|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | **Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT-16)**  **Hammamet, 25 de octubre - 3 de noviembre de 2016** | | CCITT/ITU-T 60th Anniversary logo |
|  | |  | |
|  | |  | |
| SESIÓN PLENARIA | | **Documento 19-S** | |
|  | | **Junio de 2016** | |
|  | | **Original: inglés** | |
|  | | | |
| Comisión de Estudio 17 del UIT-T | | | |
| Seguridad | | | |
| INFORME DE LA CE 17 del uit-t A LA ASAMBLEA MUNDIAL DE NORMALIZACIÓN DE LAS TELECOMUNICACIONES (Amnt-16), PARTe I: GENERALidades | | | |

|  |  |
| --- | --- |
| **Resumen:** | Esta contribución contiene el informe de la Comisión de Estudio 17 del UIT-T a la AMNT-16 sobre sus actividades durante el periodo de estudios 2013-2016. |

Nota de la TSB:

El Informe de la Comisión de Estudio 17 a la AMNT-16 se presenta en los siguientes documentos:

Parte I: **Documento 19** – Generalidades, incluida una propuesta de modificación de la Resolución 2 de la AMNT en el Anexo 2

Parte II: **Documento 20** – Cuestiones propuestas para estudio durante el periodo de estudios 2017‑2020

**ÍNDICE**

**Página**

[1 Introducción 3](#_Toc456887934)

[2 Organización del trabajo 8](#_Toc456887935)

[3 Resultados de los trabajos realizados durante el periodo de estudios 2013-2016 12](#_Toc456887936)

[4 Observaciones en relación con el trabajo futuro 43](#_Toc456887937)

[ANEXO 1 – Lista de Recomendaciones, Suplementos y otros documentos producidos   
o suprimidos durante el periodo de estudios 46](#_Toc456887938)

[ANEXO 2 – Propuesta de actualización del mandato y la función de Comisión de Estudio  
Rectora de la Comisión de Estudio 17 63](#_Toc456887939)

# 1 Introducción

## 1.1 Responsabilidades de la Comisión de Estudio 17

La Asamblea Mundial de Normalización de las Telecomunicaciones (Dubái, 2012) encomendó a la Comisión de Estudio 17 el examen de 12 Cuestiones relacionadas con la seguridad, incluida la ciberseguridad, la lucha contra el correo basura y la gestión de identidades. La CE 17 también es responsable de la aplicación de comunicaciones de sistemas abiertos, incluidos el directorio y los identificadores de objetos, así como de los lenguajes técnicos, el método de utilización de los mismos y otros temas relacionados con los aspectos del software de los sistemas de telecomunicación.

En el anexo A a la Resolución 2 de la AMNT-12 se concede el siguiente mandato a la Comisión de Estudio 17 (Seguridad):

*La Comisión de Estudio 17 del UIT-T se encarga de la creación de confianza y seguridad en el uso de las tecnologías de la información y la comunicación (TIC). Ello incluye los estudios relativos a la ciberseguridad, la gestión de la seguridad, la lucha contra el correo basura y la gestión de identidades. También incluye la arquitectura y marco de la seguridad, la protección de la información de identificación personal y la seguridad de las aplicaciones y servicios para la Internet de las Cosas (IoT), la red eléctrica inteligente, los teléfonos inteligentes, la televisión por el protocolo Internet (TVIP), los servicios web, las redes sociales, la computación en la nube, los sistemas financieros móviles y la telebiometría. Es también responsable de la aplicación de comunicaciones de sistemas abiertos, incluidos el directorio y los identificadores de objetos, así como de los lenguajes técnicos, el método de utilización de los mismos y otros temas relacionados con los aspectos del software de los sistemas de telecomunicación, y de las pruebas de conformidad para mejorar la calidad de las Recomendaciones.*

En el Anexo A a la Resolución 2 de la AMNT-12 se otorgan a la Comisión de Estudio 17 (Seguridad) las siguientes responsabilidades de Comisión de Estudio Rectora:

– Comisión de Estudio Rectora sobre seguridad

– Comisión de Estudio Rectora sobre gestión de identidad (IdM)

– Comisión de Estudio Rectora sobre lenguajes y técnicas de descripción

En el Anexo B a la Resolución 2 de la AMNT-12 se definen las responsabilidades de la CE 17:

*La Comisión de Estudio 17 del UIT-T se encarga de la creación de confianza y seguridad en el uso de las tecnologías de la información y la comunicación (TIC). Ello incluye los estudios relativos a la seguridad, incluida la ciberseguridad, la lucha contra el correo basura (spam) y la gestión de identidad. También incluye la arquitectura y marco de la seguridad, la gestión de la seguridad, la protección de la información de identificación personal (IIP) y la seguridad de las aplicaciones y servicios para Internet de las Cosas (IoT), la red eléctrica inteligente, los teléfonos inteligentes, la televisión por el protocolo Internet (TVIP), los servicios web, las redes sociales, la computación en la nube, los sistemas financieros móviles y la telebiometría. También es responsable de la aplicación de las comunicaciones basadas en sistemas abiertos, incluyendo el directorio y los identificadores de objetos; así como de los relativos a los lenguajes técnicos, el método para la utilización de los mismos y otros temas relacionados con los aspectos del software de los sistemas de telecomunicación y de las pruebas de conformidad para mejorar la calidad de las Recomendaciones.*

*En materia de seguridad, la Comisión de Estudio 17 se encarga de elaborar las Recomendaciones básicas sobre seguridad de las TIC, tales como la arquitectura y los marcos de seguridad; los elementos fundamentales relativos a la ciberseguridad, incluidas las amenazas, las vulnerabilidades y los riesgos, el tratamiento/respuesta a los incidentes y el análisis forense digital, y la gestión de la seguridad incluida la gestión de la IIP y la lucha contra el spam por medios técnicos. Además, la Comisión de Estudio 17 establece la coordinación general de los estudios sobre seguridad en el UIT‑T.*

*La Comisión de Estudio 17 también es responsable de la elaboración de las Recomendaciones básicas sobre aspectos de seguridad de las aplicaciones y servicios en el área de la TVIP, red eléctrica inteligente, IoT, redes sociales, computación en la nube, teléfonos inteligentes, sistemas financieros móviles y telebiometría.*

*La Comisión de Estudio 17 es igualmente responsable de la elaboración de Recomendaciones básicas sobre un modelo genérico de gestión de la identidad que sea independiente de las tecnologías de red y que sirva de soporte para el intercambio seguro de información de identidad entre las entidades. Esta labor comprende también el estudio del proceso de descubrimiento de fuentes autorizadas de información de identidad; mecanismos genéricos para la neutralidad/compatibilidad de diversos formatos de información de identidad; amenazas de gestión de identidad, mecanismos para contrarrestarlas, la protección de IIP y la elaboración de mecanismos que garanticen que sólo se autoriza el acceso a la IIP cuando procede.*

*En el área de las comunicaciones de sistemas abiertos, la Comisión de Estudio 17 se encarga de las Recomendaciones sobre los temas siguientes:*

*• servicios y sistemas de directorio, incluida la infraestructura de clave pública (PKI) (series UIT-T F.500 y UIT-T X.500);*

*• identificadores de objeto (OID) y autoridades de registro asociadas (series UIT-T X.660/UIT-T X.670)*

*• interconexión de sistemas abiertos (OSI) incluida la notación de sintaxis abstracta uno (ASN.1) (series UIT-T F.400, UIT-T X.200, UIT-T X.600 y UIT-T X.800); y*

*• procesamiento distribuido abierto (ODP) (serie UIT-T X.900).*

*En materia de lenguajes, la Comisión de Estudio 17 se encarga de los estudios sobre técnicas de modelado, especificación y descripción. Esta labor, que incluye lenguajes tales como los ASN.1, SDL, MSC y URN, se desarrollará en consonancia con las exigencias de las Comisiones de Estudio pertinentes, tales como las CE 2, CE 9, CE 11, CE 13, CE 15 y CE 16, y en cooperación con ellas.*

En el anexo C a la Resolución 2 de la AMNT-12 (modificada por el GANT) se enumeran las Recomendaciones bajo responsabilidad de la Comisión de Estudio 17 durante el periodo de estudios 2013-2016:

*• UIT-T E.104, UIT-T E.115, UIT-T E.409 (conjuntamente con la Comisión de Estudio 2);*

*• Serie UIT-T F.400; UIT-T F.500-UIT-T F.549;*

*• Serie UIT-T X, salvo las que son responsabilidad de las Comisiones de Estudio 2, 11, 13, 15 y 16;*

*• Serie UIT-T Z, salvo las series UIT-T Z.300 y las series UIT-T Z.500.*

## 1.2 Equipo de gestión y reuniones celebradas por la Comisión de Estudio 17

La AMNT-12 nombró al Sr. Arkadiy KREMER (Federación de Rusia) Presidente de la Comisión de Estudio 17 y designó a los siguientes nueve Vicepresidentes: Sr. Khalid BELHOUL (Emiratos Árabes Unidos), Sr. Mohamed M. K. ELHAJ (Sudán), Sr. Mario Germán FROMOW RANGEL (México), Sr. Antonio GUIMARAES (Brasil), Sr. Zhaoji LIN (China), Sr. Patrick MWESIGWA (Uganda), Sr. Koji NAKAO (Japón), Sr. Said SARIKAYA (Turquía) y Sr. Heung Youl YOUM (Corea). El Sr. FROMOW RANGEL no participó en ninguna de reunión de la Comisión de Estudio 17.

Durante el periodo de estudios considerado, la Comisión de Estudio 17 se reunió en 8 ocasiones en Sesión Plenaria (véase el cuadro 1).

CUADRO 1

Reuniones de la Comisión de Estudio 17 y de Grupos de Trabajo

| Reuniones | Fecha | Informes |
| --- | --- | --- |
| Comisión de Estudio 17 | Ginebra, 17 – 26 de abril de 2013 | COM 17 – R 1 a R 8 |
| Comisión de Estudio 17 | Ginebra, 26 de agosto – 4 de septiembre de 2013 | COM 17 – R 9 a R 22 |
| Comisión de Estudio 17 | Ginebra, 15 – 24 de enero de 2014 | COM 17 – R 23 a R 29 |
| Comisión de Estudio 17 | Ginebra, 17 – 26 de septiembre de 2014 | COM 17 – R 30 a R 36 |
| Comisión de Estudio 17 | Ginebra, 8 – 17 de abril de 2015 | COM 17 – R 37 a R 45 |
| Comisión de Estudio 17 | Ginebra, 8 – 17 de septiembre de 2015 | COM 17 – R 46 a R 57 |
| Comisión de Estudio 17 | Ginebra, 14 – 23 de marzo de 2016 | COM 17 – R 58 a R 66 |
| Comisión de Estudio 17 | Ginebra, 29 de agosto – 7 de septiembre de 2016 | COM 17 – R 67 a R ?? |

Las reuniones del Equipo de Gestión se celebraron en paralelo a las reuniones de la Comisión de Estudio 17.

Durante el periodo de estudios considerado se celebraron numerosas reuniones de Grupos de Relator, incluidas reuniones por medios electrónicos, en diversos lugares (véase el Cuadro 1-bis).

CUADRO 1-bis

Reuniones de Relator organizadas por la Comisión de Estudio 17 durante el periodo de estudios

| Fechas | Lugar/Anfitrión | Cuestión(es) | Nombre del evento |
| --- | --- | --- | --- |
| 14-01-2013 | Corea (Rep. de) [Seúl]/ Universidad de Soonchunhyang y KISA | 3/17 | Reunión del Grupo de Relator en funciones de la C3/17 |
| 22-01-2013 a 24-01-2013 | China [Beijing]/China Academy of Telecommunication Research of MIIT (CATR) | 8/17 | Reunión del Grupo de Relator en funciones de la C8/17 |
| 23-01-2013 a 25-01-2013 | Reunión virtual | 4/17 | Reunión del Grupo de Relator en funciones de la C4/17 |
| 19-02-2013 a 22-02-2013 | Suiza [Ginebra]/UIT | 8/17 | Reunión del Grupo de Relator en funciones de la C8/17 |
| 17-06-2013 a 21-06-2013 | Corea (Rep. de) [Seúl]/Korean Agency for Technology and Standards (KATS) | 11/17 | Reunión del Grupo de Relator en funciones de la C11/17 con el JTC 1/SC 6 de la ISO/CEI |
| 02-07-2013 a 03-07-2013 | *Reunión virtual* | 4/17 | Reunión del Grupo de Relator en funciones de la C4/17 |
| 08-07-2013 a 10-07-2013 | China [Guangzhou]/China Telecom | 8/17 | Reunión del Grupo de Relator en funciones de la C8/17 |
| 09-07-2013 a 10-07-2013 | Francia [París]/LegalBox | 11/17 | Reunión del Grupo de Relator en funciones de la C11/17 |
| 04-12-2013 a 05-12-2013 | Corea (Rep. de) [Seúl]/TOZ | 3/17 | Reunión del Grupo de Relator en funciones de la C3/17 |
| 17-02-2014 a 21-02-2014 | Canadá [Ottawa]/Ericsson | 11/17 | Reunión del Grupo de Relator en funciones de la C11/17 conjuntamente con el JTC 1/SC 6/WG 10 de la ISO/CEI |
| 07-04-2014 a 11-04-2014 | Hongkong [China]/ JTC 1/SC 27 de la ISO/CEI | 3/17 | Reunión del Grupo de Relator en funciones de la C3/17 conjuntamente con el JTC 1/SC 27/WG 5 de la ISO/CEI |
| 07-05-2014 a 08-05-2014 | *Reunión virtual* | 10/17 | Reunión del Grupo de Relator en funciones de la C10/17 |
| 17-06-2014 a 18-06-2014 | Estado Unidos [Charlotte, Carolina del Norte]/Bank of America | 10/17 | Reunión del Grupo de Relator en funciones de la C10/17 |
| 24-06-2014 a 26-06-2014 | Corea (Rep. de) [Seúl]/organizaciones coreanas | 6/17 | Reunión del Grupo de Relator en funciones de la C6/17 |
| 25-06-2014 a 26-06-2014 | Corea (Rep. de) [Seúl]/ organizaciones coreanas | 7/17 | Reunión del Grupo de Relator en funciones de la C7/17 |
| 25-06-2014 a 26-06-2014 | Corea (Rep. de) [Seúl]/ organizaciones coreanas | 3/17 | Reunión del Grupo de Relator en funciones de la C3/17 |
| 01-07-2014 a 03-07-2014 | China [Beijing]/China Academy of Telecommunication Research of MIIT (CATR) | 8/17 | Reunión del Grupo de Relator en funciones de la C8/17 |
| 16-07-2014 a 17-07-2014 | *Reunión virtual* | 4/17 | Reunión del Grupo de Relator en funciones de la C4/17 |
| 16-07-2014 | *Reunión virtual* | 11/17 | Reunión del Grupo de Relator en funciones de la C11/17 |
| 20-10-2014 a 24-10-2014 | Reino Unido [Londres]/British Standards Institution | 11/17 | Reunión del Grupo de Relator en funciones de la C11/17 conjuntamente con el JTC 1/SC 6/WG 10 de la ISO/CEI |
| 15-12-2014 a 17-12-2014 | China [Beijing]/China Academy of Telecommunication Research of MIIT (CATR) | 8/17 | Reunión del Grupo de Relator en funciones de la C8/17 |
| 15-01-2015 a 16-01-2015 | Corea (Rep. de) [Seúl]/Telecommunications Technology Association (TTA) | 3/17, 6/17 | Reunión de los Grupos de Relator en funciones de la C6/17 y la C3/17 |
| 27-01-2015 a 28-01-2015 | *Reunión virtual* | 4/17 | Reunión del Grupo de Relator en funciones de la C4/17 |
| 29-01-2015 | *Reunión virtual* | 10/17 | Reunión del Grupo de Relator en funciones de la C10/17 |
| 02-02-2015 | *Reunión virtual* | 10/17 | Reunión del Grupo de Relator en funciones de la C10/17 |
| 05-02-2015 | *Reunión virtual* | 10/17 | Reunión del Grupo de Relator en funciones de la C10/17 |
| 25-05-2015 a 29-05-2015 | Bélgica [Gante]/ Universidad de Gante - iMinds | 11/17 | Reunión del Grupo de Relator en funciones de la C11/17 conjuntamente con el JTC 1/SC 6/WG 10 de la ISO/CEI |
| 09-07-2015 a 10-07-2015 | *Reunión virtual* | 4/17 | Reunión del Grupo de Relator en funciones de la C4/17 |
| 09-07-2015 a 10-07-2015 | Corea (Rep. de) [Seúl]/KISA | 6/17 | Reunión del Grupo de Relator en funciones de la C6/17 |
| 09-07-2015 | Corea (Rep. de) [Seúl]/KISA | 3/17 | Reunión del Grupo de Relator en funciones de la C3/17 |
| 16-07-2015 a 17-07-2015 | China [Beijing]/China Academy of Telecommunication Research of MIIT (CATR) | 8/17 | Reunión del Grupo de Relator en funciones de la C8/17 |
| 22-07-2015 a 24-07-2015 | Estados Unidos [Nueva York]/Aetna | 10/17 | Reunión del Grupo de Relator en funciones de la C10/17 |
| 07-01-2016 a 08-01-2016 | Corea (Rep. de) [Seúl]/TOZ | 10/17 | Reunión del Grupo de Relator en funciones de la C10/17 |
| 07-01-2016 a 08-01-2016 | Corea (Rep. de) [Seúl]/TOZ | 3/17 | Reunión del Grupo de Relator en funciones de la C3/17 |
| 07-01-2016 a 08-01-2016 | Corea (Rep. de) [Seúl]/TOZ | 6/17 | Reunión del Grupo de Relator en funciones de la C6/17 |
| 18-01-2016 a 19-01-2016 | *Reunión virtual* | 4/17 | Reunión del Grupo de Relator en funciones de la C4/17 |
| 29-02-2016 a 04-03-2016 | China [Xian]/ Comisión Nacional de Normalización de la República Popular de China | 11/17 | Reunión del Grupo de Relator en funciones de la C11/17 conjuntamente con el JTC 1/SC 6/WG 10 de la ISO/CEI |
| 15-06-2016 a 15-07-2016 (fechas previstas) | *Reunión virtual* | 4/17 | Reunión del Grupo de Relator en funciones de la C4/17 |
| 28-26-2016 a 29-06-2016 (fechas previstas) | Corea (Rep. de) [Seúl]/KISA | 3/17 | Reunión del Grupo de Relator en funciones de la C3/17 |
| 28-06-2016 a 29-06-2016 (fechas previstas) | Corea (Rep. de) [Seúl]/KISA | 2/17 | Reunión del Grupo de Relator en funciones de la C2/17 |
| 28-06-2016 a 29-06-2016 (fechas previstas) | Corea (Rep. de) [Seúl]/KISA | 7/17 | Reunión del Grupo de Relator en funciones de la C7/17 |
| 28-06-2016 a 29-06-2016 (fechas previstas) | Corea (Rep. de) [Seúl]/KISA | 6/17 | Reunión del Grupo de Relator en funciones de la C6/17 |
| 30-06-2016 a 01-07-2016 (fechas previstas) | China [Guangzhou]/China Telecom | 8/17 | Reunión del Grupo de Relator en funciones de la C8/17 |
| 14-07-2016 a 15-07-2016 (fechas previstas) | Estados Unidos [Nueva York]/Aetna | 10/17 | Reunión del Grupo de Relator en funciones de la C10/17 |

# 2 Organización del trabajo

## 2.1 Organización de los estudios y atribución de trabajos

**2.1.1** En su primera reunión del periodo de estudios, la Comisión de Estudio 17 decidió crear 5 Grupos de Trabajo.

**2.1.2** En el Cuadro 2 se indica el número y título de cada Grupo de Trabajo, junto con el número de Cuestiones que tiene asignadas y el nombre de su Presidente.

**2.1.3** En el Cuadro 3 se enumeran otros grupos creados por la Comisión de Estudio 17 durante el periodo de estudios.

**2.1.4** De conformidad con la Resolución 54 de la AMNT‑12, en la reunión de abril de 2015 de la CE 17, se creó el Grupo Regional de la CE 17 para África (véase la sección 3.3.5).

Durante el periodo de estudios considerado, el GANT dio continuidad y refrendó dos **Actividades Mixtas de Coordinación (JCA)** que había propuesto la Comisión de Estudio 17.

– **Actividad Mixta de Coordinación sobre Gestión de Identidades (JCA-IdM)**

La Actividad Mixta de Coordinación sobre Gestión de Identidades (JCA-IdM) prosiguió los trabajos realizados durante el anterior periodo de estudios, con el objetivo de coordinar los trabajos sobre gestión de identidades (IdM) del UIT-T en colaboración con organismos externos. En la sección 3.3.4.1 se presentan los logros de la JCA-IdM.

**– Actividad Mixta de Coordinación sobre Protección de la Infancia en Línea (JCA-COP)**

La Actividad Mixta de Coordinación sobre Protección de la Infancia en Línea (JCA-COP) prosiguió los trabajos realizados durante el anterior periodo de estudios, con el objetivo de coordinar los trabajos sobre protección de la infancia en línea (COP) del UIT-T entre las distintas Comisiones de Estudio del UIT-T, así como de establecer una coordinación con el UIT- R, el UIT-D y el Grupo de Trabajo del Consejo sobre la Protección de la Infancia en Línea. En la sección 3.3.4.2 se presentan los logros de la JCA-COP.

**2.1.5** Durante el periodo de estudios considerado, la Comisión de Estudio 17 siguió adelante con dos **proyectos**.

**– Proyecto ASN.1**

Creado durante el periodo de estudios 2001-2004, el proyecto ASN.1 ha seguido prestando asistencia a los usuarios de la notación ASN.1 (Recomendaciones UIT-T de las series X.680, X.690 y X.890) dentro y fuera del UIT-T, y promoviendo la utilización del ASN.1 en diversas industrias y organismos de normalización. En la sección 3.4.1 se presentan los logros de este proyecto.

**– Proyecto OID**

Creado durante el periodo de estudios 2001-2004, el proyecto OID ha seguido prestando asistencia y apoyo a los usuarios de los identificadores de objeto (OID) registrados con arreglo a las Recomendaciones de las series X.660 y X.670 dentro y fuera del UIT-T. En la sección 3.4.2 se presentan los logros de este proyecto.

CUADRO 2

Organización de la Comisión de Estudio 17

| Designación | Cuestiones que se han de estudiar | Título del Grupo de Trabajo | Presidentes de los Grupos de Trabajo |
| --- | --- | --- | --- |
| GT 1/17 | 1, 2, 3 | Seguridad básica | Koji NAKAO |
| GT 2/17 | 4, 5 | Seguridad de las redes y de la información | Sacid SARIKAYA |
| GT 3/17 | 8, 10 | Gestión de identidades y seguridad de la computación en la nube | Heung Youl YOUM |
| GT 4/17 | 6, 7, 9 | Seguridad de las aplicaciones | Antonio GUIMARAES |
| GT 5/17 | 11, 12 | Lenguajes formales | Zhaoji LIN |

CUADRO 3

Otros grupos (en su caso)

| Título del Grupo | Presidente | Vicepresidentes | |
| --- | --- | --- | --- |
| JCA-IdM | Copresidentes: Richard BRACKNEY(1), Jon SHAMAH(2), Hiroshi TAKECHI(3), Abbie BARBIR(4) |  |
| JCA-COP | Copresidentes: Ashley HEINEMAN(5), Philip RUSHTON |  |
| (GR CE17-AFR) | Michael KATUNDU | Mohamed M. K. Elhaj, Patrick Mwesigwa, Mohamed Touré |
| Proyecto ASN.1 | Jefe de proyecto: Paul THORPE |  |
| Proyecto OID | Jefe de proyecto: Olivier DUBUISSON |  |

Notas:

1) El Copresidente falleció el 12 de septiembre de 2013.

2) Copresidente hasta septiembre de 2013.

3) Copresidente desde el 4 de septiembre de 2013.

4) Copresidente desde el 24 de enero de 2014.

5) Copresidente has el 31 de enero de 2016.

## 2.2 Cuestiones y Relatores

**2.2.1** La AMNT-12 asignó a la Comisión de Estudio 17 las 12 Cuestiones que figuran en el Cuadro 4, y la CE G17 nombró a los Relatores y los Relatores Asociados citados en el mismo.

**2.2.2** Durante el periodo de estudios considerado, se adoptaron una vez más las Cuestiones que figuran en la lista del Cuadro 5.

Nota – Aunque no se adoptaron Cuestiones nuevas, las Cuestiones 6/17, 8/17 y 12/17 fueron modificadas durante este período de estudios.

**2.2.3** Durante el periodo de estudios considerado, se suprimieron las Cuestiones que figuran en la lista del Cuadro 6.

CUaDRO 4

Comisión de Estudio 17 – Cuestiones asignadas por la AMNT-08 y Relatores

| Cuestión | Título de la Cuestión | GT | Relator |
| --- | --- | --- | --- |
| C 1/17 | Coordinación de la seguridad en las telecomunicaciones/TIC | 1/17 | Mohamed M. K. ELHAJ  Relatores Asociados: Hua JIANG(7), Young Wha KIM(2), Cai CHEN(13), Isaac Kobina KWARKO, Yiwen WANG(12) |
| C 2/17 | Arquitectura y marco genérico de la seguridad | 1/17 | Patrick Mwesigwa  Relatores Asociados: Zhiyuan HU(1), Dmitry V. KOSTROV(7), Heung Ryong Oh |
| C 3/17 | Gestión de la seguridad de la información en las telecomunicaciones | 1/17 | Miho Naganuma  Relator Asociado: Kyeong Hee OH |
| C 4/17 | Ciberseguridad | 2/17 | Youki Kadobayashi  Relatores Asociados: Michael KATUNDU(1), Jong Hyun Kim, Ibrahim Hamza AL MALLOUHI |
| C 5/17 | Medios técnicos contra el correo basura | 2/17 | Hongwei Luo(10)  Yanbin ZHANG(11)  Relator Asociado: Seokung YOON(3) |
| C 6/17 | Aspectos relativos a la seguridad en los servicios de telecomunicaciones ubicuos | 4/17 | Jonghyun Baek  Relatores Asociados: Yutaka Miyake, Bo YU(12) |
| C 7/17 | Servicios de aplicación seguros | 4/17 | Jae Hoon Nah  Relatores Asociados: Lijun LIU(5) Huirong TIAN(8) |
| C 8/17 | Seguridad de la computación en la nube | 3/17 | Liang Wei  Relatores Asociados: Mark JEFFREY(9), Victor KUTUKOV |
| C 9/17 | Telebiometría | 4/17 | John George CARAS  Relator Asociado: Yong Nyuo SHIN |
| C 10/17 | Arquitectura y mecanismos de la gestión de identidades | 3/17 | Abbie Barbir  Relatores Asociados: Richard BRACKNEY(6), Hiroshi TAKECHI(4), Junjie XIA(3) |
| C 11/17 | Tecnologías genéricas para aplicaciones seguras | 5/17 | Erik Andersen  Relator Asociado:  Jean-Paul LEMAIRE |
| C 12/17 | Lenguajes formales para software de telecomunicaciones y pruebas | 5/17 | Dieter Hogrefe  Relatores Asociados:  Gunter MUSSBACHER,  Rick Reed |

Notas:

1) Relator Asociado nombrado el 17 de abril de 2015

2) Relator Asociado nombrado el 8 de abril de 2015

3) Relator Asociado nombrado el 24 de enero de 2014

4) Relator Asociado nombrado el 4 de septiembre de 2013

5) Relator Asociado nombrado el 9 de octubre de 2015

6) El Relator Asociado falleció el 12 de septiembre de 2013

7) Relator Asociado hasta marzo de 2015

8) El Relator Asociado renunció el 27 de septiembre de 2015

9) El Relator Asociado renunció el 26 de febrero de 2016

10) Relator hasta el 17 de septiembre de 2015

11) Relator nombrado el 14 de marzo de 2016

12) Relator Asociado nombrado el 23 de marzo de 2016

13) Relator Asociado nombrado el 17 de septiembre 2015.

CUADRO 5

Comisión de Estudio 17 – Nuevas Cuestiones adoptadas y Relatores

| Cuestión | Título de la Cuestión | GT | Relator |
| --- | --- | --- | --- |
| Ninguna |  |  |  |

CUADRO 6

Comisión de Estudio 17 – Cuestiones suprimidas

| Cuestión | Título de la Cuestión | Relator | Resultados |
| --- | --- | --- | --- |
| Ninguna |  |  |  |

# 3 Resultados de los trabajos realizados durante el periodo de estudios 2013-2016

## 3.1 Generalidades

Durante el periodo de estudios considerado, y hasta su reunión de marzo de 2016, la Comisión de Estudio 17 examinó 529 contribuciones y numerosos DT y Declaraciones de Coordinación

Sobre la base de esos documentos, hasta el 29 de abril de 2016, la Comisión de Estudio 17:

– elaboró 42 nuevas Recomendaciones;

– revisó 55 Recomendaciones existentes;

– enmendó 7 Recomendaciones;

– suprimió 3 Recomendaciones;

– elaboró 11 Suplementos;

– elaboró 17 Corrigenda Técnicos;

– elaboró 2 Informes Técnicos (no se elaboró ningún Manual).

## 3.2 Logros más destacados

A continuación se resumen brevemente los principales resultados obtenidos con respecto a las diversas Cuestiones asignadas a la Comisión de Estudio 17. En el cuadro sinóptico que figura en el Anexo 1 al presente informe se recogen las respuestas oficiales a las Cuestiones.

a) C 1/17, Coordinación de la seguridad en las telecomunicaciones/TIC

Esta Cuestión sigue centrándose en la coordinación y organización de toda una serie de actividades en materia de seguridad en el UIT-T y ha seguido elaborando y actualizando documentos en pro de la coordinación y la divulgación. La C1/17 centraliza los temas de coordinación de la seguridad en la CE 17.

La C1/17 no es responsable de ninguna Recomendación específica.

Durante el período de estudios considerado, la C1/17 ha elaborado y actualizado diversos documentos de divulgación, promoción y referencia, que el UIT-T considera de valor a la hora de promocionar sus trabajos sobre seguridad y los resultados del mismo. Como ejemplos se pueden citar los siguientes:

– El Manual de seguridad, *La seguridad de las telecomunicaciones y las tecnologías de la información – Visión general de asuntos relacionados con la seguridad de las telecomunicaciones y la implementación de las Recomendaciones UIT‑T existentes*, que recoge los aspectos más destacados de la labor que desempeñan las Comisiones de Estudio del UIT-T en materia de seguridad. Durante este periodo de estudios, la TSB, con la asistencia de la C1/17, ha actualizado el manual de seguridad. La 6ª edición se publicó como Informe Técnico.

– El *Compendio de Recomendaciones sobre seguridad* es un documento en línea que consta de cinco partes, a saber: el catálogo de Recomendaciones UIT-T aprobadas que guardan relación con la seguridad en las telecomunicaciones; un extracto de las definiciones de seguridad aprobadas por el UIT-T; un resumen de las actividades de las Comisiones de Estudio del UIT-T en materia de seguridad; un resumen de los textos sobre seguridad recientemente aprobados o en fase de aprobación; y un resumen de otras actividades de la UIT relativas a la seguridad.

– El *Plan de trabajo sobre normas de seguridad* es un recurso en línea que facilita información acerca de las normas de seguridad en las tecnologías de la información y la comunicación (TIC) existentes, así como de los adelantos en las organizaciones de normalización competentes. El Plan de trabajo consta de seis partes:

– Organizaciones de normalización de TIC y su trabajo, que contiene información sobre la estructura del Plan de trabajo y sobre cada una de las organizaciones normalizadoras enumeradas. También contiene enlaces a glosarios y vocabularios de seguridad.

– [Normas sobre seguridad de las TIC aprobadas, que contiene una base de datos donde se pueden consultar las normas sobre seguridad aprobadas](http://www.itu.int/ITU-T/studygroups/com17/ict/part02.html).

– [Normas sobre seguridad en fase de elaboración](http://www.itu.int/ITU-T/studygroups/com17/ict/part03.html).

– [Futuras necesidades y nuevas normas sobre seguridad propuestas](http://www.itu.int/ITU-T/studygroups/com17/ict/part04.html).

– [Prácticas idóneas](http://www.itu.int/ITU-T/studygroups/com17/ict/part05.html).

– [Panorama de la gestión de identidades (IdM): Normas sobre IdM, organizaciones y análisis de la brecha](http://www.itu.int/ITU-T/studygroups/com17/ict/part06.html).

Además de información acerca de las Recomendaciones UIT-T sobre seguridad y otras actividades conexas, el Plan de trabajo también incluye información sobre la labor normalizadora de ISO/CEI, ATIS, ENISA, ETSI, IEEE, IETF, OASIS, 3GPP y 3GPP2.

La Unión Postal Universal (UPU) y la UIT organizaron conjuntamente un mini taller, que se celebró en paralelo a la reunión de la CE 17 del UIT-T el 21 de enero de 2014. La colaboración entre el UIT-T y la UPU se enmarca en la histórica Resolución 11 de la AMNT-12. En dicho taller se abordaron diversos temas de interés común, entre ellos, el sistema de identificación PostID, la Arquitectura de Objeto Digital, las finanzas de las telecomunicaciones, la seguridad de los pagos móviles, la seguridad del correo electrónico y la colaboración entre la UIT y la UPU.

La UIT organizó un taller sobre dificultades en materia de normalización de la seguridad en las TIC para los países en desarrollo, que tuvo lugar en Ginebra (Suiza) del 15 al 16 de septiembre de 2014. El objetivo principal de este taller fue exponer y examinar los retos vinculados a la seguridad de las TIC, especialmente, para los países en desarrollo. Por consiguiente, el evento se centró en el análisis de dichos retos y en el refuerzo de las capacidades necesarias para la elaboración de normas internacionales de seguridad en las TIC. El taller tuvo asimismo por objeto la mejora de las competencias en el ámbito de la normalización, mediante la provisión de asesoramiento con respecto a la composición técnica de las normas internacionales de seguridad en las TIC y las prácticas idóneas en la materia. El evento también estuvo encaminado a reforzar la coordinación de las actividades atinentes a la seguridad de los Sectores de Normalización y Desarrollo de la UIT (a saber, el UIT-T y el UIT-D), así como a permitir la colaboración del UIT-T con otras organizaciones de normalización. Los temas principales del taller fueron: la ciberseguridad, la protección de los datos, los servicios de confianza, la computación en la nube (incluidos los macrodatos), la normalización y el papel de las TIC en la protección de la infraestructura esencial.

La UIT organizó, en colaboración con la CE 2 del UIT-D, un taller relativo a los “Problemas planteados por la ciberseguridad en todo el mundo: Colaboración destinada a una mejora efectiva de la ciberseguridad en los países en desarrollo", que se celebró el 8 de septiembre de 2015, en paralelo a las reuniones de la CE 17 del UIT-T y la CE 2 del UIT-D. Diversos representantes de la CE 17 con funciones rectoras participaron activamente en el taller, entre ellos, la Sra. Miho Naganuma (moderadora del taller) y los Sres. Mohamad Elhaj y Patrick Mwesigwa (moderadores de las dos sesiones principales). En el taller se formularon valiosas observaciones sobre los desafíos en materia de ciberseguridad a los que se enfrentaban los países en desarrollo, y se evocaron prácticas idóneas para superarlos. Este taller tradujo el buen nivel de colaboración existente entre el UIT-T y el UIT-D, quienes se comprometieron a estrechar sus lazos durante la clausura del mismo. La CE 17 remitió el informe del taller a todas las organizaciones regionales.

Por último, se ha establecido una activa coordinación entre todas las Cuestiones de la Comisión de Estudio 17, las demás Comisiones de Estudio que también abordan la seguridad y las organizaciones de normalización externas cuyos trabajos versan sobre la seguridad de las TIC.

b) C2/17, Arquitectura y marco genérico de la seguridad

Las Recomendaciones X.800, X.802 y X.803 describen la seguridad en el contexto de los sistemas abiertos. En la Recomendación X.805 se especifica la arquitectura de seguridad para los sistemas de comunicaciones de extremo a extremo. Se ha establecido un conjunto completo de marcos de seguridad detallados que abarcan aspectos de la seguridad tales como la autenticación, el control de acceso, el no rechazo, la confidencialidad, la integridad y la auditoría y las alarmas de seguridad (X.810, X.811, X.812, X.813, X.814, X.815 y X.816). Para crear condiciones de seguridad genérica de capas superiores (GULS, *generic upper layers security*) se elaboraron las Recomendaciones X.830, X.831, X.832, X.833, X.834 y X.835. En cooperación con el JTC 1/SC 27 de la ISO/CEI, se prepararon las Recomendaciones X.841, X.842 y X.843 relativas a objetos de información sobre seguridad y servicios de tercero fiable.

Durante el periodo de estudios considerado, la C2/17 ha elaborado dos nuevas Recomendaciones y un nuevo Suplemento:

• X.1033, *Directrices relativas a la seguridad de los servicios de información prestados por los operadores*, contiene directrices relativas a la seguridad de los servicios de información prestados por los operadores de telecomunicaciones. En esta Recomendación se abordan cuestiones tales como la clasificación de los servicios de información, los requisitos de seguridad, los mecanismos y la coordinación.

• X.1037, *Directrices técnicas de seguridad para la implantación de IPv6,* facilita una serie de directrices técnicas de seguridad para que las organizaciones de telecomunicaciones implanten y exploten las redes y los servicios IPv6. El contenido de esta Recomendación se centra en cómo implantar de manera segura las instalaciones de red para organizaciones de telecomunicaciones y cómo ejecutar las operaciones de manera segura en el entorno IPv6.

• X. Suppl. 23, *Suplemento a la Recomendación UIT-T X.1037 –Suplemento sobre directrices de gestión de la seguridad para la implantación de IPv6 en organizaciones de telecomunicaciones*, proporciona directrices de gestión de la seguridad para la implantación de IPv6 en organizaciones de telecomunicaciones, con el fin de garantizar la protección de la información en las redes y de la estructura de red de apoyo durante la transición de IPv4 a IPv6 y la implantación de IPv6.

c) C3/17, Gestión de la seguridad de la información en las telecomunicaciones

La C3/17 estudia la gestión de la seguridad de la información en las telecomunicaciones, reconociendo así que, para las organizaciones de telecomunicaciones, la información y sus procesos subyacentes, las instalaciones de telecomunicaciones, las redes y los medios de transmisión son importantes activos comerciales. En colaboración con la ISO/CEI, se revisó la importante Recomendación UIT-T X.1051, donde se dan directrices sobre gestión de la seguridad de la información.

A lo largo del periodo de estudios considerado, la C3/17 ha elaborado una Recomendación revisada:

• X.1051 (revisada), *Tecnología de la información - Técnicas de seguridad – Código de prácticas en materia controles de seguridad de la información basados en la norma ISO/CEI 27002 para organizaciones de telecomunicaciones*, establece directrices y principios generales para iniciar, aplicar, mantener y mejorar los controles de seguridad de la información en las organizaciones de telecomunicaciones, de conformidad con la norma ISO/CEI 27002. Además, proporciona una base para la implantación de los controles de seguridad de la información en el seno de dichas organizaciones, con el fin de garantizar la confidencialidad, la integridad y la disponibilidad de las instalaciones de telecomunicaciones, los servicios y la información que se maneja, procesa o almacena en los servicios e instalaciones.

La C3/17 coopera estrechamente con el JTC 1/SC 27/ WG 1 de la ISO/CEI en lo que se refiere a gestión de la seguridad de la información.

Esta Cuestión es distinta de las que trata la Comisión de Estudio 2, pues estas últimas abordan el intercambio de información de gestión de red entre elementos de red y sistemas de gestión, y entre sistemas de gestión en un entorno de red de gestión de telecomunicaciones (RGT). Esta Cuestión se ocupa principalmente de la protección de los activos comerciales, incluidos la información y sus procesos, con miras a gestionar la seguridad de la información.

d) C4/17, Ciberseguridad

La C4/17 estudia la ciberseguridad, reconociendo así que el panorama de la ciberseguridad varía constantemente y, con él, los requisitos aplicables a la seguridad de las telecomunicaciones/TIC. En este ciberentorno, resulta indispensable garantizar la seguridad de los protocolos, la infraestructura y las aplicaciones que son indispensables para nuestras comunicaciones cotidianas. La ciberseguridad consiste en asegurar y proteger los servicios, la información personal y la información de identificación personal, así como en garantizar la protección de la información entre entidades comunicantes. La C4/17 elaboró un conjunto de especificaciones importantes para el intercambio fiable de información de seguridad, necesario para poder medir la seguridad y permitir un control de seguridad continuo. Estas especificaciones han recibido el nombre de CYBEX, que es la sigla en inglés para Intercambio de información de ciberseguridad. La C4/17 también estudia cuestiones de ciberseguridad que no guardan relación con CYBEX, tales como la detección de tráfico anómalo, la defensa contra las redes robot y la identificación del origen de los ataques (incluido el rastreo).

La C4/17 es la principal responsable de responder a la Resolución 50 (Ciberseguridad) de la AMNT-12 y, junto con la C3/17, a la Resolución 58 (Fomento de la creación de equipos nacionales de intervención en caso de incidente informático, especialmente para los países en desarrollo).

Durante el periodo de estudios considerado, la C4/17 ha elaborado ocho nuevas Recomendaciones, tres Recomendaciones revisadas, siete nuevas Enmiendas, dos nuevos Suplementos y un Suplemento revisado:

• X.1208*, Un indicador de riesgo de ciberseguridad para mejorar la confianza y la seguridad en la utilización de las telecomunicaciones y las tecnologías de la información y la comunicación*, describe una metodología para que las organizaciones utilicen indicadores de ciberseguridad en el cálculo de la medida de riesgo y facilita una lista de posibles indicadores de ciberseguridad. Esta Recomendación no propone utilizar un índice o un solo indicador para expresar las capacidades de una organización en materia de ciberseguridad.

• X.1210, *Aspectos generales de los mecanismos de detección del origen de los problemas de seguridad en las redes de protocolo Internet*,presenta los mecanismos de detección del origen de los problemas de seguridad, además de los criterios de selección y las directrices de seguridad básica de esos mecanismos.

• X.1211, *Técnicas para prevenir ataques en la web*,describe técnicas que pueden atenuar los ataques en la web que ocurren cuando se explotan las vulnerabilidades de los servidores de sitios web y se introducen códigos malignos que pueden infectar la computadora del usuario.

• X.1303*bis*, *Protocolo de alerta común (CAP 1.2),* tiene un formato simple pero general que favorece el intercambio de alertas de emergencia y públicas de cualquier peligro por todo tipo de redes. Con el CAP se puede difundir un mensaje de alerta coherente de forma simultánea a través de numerosos sistemas de alerta, aumentando de esa manera la eficacia de la tarea y, al mismo tiempo, simplificando su realización.

• *Enmiendas 3, 4, 5, 6, 7, 8 y 9 a la Recomendación X.1500:* *Técnicas revisadas de intercambio de información estructurada sobre ciberseguridad*, facilita una lista de técnicas revisadas de intercambio de información estructurada sobre ciberseguridad, que ha de actualizarse a medida que surgen nuevas técnicas o que las ya existentes evolucionan, se amplían o se sustituyen. La lista se ajusta a lo estipulado en el cuerpo de la Recomendación. Estas enmiendas reflejan la situación de las técnicas recomendadas en abril de 2013, septiembre de 2013, enero de 2014, septiembre de 2014, abril de 2015, septiembre de 2015 y marzo de 2016, e incluyen referencias bibliográficas.

• X.1520 (revisada), *Vulnerabilidades y exposiciones comunes*,ofrece una forma estructurada de intercambio de información de seguridad sobre vulnerabilidades y exposiciones con el objetivo de proporcionar nombres comunes para problemas conocidos públicamente en el área del software comercial o de fuente abierta utilizado en redes de telecomunicaciones, dispositivos de usuarios finales o en otros tipos de tecnologías de la información y las comunicaciones (TIC) que ejecutan programas informáticos. El objetivo de esta Recomendación es facilitar el intercambio de datos entre capacidades destinadas a combatir vulnerabilidades (herramientas, repositorios y servicios) empleando las denominaciones comunes incluidas en la misma.

• X.1521 (revisada), *Sistema común de puntuación de vulnerabilidades 3.0*,describe un marco abierto para la comunicación de las características y repercusiones de las vulnerabilidades de las tecnologías de la información y las comunicaciones (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 TIC capaces de ejecutar software.

• X.1525, *Sistema común de puntuación de puntos débiles*, describe un marco abierto para la comunicación de las características y repercusiones de los puntos débiles de las tecnologías de la información y las comunicaciones (TIC) durante el desarrollo de capacidades de software.

• X.1526 (revisada), *Lenguaje para la definición abierta de vulnerabilidades y la evaluación del estado del sistema,* incluye las tres fases principales del proceso de evaluación: la representación de la información de configuración de los puntos extremos en cada prueba; el análisis del punto extremo para la detección de los estados de máquina especificados (vulnerabilidad, configuración, parche, etc.); y la c información de los resultados de la evaluación. La finalidad de OVAL es proporcionar una norma comunitaria internacional sobre seguridad de la información para promover contenidos de seguridad abiertos y públicamente disponibles y normalizar la transferencia de esa información a través de toda la serie de instrumentos y servicios de seguridad. OVAL incluye un lenguaje utilizado para codificar los detalles del punto extremo, así como una compilación de repositorios de contenido a lo largo de toda la comunidad.

• X.1544, *Enumeración y clasificación de pautas de ataques comunes*, es una especificación basada en XML/XSD para la identificación, descripción y enumeración de pautas de ataques.

• X.1546, *Enumeración y caracterización de atributos de malware*, se centra en la creación de la enumeración de atributos de malware de bajo nivel y comprende enumeraciones de los atributos y comportamientos del malware con los que se forma un vocabulario común.

• X.1582, *Protocolos de transporte para el intercambio de información de ciberseguridad*, presenta los protocolos de transporte que se han adoptado para el intercambio de información de ciberseguridad (CYBEX) y que se han adaptado al mismo. También describe las aplicaciones de transporte, las características de los protocolos de transporte y los aspectos relativos a la seguridad.

• X. Suppl.10 (revisado), *Suplemento a la Recomendación UIT*‑*T* *X.1205 – Suplemento sobre utilización del rastreo de red*, presenta el rastreo de red para responder a determinados problemas de las redes de un proveedor o de un conjunto complejo de proveedores de servicios. El rastreo puede ayudar a descubrir los puntos de ingreso, trayectos, trayectos parciales u orígenes de eventos problemáticos en la red. Esta información puede ayudar a los proveedores de servicios a mitigar tales eventos.

• X.Suppl.18, *Suplemento a la Recomendación UIT-T X.1205 – Suplemento sobre directrices para la detección y el control del tráfico anómalo en redes de telecomunicaciones basadas en IP*, identifica tecnologías de detección del tráfico anómalo y medidas de control para las redes de telecomunicaciones basadas en IP. El objeto de este Suplemento es proporcionar a los operadores de telecomunicaciones una serie de directrices exhaustivas para el seguimiento, la detección y el control del tráfico IP anómalo.

• X.Suppl.20, *Suplemento a la Recomendación UIT-T X.1205 – Suplemento sobre marcos para la negociación del intercambio de información de seguridad*, proporciona un marco para la negociación de acuerdos relativos al intercambio de información de seguridad entre las entidades que integran el ámbito de la ciberseguridad, entre ellas, las solicitantes y las proveedoras de información. En este Suplemento se definen las capacidades funcionales y un modelo de referencia para las negociaciones atinentes al intercambio de información de seguridad y la modelación de datos conceptuales relativos a los acuerdos de intercambio de información de seguridad (SSA), a la política de intercambio de información de seguridad (SSP) y al proceso de negociación de los SSA.

e) C5/17, Medios técnicos contra el correo basura

La C5/17 estudia las medidas técnicas para luchar contra el correo basura (spam), en la medida en que afecta a la estabilidad y robustez de las redes de telecomunicaciones. El correo basura es un problema que se ha generalizado creando una compleja serie de dificultades a los usuarios, proveedores de servicios y operadores de red de todo el mundo. Con sus estudios, la C5/17 responde directamente a las Resoluciones 52 y 50 de la AMNT-12.

La C5/17 siguió utilizando la misma estructura de árbol de series de Recomendaciones sobre la lucha contra el correo basura, que abarca la mayoría de tipos actuales y futuros de spam. Dicha estructura comprende tres niveles: el primero lo forman las estrategias técnicas de la lucha contra el correo basura; el segundo se centra en esferas específicas de esta lucha, incluidos los SMS, el correo electrónico y las aplicaciones multimedios IP; y el tercero abarca las tecnologías generales para luchar contra el correo basura.

Durante el periodo de estudios considerado, la C5/17 ha elaborado dos nuevas Recomendaciones, un nuevo Suplemento y un Corrigéndum (X.1243 Cor.1):

• X.1246, *Tecnologías implicadas en la lucha contra el spam de voz en las organizaciones de telecomunicaciones*, ofrece una visión general del spam de voz y resume las tecnologías antispam existentes, que aplican tanto los usuarios como los operadores de red, y el mecanismo de colaboración entre ellos.

• X.1247, *Marco técnico para luchar contra el correo basura en la mensajería móvil*, ofrece una visión general de los procesos encaminados a contrarrestar‎ 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 describe 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.

• X.Suppl.25, *Suplemento a la Recomendación UIT-T X.1231, Suplemento sobre pautas para ayudar a los desarrolladores de teléfonos móviles a luchar contra el correo basura*, proporciona pautas para ayudar a los desarrolladores de teléfonos móviles a luchar contra el correo basura. En este Suplemento se describen amenazas a la seguridad de los teléfonos móviles y aspectos relacionados con la aplicación.

f) C6/17, Aspectos relativos a la seguridad en los servicios de telecomunicaciones ubicuos

La C6/17 estudia los aspectos relativos a la seguridad en los servicios de telecomunicaciones ubicuos, es decir, los servicios que permiten a cualquier persona acceder a toda la información deseada fácilmente, en cualquier momento y en cualquier lugar, utilizando un dispositivo cualquiera. Concretamente, la C6/17 estudia la seguridad en las telecomunicaciones ubicuas específicas del domino entre dispositivos heterogéneos que utilizan tecnologías a nivel de aplicación, como la web ubicua para redes de sensores, redes domésticas, redes móviles, redes de multidifusión, redes de TVIP, IoT, SDN, redes eléctricas inteligentes e ITS ubicuos. Durante este período de estudios, el GANT enmendó la C6/17.

Durante el periodo de estudios considerado, la C6/17 ha elaborado dos nuevas Recomendaciones, dos Corrigenda Técnicos (X.1311 Cor.1, X.1314 Cor.1), y tres nuevos Suplementos:

• X.1198, *Plataforma virtual de seguridad basada en la máquina para el servicio de TVIP renovable y la protección de contenidos*, se especifica una plataforma virtual de seguridad basada en la máquina para el servicio de TVIP renovable y el sistema de protección de contenidos (SCP). En esta Recomendación se define una interfaz común y una lógica funcional en el dispositivo terminal de televisión por el protocolo Internet (TVIP) e incluye la estructura de datos del cliente SCP y los componentes de sistema de un dispositivo terminal, como un SCP incorporado, un cliente de medios y un cliente de control.

• X.1314, *Requisitos y marco de seguridad de las redes ubicuas*,presenta un marco de seguridad de alto nivel para las redes ubicuas, analiza las amenazas a la seguridad y define los requisitos de seguridad para mitigar dichas amenazas en un entorno de red ubicua.

• X.Suppl.19, *Suplemento a las Recomendaciones UIT-T de las series X.1120-X.1139 – Suplemento sobre aspectos de seguridad de los teléfonos inteligentes*, tiene por objeto proteger la privacidad de los usuarios y mejorar la seguridad de la información de los teléfonos inteligentes. A fin de satisfacer dichos objetivos de seguridad, este Suplemento especifica un marco de seguridad jerárquico y los correspondientes requisitos de seguridad para los teléfonos inteligentes. Además, identifica una serie de amenazas a los teléfonos inteligentes, que se dividen en vulnerabilidades y ataques. Con respecto al marco de seguridad, este Suplemento propone soluciones de seguridad necesarias a través de mejoras en el sistema y herramientas de seguridad.

• X.Suppl.24, *Suplemento a las Recomendaciones UIT-T de las series X.1120-X.1139 – Suplemento sobre marcos seguros de distribución de aplicaciones para dispositivos de comunicación*, proporciona un marco seguro de distribución de aplicaciones para dispositivos de comunicación y un conjunto de requisitos de seguridad para los sitios de distribución de aplicaciones, con objeto de mejorar la seguridad del entorno de comunicación para los usuarios.

• X.Suppl.26, *Suplemento a la Recomendación UIT-T X.1111, Suplemento sobre la arquitectura funcional de seguridad para los servicios de red eléctrica inteligente que utilizan redes de telecomunicaciones*, describe una arquitectura funcional de seguridad para los servicios de red inteligente que utilizan redes de telecomunicaciones, e identifica riesgos y requisitos de seguridad. Este Suplemento define asimismo una arquitectura funcional de seguridad para los servicios de red inteligente que utilizan redes de telecomunicaciones, con arreglo a un modelo funcional general.

La C6/17 colabora con los JTC 1/SC 6, 25, 27 y 31 de la ISO/CEI en materia de seguridad de las RSU.

g) C7/17, Servicios de aplicación seguros

La C7/17 estudia temas relacionados con los servicios de aplicación seguros, por ejemplo, la seguridad de los servicios punto a punto (P2P), la autentificación por contraseña segura con intercambio de claves y diversos servicios de tercero fiable (TTP), y servicios web.

Durante el periodo de estudios considerado, la C7/17 ha elaborado ocho nuevas Recomendaciones y dos nuevos Suplementos:

• X.1144, *Lenguaje de marcaje de control de acceso extensible (XACML) 3.0*, trata del lenguaje de marcaje de control de acceso extensible (XACML 3.0), que es una versión actualizada de la Recomendación UIT-T X.1142 (equivalente a OASIS XACML 2.0 (06/2006)), y define el núcleo de XACML, incluida la sintaxis del lenguaje, los modelos, el contexto con modelo de lenguaje político, sintaxis y reglas de procesamiento.

• X.1154, *Marco general para la autentificación combinada en entornos con múltiples proveedores de servicio de identidad*, presenta un marco general sobre autentificación combinada en entornos con múltiples IdSP para un proveedor de servicio. En esta Recomendación, se consideran tres tipos de métodos de autentificación combinada: autentificación multifactorial, autentificación multimétodo y autentificaciones múltiples.

• X.1155, *Directrices sobre autenticación anónima enlazable local para servicios electrónicos*, contiene directrices sobre autenticación anónima enlazable local para servicios electrónicos. Ello incluye amenazas a la privacidad de los servicios electrónicos, requisitos de autenticación anónima enlazable local, funciones para satisfacer dichos requisitos y un modelo general de autenticación anónima enlazable local para servicios electrónicos.

• X.1156, *Marco de no repudio basado en una contraseña de uso único*, presenta un marco de no repudio basado en una contraseña de uso único (OTP) para aumentar la confianza entre entidades que realizan transacciones.

• X.1157, *Capacidades técnicas de detección y respuesta al fraude para servicios con requisitos de alto nivel de seguridad*, describe las capacidades necesarias para el servicio de detección y respuesta al fraude de los servicios basados en aplicaciones de tecnologías de la información y la comunicación (TIC) sensibles a la seguridad.

• X.1158, *Mecanismo de autentificación multifactorial utilizando un dispositivo móvil*, describe las debilidades de los mecanismos de autenticación de factor único, la necesidad de mecanismos de autenticación de múltiples factores y de diversas combinaciones de mecanismos de autenticación de múltiples factores que utilizan un dispositivo móvil, y las amenazas para los mecanismos de autenticación de dos factores.

• X.1159, *Arquitectura de no repudio delegada, basada en la Recomendación UIT-T X.813*, describe operaciones y modelos de servicio de no repudio delegado.

• X.1163, *Requisitos y mecanismos de seguridad para redes de telecomunicaciones entre pares*,presenta unas directrices de seguridad para redes de telecomunicaciones basadas en la tecnología P2P. Además, describe brevemente las características de la red, analiza los requisitos de seguridad de la red y los servicios y especifica los mecanismos de seguridad necesarios para cumplir tales requisitos.

• X.Suppl.21, *Suplemento a la Recomendación UIT-T X.1143 – Suplemento sobre marcos de seguridad para los servicios de las aplicaciones web híbridas*, detalla un marco de seguridad para los servicios de las aplicaciones web híbridas y describe diversos tipos de aplicaciones web híbridas y una arquitectura de referencia.

• X.Suppl.22, *Suplemento a la Recomendación UIT-T X.1144 – Suplemento sobre mejoras y nuevas características del lenguaje de marcaje de control de acceso extensible (XACML) 3.0*, resume las mejoras y nuevas características de la Recomendación UIT-T X.1144 (XACML 3.0) en comparación con la Recomendación UIT-T X.1142 (XACML 2.0).

h) C8/17, Seguridad de la computación en la nube

La C8/17 sobre seguridad de la computación en la nube de la CE17 elaboró, en colaboración con los Presidentes de la CE 13 y la CE 17, principios de alto nivel para la separación de los trabajos relacionados con la seguridad de la computación en la nube. Durante este periodo de estudios, el GANT enmendó la C8/17.

Durante el periodo de estudios considerado, la C8/17 ha elaborado cuatro nuevas Recomendaciones y una Recomendación revisada:

• X.1601 y X.1601 (revisada), *Marco de seguridad para la computación en la nube*,describe el marco de seguridad para la computación en la nube. Esta Recomendación analiza las amenazas y los problemas de seguridad en el contexto de la computación en la nube y describe las capacidades de seguridad que podrían mitigar estas amenazas y resolver los problemas de seguridad. Además, facilita una metodología marco para determinar qué capacidades de seguridad se han de especificar para mitigar las amenazas y resolver los problemas de seguridad en la computación en la nube.

• X.1602, *Requisitos de seguridad para los entornos de aplicación del software como servicio*, 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.

• X.1631, *Tecnologías de la información – Técnicas de seguridad –Código de prácticas para controles de seguridad de la información basados en SO/IEC 27002 para los servicios en la nube*,contiene directrices para los controles de seguridad de la información aplicables a la prestación y utilización de servicios en la nube, mediante la provisión de orientaciones adicionales para la aplicación de los controles pertinentes especificados en ISO/CEI 27002, así como para otros controles adicionales en relación con los cuales se facilitan pautas de ejecución específicamente relacionadas con los servicios en la nube. En esta Recomendación | Norma Internacional se detallan controles y directrices de aplicación para los proveedores y los clientes de los servicios en la nube.

• X.1642, *Directrices para la seguridad operativa de la computación en la nube*, ofrece directrices operativas genéricas de seguridad para la computación en la nube desde la perspectiva de los Proveedores de servicios en la nube (CSP). En esta Recomendación se analizan los requisitos de seguridad y las métricas para el funcionamiento de la computación en la nube. Además, ofrece un conjunto de medidas de seguridad y de actividades detalladas de seguridad relacionadas con el funcionamiento diario y el mantenimiento, para ayudar a los CSP a reducir los riesgos de seguridad y abordar los retos en materia de seguridad para el funcionamiento de la computación en la nube.

i) C9/17, Telebiometría

La C9/17 estudia la telebiometría y los requisitos y directrices de seguridad para las aplicaciones de la telebiometría, incluidos los requisitos de los protocolos genéricos adecuados, que proporcionen seguridad y protección de la privacidad y autoricen el "empleo de datos biométricos" en cualquier aplicación de telebiometría, por ejemplo, la cibersalud o la telemedicina.

Durante el periodo de estudios considerado, la C9/17 ha elaborado una nueva Recomendación:

• X.1092, *Marco integrado para la protección de datos telebiométricos en cibersalud y telemedicina*,ofrece un marco integrado para la protección de los datos biométricos y la información privada en cibersalud y telemedicina.

j) C10/17, Arquitectura y mecanismos de la gestión de identidades

Esta Cuestión se dedica a fijar la orientación y a coordinar y organizar toda la gama de actividades de IdM del UIT-T. En colaboración con otras Comisiones de Estudio y organizaciones de normalización (SDO), se aborda la IdM con un método deductivo. Hay otras Cuestiones que abordan aspectos específicos de la IdM, es decir, protocolos, requisitos, identificadores de dispositivos de red, etc.

Durante el periodo de estudios considerado, la C10/17 ha elaborado tres nuevas Recomendaciones:

• X.1255, *Marco para la indagación de información de gestión de identidades*, tiene por objeto describir una arquitectura marco abierta que permita la indagación de información de gestión de identidades (IdM). Los componentes fundamentales del marco descrito en esta Recomendación son: 1) un modelo de datos de entidades digitales, 2) un protocolo interfaz de entidades digitales, 3) uno o varios identificadores/sistemas de resolución y 4) uno o varios registros de metadatos. Estos son los componentes básicos de la arquitectura marco abierta.

• X.1256, *Directrices y marco para la compartición de los resultados de la autentificación de la red con las aplicaciones de los servicios*, desarrolla directrices para que los operadores de red y los proveedores de servicios puedan compartir 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.

• X.1257, *Taxonomía de la gestión del acceso y de la identidad*, 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.

k) C11/17, Tecnologías genéricas para aplicaciones seguras

La C11/17 estudia los servicios y sistemas de directorio, incluidos los certificados de clave pública/atributos. Una gran parte del trabajo realizado conjuntamente con el JTC 1/SC 6/GT 10 de la ISO/CEI consiste en actualizar la serie de Recomendaciones X.500.

Durante el periodo de estudios considerado, se ha acometido una importante labor relacionada con la Recomendación UIT-T X.509, incluidas medidas encaminadas a:

a) Simplificar su contenido de forma que, en la especificación, solo se aborden la infraestructura de clave pública (PKI) y la infraestructura de gestión de privilegios (PMI), trasladando ciertas secciones del directorio X.500 a otras partes de la serie X.500. De esta forma, la Recomendación UIT-T X.509 ha adquirido el carácter de documento independiente.

b) Armonizar el estilo y la terminología del documento con los que se utilizan actualmente en la industria, y establecer una clara separación entre la PKI y PMI.

c) Añadir la llamada capacidad de lista de autorización y validación, solicitada y recogida en la norma IEC 62351-9, IEC TC 57 *Power Systems Management and Associated Information Exchange - Part 9 – Data and Communication Security - Key Management*.

d) Realizar otras modificaciones con objeto de que la Recomendación UIT-T X.509 estuviese preparada para los futuros requisitos impuestos por la seguridad de redes eléctricas inteligentes y la Internet de las Cosas.

La C11/17 se encarga del mantenimiento de las Recomendaciones sobre ASN.1 y está trabajando en las Recomendaciones sobre OID. Este trabajo también se realiza en colaboración con el JTC 1/SC 6/WG 10 de la ISO/CEI. ASN.1 se mantiene estable desde su revisión aprobada en septiembre de 2015. Desde entonces se han aprobado sólo unas cuantas correcciones con categoría de Corrigenda. La base de datos de módulos ASN.1 sigue alimentándose, lo que permite a los implementadores obtener especificaciones ASN.1 publicadas, de lectura automática y con la sintaxis verificada.

A lo largo de varios periodos de estudio, la Comisión de Estudio 17 ha elaborado un sistema mundial de identificación basado en autoridades de registro jerárquico, denominado "Árbol de identificador de objeto", que las Recomendaciones UIT-T y UIT-R, así como las normas internacionales de la ISO/CEI, utilizan ampliamente para muchas aplicaciones. Se han registrado públicamente más de 954 046 identificaciones, y muchas más se han registrado para uso interno de varias organizaciones. El árbol de identificador de objeto original identificaba los arcos del árbol con números y nombres formados con el alfabeto latino.

La C11/17 en colaboración con el JTC 1/SC 7/WG 19 de la ISO/CEI ha elaborado dos revisiones de las Recomendaciones UIT-T X.906 y X.911 sobre procesamiento distribuido abierto.

La C11/17 se ocupa de mantener las Recomendaciones sobre interconexión de sistemas abiertos (OSI) de la serie X. Durante el periodo de estudios considerado, la C11/17 no ha elaborado ni revisado Recomendación alguna a ese respecto, pero ha desarrollado los Corrigenda Técnicos X.226 Cor.1yX.227*bis* Cor.1.

Durante el periodo de estudios considerado, la C11/17 ha elaborado cuatro Recomendaciones nuevas, 14 Recomendaciones revisadas, 12 Corrigenda Técnicos a las Recomendaciones de las series X.500, X.680 y X.690 (X.226 Cor.1, X.227*bis* Cor.1, X.509 Cor.1, X.509 Cor.2, X.680 Cor.2, X.682 Cor.1, X.683 Cor.1, X.690 Cor.2, X.694 Cor.2, X.520 Cor.1, X.691 Cor.3 y X.691 Cor.4), y un Informe Técnico:

• F.511, *Servicio de directorio - Servicios de identificación por etiquetas*, ofrece orientaciones relativas a la utilización de los servicios de directorio para dar soporte a aplicaciones que utilicen o dependan de la identificación basada en marcadores en función de las capacidades de directorio especificadas en la serie de Recomendaciones UIT-T X.500 | ISO/IEC 9594 (todas las partes), y en especificaciones atinentes al Protocolo ligero de acceso al directorio (LDAP), tales como las elaboradas en el seno del Grupo Especial sobre Ingeniería de Internet (IETF).

• X.667 (revisada), *Tecnología de la información - Procedimientos para el funcionamiento de las autoridades de registro de los identificadores de objeto: Generación of identificadores únicos universales y su utilización como componentes de identificador de objetos*, especifica los procedimientos para la generación de identificadores únicos universales (UUID) y para su utilización en el árbol identificador de objetos internacional bajo el arco UUID conjunto.

• X.675, *Marco de resolución basado en OID para identificadores y localizadores heterogéneos*,analiza requisitos como la independencia de los identificadores, la separación de los identificadores, la compatibilidad, la exclusividad, la tolerancia, la estabilidad y la seguridad. En esta Recomendación se especifica la arquitectura general del marco de resolución basado en el identificador de objeto con diversas hipótesis de aplicación, donde se muestra cómo funciona el marco de resolución para identificadores y localizadores heterogéneos.

• X.680 (revisada), *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica*, proporciona una notación llamada notación de sintaxis abstracta uno (ASN.1) para la definición de la sintaxis de datos de información. Se definen en ella varios tipos de datos sencillos y se especifica una notación para hacer referencia a esos tipos y especificar valores de los mismos. La notación ASN.1 puede aplicarse cuando sea necesario definir la sintaxis abstracta de la información sin restringir de ningún modo la manera de codificar la información para la transmisión.

• X.681 (revisada), *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de objetos de información,* proporciona la notación ASN.1, que permite definir y dar nombres de referencia a clases de objetos de información así como a objetos de información individuales y conjuntos de los mismos.

• X.682 (revisada), *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de constricciones,* proporciona la notación ASN.1 para el caso general de especificación de constricciones y excepciones, por la cual se pueden limitar los valores de datos de un tipo de datos estructurado.

• X.683 (revisada), *Tecnología de la información – Notación de sintaxis abstracta uno: Parametrización de especificaciones de notación de sintaxis abstracta uno*,define las disposiciones para los nombres de referencia parametrizados y las asignaciones parametrizadas para tipos de datos, que son útiles a los diseñadores cuando escriben especificaciones en las que algunos aspectos se dejan indefinidos en determinadas etapas del desarrollo para ser completadas en una etapa ulterior con objeto de producir una definición completa de una sintaxis abstracta.

• X.690 (revisada), *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación básica, de las reglas de codificación canónica y de las reglas de codificación distinguida*, define un conjunto de reglas de codificación básica (BER), que se pueden aplicar a valores de tipos definidos utilizando la notación ASN.1, y sendos conjuntos de reglas de codificación distinguida (DER) y reglas de codificación canónica (CER), que proporcionan constricciones de las reglas de codificación básica.

• X.691 (revisada), *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación compactada*,describe un conjunto de reglas de codificación que pueden aplicarse a valores de todos los tipos ASN.1 para lograr una representación más compacta que la proporcionada por las reglas de codificación básica y sus derivadas (descritas en la Rec. UIT-T X.690 | ISO/CEI 8825-1).

• X.692 (revisada), *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de la notación de control de codificación*, define la notación de control de codificación (ECN) utilizada para especificar codificaciones (de tipos ASN.1) que difieren de las obtenidas aplicando reglas de codificación normalizadas, tales como las reglas de codificación básica (BER) y las reglas de codificación compactada (PER).

• X.693 (revisada), *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Reglas de codificación del lenguaje de marcaje extensible*, especifica normas para la codificación de valores de tipos ASN.1 que utilizan el lenguaje de marcaje extensible (XML).

• X.694 (revisada), *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Correspondencia en notación de sintaxis abstracta uno de las definiciones W3C de los esquemas de lenguaje de marcaje extensible*,define reglas para establecer la correspondencia de un esquema XSD (un esquema conforme a la especificación de esquema XML W3C) con un esquema ASN.1 con el fin de utilizar reglas de codificación ASN.1 – tales como las reglas de codificación básica (BER), las reglas de codificación distinguida (DER), las reglas de codificación compactada (PER) o las reglas de codificación XML (XER) – para la transferencia de información definida por el esquema XSD.

• X.695 (revisada), *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Registro y aplicación de instrucciones de codificación de las reglas de codificación compactada*,especifica reglas de aplicación de las instrucciones de codificación PER que utilizan prefijos de tipo o una sección de control de codificación.

• X.696, *Tecnología de la información - Especificación de reglas de codificación de octetos (OER)*, especifica dos conjuntos de reglas de codificación binaria que pueden aplicarse a valores de todos los tipos ASN.1 utilizando menos recursos de procesamiento que las reglas de codificación básica y sus derivadas.

• X.696 (revisada), *Tecnología de la información - Reglas de codificación de notación de sintaxis abstracta uno: Especificación de reglas de codificación de octetos (OER)*, especifica dos conjuntos de reglas de codificación binaria que pueden aplicarse a valores de todos los tipos ASN.1 utilizando menos recursos de procesamiento que las reglas de codificación básica y sus derivadas (descritas en la Recomendación UIT-T X.690 | ISO/CEI 8825-1) y las reglas de codificación compactada (descritas en la Recomendación UIT-T X.691 | ISO/CEI 8825 2).

• X.906 (revisada), *Tecnología de la información – Procesamiento distribuido abierto – Utilización del lenguaje de modelado unificado para la especificación de sistemas de procesamiento distribuido abierto*, precisa y amplía la definición del modo en que los sistemas de procesamiento distribuido abierto (ODP) se especifican definiendo la utilización del lenguaje de modelización unificado para la expresión de especificaciones de sistema ODP.

• X.911 (revisada), *Tecnología de la información – Procesamiento distribuido abierto – Modelo de referencia – Lenguaje de empresa*,perfecciona y extiende la definición del modo en que los sistemas ODP están especificados desde el punto de vista de la empresa, y está destinada al desarrollo o la utilización de especificaciones de empresa de sistemas ODP.

• X.1341, *Protocolos de transferencia de correo certificado y de oficina postal certificada*, define el Protocolo de transferencia de correo certificado (CMTP) y el Protocolo de oficina postal certificada (CPOP) con el fin de fomentar los intercambios de correos electrónicos certificados en todo el mundo y de manera segura proporcionando confidencialidad, identificación de los corresponsales e integridad y evitando el repudio.

• Informe Técnico, *Desafíos actuales y nuevos en materia de normalización de la infraestructura de clave pública,* explora las amenazas y los problemas relacionados con la implantación de la infraestructura de clave pública (PKI), y los nuevos retos a los que se enfrentará la PKI en ámbitos tales como la PKI inalámbrica (WPKI), la computación en la nube, las redes eléctricas inteligentes y la tecnología de máquina a máquina (M2M) en general.

l) C12/17, Lenguajes formales para software de telecomunicaciones y pruebas

La C12/17 estudia los lenguajes formales para definir los requisitos, la arquitectura y el comportamiento de los sistemas de telecomunicaciones: lenguajes de requisitos, lenguajes de especificación y lenguajes de aplicación. La C12/17 también estudia los lenguajes de prueba como medio de apoyo a la interoperatividad y la conformidad.

Durante el periodo de estudios considerado, las Comisiones de Estudio 11 y 17 acordaron a través del GANT:

– Revisar la Cuestión 11/11 para añadir trabajos relativos a las metodologías y el marco de las pruebas de conformidad e interoperatividad.

– Revisar la Cuestión 12/17 para suprimir trabajos relativos a las metodologías y el marco de las pruebas de conformidad y añadir trabajos sobre TTCN-3.

– Revisar el Anexo C a la Resolución 2, con objeto de reflejar la situación de las series Z.160/Z.170 en la CE 17 y la situación de las series X.290 (excepto la Recomendación X.292), X.Suppl.4, X.Suppl.5 y Z.500 en la CE 11.

Durante el periodo de estudios considerado, la C12/17 ha elaborado seis nuevas Recomendaciones, 25 Recomendaciones revisadas, tres Guías del implementador revisadas, y un Suplemento revisado:

• Z.100 (revisada), *Lenguaje de especificación y descripción - Visión general de SDL-2010*, introduce el lenguaje de descripción y especificación, destinado a describir y especificar sin ambigüedad los sistemas de telecomunicaciones.

• Anexo F1 a la Recomendación Z.100 (revisado), *Lenguaje de especificación y descripción – Visión general de SDL-2010 – Definición formal de SDL: Visión general*, expone la motivación, resume la estructura de la semántica formal, y presenta una introducción al formalismo de la máquina de estados abstractos (ASM) que se utiliza para definir la semántica SDL-2010.

• Anexo F2 a la Recomendación Z.100 (revisado), *Lenguaje de especificación y descripción – Visión general de SDL-2010 – Definición formal de SDL: Semántica estática*, describe las restricciones semánticas estáticas de SDL-2010 y expone las transformaciones identificadas en las cláusulas “Modelo” de las Recomendaciones UIT-T Z.101, Z.102, Z.103, Z.104, Z.105 y Z.107, que se incluyen por referencia en la Recomendación UIT-T Z.100.

• Anexo F3 a la Recomendación Z.100 (revisado), *Lenguaje de especificación y descripción – Visión general de SDL-2010 – Definición formal de SDL: Semántica dinámica*, define la semántica dinámica de SDL-2010.

• Z.101 (revisada), *Lenguaje de especificación y descripción - SDL-2010 básico*, define las características básicas del lenguaje de especificación y descripción. En el presente documento se describen las características fundamentales del lenguaje, que se define con mayor detalle en otras Recomendaciones UIT-T de la serie Z.100.

• Z.102 (revisada), *Lenguaje de especificación y descripción - SDL-2010 integral*, define las características exhaustivas del lenguaje de especificación y descripción. El lenguaje definido en este documento comprende características del lenguaje no incluidas en el SDL básico de 2010 que se especifica en la Recomendación UIT-T Z.101. Estas características abarcan de manera exhaustiva la gramática abstracta del lenguaje, excepto algunas características de datos definidas en la Recomendación UIT-T Z.104 (y la Recomendación UIT-T Z.107 para los datos orientados a objetos).

• Z.103 (revisada), *Lenguaje de especificación y descripción - Notación abreviada y anotación en SDL-2010*,define las características de la notación abreviada y la anotación del lenguaje de especificación y descripción. El lenguaje definido en este documento incluye características no incluidas en el SDL básico de 2010 de la Recomendación UIT-T Z.101 o el SDL integral de 2010 de la Recomendación UIT-T Z.102. Las características definidas en esta Recomendación no tienen su propia gramática abstracta y se transforman a la gramática concreta definida en las Recomendaciones UIT-T Z.101, UIT-T Z.102 y UIT-T Z.104 (y UIT-T Z.107 para los datos orientados a objetos), o bien son anotaciones sin significado formal.

• Z.104 (revisada), *Lenguaje de especificación y descripción - Datos y lenguaje de acción en SDL-2010*, define las características de datos del lenguaje de especificación y descripción, de modo que las definiciones y expresiones de datos quedan bien definidas. El lenguaje definido en este documento se solapa en parte con las características del lenguaje incluidas en el SDL básico de 2010 de la Recomendación UIT-T Z.101 y utilizadas en el SDL integral de 2010 de la Recomendación UIT-T Z.102, así como con las características especificadas en la Recomendación UIT-T Z.103.

• Z.105 (revisada), *Lenguaje de especificación y descripción - SDL-2010 combinado con módulos ASN.1*, define el modo en que pueden utilizar los módulos de notación de sintaxis abstracta uno (ASN.1) en combinación con el lenguaje de especificación y descripción de 2010 (SDL-2010). Este texto sustituye la Recomendación UIT-T Z.105 (2003), en aras de la armonización con las Recomendaciones UIT-T Z.100, UIT-T Z.101, UIT-T Z.102, UIT-T Z.103, UIT-T Z.104, UIT-T Z.106 y UIT-T Z.107 para SDL-2010. La Recomendación UIT-T Z.105 (2003) sustituyó las correspondencias semánticas de ASN.1 a SDL-2000 definidas en la Rec. UIT-T Z.105 (1999).

• Z.106 (revisada), *Lenguaje de especificación y descripción - Formato de intercambio común para SDL-2010*,define el formato de intercambio común del lenguaje de especificación y descripción (SDL-CIF). El SDL-CIF está destinado al intercambio de especificaciones SDL-2010 gráficas (SDL-GR) preparadas con diferentes herramientas que no utilizan el mismo formato de almacenamiento. En esta Recomendación se introducen dos nuevos niveles de SDL-CIF, y se definen dos nuevos niveles de conformidad, uno en un nivel SDL-PR más liberal y el segundo que incluye información gráfica.

• Z.107 (revisada), *Lenguaje de especificación y descripción - datos orientados a objetos en SDL-2010*,define las características de los datos orientados a objetos del lenguaje de especificación y descripción, basándose en las definiciones de datos y las expresiones contempladas en la Recomendación UIT-T Z.104. El lenguaje definido en este documento se solapa en parte con las características del lenguaje incluidas en el SDL básico de 2010 de la Recomendación UIT-T Z.101 y utilizadas en el SDL integral de 2010 de la Recomendación UIT-T Z.102, así como con las características especificadas en las Recomendaciones UIT-T Z.103 y UIT-T Z.104.

• Z.109 (revisada), *Lenguaje de especificación y descripción - Perfil del lenguaje de modelado unificado para SDL-2010*,define un perfil del lenguaje de modelado unificado (UML) que se corresponde con la semántica del SDL de 2010, de modo que puede utilizarse en combinación con el SDL. La combinación de SDL-2010 y UML permite especificar de manera coherente la estructura y el comportamiento de los sistemas de telecomunicaciones, y los datos. La Recomendación UIT-T Z.109 se ha revisado por motivos de coherencia con el resto de Recomendaciones UIT-T de la serie Z.100 sobre SDL-2010.

• Z.111 (revisada), *Notaciones y directrices para la definición de lenguajes del UIT-T*,describe metagramáticas para las Recomendaciones UIT-T, que definen lenguajes del UIT-T en las Recomendaciones UIT-T de la serie X.680 y de la serie Z sobre lenguajes de especificación, aplicación, modelización y pruebas. Así se pueden describir las metagramáticas que definen la gramática abstracta o concreta (sintaxis, restricciones y semántica) de los lenguajes sin tener que incluir como preámbulo o anexo a cada definición de lenguaje la metagramática en cuestión (por ejemplo, reglas de denominación léxica o descripción de la sintaxis de forma Backus-Naur).

• Z.161 (revisada), *Notación de pruebas y de control de pruebas versión 3: Lenguaje núcleo de TTCN-3*,define la TTCN‑3 (notación de pruebas y control de pruebas 3) prevista para la especificación de series de pruebas independientemente de las plataformas, los métodos de pruebas, las capas de protocolo y los protocolos utilizados. La primera revisión de Z.161 añade numerosas extensiones al lenguaje (valores de parámetro por defecto –la parametrización de tipos se ha trasladado a otro documento (parametrización avanzada) –, valores reales especiales y límites de gama exclusivos, restricciones de visibilidad de definiciones importadas, restricciones de plantilla, campos implícitamente omitidos en valores y plantillas, declaraciones de continuidad/discontinuidad, nuevas funciones predefinidas, etc.) y contiene múltiples aclaraciones (por ejemplo, sobre subclasificación de tipos estructurados, homologación, ejecución de la declaración de detención, etc.) y correcciones de fondo y de forma.

• Z.161.1, Z.161.1 (revisada), *Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Soporte de interfaces con señales continuas*, define el lote de "apoyo de la señal continua" de la TTCN 3. Esta notación puede utilizarse para la especificación de todos los tipos de pruebas de sistemas reactivos en diversos puertos de comunicación. Las aplicaciones típicas de la TTCN-3 son las pruebas de protocolos (incluidos los protocolos móviles e Internet) y las pruebas de servicios (incluidos los servicios suplementarios), las pruebas de módulos, las pruebas de plataformas basadas en la arquitectura de intermediario de petición de objeto común (CORBA), las pruebas de interfaces de programas de aplicación (API), etc. La TTCN-3 no está restringida a las pruebas de conformidad, sino que puede utilizarse para muchas otras clases de pruebas, incluidas pruebas de interoperabilidad, robustez, regresión, sistemas e integración. La especificación de series de pruebas para protocolos de capa física está fuera del ámbito del presente documento.

• Z.161.2, Z.161.2 (revisada), *Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Apoyo para la configuración e implantación*,define el lote de ayuda a la configuración e implantación de la TTCN-3.

• Z.161.3, Z.161.3 (revisada), *Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Parametrización avanzada*, define el lote de parametrización avanzada de la TTCN-3.

• Z.161.4, Z.161.4 (revisada), *Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Tipos de comportamiento*,define el lote de tipos de comportamiento de la TTCN-3.

• Z.161.5, Z.161.5 (revisada), *Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Resultados y realización de pruebas en tiempo real*, define el lote de soporte de las pruebas de calidad de funcionamiento y en tiempo real de la TTCN-3.

• Z.165 (revisada), *Notación de pruebas y de control de pruebas versión 3: Interfaz de ejecución*, especifica la interfaz de ejecución en las aplicaciones de TTCN‑3 (notación de pruebas y de control de pruebas 3) en sistemas de pruebas. La segunda revisión de Z.165 contiene enmiendas, aclaraciones y correcciones de fondo y de forma.

• Z.165.1, Z.165.1 (revisada), *Notación de prueba y de control de prueba versión 3: Paquete de ampliación de la TTCN-3: Extended TRI*, define el lote TRI ampliado de la TTCN-3. La notación TTCN-3 puede emplearse para la especificación de todos los tipos de pruebas de sistemas reactivos en diversos puertos de comunicación. Las aplicaciones típicas son las pruebas de protocolos (incluidos los protocolos móviles y de Internet), las pruebas de servicios (incluidos los servicios suplementarios), las pruebas de módulos, las pruebas de plataformas basadas en la arquitectura de intermediario de petición de objeto común (CORBA), las pruebas de interfaces de programas de aplicación (API), etc. La TTCN-3 no está restringida a las pruebas de conformidad, sino que puede utilizarse para muchas otras clases de pruebas, incluidas pruebas de interoperabilidad, robustez, regresión, sistemas e integración. La especificación de series de pruebas para protocolos de capa física está fuera del ámbito del presente documento.

• Z.166 (revisada), *Notación de pruebas y de control de pruebas versión 3: Interfaz de control*,especifica las interfaces de control en las aplicaciones de TTCN‑3 en sistemas de pruebas. La segunda revisión de Z.166 contiene enmiendas, aclaraciones y correcciones de fondo y de forma.

• Z.167 (revisada), *Notación de pruebas y de control de pruebas versión 3 (TTCN-3): Utilización de ASN.1 con TTCN-3*, define la normativa para utilizar ASN.1, como se define en las Recomendaciones UIT‑T X.680, UIT‑T X.681, UIT‑T X.682 y UIT‑T X.683, con TTCN‑3. La segunda revisión de Z.167 contiene enmiendas (conformidad y compatibilidad, requisitos y descripciones relacionadas con el tipo identificador de objeto se han trasladado a este documento procedentes de todas las demás Recomendaciones de la serie Z.16x, soporte de valores XML dentro de los módulos ASN.1, conversión de los tipos OID-IRI y RELATIVE-OID-IRI, valores reales especiales y subtipos con valores especiales y límites exclusivos, actualización de cadenas de lenguaje predefinidas, etc.), aclaraciones (por ejemplo sobre visibilidad de definiciones ASN.1 importadas, sobre reglas de transformación), y correcciones de fondo y de forma.

• Z.168 (revisada), *Notación de pruebas y de control de pruebas versión 3: Correspondencia del lenguaje de definición de interfaz de CORBA con TTCN-3*,define las reglas de correspondencia entre CORBA IDL (como se define en el capítulo 3 del proyecto de especificación aprobada ptc/06-05-01 (2006)) y TTCN‑3 (como se define en la Recomendación UIT‑T Z.161) para permitir las pruebas en los sistemas CORBA. La segunda revisión de Z.168 contiene enmiendas, aclaraciones y correcciones de fondo y de forma.

• Z.169 (revisada), *Notación de pruebas y control de pruebas versión 3 (TTCN-3): Utilización de esquemas XML con TTCN-3*,define las reglas de correspondencia entre el esquema W3C y TTCN‑3 para poder probar los sistemas, interfaces y protocolos XML. La tercera revisión de Z.169 contiene enmiendas, aclaraciones y correcciones de fondo y de forma.

• Z.170 (revisada), *Notación de pruebas y de control de pruebas versión 3: especificación de los comentarios de documentación TTCN-3*, define la documentación del código fuente de TTCN-3 utilizando comentarios de documentación especiales. La segunda revisión de Z.170 contiene enmiendas, aclaraciones y correcciones de fondo y de forma.

• Z.Sup1 (revisado), *Suplemento a las Recomendaciones UIT-T de la serie Z.100 – Suplemento metodológico sobre la utilización de las técnicas de descripción*, (véanse las Recomendaciones UIT-T Z.100 a Z.107, Z.109, Z.110, Z.120, Z.121, Z.150, Z.151, y Z.160 a Z.170), describe una metodología (denominada SDL+) para la utilización combinada de estos lenguajes, en particular, cuando se utiliza el lenguaje de especificación y descripción de la UIT.

• Z.Imp100 (revisada), *Guía del implementador – Lenguaje de especificación y descripción* *– Versión 2.0.1*, es una compilación de los defectos detectados en las Recomendaciones UIT‑T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.109, Z.111 y Z.119, relativas al lenguaje de especificación y descripción, y las soluciones propuestas. Esta guía se ha concebido como una fuente de información normativa adicional para los implementadores, que debe consultarse junto con las Recomendaciones correspondientes. La guía propiamente dicha no es una Recomendación UIT-T, aunque recoge las correcciones convenidas a los defectos notificados. Esta Guía se refiere a la versión SDL-2010 del lenguaje.

• Z.Imp100 (revisada), *Guía del implementador – Lenguaje de especificación y descripción* *– Versión 2.0.2*, es una compilación de los defectos detectados en las Recomendaciones UIT‑T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.109, Z.111 y Z.119, relativas al lenguaje de especificación y descripción, y las soluciones propuestas. Esta guía se ha concebido como una fuente de información normativa adicional para los implementadores, que debe consultarse junto con las Recomendaciones correspondientes. La guía propiamente dicha no es una Recomendación UIT-T, aunque recoge las correcciones convenidas a los defectos notificados. Esta Guía se refiere a la versión SDL-2010 del lenguaje.

• Z.Imp100 (revisada), *Guía del implementador – Lenguaje de especificación y descripción* *– Versión 3.0.0,* incluye todos los cambios acordados por la C12/17 con respecto a los textos de las Recomendaciones pertinentes que eran objeto de consentimiento o se hallaban en vigor en la fecha en que la CE 17 aprobó la guía, y se aplicará bien hasta que la guía del implementador se actualice, bien hasta que todos los cambios se integren en las Recomendaciones pertinentes y la guía se actualice a la versión 3.0.1.

## 3.3 Informe sobre las actividades de la Comisión de Estudio Rectora, las GSI, las JCA, los Grupos Regionales y los proyectos

La Comisión de Estudio 17 es la Comisión de Estudio Rectora sobre seguridad de las telecomunicaciones, gestión de identidades y lenguajes y técnicas de descripción. Las actividades de Comisión de Estudio Rectora se dividen de la siguiente manera:

– Seguridad, tema del que se ocupa la Cuestión 1/17.

– Gestión de identidades, tema del que se ocupa la Cuestión 10/17.

– Lenguajes y técnicas de descripción, tema del que se ocupa el GT 3/17.

– Lenguajes y técnicas de descripción, tema del que se ocupa el GT 5/17.

### 3.3.1 Actividades de la Comisión de Estudio Rectora sobre seguridad

La Comisión de Estudio 17 fue nombrada la Comisión de Estudio Rectora sobre seguridad en virtud de la Resolución 2 de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT‑12).

En su calidad de Comisión de Estudio Rectora sobre seguridad de las telecomunicaciones, la Comisión de Estudio 17 es responsable del estudio de las Cuestiones más importantes sobre seguridad. Además, en consulta con las Comisiones de Estudio pertinentes y en colaboración, cuando proceda, con otros organismos de normalización, la Comisión de Estudio 17 se ocupa de definir y mantener el marco general y de coordinar, asignar (en función del mandato de cada Comisión de Estudio) y establecer prioridades entre los estudios que han de realizar otras Comisiones de Estudio, así como de garantizar la preparación de Recomendaciones coherentes, completas y oportunas.

Dentro de la CE 17, la Cuestión 1/17 asume la función de coordinación de las actividades de la Comisión de Estudio Rectora en materia de seguridad, cometido que lleva a cabo en estrecha colaboración con otras Comisiones de Estudio a fin de identificar y elaborar soluciones de seguridad. No obstante, la experiencia necesaria para integrar estas soluciones en cada una de las tecnologías que se están desarrollando sólo puede proceder de la Cuestión encargada de tal desarrollo.

En tanto que Comisión de Estudio Rectora sobre seguridad, la Comisión de Estudio 17 ha establecido una duradera coordinación con todas las Comisiones de Estudio del UIT-T cuyo trabajo atañe de alguna manera a la seguridad. La CE 17 también colabora con un amplio conjunto de organismos y foros de normalización en materia de seguridad de las telecomunicaciones y las TIC. Se ha insistido particularmente en evitar todo posible conflicto entre los trabajos que realizan las Comisiones de Estudio y los de organismos externos.

Además, en el marco de las reuniones de la Comisión de Estudio 17 se han celebrado reuniones de coordinación sobre seguridad y se ha elaborado una lista de personas de contacto de todas las Comisiones de Estudio que abordan la seguridad.

En cuanto a los asuntos examinados por la CE 17 en su condición de Comisión de Estudio Rectora, se han recibido y tramitado Declaraciones de Coordinación interna procedentes de la CITS de la UIT, el CT-CCVOCAB, el SCV de la UIT, la Cuestión 26/2 del UIT-D, la CE 1 (C22-1/1) del UIT-D, la CE 2 (C3/2) del UIT-D, la CE 6 del UIT-R, diversos grupos de trabajo del UIT-R (5A, 5B, 5C, 5D, 7C), diversos grupos temáticos del UIT-T(AC, DFS, DR&NRR, Innovation, SmartCable, SSC), diversas actividades mixtas de coordinación del UIT-T (AHF, CIT, Cloud, COP, IoT, Res178, SDN, SG&HN), el RevCom del UIT-T, diversas Comisiones de Estudio del UIT-T (2, 3, 9, 11, 12, 13 (GT 3/13), 15, 16 (C14/16, C27/16, C28/16), 20), y el GANT del UIT-T.

En cuanto a los asuntos examinados por la CE 17 en su condición de Comisión de Estudio Rectora, se han recibido y tramitado Declaraciones de Coordinación externa procedentes del 3GPP (SA3, TSG GERAN), el CSA, el ETSI ISG (ISI, QSC), diversos comités técnicos de ETSI (CYBER, ITS, M2M, MTS), el GSMA SG, el ICANN SSAC, diversos comités técnicos de la CEI (25 (JWG 1, WG 5, WG 6), 57/WG15), el IETF (IAB, Security Area, STIR WG), el comité técnico 12 de la ISO (JWG 20, WG 18), diversos subcomités del JTC de la ISO/CEI (6/WG 7, 7/WG 19, 27 (SC27/WG 1, WG 2), 37, 38), el JTC 1/WG 10 de la ISO/CEI, MEF, OASIS, el GT4 de oneM2M y la UPU.

La CE 17 envió Declaraciones de Coordinación interna a la CITS de la UIT, diversas Comisiones de Estudio del UIT-D (1(C22-1/1), 2 (C3/2, C5/2)), diversas Comisiones de Estudio del UIT-R (4, (GT 4A, 4B, 4C), 5 (GT 5A), 7), diversos grupos temáticos del UIT-T (DFS, Innovation, SSC), diversas actividades mixtas de coordinación del UIT-T (AHF, CIT, Cloud, COP, IoT, Res178, SDN, SG&HN), el RevCom del UIT-T, el SCV del ITU- T, diversas Comisiones de Estudio del UIT-T (2, 3, 5, 9, 11, 12, 13, 15, 16 y 20), y el GANT del UIT-T.

La CE 17 envió Declaraciones de Coordinación externa al 3GPP (SA3, TSG GERAN), el CSA, la ENISA, el ETSI (ISG ISI, SAGE, TC (CYBER, ITS (WG2, WG5), M2M, MTS, SmartM2M)), la FIDO Alliance, la GSMA (MMG, FASG, SG), la CIUMR, el IEC SEG, diversos comités técnicos de la CEI (25 (JWG 1), 57 WG 15, 65/WG10), el IESG, el IETF (SEC Area, STIR WG), el SAG-S de la ISO, diversos comités técnicos de la ISO (12 (JWG 20, WG 18), TC 68/SC2, 154, 204, 215, 292), el TMB de la ISO, diversos subcomités del JTC 1 de la ISO/CEI (6 (WG 10), 27 (SG sobre IoT, WG 1, WG 2, WG 3, WG 4, WG 5), 37 (WG 4)), el M3AAGT, el NIST, el NSTIC, diversos comités técnicos de OASIS (Identity in the cloud, IBOPS, MQTT, Trust Elevation), la OIDF, la OMA, oneM2M (GT4), UPnP y la UPU.

De conformidad con la Resolución 7 de la AMNT-12, *Colaboración con la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI)*, la Comisión de Estudio 17 mantiene un cuadro en línea donde se consignan sus relaciones con los Comités Técnicos (TC) de la ISO y la CEI y con los Subcomités (SC) del JTC 1 de la ISO/CEI, incluida su naturaleza en tanto que labor conjunta (por ejemplo, textos comunes o gemelos), colaboración técnica mediante coordinación o coordinación informal.

En 2013, en nombre de la UIT, la CE 17 participó en dos talleres sobre lucha contra el correo basura, a saber, el taller de la UIT sobre respuesta y lucha contra el correo basura, que se celebró en Durban (Sudáfrica) el 8 de julio de 2013, y el taller conjunto de la CITEL (CCP.I), la UIT e Internet Society sobre lucha contra el correo basura, que tuvo lugar en Mendoza (Argentina) el 7 de octubre de 2013. Ambos eventos fueron fructíferos y tuvieron repercusiones notables.

En 2014, la CE 17 organizó un taller sobre dificultades en materia de normalización de la seguridad en las TIC para los países en desarrollo, de día y medio de duración, que se celebró en Ginebra del 14 al 15 de septiembre de 2014. Este taller atrajo a más de 90 participantes, procedentes en su mayoría de países en desarrollo. Los asistentes vieron reforzadas sus competencias en materia de normalización, tras recibir asesoramiento relativo a la composición técnica de las normas internacionales de seguridad en las TIC y las mejores prácticas en la materia. El evento también estuvo encaminado a reforzar la coordinación de las actividades en materia de seguridad de los Sectores de Normalización y Desarrollo de la UIT (a saber, el UIT-T y el UIT-D), así como a permitir la colaboración del UIT-T con otras organizaciones de normalización. Fruto de este taller fue la creación de un grupo por correspondencia sobre investigación de nuevos temas para la normalización de la CE 17.

En 2015, la UIT organizó un taller de ciberseguridad sobre "Problemas planteados por la ciberseguridad en todo el mundo: Colaboración destinada a una mejora efectiva de la ciberseguridad en los países en desarrollo", que se celebró la tarde del 8 de septiembre de 2015, en paralelo a las reuniones de la CE 17 del UIT-T y la CE 2 del UIT-D. En el taller se formularon valiosas observaciones sobre los desafíos en materia de ciberseguridad a los que se enfrentaban los países en desarrollo, y se evocaron prácticas idóneas para superarlos. Este taller tradujo el buen nivel de colaboración existente entre el UIT-T y el UIT-D, quienes se comprometieron a estrechar sus lazos durante la clausura del mismo.

En concreto, el plan de trabajo de la CE 17 en materia de seguridad comprende:

• la aplicación de las Resoluciones 7, 11, 40, 50, 52, 58, 64, 65, 67, 70, 73, 75, 76 y 78 de la AMNT-12;

• la aplicación de las Resoluciones 101, 130, 136, 174, 177, 178, 179, 181, 188, 189, 197, 199, 200 y 201 de la PP-10 y la PP-14; y

• la aplicación de las Resoluciones 23, 30, 34, 45, 47, 54, 63, 67, 69, 79 y 80 de la CMDT-10 y la CMDT-14.

La Comisión de Estudio 17 elaboró un Plan de Acción para la aplicación de las Resoluciones de la AMNT-12 que actualizó en cada una de sus reuniones.

Además, la Comisión de Estudio 17 se encarga del mantenimiento de la página web de la Comisión de Estudio Rectora sobre seguridad, la cual contiene enlaces a los productos y servicios de seguridad más importantes.

A medida que se aprueban nuevas normas en materia de seguridad de las TIC, la CE 17 actualiza la base de datos sobre normas de seguridad del Plan de Normalización de Seguridad de las TIC, una importante herramienta que ayuda a los encargados de la elaboración de normas a evitar las duplicaciones. Las páginas web correspondientes a las Partes 1, 2 y 3 de dicho Plan fueron objeto de actualización.

La CE 17 también se encarga de actualizar el Compendio sobre Seguridad, el cual contiene información acerca de la actividad normativa de la UIT en el ámbito de la seguridad, incluido un catálogo de las Recomendaciones del UIT-T que guardan relación con la seguridad y un catálogo de definiciones y abreviaturas de seguridad aprobadas por el UIT-T.

La Comisión emprendió las labores relativas a un nuevo tema de trabajo (X.TRsuss), con miras a la elaboración de un informe técnico sobre la aplicación eficaz de las normas de seguridad, que ayudará a los usuarios, especialmente a los procedentes de países en desarrollo, a ampliar sus conocimientos sobre los beneficios derivados de la aplicación de las Recomendaciones UIT-T relacionadas con la seguridad en diversos contextos (por ejemplo, en las esferas empresarial, comercial, gubernamental e industrial). En dicho informe se abordarán distintas aplicaciones de las normas de seguridad y se facilitará información sobre la pertinencia y la importancia de ciertas normas básicas de seguridad, entre ellas, las atinentes a la arquitectura, la metodología, las definiciones y otras orientaciones de alto nivel. El objetivo principal consistirá en fomentar una aplicación eficaz y productiva de estas normas.

Se concluyeron los trabajos encaminados a la preparación de la 6ª edición del Manual de Seguridad como un Informe Técnico. El Manual de Seguridad es una importante herramienta de promoción del UIT-T que pone de relieve, en palabras llanas, la importante labor de todas las Comisiones de Estudio del UIT-T en materia de seguridad.

Las Comisiones de Estudio del UIT-T (distintas de la CE17) lograron los siguientes resultados en el marco de sus actividades relacionadas con las Recomendaciones sobre seguridad:

Recomendaciones aprobadas:

| CE | Recomendación | Título |
| --- | --- | --- |
| CE5 | K.58 | Compatibilidad electromagnética, resistibilidad y requisitos y orientaciones de seguridad para determinar responsabilidades en las instalaciones de tecnologías de la información y la comunicación coubicadas |
| CE9 | J.1002 | Especificación del protocolo de emparejamiento para el sistema de acceso condicional renovable |
| CE9 | J.1003 | Especificaciones del protocolo de red para los sistemas de acceso condicional renovable |
| CE9 | J.1004 | Especificaciones de las interfaces de centro de autorización para el sistema de acceso condicional renovable |
| CE9 | J.1005 | Arquitectura y requisitos de la gestión de derechos digitales (DRM) para las multipantallas de televisión por cable |
| CE13 | Y.2705 | Requisitos mínimos de seguridad para la interconexión del servicio de telecomunicaciones de emergencia (ETS) |
| CE13 | Y.2725 | Soporte de OpenID en redes de la próxima generación |
| CE13 | Y.2770 | Requisitos para la inspección detallada de paquetes en las redes de la próxima generación |
| CE13 | Y.2771 | Marco para la inspección detallada de paquetes |
| CE13 | Y.3032 | Configuraciones de los identificadores de nodo y la cartografía de los mismos mediante localizadores en las redes futuras |
| CE13 | Y.3520 (revisada) | Marco de computación en nube para la gestión de recursos de extremo a extremo |
| CE15 | G.808.1 | Conmutación de protección genérica – Protección lineal de camino y de subred |
| CE15 | G.808.3 | Conmutación de protección genérica – Protección por malla compartida |
| CE15 | G.873.1 | Red óptica de transporte: Protección lineal |
| CE15 | G.873.1 Enm.1 | Red óptica de transporte: Protección lineal - Enmienda 1: Nuevo Apéndice III – Protección de la capa óptica |
| CE15 | G.873.2 | Protección de anillo compartido de ODUk |
| CE15 | G.8031/Y.1342 (revisada) | Conmutación de protección lineal Ethernet |
| CE16 | F.748.1 | Requisitos y características comunes del identificador IoT para el servicio IoT |
| CE16 | F.771 Enm.1 | Descripción y requisitos del servicio de acceso a las informaciones multimedios según identificación basada en etiquetas – Enmienda 1: Soporte de interfaces radioeléctricas múltiples |
| CE16 | H.235.0 (revisada) | Marco de seguridad H.323: Marco de seguridad para sistemas multimedia de la serie H (H.323 y otros basados en H.245) |
| CE16 | H.235.6 (revisada) | Marco de seguridad H.323: Perfil de criptación con la gestión de claves UIT-T H.235/H.245 nativa |
| CE16 | H.248.84 | Protocolo de control de pasarela: Traspaso de NAT para los servicios de punto a punto |
| CE16 | H.248.86 | Protocolo de control de pasarela: Soporte para sistemas UIT-T H.248 de la inspección detallada de paquetes |
| CE16 | H.248.90 | Protocolo de control de pasarela: paquetes UIT-T H.248 para controlar la seguridad del transporte utilizando seguridad en la capa de transporte (TLS) |
| CE16 | H.248.91 | Protocolo de control de pasarela: Directrices para la utilización de las capacidades de UIT-T H.248 para la seguridad del transporte en redes TLS con perfiles UIT -T H.248 |
| CE16 | H.248.93 | Protocolo de control de pasarela: Apoyo de UIT-T H.248 para el control de la seguridad del transporte utilizando el protocolo de datagrama de seguridad de la capa de transporte (DTLS) |
| CE16 | H.460.18 | Paso de señalización UIT-T H.323 a través de traductores de dirección de red y cortafuegos |
| CE16 | H.460.19 | Paso de medios UIT-T H.323 por traductores de dirección de red y cortafuegos |
| CE16 | H.460.22 | Negociación de protocolos de seguridad para proteger los mensajes de señalización de llamada UIT-T H.225.0 |
| CE16 | H.621 Enm.1 | Arquitectura del sistema de acceso a las informaciones multimedios según identificación basada en etiquetas: Enmienda 1: Soporte de interfaces radioeléctricas múltiples |
| CE16 | H.751 | Metadatos para la interoperabilidad de los derechos de información en los servicios de TVIP |
| CE16 | H.810 | Directrices de diseño de la interoperabilidad para los sistemas personales de salud |

**Nota:**

**\*** Recomendaciones aprobadas mediante el procedimiento de aprobación tradicional.

Suplementos y Apéndices acordados

| CE | Número | Título |
| --- | --- | --- |
| CE13 | Y.Sup19 | Serie UIT-T Y.2200 – Suplemento sobre análisis de riesgos en las redes de próxima generación |
| CE13 | Y.Sup18 | Serie UIT-T Y.2200 – Suplemento sobre gestión de certificados en las redes de próxima generación |
| CE13 | Suplemento 23 a las Recomendaciones de la serie Y.2770 | Serie UIT-T Y.2200 – Suplemento sobre terminología en materia de IDP |
| CE13 | Suplemento 25 | Serie UIT-T Y.2200 – Suplemento sobre casos de utilización y aplicación de la IDP |
| CE15 | G.Suppl.52 | Recomendaciones UIT-T de la serie G – Suplemento sobre conmutación de protección del anillo Ethernet |
| CE15 | G.sup54 | Recomendaciones UIT-T de la serie G – Suplemento sobre conmutación de protección lineal Ethernet |
| CE16 | H.460.24 (2009) Enm.2 | Transmisión punto a punto de medios a través de cortafuegos y traductores de dirección de red dentro de los sistemas UIT-T H.323: Soporte del modo de multiplexación de medios de UIT-T H.460.19 para los medios punto a punto |

### 3.3.2 Actividades de la Comisión de Estudio Rectora sobre gestión de identidad

La Comisión de Estudio 17 fue nombrada la Comisión de Estudio Rectora sobre gestión de identidad en virtud de la Resolución 2 de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT-12).

En su calidad de Comisión de Estudio Rectora sobre gestión de identidad (IdM), la Comisión de Estudio 17 es responsable del estudio de las Cuestiones más importantes sobre IdM. Además, en consulta con las Comisiones de Estudio pertinentes y en colaboración, cuando proceda, con otros organismos de normalización, la Comisión de Estudio 17 se ocupa de definir y mantener el marco general y de coordinar, asignar (en función del mandato de cada Comisión de Estudio) y establecer prioridades entre los estudios que han de realizar otras Comisiones de Estudio, así como de garantizar la preparación de Recomendaciones coherentes, completas y oportunas.

En concreto, la Comisión de Estudio 17 es responsable de los estudios relacionados con la preparación de un modelo genérico de gestión de identidades que sea independiente de las tecnologías de red y que sirva de soporte para el intercambio seguro de información de identidad entre las entidades. Esta labor comprende también el estudio del proceso de descubrimiento de fuentes autorizadas de información de identidad, los mecanismos genéricos para la neutralidad/compatibilidad de diversos formatos de información de identidad, las amenazas a la gestión de identidad, los mecanismos para contrarrestarlas, la protección de la información de identificación personal (IIP) y la elaboración de mecanismos que garanticen que sólo se autoriza el acceso a la IIP cuando procede.

A continuación se muestra la situación en que se encuentran los trabajos en materia de IdM que realizan las Comisiones de Estudio del UIT‑T:

Las Comisiones de Estudio del UIT-T (distintas de la CE17) lograron los siguientes resultados en el marco de sus actividades relacionadas con las Recomendaciones sobre IdM:

Recomendaciones aprobadas

| CE | Recomendación | Título |
| --- | --- | --- |
| CE13 | Y.2084 | Funciones de distribución de contenidos de la interconexión de servicios distribuidos |
| CE13 | Y.2723 | Soporte de OAuth en las redes de la próxima generación |
| CE13 | Y.2724 | Marco para el soporte y utilización de OAuth y OpenID en las redes de la próxima generación |
| CE13 | Y.2725 | Soporte de OpenID en redes de la próxima generación |
| CE13 | Y.3031 | Marco de identificación en las redes futuras |
| CE13 | Y.3032 | Configuraciones de los identificadores de nodo y la cartografía de los mismos mediante localizadores en las redes futuras |
| CE13 | Y.3034 | Arquitectura para el interfuncionamiento de redes de componentes heterogéneos en redes futuras basadas en la separación identificador/localizador |
| CE16 | F.748.1 | Requisitos y características comunes del identificador IoT para el servicio IoT |
| CE16 | F.771 Enm.1 | Descripción y requisitos del servicio de acceso a las informaciones multimedios según identificación basada en etiquetas – Enmienda 1: Soporte de interfaces radioeléctricas múltiples |
| CE16 | H.621 Enm.1 | Arquitectura del sistema de acceso a las informaciones multimedios según identificación basada en etiquetas: Enmienda 1: Soporte de interfaces radioeléctricas múltiples |
| CE16 | H.642.1 | Acceso a información multimedios mediante identificación basada en etiquetas - Sistema de identificación |
| CE16 | H.642.2 | Acceso a información multimedios mediante identificación basada en etiquetas - Procedimientos de inscripción de identificadores |
| CE16 | H.642.3 | Tecnología de la información – Técnica de identificación y captación de datos automática – Protocolo de resolución de identificador para el acceso a información multimedios a través de la identificación basada en etiquetas |
| CE16 | H.642.2 | Acceso a información multimedios mediante identificación basada en etiquetas - Procedimientos de inscripción de identificadores |

Suplementos acordados

| CE | Suplemento | Título |
| --- | --- | --- |
| CE13 | Y.Suppl.18 | Serie UIT-T Y.2200 – Suplemento sobre gestión de certificados en las redes de próxima generación |

En la página web de la CE 17 se ha incluido un WIKI con el Plan IdM, donde se recopilan todas las normas sobre IdM vigentes y en proceso de elaboración en todo el mundo. Este Plan es reflejo de la coordinación que se está llevando a cabo con otras organizaciones de normalización y otros foros en materia de gestión de identidades, y contribuye a evitar la duplicación de esfuerzos.

Además, dentro del sitio web de la Comisión de Estudio 17, hay una página dedicada a sus labores en cuanto que Comisión de Estudio Rectora sobre gestión de identidad con enlaces directos a los recursos más importantes.

### 3.3.3 Comisión de Estudio Rectora sobre lenguajes y técnicas de descripción

La Comisión de Estudio 17 fue nombrada la Comisión de Estudio Rectora sobre lenguajes y técnicas de descripción en virtud de la Resolución 2 de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT-12).

En su condición de Comisión de Estudio Rectora sobre lenguajes y técnicas de descripción, la Comisión de Estudio 17 tiene las siguientes responsabilidades con respecto a los lenguajes y técnicas de descripción para las telecomunicaciones:

– Orientar a los miembros del UIT-T y a otras Comisiones de Estudio en materia de utilización de lenguajes y técnicas de descripción.

– Mantener las Recomendaciones UIT-T y otras directrices dedicadas a los lenguajes y las técnicas de descripción utilizados en telecomunicaciones.

– Identificar los lenguajes externos disponibles que pueden emplearse cuando ninguna Recomendación UIT-T define un lenguaje adecuado.

– Interactuar con otros organismos reconocidos, como IETF y OMG, que utilizan o definen lenguajes y técnicas de descripción complementarios.

Las Cuestiones 11/17 y 12/17 y el Grupo de Trabajo 5/17 han trabajado sobre lenguajes y técnicas de descripción para ASN.1, ODP, SDL, MSC, URN y TTCN. Gracias a una intensa colaboración con otras organizaciones y Comisiones de Estudio se han podido avanzar los trabajos.

La Cuestión 11/17 trabaja de consuno con el JTC 1/SC 6/WG 10 de la ISO/CEI sobre la notación de sintaxis abstracta uno (ASN.1), y sus trabajos se publican como textos comunes en las series X.680/X.690/X.890. Todas las Recomendaciones sobre ASN.1 de las series X.680/X.690 fueron objeto de revisión en 2015.

La Cuestión 11/17 también colabora con el JTC 1/SC 7/WG 19 de la ISO/CEI en la elaboración de textos comunes sobre procesamiento distribuido abierto (ODP). Las Recomendaciones X.906 (UML para ODP) y X.911 (Lenguaje de empresa) fueron objeto de revisión.

Los Relatores para la Cuestión 12/17 han organizado y participado en talleres para lograr una mayor participación de la industria y las instituciones académicas en la elaboración de las Recomendaciones y otras herramientas de apoyo sobre lenguajes. Durante el periodo de estudios considerado se celebraron los siguientes talleres:

– 16º Foro Internacional de Lenguajes de Diseño de Sistemas, ingeniería de sistemas fiables guiada por modelos, 26-28 de junio de 2013, Montreal (Canadá).

– 8ª Conferencia sobre Análisis y Modelización de Sistemas (SAM-2014), dentro de MODELS-2014, 29-30 de septiembre de 2014, Valencia (España).

– 17º Foro Internacional de Lenguajes de Diseño de Sistemas, 12-14 de octubre de 2015, Berlín (Alemania).

La UIT colabora en la organización de estos eventos, con la aprobación de la CE 17, y participa en la publicidad. Los miembros de la sociedad participan en la revisión que realiza la C12/17 de la serie Z.100 sobre el lenguaje de normalización y descripción (SDL‑2010).

La Cuestión 12/17 está estrechamente relacionada con ETSI TC MTS y junto con él mantiene las Recomendaciones de las series Z.160 y Z.170 sobre TTCN‑3. Se han aprobado seis textos nuevos y 24 textos revisados.

Además, en el sitio web de la Comisión de Estudio 17 puede encontrarse la página de la Comisión de Estudio Rectora sobre lenguajes y técnicas de descripción, donde se hace un repaso de todos y cada uno de los lenguajes.

Las Comisiones de Estudio del UIT-T (distintas de la CE17) lograron los siguientes resultados en el marco de sus actividades relacionadas con las Recomendaciones sobre lenguaje:

Recomendaciones aprobadas

| CE | Recomendación | Título |
| --- | --- | --- |
| CE13 | Y.3320 | Requisitos para la aplicación de métodos formales a redes definidas por software |

### 3.3.4 GSI y JCA

La CE 17 no ha tenido bajo su responsabilidad ninguna Iniciativa Mundial de Normalización (GSI) durante este periodo de estudios. Dos Actividades Mixtas de Coordinación (JCA), dependientes de la CE 17, ponen de manifiesto el papel de Comisión de Estudio Rectora que se le ha otorgado.

#### 3.3.4.1 JCA-IdM

La Actividad Mixta de Coordinación sobre la gestión de la identidad (JCA-IdM) del anterior periodo de estudios ha proseguido sus trabajos durante este periodo de estudios, de acuerdo con la propuesta que aprobó el GANT. El objetivo de la JCA-IdM es garantizar el progreso coordinado de todas las actividades sobre IdM que realizan las Comisiones de Estudio del UIT-T (en particular, las CE 2, 13, 17 y 20) y actuar como punto de contacto en el seno del UIT-T y con otros organismos de normalización, consorcios y foros en materia de IdM, con el fin de evitar la duplicación del trabajo y facilitar tanto la ejecución de las tareas relacionadas con la IdM que figuran en la Resolución 2 de la AMNT-12, como la aplicación de la Resolución 4 de la GSC-16 sobre gestión de identidades. La JCA-IdM acordó reorientar sus trabajos, por ejemplo, para ahondar en los obstáculos a la normalización de la IdM, y sacar un mayor provecho de la colaboración.

Representantes de las Comisiones de Estudio 13 y 17, así como de los organismos externos más importantes, participaron en las nueve reuniones de la JCA-IdM, durante las cuales se manejaron 42 documentos y se llevó a cabo una significativa coordinación entre las comisiones de estudio y varios organismos de normalización externos. En general, las reuniones de la JCA-IdM gozaron de un elevado nivel de participación y fueron bastante fructíferas. Entre los organismos de normalización que participaron en las reuniones de la JCA-IdM se cuentan el JTC 1/SC 27/WG 5 de la ISO/CEI, ETSI/ISG, ENISA, OASIS/IdCloud TC, OASIS/Trust Elevation TC, OASIS IBOPS, OpenID Foundation, FIDO Alliance, OASIS TC IBOPS, Kantara Initiative, American Bar Association, GLEIF, STORK 2.0 project y la UPU.

La CE 17 aprobó la calificación de la Fundación OpenID de conformidad con las Recomendaciones UIT-T A.4 y A.5.

En la página web de la CE 17 se ha incluido un WIKI con el Plan IdM, donde se recopilan todas las normas sobre IdM vigentes y en proceso de elaboración en todo el mundo. Este Plan es reflejo de la coordinación que se está llevando a cabo con otras organizaciones de normalización y otros foros en materia de gestión de identidades, y contribuye a evitar la duplicación de esfuerzos.

#### 3.3.4.2 JCA-PIEL

El objetivo de la JCA‑PIEL es coordinar los trabajos sobre protección de la infancia en línea (PIEL) que llevan a cabo las Comisiones de Estudio del UIT-T y establecer una coordinación con el UIT-R, el UIT-D y el Grupo de Trabajo del Consejo sobre protección de la infancia en línea. La JCA-PIEL reúne a distintas partes interesadas con miras a determinar actividades y mejores prácticas, identificar lagunas y concebir un plan de trabajo encaminado a la elaboración de normas sobre COP.

Durante el periodo de estudios considerado, la JCA-COP celebró ocho reuniones (seis de ellas presenciales y en paralelo a las reuniones de la CE 17, y dos virtuales). Todas las reuniones de la JCA-COP fueron muy concurridas.

Se recibieron contribuciones del JTC 1/SC 27/WG 5 de la ISO/CEI, IETF/ISOC, la C3/2 del UIT-D, DeafKidzInternational, ECPAT, EFC, FCACP, FOSI, GSMA, ICMEC, I-KiZ, e Irán (República Islámica del).

Se recibieron declaraciones de coordinación de la C22-1/1 de la CE 1 del UIT-D, diversos grupos temáticos del UIT-T (SSC, DR&NRR), diversas actividades mixtas de coordinación del UIT-T (AHF, SG&HN), diversas Comisiones de Estudio del UIT-T (2, 3, 9, 16, 17 y 20), el RevCom del UIT-T, e informes periódicos del GTC-PIEL de la UIT.

Se enviaron declaraciones de coordinación al FG-SSC del UIT-T, la JCA-AHF del UIT-T y la C22-1/1 del UIT-D.

### 3.3.5 Grupo Regional para África de la Comisión de Estudio 17 (GR CE17-AFR)

En su reunión de abril de 2015, la CE 17 creó el Grupo Regional para África. El Sr. Michael KATUNDU (Kenya) es el presidente de este Grupo, y los Sres. Mohamed ELHAJ (Sudán), Patrick MWESIGWA (Uganda) y Mohamed TOURÉ (Guinea) son sus Vicepresidentes. El Grupo Regional para África de la Comisión de Estudio 17 se reunió en un ocasión en Abidjan (Côte d’Ivoire), los días 21 y 22 de enero de 2016. En dicha reunión se identificaron temas actuales que revestían un interés particular para África, y se evocaron diversas ideas en relación con la estructura del grupo regional, incluidas propuestas de temas para coordinadores. Además, se analizaron tres contribuciones recibidas y se elaboraron dos contribuciones salientes para su consideración en la reunión de marzo de 2016 de la CE 17.

## 3.4 Proyectos

Los proyectos ASN.1 y OID de la CE 17 siguen prestando asistencia:

• A los actuales usuarios de ASN.1 y de los identificadores de objeto (OID) dentro y fuera del UIT-T (por ejemplo, la CE 16 del UIT-T, el JTC 1/SC 27 de la ISO/CEI, el TC 215 de la ISO, el 3GPP, etc.).

• A los países, y en particular los países en desarrollo, en la creación de una autoridad nacional de registro de OID.

Estos proyectos facilitan oradores y material didáctico y coordinan el suministro de herramientas de apoyo a los usuarios y de contenidos de los sitios web conexos.

### 3.4.1 Proyecto ASN.1

El proyecto ASN.1, bajo la dirección del Sr. Paul Thorpe, proporciona asistencia a los usuarios de ASN.1 (Rec. UIT-T de las series X.680, X.690 y X.890) dentro y fuera del UIT-T (por ejemplo, la CE 16 del UIT-T, el JTC 1/SC 27 de la ISO/CEI, el TC 215 de la ISO, el ETSI LI, el 3GPP, etc.). También ayuda a la TSB a mantener actualizada una base de datos de módulos ASN.1 sin errores. La base de datos de módulos ASN.1 sigue alimentándose, lo que permite a los implementadores obtener especificaciones ASN.1 publicadas, de lectura automática y con la sintaxis verificada. Esta base de datos contiene los módulos de más de 200 Recomendaciones UIT-T, así como de otros organismos de normalización a los que se hace referencia en las mismas.

En cooperación con la TSB, se ha creado una base de datos que contiene una copia procesable por computador de la versión actual de todos los módulos ASN.1 incluidos en las Recomendaciones UIT-T. El acceso en línea a esta base de datos de módulos ASN.1 aporta un gran valor añadido al UIT-T en comparación con otras organizaciones de normalización y mejora la eficiencia en la industria, ya que permite ahorrar tiempo y dinero. Para aplicar las Recomendaciones UIT-T conexas se requiere un formato electrónico (con codificación ASCII) que permita procesar directamente las definiciones oficiales mediante las herramientas existentes. Si el código ASCII se obtiene en papel o en formato post-script, se habrá de volver a escribir, lo que ralentiza su utilización y puede causar errores. El hecho de disponer de todos los módulos ASN.1 en un mismo lugar facilita sobremanera la implementación de los correspondientes protocolos. Además, la base de datos de ASN.1 contiene también módulos seleccionados de otros organismos de normalización.

### 3.4.2 Proyecto OID

Los OID son un mecanismo universal para hacer referencia sin ambigüedad a los objetos utilizados o definidos en normas. Las labores de la Cuestión 11/17 sobre el registro jerárquico de identificadores de objetos (OID) del UIT-T (Recomendaciones UIT-T de las series X.660 y X.670) prosiguieron con diligencia en colaboración con el JTC 1/SC 6 de la ISO/CEI.

El árbol de OID internacional cuenta con más de 954 046 registros inscritos en el repositorio de OID (<http://www.oid-info.com>), y permite la identificación de objetos (de cualquier tipo) a través de un esquema de asignación jerárquica que se halla bajo el control del UIT-T y la ISO/CEI. Los OID también permiten la identificación de los objetos mediante el uso de cualquier idioma del mundo (de forma estructurada y jerárquica).

El Proyecto OID, bajo la dirección del Sr. Olivier Dubuisson, sirve de ayuda a las administraciones nacionales y a los órganos nacionales de la ISO/CEI para establecer una autoridad de registro para su OID nacional. Entre los países beneficiarios del proyecto figuran Argelia, Andorra, Argentina, Bangladesh, Bolivia, Bosnia y Herzegovina, Brasil, Canadá, Honduras, Irán, Lituania, Malasia, Mongolia, Nicaragua, Omán, Filipinas, Rwanda, Sri Lanka, Túnez, Ucrania y Uruguay.

## 3.5 Otras actividades

### 3.5.1 Reducción de la brecha en materia de normalización

Desde septiembre de 2013, la CE 17 organiza periódicamente una sesión sobre reducción de la brecha en materia de normalización en el marco de sus reuniones. Estas sesiones han permitido compilar un amplio acervo de información sobre los programas, actividades y proyectos que ha emprendido la UIT en esta esfera, y han constituido un medio excelente para que los países en desarrollo pudiesen transmitir sus sugerencias a la CE 17. Estas sesiones también han inducido a los países en desarrollo a expresar sus intereses y necesidades.

### 3.5.2 Memorando de Entendimiento sobre el negocio electrónico

La Comisión Electrotécnica Internacional (CEI), la Organización Internacional de Normalización (ISO), el UIT-T y la Comisión Económica de las Naciones Unidas para Europa (UN/ECE) firmaron un Memorando de Entendimiento sobre el negocio electrónico. También participan en la aplicación de este Memorando asociaciones internacionales de usuarios, foros y consorcios. La finalidad del Memorando es minimizar la posibilidad de adoptar enfoques de normalización divergentes y rivales, evitar la duplicación de tareas e impedir que se cause confusión a los usuarios.

El grupo de gestión del Memorando de Entendimiento ha mejorado la coordinación y el intercambio de información acerca de las actividades de la Comisión de Estudio 17 en los ámbitos de la seguridad, la telebiometría, la gestión de identidades, las redes de sensores ubicuas (USN), ASN.1 y los identificadores de objeto (OIDs), así como de las tareas conexas de otras Comisiones de Estudio.

### 3.5.3 Grupo Asesor Estratégico del UIT-T/ISO/CEI/ sobre seguridad (SAG-S)

El SAG-S era un grupo subordinado al Consejo de Administración Técnica de la ISO, que fue objeto de construcción. La CE 17 del UIT-T, en su calidad de Comisión de Estudio Rectora sobre seguridad, participó en las reuniones virtuales que el SAG-S celebró a lo largo del año 2013 y aportó materiales relativos a las recomendaciones UIT-T sobre seguridad y a otros proyectos de textos en la materia, según se refleja en su inventario de normas relacionadas con la seguridad (*Threat Collection*). El nuevo SAG-S se centró en la ISO y, desafortunadamente, no se encargó de coordinar las labores de la ISO, la CEI y el ITU-T, como hacía anteriormente. El Consejo de Administración Técnica de la ISO puso término al SAG-S en 2014.

# 4 Observaciones en relación con el trabajo futuro

La Comisión de Estudio 17 prosiguió sus trabajos sobre seguridad, que experimentaron un extraordinario crecimiento a lo largo del periodo de estudios y se tradujeron en la creación de un Centro de Excelencia especializado en temas de seguridad. La Comisión de Estudio 17 es la Comisión de Estudio Rectora sobre seguridad del Sector de Normalización. Los trabajos de la CE 17 prosiguieron a lo largo de este período de estudios. Además, se ha creado una base sólida de Recomendaciones relativas a la seguridad, se ha llegado a acuerdos de colaboración con otros organismos y, en la Parte II del Informe de la Comisión de Estudio 17, se ha propuesto la continuación de un programa de trabajo sobre Cuestiones relacionadas con la seguridad. Dado que la creación de confianza y seguridad en el uso de las tecnologías de la información y la comunicación (TIC) es una de las mayores prioridades de la UIT, es esencial que esta competencia de seguridad del UIT-T se consolide y mejore, y que no se vea fragmentada.

La distinción entre las redes de telecomunicaciones y las aplicaciones y redes de información sigue desdibujándose. Por consiguiente, es necesario proseguir la labor realizada por la Comisión de Estudio 17 con respecto a la seguridad (en particular, la arquitectura genérica de la seguridad, el marco, los mecanismos y las directrices de gestión para redes/sistemas/servicios heterogéneos) y se ha de designar una Comisión de Estudio Rectora sobre seguridad que se encargue de coordinar dicha labor en la UIT y con otras organizaciones de normalización. La Comisión de Estudio 17 también prevé la creciente necesidad de elaborar directrices en materia de seguridad que satisfagan las necesidades de todos los países.

El fortalecimiento del marco de confianza, autenticación y protección de la información de identificación personal es un requisito previo para el desarrollo de la Sociedad de la Información y el fomento de la confianza entre los usuarios de las TIC. La seguridad de y para las telecomunicaciones y las tecnologías de la información y la comunicación (seguridad de las TIC) sigue siendo una esfera en la que se necesitarán normas de seguridad. Las nuevas tecnologías emergentes –entre ellas, la computación en nube, las redes eléctricas inteligentes, los sistemas de transporte inteligente, la 5ª generación de redes celulares, las redes definidas por software, el análisis de macrodatos y la Internet de las Cosas– requieren medidas técnicas para proteger la información de identificación personal de los particulares, así como medidas técnicas para proteger a la infancia en línea. Además, podrían necesitarse nuevos enfoques en la materia, que solucionen adecuadamente las amenazas a la seguridad. A la Comisión de Estudio 17 le aguarda un papel crucial en la elaboración de recomendaciones internacionales a ese respecto. La Comisión de Estudio que posee experiencia con los enfoques de seguridad vigentes puede abordar con mayor desenvoltura la imperiosa necesidad de crear nuevos enfoques de seguridad que puedan aplicarse a unas tecnologías en constante evolución.

A través de las actividades que realiza en calidad de Comisión de Estudio Rectora sobre seguridad y como resultado de su labor en el ámbito de la coordinación, la CE 17 se mantiene informada sobre los trabajos en materia de seguridad de otras comisiones de estudio, así como de la labor de otros organismos de normalización y consorcios. Se ha previsto que las actividades de enlace y coordinación de la CE 17 seguirán siendo importantes en el futuro. La CE 17 cuenta con una excelente trayectoria de colaboración con otras organizaciones de normalización, con las que ha elaborado conjuntamente Recomendaciones y/o normas. La CE 17, en su condición de Comisión de Estudio Rectora y con el fin de brindar un mayor apoyo a sus actividades normativas en el ámbito de la seguridad, suele hacer un buen uso de los mecanismos de coordinación (correspondencia, Declaraciones de Coordinación A.4/A.5/A.6 formales), así como de los de referencia y desarrollo conjunto (A.23/A.25).

La CE 17 también es la Comisión de Estudio Rectora sobre gestión de identidad (IdM) y actúa como fuerza catalizadora mundial para la gestión de identidades digitales, la creación de confianza, la protección de la información de identificación personal, la explotación de las redes que cuentan con control de acceso a la red o a los servicios, la realización de transacciones electrónicas en línea, la prestación de servicios financieros digitales, etc. Dada la importante función que desempeña en la creación de confianza y seguridad en la utilización de las TIC, la gestión de identidades forma parte integrante de las actividades de la CE 17 en cuanto que Comisión de Estudio Rectora del UIT-T sobre seguridad. La CE 17 sigue coordinando la gestión de identidades en el seno de la UIT y en el marco de la colaboración con otras organizaciones de normalización. Sus trabajos en materia de PKI, ASN.1, y OID han resultado de utilidad en varios sectores de las TIC.

En aras de la seguridad, será preciso definir nuevas normas. La UIT es consciente desde hace mucho tiempo de que las plataformas de expresión estructurada (véase la notación de sintaxis abstracta uno o ASN.1) son importantes. En el caso de la ASN.1, uno de los logros principales ha sido garantizar que la ASN.1 incluida en las Recomendaciones UIT-T se armonizase con la definición de ASN.1, y facilitar el código en ficheros que puedan leer las máquinas. La ampliación de este enfoque (y de los recursos de apoyo de la UIT) a otros lenguajes de especificación, tales como el lenguaje de especificación y descripción (SDL), permitirá aumentar la seguridad inherente en Recomendaciones de buena calidad. Los productos pueden beneficiarse de la utilización de estas recomendaciones. Además de los lenguajes formales para la redacción de Recomendaciones, la UIT ha creado también la notación de pruebas y control de pruebas (TTCN) para diseñar pruebas de conformidad y de otro tipo.

Los nuevos entornos, véase la Internet de las Cosas (IoT), y la seguridad de las redes eléctricas inteligentes imponen requisitos a las PKI que no figuran aún en la Rec. UIT-T X.509 en vigor. La actual PKI estaba pensada originalmente para garantizar la seguridad en los sectores bancario y del cibergobierno, y no estaba diseñada para hacer frente a entornos con entidades de baja capacidad y/o con millones o miles de millones de entidades sin interacción humana. Si no se mejora la PKI con el fin de adaptarla a estos nuevos entornos, los aspectos principales de la IoT y la seguridad de las redes eléctricas inteligentes fallarán, lo cual repercutirá ampliamente en la sociedad ya que incidirá en la estabilidad de gran parte de las infraestructuras esenciales. Durante el próximo período de estudios, cabría otorgar prioridad a los trabajados relativos a la mejora de la PKI con miras a su adaptación a estos nuevos entornos.

# 5 Actualizaciones de la Resolución 2 de la AMNT para el periodo de estudios 2017-2020

En el Anexo 2 figuran las actualizaciones de la Resolución 2 de la AMNT propuestas por la Comisión de Estudio 17 con respecto a las áreas de estudio, el título, el mandato, los cometidos como Comisión de Estudio Rectora y los puntos de orientación en el próximo periodo de estudios.

ANEXO 1

Lista de Recomendaciones, Suplementos y otros documentos   
producidos o suprimidos durante el periodo de estudios

En el Cuadro 7 figura la lista de las Recomendaciones nuevas y revisadas aprobadas durante el periodo de estudios.

En el Cuadro 7 figura la lista de **Recomendaciones, Enmiendas y Corrigenda** aprobados durante el periodo de estudios considerado **hasta a la fecha** en que se preparó el cuadro. Los textos aparecen en orden (alfanumérico) de Recomendación y luego por fecha de aprobación (comenzando por la más antigua). Las Recomendaciones con numeración doble aparecerán una sola vez. Toda Recomendación en la que participaron otras Comisiones de Estudio sólo aparece para la Comisión de Estudio que la aprobó.

En el Cuadro 8 figura la lista de Recomendaciones determinadas/consentidas durante la última reunión de la Comisión de Estudio 17.

Los textos están ordenados por Recomendación (alfanuméricamente). Las Recomendaciones con doble signatura sólo aparecen una vez. Las Recomendaciones tratadas por más de una Comisión de Estudio sólo aparecen junto a la Comisión que la aprobó.

NOTA – La última reunión a que se hace referencia en este Informe se celebró el 23 de marzo de 2016. Se añadirá al presente Informe un Addéndum con la información dimanante de la última reunión de la CE17, que se celebrará del 29 de agosto al 7 de septiembre de 2016.

En el Cuadro 9 figura la lista de Recomendaciones suprimidas por la Comisión de Estudio 17 durante el periodo de estudio. Los textos están ordenados por Recomendación (alfanuméricamente). Las Recomendaciones con doble signatura sólo aparecen una vez.

En el Cuadro 10 figura la lista de las Recomendaciones sometidas por la Comisión de Estudio 17 a la AMNT-16 para aprobación.

En los Cuadros 11 y siguientes figura la lista de otras publicaciones aprobadas y/o suprimidas por la Comisión de Estudio 17 durante el periodo de estudios.

En el cuadro 11 se enumeran los Suplementos acordados durante el presente periodo de estudios **hasta la fecha** en que se preparó el cuadro.

CUADRO 7

Comisión de Estudio 17 – Recomendaciones aprobadas durante el periodo de estudios

| Recomendación | Aprobación | N/R | Situación | TAP/AAP | Título |
| --- | --- | --- | --- | --- | --- |
| F.511 | 2014-04-06 | Nueva | En vigor | AAP | Servicio de directorio - Servicios de identificación por etiquetas |
| X.226 Cor.1 | 2015-07-14 |  | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – Protocolo de presentación con conexión: Especificación del protocolo – Corrigéndum técnico 1 |
| X.227*bis* Cor.1 | 2015-07-16 |  | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – Protocolo en modo con conexión del elemento de servicio de control de asociación para objetos de servicio de aplicación – Corrigéndum técnico 1 |
| X.509 (2012) Cor.1 | 2015-05-28 |  | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos – Corrigéndum técnico 1 |
| X.509 (2012) Cor.2 | 2016-04-29 |  | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos – Corrigéndum técnico 2 |
| X.520 (2012) Cor.1 | 2014-11-13 |  | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Tipos de atributos seleccionados – Corrigéndum técnico 1 |
| X.667 | 2012-10-14 | Revisada | En vigor | AAP | Tecnología de la información - Procedimientos para el funcionamiento de las autoridades de registro de los identificadores de objeto: Generación of identificadores únicos universales y su utilización como componentes de identificador de objetos |
| X.675 | 2015-06-15 | Nueva | En vigor | AAP | Marco de resolución basado en OID para identificadores y localizadores heterogéneos |
| X.680 | 2015-08-13 | Revisada | En vigor | AAP | Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica |
| X.680 (2008) Cor.2 | 2014-03-01 |  | Suprimida | AAP | Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica – Corrigéndum técnico 2 |
| X.681 | 2015-08-13 | Revisada | En vigor | AAP | Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de objetos de información |
| X.682 | 2015-08-13 | Revisada | En vigor | AAP | Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de constricciones |
| X.682 (2008) Cor.1 | 2014-03-01 |  | Suprimida | AAP | Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de constricciones – Corrigéndum técnico 1 |
| X.683 | 2015-08-13 | Revisada | En vigor | AAP | Tecnología de la información – Notación de sintaxis abstracta uno: Parametrización de especificaciones de notación de sintaxis abstracta uno |
| X.683 (2008) Cor.1 | 2014-03-01 |  | Suprimida | AAP | Tecnología de la información – Notación de sintaxis abstracta uno: Parametrización de especificaciones de notación de sintaxis abstracta uno – Corrigéndum técnico 1 |
| X.690 | 2015-08-13 | Revisada | En vigor | AAP | Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación básica, de las reglas de codificación canónica y de las reglas de codificación distinguida |
| X.690 (2008) Cor.2 | 2014-03-01 |  | Suprimida | AAP | Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación básica, de las reglas de codificación canónica y de las reglas de codificación distinguida – Corrigéndum técnico 2 |
| X.691 | 2015-08-13 | Revisada | En vigor | AAP | Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación compactada |
| X.691 (2008) Cor.3 | 2014-11-13 |  | Suprimida | AAP | Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación compactada – Corrigéndum técnico 3 |
| X.691 (2008) Cor.4 | 2014-11-13 |  | Suprimida | AAP | Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación compactada – Corrigéndum técnico 4 |
| X.692 | 2015-08-13 | Revisada | En vigor | AAP | Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de la notación de control de codificación |
| X.693 | 2015-08-13 | Revisada | En vigor | AAP | Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Reglas de codificación del lenguaje de marcaje extensible |
| X.693 (2008) Cor.2 | 2014-03-01 |  | Suprimida | AAP | Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Reglas de codificación del lenguaje de marcaje extensible – Corrigéndum técnico 2 |
| X.694 | 2015-08-13 | Revisada | En vigor | AAP | Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Correspondencia en notación de sintaxis abstracta uno de las definiciones W3C de los esquemas de lenguaje de marcaje extensible |
| X.694 (2008) Cor.2 | 2014-03-01 |  | Suprimida | AAP | Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Correspondencia en notación de sintaxis abstracta uno de las definiciones W3C de los esquemas de lenguaje de marcaje extensible – Corrigéndum técnico 2 |
| X.695 | 2015-08-13 | Revisada | En vigor | AAP | Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Registro y aplicación de instrucciones de codificación de las reglas de codificación paquetizada |
| X.696 | 2014-08-29 | Nueva | Suprimida | AAP | Tecnología de la información - Especificación de reglas de codificación de octetos (OER) |
| X.696 | 2015-08-13 | Revisada | En vigor | AAP | Tecnología de la información - Especificación de reglas de codificación de octetos (OER) |
| X.906 | 2014-10-07 | Revisada | En vigor | AAP | Tecnología de la información – Procesamiento distribuido abierto – Utilización del lenguaje de modelado unificado para la especificación de sistemas de procesamiento distribuido abierto |
| X.911 | 2014-09-13 | Revisada | En vigor | AAP | Tecnología de la información – Procesamiento distribuido abierto – Modelo de referencia – Lenguaje de empresa |
| X.1033 | 2016-04-29 | Nueva | En vigor | AAP | Directrices relativas a la seguridad de los servicios de información prestados por los operadores |
| X.1037 | 2013-10-07 | Nueva | En vigor | AAP | Directrices técnicas de seguridad para la implantación de IPv6 |
| X.1051 | 2016-04-29 | Revisada | En vigor | AAP | Tecnología de la información - Técnicas de seguridad - Código de prácticas en materia de controles de seguridad de la información basados en la norma ISO/CEI 27002 para organizaciones de telecomunicaciones |
| X.1092 | 2013-06-13 | Nueva | En vigor | AAP | Marco integrado para la protección de datos telebiométricos en cibersalud y telemedicina |
| X.1144 | 2013-10-14 | Nueva | En vigor | AAP | Lenguaje de marcaje de control de acceso extensible (XACML) 3.0 |
| X.1154 | 2013-04-26 | Nueva | En vigor | TAP | Marco general para la autentificación combinada en entornos con múltiples proveedores de servicio de identidad |
| X.1155 | 2015-10-29 | Nueva | En vigor | AAP | Directrices sobre autenticación anónima enlazable local para servicios electrónicos |
| X.1156 | 2013-06-13 | Nueva | En vigor | AAP | Marco de no repudio basado en una contraseña de uso único |
| X.1157 | 2015-09-17 | Nueva | En vigor | TAP | Capacidades técnicas de detección y respuesta al fraude para servicios con requisitos de alto nivel de seguridad |
| X.1158 | 2014-11-13 | Nueva | En vigor | AAP | Mecanismo de autentificación multifactorial utilizando un dispositivo móvil |
| X.1159 | 2014-11-13 | Nueva | En vigor | AAP | Arquitectura de no repudio delegada, basada en la Recomendación UIT-T X.813 |
| X.1163 | 2014-05-28 | Nueva | En vigor | AAP | Requisitos y mecanismos de seguridad para redes de telecomunicaciones entre pares |
| X.1198 | 2013-06-13 | Nueva | En vigor | AAP | Plataforma virtual de seguridad basada en la máquina para el servicio de TVIP renovable y la protección de contenidos |
| X.1208 | 2014-01-24 | Nueva | En vigor | TAP | Un indicador de riesgo de ciberseguridad para mejorar la confianza y la seguridad en la utilización de las tecnologías de la información y la comunicación |
| X.1210 | 2014-01-24 | Nueva | En vigor | TAP | Aspectos generales de los mecanismos de detección del origen de los problemas de seguridad en las redes de protocolo Internet |
| X.1211 | 2014-09-26 | Nueva | En vigor | TAP | Técnicas para prevenir ataques en la web |
| X.1243 (2010) Cor.1 | 2014-01-24 |  | En vigor | TAP | Sistema de pasarela interactivo para la lucha contra el correo basura: Corrigéndum 1 |
| X.1246 | 2015-09-17 | Nueva | En vigor | TAP | Tecnologías implicadas en la lucha contra el spam de voz en las organizaciones de telecomunicaciones |
| X.1247 | 2016-03-23 | Nueva | En vigor | TAP | Marco técnico para luchar contra el correo basura en la mensajería móvil |
| X.1255 | 2013-09-04 | Nueva | En vigor | TAP | Marco para la indagación de información de gestión de identidades |
| X.1256 | 2016-03-23 | Nueva | En vigor | TAP | Directrices y marco para la compartición de los resultados de la autentificación de la red con las aplicaciones de los servicios |
| X.1257 | 2016-03-23 | Nueva | En vigor | TAP | Taxonomía de la gestión del acceso y de la identidad |
| X.1303 *bis* | 2014-03-01 | Nueva | En vigor | AAP | Protocolo de alerta común (CAP 1.2) |
| X.1311 (2011) Cor.1 | 2014-11-29 |  | En vigor | AAP | Tecnología de la información – Marco de seguridad para red de sensores ubicuos - Corrigéndum técnico 1 |
| X.1314 | 2014-11-13 | Nueva | En vigor | AAP | Requisitos y marco de seguridad de las redes ubicuas |
| X.1314 Cor.1 | 2015-10-29 |  | En vigor | AAP | Requisitos y marco de seguridad de las redes ubicuas - Corrigéndum 1 |
| X.1341 | 2015-09-17 | Nueva | En vigor | TAP | Protocolos de transferencia de correo certificado y de oficina postal certificada |
| X.1500 Enm.3 | 2013-04-26 | Nueva | Suprimida | Acuerdo | Aspectos generales del intercambio de información de ciberseguridad – Enmienda 3 - Técnicas revisadas de intercambio de información estructurada sobre ciberseguridad |
| X.1500 Enm.4 | 2013-09-04 | Nueva | Suprimida | Acuerdo | Aspectos generales del intercambio de información de ciberseguridad – Enmienda 4 - Técnicas revisadas de intercambio de información estructurada sobre ciberseguridad |
| X.1500 Enm.5 | 2014-01-24 | Nueva | Suprimida | Acuerdo | Aspectos generales del intercambio de información de ciberseguridad – Enmienda 5 - Técnicas revisadas de intercambio de información estructurada sobre ciberseguridad |
| X.1500 Enm.6 | 2014-09-26 | Nueva | Suprimida | Acuerdo | Aspectos generales del intercambio de información de ciberseguridad – Enmienda 6 - Técnicas revisadas de intercambio de información estructurada sobre ciberseguridad |
| X.1500 Enm.7 | 2015-04-17 | Nueva | Suprimida | Acuerdo | Aspectos generales del intercambio de información de ciberseguridad – Enmienda 7 - Técnicas revisadas de intercambio de información estructurada sobre ciberseguridad |
| X.1500 Enm.8 | 2015-09-17 | Nueva | En vigor | Acuerdo | Aspectos generales del intercambio de información de ciberseguridad – Enmienda 8 - Técnicas revisadas de intercambio de información estructurada sobre ciberseguridad |
| X.1500 Enm.9 | 2016-03-23 | Nueva | En vigor | Acuerdo | Aspectos generales del intercambio de información de ciberseguridad – Enmienda 9 - Técnicas revisadas de intercambio de información estructurada sobre ciberseguridad |
| X.1520 | 2014-01-24 | Revisada | En vigor | TAP | Vulnerabilidades y exposiciones comunes |
| X.1521 | 2016-03-23 | Revisada | En vigor | TAP | Sistema común de puntuación de vulnerabilidades 3.0 |
| X.1525 | 2015-04-17 | Nueva | En vigor | TAP | Sistema común de puntuación de puntos débiles |
| X.1526 | 2013-04-26 | Nueva | Suprimida | TAP | Lenguaje abierto de vulnerabilidades y evaluación |
| X.1526 | 2014-01-24 | Revisada | En vigor | TAP | Lenguaje para la definición abierta de vulnerabilidades y la evaluación del estado del sistema |
| X.1544 | 2013-04-26 | Nueva | En vigor | TAP | Enumeración y clasificación de pautas de ataques comunes |
| X.1546 | 2014-01-24 | Nueva | En vigor | TAP | Enumeración y caracterización de atributos de malware |
| X.1582 | 2014-01-24 | Nueva | En vigor | TAP | Protocolos de transporte para el intercambio de información de ciberseguridad |
| X.1601 | 2014-01-24 | Nueva | Suprimida | TAP | Marco de seguridad para la computación en la nube |
| X.1601 | 2015-10-29 | Revisada | En vigor | AAP | Marco de seguridad para la computación en la nube |
| X.1602 | 2016-03-23 | Nueva | En vigor | TAP | Requisitos de seguridad para los entornos de aplicación del software como servicio |
| X.1631 | 2015-07-15 | Nueva | En vigor | AAP | Tecnologías de la información – Técnicas de seguridad –Código de prácticas para controles de seguridad de la información basados en SO/IEC 27002 para los servicios en la nube |
| X.1642 | 2016-03-23 | Nueva | En vigor | TAP | Directrices para la seguridad operativa de la computación en la nube |
| Z.100 | 2016-04-29 | Revisada | En vigor | AAP | Lenguaje de especificación y descripción - Visión general de SDL-2010 |
| Z.100 Anexo F1 | 2015-01-13 | Revisada | En vigor | AAP | Lenguaje de especificación y descripción - Visión general de SDL-2010 - Anexo F1 - Definición formal del lenguaje de especificación y descripción: Visión general |
| Z.100 Anexo F2 | 2015-01-13 | Revisada | En vigor | AAP | Lenguaje de especificación y descripción - Visión general de SDL-2010 - Anexo F2 - Definición formal del lenguaje de especificación y descripción: Semántica estática |
| Z.100 Anexo F3 | 2015-01-13 | Revisada | En vigor | AAP | Lenguaje de especificación y descripción - Visión general de SDL-2010 - Anexo F3 - Definición formal del lenguaje de especificación y descripción: Semántica dinámica |
| Z.101 | 2016-04-29 | Revisada | En vigor | AAP | Lenguaje de especificación y descripción - SDL-2010 básica |
| Z.102 | 2016-04-29 | Revisada | En vigor | AAP | Lenguaje de especificación y descripción - SDL-2010 integral |
| Z.103 | 2016-04-29 | Revisada | En vigor | AAP | Lenguaje de especificación y descripción - Notación abreviada y anotación en SDL-2010 |
| Z.104 | 2016-04-29 | Revisada | En vigor | AAP | Lenguaje de especificación y descripción - Datos y lenguaje de acción en SDL-2010 |
| Z.105 | 2016-04-29 | Revisada | En vigor | AAP | Lenguaje de especificación y descripción - SDL-2010 combinado con módulos ASN.1 |
| Z.106 | 2016-04-29 | Revisada | En vigor | AAP | Lenguaje de especificación y descripción - Formato de intercambio común para SDL-2010 |
| Z.107 | 2016-04-29 | Revisada | En vigor | AAP | Lenguaje de especificación y descripción - Datos orientados a objetos en SDL-2010 |
| Z.109 | 2013-10-14 | Revisada | En vigor | AAP | Lenguaje de especificación y descripción - Perfil del lenguaje de modelado unificado para SDL-2010 |
| Z.111 | 2016-04-29 | Revisada | En vigor | AAP | Notaciones y directrices para la definición de lenguajes del UIT-T |
| Z.161 | 2013-07-14 | Revisada | Suprimida | AAP | Notación de pruebas y de control de pruebas versión 3: Lenguaje núcleo de TTCN-3 |
| Z.161 | 2014-11-13 | Revisada | Suprimida | AAP | Notación de pruebas y de control de pruebas versión 3: Lenguaje núcleo de TTCN-3 |
| Z.161 | 2015-10-29 | Revisada | En vigor | AAP | Notación de pruebas y de control de pruebas versión 3: Lenguaje núcleo de TTCN-3 |
| Z.161.1 | 2014-11-13 | Revisada | Suprimida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Soporte de interfaces con señales continuas |
| Z.161.1 | 2015-10-29 | Revisada | En vigor | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Soporte de interfaces con señales continuas |
| Z.161.2 | 2014-11-13 | Revisada | Suprimida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Apoyo para la configuración e implantación |
| Z.161.2 | 2013-07-14 | Nueva | Suprimida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Apoyo para la configuración e implantación |
| Z.161.2 | 2015-10-29 | Revisada | En vigor | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Apoyo para la configuración e implantación |
| Z.161.3 | 2013-07-14 | Nueva | Suprimida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Parametrización avanzada |
| Z.161.3 | 2014-11-13 | Revisada | Suprimida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Parametrización avanzada |
| Z.161.3 | 2015-10-29 | Revisada | En vigor | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Parametrización avanzada |
| Z.161.4 | 2013-07-14 | Nueva | Suprimida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Tipos de comportamiento |
| Z.161.4 | 2015-10-29 | Nueva | En vigor | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Tipos de comportamiento |
| Z.161.5 | 2014-11-13 | Nueva | Suprimida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Resultados y realización de pruebas en tiempo real |
| Z.161.5 | 2015-10-29 | Nueva | En vigor | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Resultados y realización de pruebas en tiempo real |
| Z.165 | 2013-07-14 | Revisada | Suprimida | AAP | Notación de pruebas y de control de pruebas versión 3: Interfaz de ejecución |
| Z.165 | 2014-11-13 | Revisada | Suprimida | AAP | Notación de pruebas y de control de pruebas versión 3: Interfaz de ejecución |
| Z.165 | 2015-10-29 | Revisada | En vigor | AAP | Notación de pruebas y de control de pruebas versión 3: Interfaz de ejecución |
| Z.165.1 | 2013-07-14 | Revisada | Suprimida | AAP | Notación de prueba y de control de prueba versión 3: Paquete de ampliación de la TTCN-3: Extended TRI |
| Z.165.1 | 2014-11-13 | Revisada | Suprimida | AAP | Notación de prueba y de control de prueba versión 3: Paquete de ampliación de la TTCN-3: Extended TRI |
| Z.165.1 | 2015-10-29 | Revisada | En vigor | AAP | Notación de prueba y de control de prueba versión 3: Paquete de ampliación de la TTCN-3: Extended TRI |
| Z.166 | 2013-07-14 | Revisada | Suprimida | AAP | Notación de pruebas y de control de pruebas versión 3: Interfaz de control |
| Z.166 | 2014-11-13 | Revisada | Suprimida | AAP | Notación de pruebas y de control de pruebas versión 3: Interfaz de control |
| Z.166 | 2015-10-29 | Revisada | En vigor | AAP | Notación de pruebas y de control de pruebas versión 3: Interfaz de control |
| Z.167 | 2013-07-14 | Revisada | En vigor | AAP | Notación de pruebas y de control de pruebas versión 3 (TTCN-3): Utilización de ASN.1 con TTCN-3 |
| Z.168 | 2013-07-14 | Revisada | Suprimida | AAP | Notación de pruebas y de control de pruebas versión 3: Correspondencia del lenguaje IDL con la notación TTCN-3 |
| Z.168 | 2015-10-29 | Revisada | En vigor | AAP | Notación de pruebas y de control de pruebas versión 3: Correspondencia del lenguaje IDL con la notación TTCN-3 |
| Z.169 | 2013-07-14 | Revisada | Suprimida | AAP | Notación de pruebas y control de pruebas versión 3 (TTCN-3): Utilización de esquemas XML con TTCN-3 |
| Z.169 | 2015-10-29 | Revisada | En vigor | AAP | Notación de pruebas y control de pruebas versión 3 (TTCN-3): Utilización de esquemas XML con TTCN-3 |
| Z.170 | 2013-07-14 | Revisada | En vigor | AAP | Notación de pruebas y de control de pruebas versión 3: Especificación de los comentarios de documentación TTCN-3 |

CUADRO 8

Comisión de Estudio 17 – Recomendaciones consentidas/determinadas durante la última reunión

| Recomendación | Consentimiento/Determinación | TAP/AAP | Título |
| --- | --- | --- | --- |
| X.1542 (X.simef) | 2016-03-23 | TAP | Formatos de intercambio de mensajes sobre información de sesión |
| X.1641 (X.CSCDataSec) | 2016-03-23 | TAP | Directrices para la seguridad de los datos de cliente de los servicios en la nube |
| X.1258 (X.eaaa) | 2016-03-23 | TAP | Autentificación de entidad mejorada sobre la base de atributos agregados |
| X.894 (X.cms) | 2016-03-23 | AAP | Tecnología de la información – Aplicaciones genéricas de la notación de sintaxis abstracta uno – Sintaxis de mensajes criptográficos |

CUADRO 9

Comisión de Estudio 17 – Recomendaciones suprimidas durante el periodo de estudios

| Recomendación | Última versión | Fecha de supresión | Título |
| --- | --- | --- | --- |
| Z.400 | 1993-03 | 24 de diciembre de 2015 | Estructura y formato de los manuales de calidad para soporte lógico de telecomunicación |
| Z.600 | 2000-11 | 24 de diciembre de 2015 | Arquitectura de entorno de procesamiento distribuido |
| Z.601 | 2007-02 | 24 de diciembre de 2015 | Arquitectura de datos de un sistema de software |

CUADRO 10

Comisión de Estudio 17 – Recomendaciones sometidas a la AMNT-16

| Recomendación | Propuesta | Título | Referencia |
| --- | --- | --- | --- |
| Ninguna |  |  |  |

CUADRO 11

Comisión de Estudio 17 – Suplementos

| Suplemento | Aprobación | Situación | Título |
| --- | --- | --- | --- |
| X.Suppl.10 (09/2011) (revisado) | 2014-01-24 | En vigor | UIT-T X.1205 – Suplemento sobre utilización del rastreo de red |
| X.Suppl.18 | 2013-04-26 | En vigor | UIT-T X.1205 – Suplemento sobre directrices para la detección y el control del tráfico anómalo en redes de telecomunicaciones basadas en IP |
| X.Suppl.19 | 2013-04-26 | En vigor | Series UIT-T X.1120 - Suplemento sobre aspectos de seguridad de los teléfonos inteligentes |
| X.Suppl.20 | 2013-04-26 | En vigor | UIT-T X.1205 – Suplemento sobre marcos para la negociación del intercambio de información de seguridad |
| X.Suppl.21 | 2014-01-24 | En vigor | UIT-T X.1143 – Suplemento sobre marcos de seguridad para los servicios de las aplicaciones web híbridas |
| X.Suppl.22 | 2014-01-24 | En vigor | UIT-T X.1144 – Suplemento sobre mejoras y nuevas características del lenguaje de marcaje de control de acceso extensible (XACML) 3.0 |
| X.Suppl.23 | 2014-09-26 | En vigor | UIT-T X.1037 – Suplemento sobre directrices de gestión de la seguridad para la implantación de IPv6 en las organizaciones de telecomunicaciones |
| X.Suppl.24 | 2014-09-26 | En vigor | Series UIT-T X.1120-X.1139 – Suplemento sobre marcos seguros de distribución de aplicaciones para dispositivos de comunicación |
| X.Suppl.25 | 2616-03-23 | En vigor | UIT-T X.1231 –Suplemento sobre pautas para ayudar a los desarrolladores de teléfonos móviles a luchar contra el correo basura |
| X.Suppl.26 | 2616-03-23 | En vigor | UIT-T X.1111 – Suplemento sobre la arquitectura funcional de seguridad para los servicios de red eléctrica inteligente que utilizan redes de telecomunicaciones |
| Z.Sup1 (revisado) | 2015-04-17 | En vigor | Serie UIT-T Z.100 – Suplemento metodológico sobre la utilización de las técnicas de descripción |

TABLE 12

Comisión de Estudio 17 – Publicaciones no normativas (guías, manuales) acordadas

| Publicación | Aprobación | Situación | Título |
| --- | --- | --- | --- |
| Informe técnico | 2014-09-26 | Publicado | Desafíos actuales y nuevos en materia de normalización de la infraestructura de clave pública |
| Informe técnico | 2015-09-17 | Publicado | La seguridad de las telecomunicaciones y las tecnologías de la información – Visión general de asuntos relacionados con la seguridad de las telecomunicaciones y la implementación de las Recomendaciones UIT-T existentes; 6ª edición |

CUADRO 13

Comisión de Estudio 17 – Recomendaciones que han recibido la determinación/consentimiento  
y se han rechazado

| Recomendación | Consentimiento / Determinación | TAP / AAP | Título |
| --- | --- | --- | --- |
| Proyecto X.1126 (ex X.msec-6) (Nota 1) | 2013-04 | TAP | Aspectos de seguridad de los teléfonos inteligentes |
| NOTA 1 – La CE 17 cesó la actividad de normalización X.1126 (ex X.msec-6) en abril de 2013, y la retomó como X.Suppl.19 | | | |

ANEXO 2

Propuesta de actualización del mandato y la función de Comisión de Estudio Rectora de la Comisión de Estudio 17  
(Resolución 2 de la AMNT)

A continuación se presentan las propuestas de modificación del mandato y la función de Comisión de Estudio Rectora de la Comisión de Estudio 17 acordadas en la última reunión de la Comisión de Estudio 17 durante este periodo de estudios, basadas en las partes pertinentes de la [Resolución 2 de la AMNT-12](http://www.itu.int/en/ITU-T/wtsa16/Documents/CPI/ITU-T_Res2_2016-S.DOCX).

PARTE 1 ‑ ÁREAS GENERALES DE ESTUDIO

**…**

Comisión de Estudio 17 del UIT-T

Seguridad

La Comisión de Estudio 17 del UIT-T se encarga de la creación de confianza y seguridad en el uso de las tecnologías de la información y la comunicación (TIC). Ello incluye los estudios relativos a la ciberseguridad, la gestión de la seguridad, la lucha contra el correo basura y la gestión de identidades. También incluye la arquitectura y marco de la seguridad, la protección de la información de identificación personal y la seguridad de las aplicaciones y servicios para Internet de las Cosas (IoT), la red eléctrica inteligente, los teléfonos inteligentes, las redes definidas por software (SDN), la televisión por el protocolo Internet (TVIP), los servicios web, las redes sociales, la computación en la nube, el análisis de macrodatos, los sistemas financieros móviles y la telebiometría. Es también responsable de la aplicación de comunicaciones de sistemas abiertos, incluidos el directorio y los identificadores de objetos, así como de los lenguajes técnicos, el método de utilización de los mismos y otros temas relacionados con los aspectos del software de los sistemas de telecomunicación, y de las pruebas de conformidad para mejorar la calidad de las Recomendaciones.

**…**

PARTE 2 – COMISIONES DE ESTUDIO DEL UIT-T RECTORAS EN TEMAS DE ESTUDIOS ESPECÍFICOS

**…**

CE 17 Comisión de Estudio Rectora sobre seguridad   
Comisión de Estudio Rectora sobre gestión de identidad (IdM)  
Comisión de Estudio Rectora sobre lenguajes y técnicas de descripción

**…**

Anexo B  
(a la Resolución 2)

Orientaciones a las Comisiones de Estudio del UIT-T para la elaboración  
del programa de trabajo posterior a 2012

**…**

Comisión de Estudio 17 del UIT-T

La Comisión de Estudio 17 del UIT-T se encarga de la creación de confianza y seguridad en el uso de las tecnologías de la información y la comunicación (TIC). Ello incluye los estudios relativos a la seguridad, incluida la ciberseguridad, la lucha contra el correo basura (spam) y la gestión de identidad. También incluye la arquitectura y marco de la seguridad, la gestión de la seguridad, la protección de la información de identificación personal (IIP) y la seguridad de las aplicaciones y servicios para Internet de las Cosas (IoT), la red eléctrica inteligente, los teléfonos inteligentes, las redes definidas por software (SDN), la televisión por el protocolo Internet (TVIP), los servicios web, las redes sociales, la computación en la nube, los sistemas financieros móviles y la telebiometría. También es responsable de la aplicación de las comunicaciones basadas en sistemas abiertos, incluyendo el directorio y los identificadores de objetos; así como de los relativos a los lenguajes técnicos, el método para la utilización de los mismos y otros temas relacionados con los aspectos del software de los sistemas de telecomunicación y de las pruebas de conformidad para mejorar la calidad de las Recomendaciones.

En materia de seguridad, la Comisión de Estudio 17 se encarga de elaborar las Recomendaciones básicas sobre seguridad de las TIC, tales como la arquitectura y los marcos de seguridad; los elementos fundamentales relativos a la ciberseguridad, incluidas las amenazas, las vulnerabilidades y los riesgos, el tratamiento/respuesta a los incidentes y el análisis forense digital, y la gestión de la seguridad incluida la gestión de la IIP y la lucha contra el spam por medios técnicos. Además, la Comisión de Estudio 17 establece la coordinación general de los estudios sobre seguridad en el UIT‑T.

La Comisión de Estudio 17 también es responsable de la elaboración de las Recomendaciones básicas sobre aspectos de seguridad de las aplicaciones y servicios en el área de la TVIP, red eléctrica inteligente, IoT, redes definidas por software (SDN), redes sociales, computación en la nube, análisis de macrodatos, teléfonos inteligentes, sistemas financieros, móviles y telebiometría.

La Comisión de Estudio 17 es igualmente responsable de la elaboración de Recomendaciones básicas sobre un modelo genérico de gestión de la identidad que sea independiente de las tecnologías de red y que sirva de soporte para el intercambio seguro de información de identidad entre las entidades. Esta labor comprende también el estudio del proceso de descubrimiento de fuentes autorizadas de información de identidad; mecanismos genéricos para la neutralidad/compatibilidad de diversos formatos de información de identidad; amenazas de gestión de identidad, mecanismos para contrarrestarlas, la protección de la información de identificación personal (IIP) y la elaboración de mecanismos que garanticen que sólo se autoriza el acceso a la IIP cuando procede.

En el área de las comunicaciones de sistemas abiertos, la Comisión de Estudio 17 se encarga de las Recomendaciones sobre los temas siguientes:

• servicios y sistemas de directorio, incluida la infraestructura de clave pública (PKI) (series UIT-T F.500 y UIT-T X.500);

• identificadores de objeto (OID) y autoridades de registro asociadas (series UIT-T X.660/UIT-T X.670);

• interconexión de sistemas abiertos (OSI) incluida la notación de sintaxis abstracta uno (ASN.1) (series UIT-T F.400, UIT-T X.200, UIT-T X.600 y UIT-T X.800); y

• procesamiento distribuido abierto (ODP) (serie UIT-T X.900).

En materia de lenguajes, la Comisión de Estudio 17 se encarga de los estudios sobre técnicas de modelado, especificación y descripción. Esta labor, que incluye lenguajes tales como los ASN.1, SDL, MSC y URN, se desarrollará en consonancia con las exigencias de las Comisiones de Estudio pertinentes, tales como las CE 2, CE 9, CE 11, CE 13, CE 15 y CE 16, y en cooperación con ellas.

**…**

Anexo C  
(a la Resolución 2)

Lista de Recomendaciones correspondientes a las respectivas  
Comisiones de Estudio del UIT-T y al GANT en el periodo de estudios 2013-2016

**…**

Comisión de Estudio 17 del UIT-T

UIT-T E.104, UIT-T E.115, UIT-T E.409 (conjuntamente con la Comisión de Estudio 2)

Serie UIT-T F.400; UIT-T F.500-UIT-T F.549

Serie UIT-T X, salvo las que son responsabilidad de las Comisiones de Estudio 2, 11, 13, 15 y 16

Serie UIT-T Z, salvo las series UIT-T Z.300 y UIT-T Z.500

NOTA 1 – El GANT acordó cambios en la asignación de las Recomendaciones de la serie Z después de la AMNT-12.

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