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

 Ginebra, 9 de septiembre de 2011

|  |  |  |
| --- | --- | --- |
| Ref.:Tel.:Fax: | **Circular TSB 228**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  | **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 laComisión 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.1037, X.1500.1, X.1524 y X.1541, de conformidad con las disposiciones de la Resolución 1, Sección 9, de la AMNT (Johannesburgo, 2008),Ginebra, 2 de marzo de 2012** |

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 20 de febrero al 2 de marzo de 2012, 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, 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 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 8 de febrero de 2012** 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 nueva Recomendación.

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 nueva Recomendación.

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 nueva Recomendación en la reunión de la Comisión de Estudio, **el 2 de marzo de 2012** 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 Estudio17 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.

Le saluda muy atentamente.

Malcolm Johnson
Director de la Oficina de
Normalización de las Telecomunicaciones

**Anexo: 1**

ANEXO 1
(a la Circular TSB 228)

**Resumen y ubicación de los textos**

Proyecto de nueva Recomendación UIT-T X.1037 (X.rev), Sistemas arquitectónicos
de control de seguridad para impedir actividades fraudulentas en las redes
de operadores públicos
COM 17 – R 41

Resumen

La Recomendación UIT-T X.1037 describe una metodología para sistemas de evaluación de controles de seguridad destinados a impedir actividades fraudulentas, y los criterios para seleccionar estos sistemas, en lo que respecta a las características arquitectónicas de las redes del proveedor de servicios de comunicaciones (PSC) y su nivel actual de desarrollo. La Recomendación comprende métodos técnicos para realizar controles de seguridad y calcular las pérdidas causadas por las actividades fraudulentas, así como directrices para el intercambio de información sobre actividades fraudulentas.

Proyecto de Recomendación UIT-T X.1500.1 (X.cybex.1), Procedimientos de registro
de arcos bajo el arco de identificador de objetos (OID) para el intercambio
de información sobre ciberseguridad
COM 17 – R 42

Resumen

En esta Recomendación se describe el registro de arcos de identificadores de objetos (OID) que permiten la identificación coherente, unívoca y global de información sobre ciberseguridad, así como las organizaciones que intercambian dicha información y políticas conexas. En esta Recomendación se especifican la información y la justificación que debe aportarse al solicitar un OID a los efectos de intercambiar información sobre ciberseguridad para el funcionamiento de la Autoridad de Registro.

Proyecto de nueva Recomendación UIT-T X.1524 (X.cwe), enumeración de puntos
débiles comunes (CWE)
COM 17 – R 43

Resumen

En esta Recomendación relativa a la enumeración de puntos débiles comunes (CWE) se describe un mecanismo estructurado para el intercambio de puntos débiles de seguridad de la información que proporciona nombres comunes para problemas públicamente conocidos en el software comercial o de código abierto utilizado en las redes de comunicaciones, en dispositivos de usuario o en cualquier otro tipo de tecnología de la información o la comunicación (TIC) que ejecuta software. El objetivo de la CWE es mejorar la eficiencia del examen, descripción, selección y utilización de herramientas y servicios de seguridad del software que sirven para detectar puntos débiles en el código fuente y en sistemas operativos, así como para comprender mejor y gestionar las deficiencias del software en cuanto a su arquitectura y diseño. Esta Recomendación define la utilización de CWE como mecanismo para poder utilizar conjuntamente herramientas, servicios y bases de conocimientos sobre seguridad del software y otras capacidades, y para facilitar la comparación de herramientas y servicios de seguridad. La CWE también ofrece información contextual complementaria acerca de los posibles riesgos, efectos, soluciones e información técnica detallada acerca de los peligros que representan las deficiencias software para el sistema informático. El depósito de identificadores CWE y la información contextual conexa está disponible en [cwe.mitre.org/data] en formato XML o pdf. También existe una versión web del mismo contenido accesible en [http://cwe.mitre.org/data/slices/2000.html].

La CWE, cuya utilización se define en esta Recomendación, pretende ser exhaustiva en lo que respecta a la arquitectura del software y su diseño, codificación y errores de implantación que son las causas fundamentales de las vulnerabilidades y riesgos. Aunque la CWE se ha concebido para incluir información consolidada, el principal objetivo es identificar, informar y describir estas causas fundamentales de vulnerabilidades y riesgos, a fin de que los diseñadores puedan evitarlas, y los equipos de desarrollo las verifiquen y gestionen, y para que las herramientas y servicios de seguridad las notifiquen adecuadamente.

Proyecto de nueva Recomendación UIT-T X.1541 (X.iodef), Formato para el intercambio
de descripciones de objetos de incidentes
COM 17 – R 44

Resumen

El formato de intercambio de descripciones de objetos de incidentes (IODEF) define una representación de datos que sirve de marco para compartir la información que suelen intercambiar los equipos de intervención en caso de incidente de seguridad informática (EIII) cuando se produce este tipo de incidentes. En esta Recomendación se describe el modelo de información para el IODEF y el modelo de datos correspondiente especificado en lenguaje XML.

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