes: 1) identificar la entidad legal que controla un sitio web o de servicio, y 2) permitir las comunicaciones encriptadas con dicho sitio. Entre los objetivos secundarios figuran mejorar considerablemente la ciberseguridad contribuyendo a determinar la legitimidad de una organización que declare manejar un sitio web, y facilitar un vehículo que puede aprovecharse para prestar asistencia a la hora de abordar problemas relacionados con la distribución de programas informáticos dañinos, la peska (phishing), el robo de identidades y distintas formas de fraude en línea.

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