|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | **Unión Internacional de Telecomunicaciones**  **Oficina de Normalización de las Telecomunicaciones** | | [ITUT60_blue](http://www.itu.int/en/ITU-T/60/Pages/default.aspx) |
|  | |  | |

Ginebra, 28 de noviembre de 2016

|  |  |  |
| --- | --- | --- |
| **Ref.:**  **Tel.: Fax:** | **Circular TSB 246**  SG17/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 de la UIT;  - Al Presidente y a los Vicepresidentes de la Comisión de Estudio 17 del UIT-T;  - 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 del UIT-T, del 22 al 30 de marzo de 2017, para la aprobación de los proyectos de Recomendación UIT‑T 1058 (X.gpim), X.1080.0 (X.pbact), X.1126 (X.msec-11), X.1212 (X.cogent), X.1362 (X.iotsec-1), X.1373 (X.itssec-1), y X.1550 (X.nessa), de acuerdo con las disposiciones de la Sección 9 de la Resolución 1, de la AMNT (Rev. Dubái, 2012)** | |

Muy Señora mía/Muy Señor mío:‎

1 A petición del Presidente de la Comisión de Estudio 17 del UIT-T, *Seguridad*, tengo el honor de informarle que esta Comisión de Estudio, que se reunirá del 22 al 30 de marzo de 2017, se propone aplicar el procedimiento descrito en la Sección 9 de la Resolución 1 de la AMNT (Dubái, 2012) para la aprobación de los proyectos de Recomendación arriba mencionados.

2 El **Anexo 1** contiene los títulos y los resúmenes de los proyectos de 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 **13 de marzo de 2017** si su Administración otorga a la Comisión de Estudio 17 del UIT-T la autoridad necesaria para que durante su reunión puedan considerar la aprobación de estos proyectos de 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 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 en la reunión de la Comisión de Estudio, el **30 de marzo de 2017** 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 UIT-T 17 figurarán en la Carta Colectiva 1/17.

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 ‎246‎)

Resumen y ubicación de los textos

# 1 Proyecto de Recomendación UIT-T X.1058 (ex X.gpim) ([R 69(Rev.1)](http://www.itu.int/md/T13-SG17-R-0069))

Tecnología de la información — Técnicas de seguridad — Código de prácticas relativo a la protección de la información de identificación personal

Resumen

El número de organizaciones que llevan a cabo el procesamiento de la información de identificación personal (PII, *Personally Identifiable Information*) aumenta sin cesar, del mismo modo que la cantidad de PII que tratan esas organizaciones. Al mismo tiempo, las expectativas de la sociedad respecto de la protección de la PII y la seguridad de los datos personales también están aumentando. Numerosos países incrementan su legislación para hacer frente al número cada vez mayor de graves violaciones a la seguridad de los datos. En esta Recomendación | Norma Internacional se establecen objetivos de control, controles y directrices para la implementación de controles con la finalidad de cumplir los requisitos identificados por la evaluación de los riesgos e incidencias vinculados a la protección de la información de identificación personal. En particular, en la presente Recomendación | Norma Internacional se describen directrices basadas en ISO/CEI 27002, teniendo en cuenta los requisitos necesarios para el procesamiento de la PII que puedan ser aplicables en el contexto de uno o más entornos de riesgo para la seguridad de la información de una organización.

# 2 Proyecto de Recomendación UIT-T X.1080.0 (ex X.pbact) ([R 75](http://www.itu.int/md/T13-SG17-R-0075))

Control de acceso para la protección de datos telebiométricos

Resumen

En la Recomendación UIT-T X.1080.0, Control de acceso para la protección de datos telebiométricos, se especifica cómo proteger la información telebiométrica contra el acceso no autorizado adoptando un enfoque orientado al servicio, donde sólo se facilita la información necesaria para un fin concreto, es decir, que el acceso no sólo se concede en función del derecho a saber, sino también en función de la necesidad de conocer. La piedra angular de esta Recomendación es una especificación de atributo, incluido en un certificado de atributo o certificado de clave pública, que especifica detalladamente qué privilegios posee una entidad concreta para uno o más tipos de servicios. La seguridad se da con un perfil de sintaxis de mensaje criptográfico (CMS), que garantiza la autentificación, la integridad y, cuando procede, la confidencialidad (encriptación). Este perfil está previsto para dar seguridad a las especificaciones telebiométricas en general. El perfil supone la correcta implantación de una infraestructura de clave pública (PKI) y, al mismo tiempo, depende de ella. La Recomendación UIT-T X.1080.0 también depende de la existencia de una infraestructura de gestión de privilegios (PMI).

# 3 Proyecto de Recomendación UIT-T X.1126 (ex X.msec-11) ([R 76](http://www.itu.int/md/T13-SG17-R-0076))

Directrices para la mitigación de los efectos negativos de los terminales infectados en las redes móviles

Resumen

La Recomendación UIT-T X.1126 proporciona directrices a los operadores móviles para limitar el número de terminales infectados en las redes móviles mediante la utilización de tecnologías que protejan tanto a los abonados como a los operadores móviles. Del mismo modo, describe las características y las repercusiones del software malicioso en los ecosistemas nocivos del entorno móvil. La presente Recomendación se basa en las tecnologías del lado de red y se centra en la mitigación de los efectos perniciosos de los terminales infectados. Por último, define y organiza medidas de mitigación y tecnologías pertinentes.

# 4 Proyecto de Recomendación UIT-T X.1212 (ex X.cogent) ([R 71](http://www.itu.int/md/T13-SG17-R-0071))

Consideraciones de diseño para la mejor percepción por el usuario extremo de los indicadores de fiabilidad

Resumen

Ataques de varios tipos emplean la replicación de contenido de proveedores de servicio fiables, engañando así a los usuarios extremos, que creen en esa falsa fiabilidad. En la Recomendación UIT-T X.1212 se describen las consideraciones de diseño para la mejor percepción por el usuario extremo de los indicadores de fiabilidad. En los Apéndices se describen técnicas representativas para medir la percepción por el usuario extremo de esos indicadores.

# 5 Proyecto de Recomendación UIT-T X.1362 (ex X.iotsec-1) ([R 77](http://www.itu.int/md/T13-SG17-R-0077))

**Procedimiento de encriptación simple para la Internet de las cosas**

Resumen

La Internet de las cosas (IoT) se considera unas de las esferas más significativas en materia de normalización futura. Desde el punto de vista del UIT-T, la IoT se define como una infraestructura mundial para la sociedad de la información que permite prestar servicios avanzados mediante la interconexión de objetos (tanto físicos como virtuales). En determinados casos, en particular en lo concerniente a los dispositivos IoT, es necesario llevar a cabo el procesamiento de tareas en tiempo real en un periodo de tiempo determinado. Con objeto de velar por la confidencialidad y protección integral de los datos, una de las contramedidas fundamentales es la aplicación de algoritmos de encriptación o autentificación de datos. Las aplicaciones normales de los algoritmos de encriptación o autenticación de datos presentan la dificultad de no satisfacer ese requisito. La Recomendación UIT-T X.1362 tiene como objetivo especificar la encriptación con datos de máscara asociados (EAMD) para los dispositivos de la Internet de las cosas. Permite asimismo describir la EAMD y el modo en que ésta proporciona una serie de servicios de seguridad a los efectos de tráfico de datos.

**6 Proyecto de Recomendación UIT-T X.1373 (ex X.itssec-1) (**[**R 78(Rev.2)**](http://www.itu.int/md/T13-SG17-R-0078)**)**

**Capacidad de actualización segura de software en dispositivos de comunicación de sistemas de transporte inteligente**

Resumen

La mejora de las tecnologías de los sistemas de transporte inteligente (ITS) ha permitido que sea habitual la comunicación entre vehículos y otras entidades, ya sean otros vehículos (comunicaciones vehículo a vehículo, V2V) o infraestructura (comunicaciones vehículo a infraestructura, V2I). Los dispositivos electrónicos en el interior de los vehículos, como las unidades de control electrónicas (ECU), los sistemas electrónicos de pago de peaje (ETC) y los sistemas de navegación son cada vez más sofisticados. Como resultado de ello, los módulos software de dichos dispositivos electrónicos deben actualizarse adecuadamente para subsanar errores del software y mejorar la calidad de funcionamiento y la seguridad con el fin de evitar accidentes. Con el objetivo de cumplir los requisitos mencionados, la Recomendación UIT.T X.1373 proporciona procedimientos de actualización segura de software que se ejecutan entre el servidor de actualización de software y los vehículos, en los que se aplican controles de seguridad adecuados con el fin de satisfacer esos requisitos. Esta Recomendación puede ser de utilidad para fabricantes de automóviles y para industrias relacionadas con los ITS, como conjunto de capacidades normalizadas para el desarrollo de prácticas idóneas.

# 7 Proyecto de Recomendación UIT-T X.1550 (ex X.nessa) ([R 72](http://www.itu.int/md/T13-SG17-R-0072))

**Modelos de control de acceso para redes de intercambio de incidentes**

Resumen

En la Recomendación UIT-T X.1550 se describen los métodos existentes para la implementación de las políticas de control de acceso en las redes de intercambio de incidentes. En esta Recomendación se describen varios modelos de control de acceso consolidados, modelos de compartición así como criterios para evaluar la calidad de funcionamiento de una red de intercambio de incidentes. Se analizan soluciones normalizadas para facilitar la implementación de modelos de control de acceso diferentes en modelos de compartición de información de ciberseguridad diferentes y en entornos con diversos niveles de confianza.

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