|  |  |
| --- | --- |
| **Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT-20)****Ginebra, 1-9 de marzo de 2022** |  |
|  |  |
|  |  |
| SESIÓN PLENARIA | Documento 19-S |
|  | **Diciembre de 2021** |
|  | **Original: inglés** |
|  |
| Comisión de Estudio 17 del UIT-T |
| Seguridad |
| INFORME DE LA CE 17 del uit-t A LA ASAMBLEA MUNDIALDE NORMALIZACIÓN DE LAS TELECOMUNICACIONES (Amnt-20), PARTe I: GENERALidades |
|  |

|  |  |
| --- | --- |
| **Resumen:** | Esta contribución contiene el Informe de la Comisión de Estudio 17 del UIT-T a la AMNT-20 sobre sus actividades durante el periodo de estudios 2017-2021. |
| **Contacto:** | Heung Youl YoumPresidente de la CE 17 del UIT-T Corea (República de) | Correo-e: hyyoum@sch.ac.kr |

**Nota de la TSB**:

El Informe de la Comisión de Estudio 17 a la AMNT-20 se presenta en los siguientes documentos:

Parte I: **Documento 19** – Generalidades

Parte II: **Documento 20** – Cuestiones propuestas para estudio durante el periodo de estudios 2022-2024

**ÍNDICE**

**Página**

[1 Introducción 4](#_Toc94617201)

[1.1 Responsabilidades de la Comisión de Estudio 17 4](#_Toc94617202)

[1.2 Equipo de gestión y reuniones celebradas por la Comisión de Estudio 17 6](#_Toc94617203)

[2 Organización del trabajo 11](#_Toc94617204)

[2.1 Organización de los estudios y atribución de trabajos 11](#_Toc94617205)

[2.2 Cuestiones y Relatores 14](#_Toc94617206)

[3 Resultados de los trabajos realizados durante el periodo de estudios 2017-2020 21](#_Toc94617207)

[3.1 Generalidades 21](#_Toc94617208)

[3.2 Logros más destacados 21](#_Toc94617209)

[a) C1/17, Coordinación de la seguridad en las telecomunicaciones/TIC (2017‑2020)/Estrategia de normalización y coordinación de la seguridad (2021-) 22](#_Toc94617210)

[b) C2/17, Arquitectura y marco genérico de la seguridad (2017-2020)/Arquitectura de seguridad y seguridad de red (2021-) 22](#_Toc94617211)

[c) C3/17, Gestión de la seguridad de la información en las telecomunicaciones (2017‑2020)/Gestión de la seguridad de la información en las telecomunicaciones y servicios de seguridad (2021-) 24](#_Toc94617212)

[d) C4/17, Ciberseguridad (2017-2020)/Ciberseguridad y lucha contra el correo basura (2021-) 25](#_Toc94617213)

[e) C5/17, Medios técnicos contra el correo basura (2017-2020) 28](#_Toc94617214)

[f) C6/17, Aspectos relativos a la seguridad en los servicios y redes de telecomunicaciones e Internet de las cosas (2017-2020)/Seguridad de los servicios de telecomunicaciones e Internet de las cosas (2021-) 29](#_Toc94617215)

[g) C7/17, Servicios de aplicación seguros 31](#_Toc94617216)

[h) C8/17, Seguridad de la infraestructura de la computación en la nube y los macrodatos 33](#_Toc94617217)

[i) C9/17, Telebiometría (2017-2020) 34](#_Toc94617218)

[j) C10/17, Arquitectura y mecanismos de la gestión de identidades (2017‑2020)/Arquitectura y mecanismos de gestión de identidades y telebiometría (2021-) 35](#_Toc94617219)

[k) C11/17, Tecnologías genéricas (Directorio, infraestructura de clave pública (PKI), infraestructura de gestión de privilegios (PMI), notación de sintaxis abstracta uno (ASN.1), identificadores de objeto (OID)) para aplicaciones seguras (2017‑2020)/Tecnologías genéricas (Directorio, PKI, Lenguajes formales, Identificadores de objeto, entre otras) para aplicaciones seguras (2021-) 36](#_Toc94617220)

[l) C12/17, Lenguajes formales para software de telecomunicaciones y pruebas (2017‑2020) 42](#_Toc94617221)

[m) C13/17, Aspectos de seguridad de los sistemas de trasporte inteligentes (2017-2020)/ Seguridad de los sistemas de transporte inteligente (2021-) 46](#_Toc94617222)

[n) C14/17, Aspectos de seguridad de las tecnologías de libro mayor distribuido (2018‑2020)/Seguridad de las tecnologías de libro mayor distribuido (DTL) (2021-) 47](#_Toc94617223)

[o) C15/17, Seguridad en relación con las tecnologías incipientes, en particular la seguridad cuántica 49](#_Toc94617224)

[3.3 Informe sobre las actividades de la Comisión de Estudio Rectora, las GSI, las JCA, los Grupos Regionales y los proyectos 49](#_Toc94617225)

[3.3.1 Actividades de la Comisión de Estudio Rectora sobre seguridad 49](#_Toc94617226)

[3.3.2 Actividades de la Comisión de Estudio Rectora sobre gestión de identidad 53](#_Toc94617227)

[3.3.3 Comisión de Estudio Rectora sobre lenguajes y técnicas de descripción 54](#_Toc94617228)

[3.3.4 Actividad Conjunta de Coordinación sobre la gestión de la identidad (JCA-IdM) 55](#_Toc94617229)

[3.3.5 Grupo Regional para África de la Comisión de Estudio 17 (GRCE17-AFR) 56](#_Toc94617230)

[3.3.6 Grupo Regional de la Comisión de Estudio 17 para los Estados Árabes (GRCE17-ARB) 56](#_Toc94617231)

[3.4 Proyectos 56](#_Toc94617232)

[3.4.1 Proyecto ASN.1 56](#_Toc94617233)

[3.4.2 Proyecto OID 57](#_Toc94617234)

[3.5 Reducción de la brecha en materia de normalización 57](#_Toc94617235)

[4 Observaciones en relación con el trabajo futuro 57](#_Toc94617236)

[5 Actualizaciones de la Resolución 2 de la AMNT para el
periodo de estudios 2022-2024 59](#_Toc94617237)

[ANEXO 1 – Lista de Recomendaciones, Suplementos y otros documentos
producidos o suprimidos durante el periodo de estudios 60](#_Toc94617238)

[ANEXO 2 – Propuesta de revisión de la Resolución 2 de la AMNT presentada
por la Comisión de Estudio 17 77](#_Toc94617239)

# 1 Introducción

## 1.1 Responsabilidades de la Comisión de Estudio 17

La Asamblea Mundial de Normalización de las Telecomunicaciones (Hammamet, 2016) encomendó a la Comisión de Estudio 17 el examen de 12 Cuestiones relacionadas con la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación (TIC).

En el anexo A la Resolución 2 de la AMNT-16 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 interconexión de redes definida por software (SDN), la televisión por el protocolo Internet (TVIP), los servicios web, las redes sociales, la computación en la nube, la analítica 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 los lenguajes de especificación de pruebas para la realización de pruebas de conformidad con el fin de mejorar la calidad de las Recomendaciones.*

En el Anexo A la Resolución 2 de la AMNT-16 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-16 se dan orientaciones a 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 interconexión de redes definida 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, interconexión de redes definida por software (SDN), redes sociales, computación en la nube, analítica 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, labor que incluye lenguajes tales como los ASN.1, SDL, MSC, URN y TTCN-3.*

*Este trabajo 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, CE 16 y CE 20 (en lo que respecta a los temas relacionados con la IoT y las CCI), y en cooperación con ellas.*

*La Comisión de Estudio 17 tratará los aspectos pertinentes de la gestión de identidades en colaboración con la CE 20 para la IoT y la CE 2, de acuerdo con el mandato de cada Comisión.*

En el Anexo C a la Resolución 2 de la AMNT-16 (modificada por el GANT) se enumeran las Recomendaciones bajo responsabilidad de la Comisión de Estudio 17 durante el periodo de estudios 2017-2020:

– 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-16 nombró al Sr. Heung Youl YOUM (Corea, República de) Presidente de la Comisión de Estudio 17 y designó a los siguientes nueve Vicepresidentes: Sr. Vasiliy DOLMATOV (Federación de Rusia), Sr. Muataz Elsadig ISHAG (Sudán), Sr. Gökhan EVREN (Turquía), Sra. Inette FUREY (Estados Unidos), Sra. Wala Turki LATROUS (Túnez), Sr. Zhaoji LIN (China), Sr. Hugo Darío MIGUEL (Argentina), Sr. Yutaka MIYAKE (Japón) y Sr. Patrick-Kennedy KETTIN ZANGA (República Centroafricana). El Sr. Patrick-Kenney KETTIN ZANGA no participó en ninguna de reunión de la Comisión de Estudio 17 durante este periodo de estudios.

En marzo de 2018, la Sra. Inette FUREY (Estados Unidos) fue sustituida por el Sr. Juan GONZALES (Estados Unidos) en la Vicepresidencia de la Comisión de Estudio 17. En marzo de 2020, el Sr. Hugo Darío MIGUEL (Argentina) fue sustituido por la Sra. Lia MOLINARI (Argentina) en la Vicepresidencia de la Comisión de Estudio 17. En agosto de 2020 el Sr. Patrick‑Kennedy KETTIN ZANGA (República Centroafricana) fue sustituido por el Sr. Eric Anicet MBATHAS (República Centroafricana) en la Vicepresidencia de la Comisión de Estudio 17.

Durante el periodo de estudios considerado, la Comisión de Estudio 17 se reunió en 13 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 |
| --- | --- | --- |
| CE/GT 17 | Ginebra, 22-30 de marzo de 2017 | CE 17-R1 a R9 |
| CE/GT 17 | Ginebra, 29 de agosto – 6 de septiembre de 2017 | CE 17-R10 a R17 |
| CE/GT 17 | Ginebra, 20-29 de marzo de 2018 | CE 17-R18 a R24 |
| CE/GT 17 | Ginebra, 29 de agosto – 7 de septiembre de 2018 | CE 17-R25 a R32 |
| CE/GT 17 | Ginebra, 22-30 de enero de 2019 | CE 17-R33 a R37 |
| CE/GT 17 | Ginebra, 27 de agosto – 5 de septiembre de 2019 | CE 17-R38 a R50 |
| CE/GT 17 | Virtual, 17-26 de marzo de 2020 | CE 17-R51 a R66 |
| CE 17 | Virtual, 29 de mayo de 2020 | CE 17-R67 |
| CE/GT 17 | Virtual, 24 de agosto – 3 de septiembre de 2020 | CE 17-R68 a R77 |
| CE 17 | Virtual, 7 de enero de 2021 | CE 17-R78 |
| CE/GT 17 | Virtual, 20-30 de abril de 2021 | CE 17-R79 a R85 |
| CE/GT 17 | Virtual, 24 de agosto – 3 de septiembre de 2020 | CE 17-R86 a R102 |
| CE 17 | Virtual, 7 de enero de 2022 | CE 17-R103 |

En paralelo a cada una de las reuniones de la Comisión de Estudio 17 se celebraron reuniones del equipo de gestión.

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 | Cuestión(es) | Nombre del evento  |
| 12/12/2016a13/12/2016 | China [Beijing] | [C8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5710&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-170322-TD-PLEN-0057/es)] | Reunión intermedia del Grupo de Relator sobre la C8/17 |
| 12/01/2017a13/01/2017 | *Reunión virtual* | [C4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5711&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-170322-TD-PLEN-0054/es)] | Reunión intermedia del Grupo de Relator sobre la C4/17 |
| 06/12/2017a10/02/2017 | Túnez [Túnez] | [C11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5716&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-170322-TD-PLEN-0058/es)] | Reunión Mixta del Grupo de Relator sobre la Cuestión 11/17 y el ISO/IEC JTC 1/SC 6/ WG10 |
| 08/02/2017a09/02/2017 | Corea (Rep. de) [Seúl] | [C3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5712&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-170322-TD-PLEN-0053/es)] | Reunión intermedia del Grupo de Relator sobre la C3/17 |
| 08/02/2017a09/02/2017 | Corea (Rep. de) [Seúl] | [C6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5713&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-170322-TD-PLEN-0056/es)] | Reunión intermedia del Grupo de Relator sobre la C6/17 |
| 22/06/2017a23/06/2017 | Corea (Rep. de) [Seúl] | [C3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6903&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-170829-TD-PLEN-0392/es)] | Reunión intermedia del Grupo de Relator sobre la C3/17 |
| 22/06/2017a23/06/2017 | Corea (Rep. de) [Seúl] | [C6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6904&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-170829-TD-PLEN-0393/es)] | Reunión intermedia del Grupo de Relator sobre la C6/17 |
| 27/06/2017a28/06/2017 | China [Beijing] | [C8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6909&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-170829-TD-PLEN-0394/es)] | Reunión intermedia del Grupo de Relator sobre la C8/17 |
| 29/06/2017 | Japón [Tokio] | [C4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6916&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-170829-TD-PLEN-0395/es)] | Reunión intermedia del Grupo de Relator sobre la C4/17 |
| 30/06/2017 | Japón [Tokio] | [C3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6905&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390/es)][C4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6906&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390/es)][C10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6907&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390/es)] | Reunión Mixta de los Grupos de Relator sobre las C3/17, C4/17 y C10/17 sobre SFD |
| 03/07/2017 | Japón [Tokio] | [C10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=7916&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-170829-TD-PLEN-0396/es)] | Reunión intermedia del Grupo de Relator sobre la C10/17 |
| 14/07/2017 | Corea (Rep. de) [Seúl] | [C13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=8918&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-170829-TD-PLEN-0397/es)] | Reunión intermedia del Grupo de Relator sobre la C13/17 |
| 30/10/2017a03/11/2017 | Corea (Rep. de) | [C11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9047&Group=17) [[[informe de la reunión](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0817)](https://www.itu.int/md/T17-SG17-180320-TD-PLEN-0824/es)] | Reunión Mixta de la C11/17 y el ISO/IEC JTC1/SC6 |
| 30/11/2017a01/12/2017 | Corea (Rep. de)[Bundang] | [C14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9048&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180320-TD-PLEN-0817/es)] | Reunión del Grupo de Relator sobre la C14/17 |
| 13/12/2017a14/12/2017 | China [Beijing] | [C7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9050&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180320-TD-PLEN-0822/es)] | Reunión del Grupo de Relator sobre la C7/17 |
| 09/01/2018 | Canadá [Vancúver] | [C4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9051&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180320-TD-PLEN-0821/es)][C10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9052&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180320-TD-PLEN-1006/es)] | Reunión Mixta de la C4/17 y la C10/17 |
| 22/01/2018a23/01/2018 | China [Beijing] | [C14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9057&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180320-TD-PLEN-0823/es)] | Reunión del Grupo de Relator sobre la C14/17 |
| 24/01/2018a25/01/2018 | Corea (Rep. de) [Seúl] | [C13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9056&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180320-TD-PLEN-0818/es)] | Reunión del Grupo de Relator sobre la C13/17 |
| 25/01/2018a26/01/2018 | Corea (Rep. de) [Seúl] | [C3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9054&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180320-TD-PLEN-0820/es)] | Reunión del Grupo de Relator sobre la C3/17 |
| 25/01/2018a26/01/2018 | Corea (Rep. de) [Seúl] | [C6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9055&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180320-TD-PLEN-0819/es)] | Reunión del Grupo de Relator sobre la C6/17 |
| 04/06/2018a06/06/2018 | China [Beijing] | [C14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9265&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180829-TD-PLEN-1252/es)] | Reunión intermedia del Grupo de Relator sobre la C14/17 |
| 07/06/2018a08/06/2018 | Corea (Rep. de) [Seúl] | [C6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9261&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180829-TD-PLEN-1246/es)][C13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9262&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180829-TD-PLEN-1251/es)] | Reuniones intermedias de los Grupos de Relator sobre las C6/17 y C13/17 |
| 20/06/2018a21/06/2018 | China [Yinchuan] | [C7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9259&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180829-TD-PLEN-1247/es)] | Reunión del Grupo de Relator sobre la C7/17 |
| 26/06/2018a27/06/2018 | Estados Unidos [Seattle, Washington] | [C10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9264&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180829-TD-PLEN-1249/es)] | Reunión intermedia del Grupo de Relator sobre la C10/17 |
| 27/06/2018a28/06/2018 | China [Beijing] | [C8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9263&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180829-TD-PLEN-1248/es)] | Reunión intermedia del Grupo de Relator sobre la C8/17 |
| 27/08/2018a31/08/2018 | Japón [Tokio] | [C11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9260&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-180829-TD-PLEN-1250/es)] | Reunión intermedia del Grupo de Relator sobre la C11/17 junto con ISO/IEC JTC 1/SC 6/WG 10 |
| 08/11/2018a09/11/2018 | Singapur | [C13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9405&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-190122-TD-PLEN-1727/es)] | Reunión intermedia del Grupo de Relator sobre la C13/17 |
| 12/11/2018a13/11/2018 | Japón [Tokio] | [C10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9406&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-190122-TD-PLEN-1726/es)] | Reunión intermedia del Grupo de Relator sobre la C10/17 |
| 12/11/2018a13/11/2018 | Japón [Tokio] | [C14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9407&Group=17) [[[minforme de la reunión](http://www.itu.int/md/T17-SG17-190122-TD-PLEN-1726)](https://www.itu.int/md/T17-SG17-190122-TD-PLEN-1726/es)] | Reunión intermedia del Grupo de Relator sobre la C14/17 |
| 22/04/2019a26/04/2019 | China [Beijing] | [C11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9560&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-190827-TD-PLEN-2057/es)] | Reunión intermedia del Grupo de Relator sobre la C11/17 junto con ISO/IEC JTC 1/SC 6/WG 10 |
| 04/06/2019a05/06/2019 | *Virtual* | [C10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9559&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-190827-TD-PLEN-2056/es)] | Reunión virtual intermedia del Grupo de Relator sobre la C10/17 |
| 04/06/2019a05/06/2019 | *Virtual* | [C14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9563&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-190827-TD-PLEN-2059/es)] | Reunión intermedia del Grupo de Relator sobre la C14/17 |
| 10/06/2019a12/06/2019 | China [Shangái] | [C4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9574&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-190827-TD-PLEN-2051/es)] | Reunión intermedia del Grupo de Relator sobre la C4/17 |
| 11/06/2019a12/06/2019 | China [Beijing] | [C13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9561&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-190827-TD-PLEN-2058/es)] | Reunión intermedia del Grupo de Relator sobre la C13/17 |
| 18/06/2019a19/06/2019 | China [Chongqing] | [C7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9556&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-190827-TD-PLEN-2053/es)] | Reunión intermedia del Grupo de Relator sobre la C7/17 |
| 24/06/2019a25/06/2019 | China [Beijing] | [C8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9557&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-190827-TD-PLEN-2054/es)] | Reunión intermedia del Grupo de Relator sobre la C8/17 |
| 27/06/2019a28/06/2019 | Japón [Tokio] | [C6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9555&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-190827-TD-PLEN-2052/es)] | Reunión intermedia del Grupo de Relator sobre la C6/17 |
| 27/06/2019 | *Virtual* | [C3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9554&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-190827-TD-PLEN-2050/es)] | Reunión virtual intermedia del Grupo de Relator sobre la C3/17 |
| 22/10/2019a23/10/2019 | China [Haikou] | [C7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9763&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200317-TD-PLEN-2564/es)] | Reunión intermedia del Grupo de Relator sobre la C7/17 |
| 05/12/2019a06/12/2019 | Suiza [Friburgo] | [C11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9767&Group=17) [[informe de la reunión](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2762)] [C14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9768&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200317-TD-PLEN-2762/es)] | Reunión Mixta de la C11/17 y la C14/17 |
| 11/12/2019a13/12/2019 | China [Jinan] | [C4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9882&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200317-TD-PLEN-2562/es)] | Reunión intermedia del Grupo de Relator sobre la C4/17 |
| 11/122019-12-11 | *Virtual* | [C11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9766&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200317-TD-PLEN-2567/es)] | Reunión intermedia del Grupo de Relator sobre la C11/17 |
| 11/12/2019 | China [Jinan] | [C4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9760&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200317-TD-PLEN-2754/es)] | Reunión coubicada de los Grupos de Relator sobre las C4/17 y C16/13 |
| 2019-12-12 | Japón [Tokio] | [C10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9765&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200317-TD-PLEN-2566/es)] | Reunión intermedia del Grupo de Relator sobre la C10/17 |
| 2019-12-13 | Japón [Tokio] | [C3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9759&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200317-TD-PLEN-2561/es)] | Reunión intermedia del Grupo de Relator sobre la C3/17 |
| 07/01/2020a08/01/2020 | China [Beijing] | [C8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9764&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200317-TD-PLEN-2565/es)] | Reunión intermedia del Grupo de Relator sobre la C8/17 |
| 07/01/2020a08/01/2020 | Japón [Fukuoka] | [C13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9769&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200317-TD-PLEN-2569/es)] | Reunión intermedia del Grupo de Relator sobre la C13/17 |
| 08/01/2020 | *Virtual* | [C14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9771&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200317-TD-PLEN-2570/es)] | Reunión intermedia del Grupo de Relator sobre la C14/17 |
| 13/01/2020a14/01/2020 | Malasia [Kuala Lumpur] | [C6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9783&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200317-TD-PLEN-2563/es)] | Reunión intermedia del Grupo de Relator sobre la C6/17 |
| 03/02/2020a07/02/2020 | Reino Unido [Londres] | [C11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9770&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200317-TD-PLEN-2568/es)] | Reunión intermedia del Grupo de Relator sobre la C11/17 junto con ISO/IEC JTC 1/SC 6/WG 10 |
| 17/02/2020 | *Virtual* | [C4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10081&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200529-TD-PLEN-2963/es)] | Reunión intermedia del Grupo de Relator sobre la C4/17 |
| 22/04/2020 | *Virtual* | [C11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10087&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200529-TD-PLEN-2966/es)] | Reunión intermedia del Grupo de Relator sobre la C11/17 |
| 11/05/2020a12/05/2020 | *Virtual* | [C6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10083&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3093/es)] | Reunión intermedia del Grupo de Relator sobre la C6/17 |
| 13/05/2020 | *Virtual* | [C13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10088&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200529-TD-PLEN-2979/es)] | Reunión intermedia del Grupo de Relator sobre la C13/17 |
| 02/06/2020a03/06/2020 | *Virtual* | [C3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10080&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3090/es)] | Reunión intermedia del Grupo de Relator sobre la C3/17 |
| 10/06/2020a11/06/2020 | *Virtual* | [C13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10089&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3096/es)] | Reunión intermedia del Grupo de Relator sobre la C13/17 |
| 19/06/2020 | *Virtual* | [C4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10347&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3091/es)] | Reunión intermedia del Grupo de Relator sobre la C4/17 |
| 22/06/2020a23/06/2020 | *Virtual* | [C14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10090&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3097/es)] | Reunión intermedia del Grupo de Relator sobre la C14/17 |
| 13/07/2020 | *Virtual* | [C10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10086&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3095/es)] | Reunión intermedia del Grupo de Relator sobre la C10/17 |
| 16/07/2020a17/07/2020 | *Virtual* | [C8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10084&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3094/es)] | Reunión intermedia del Grupo de Relator sobre la C8/17 |
| 19/10/2020a30/10/2020 | *Virtual* | [C11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11694&Group=17) [[informe de la reunión](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3447)] | Reunión Intermedia del Grupo de Relator sobre la C11/17 junto con ISO/IEC JTC 1/SC 6/WG 10 |
| 18/11/2020 | *Virtual* | [C10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11588&Group=17) [[informe de la reunión](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3462)] | Reunión intermedia del Grupo de Relator sobre la C10/17 |
| 25/11/2020a26/11/2020 | *Virtual* | [C13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11589&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3467)] | Reunión intermedia del Grupo de Relator sobre la C13/17 |
| 26/11/2020a27/11/2020 | *Virtual* | [C4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11570&Group=17) [[informe de la reunión](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3460)] | Reunión intermedia del Grupo de Relator sobre la C4/17 |
| 07/12/2020a08/12/2020 | *Virtual* | [C2/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11569&Group=17) [[informe de la reunión](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3459)] | Reunión intermedia del Grupo de Relator sobre la C2/17 |
| 09/12/2020a10/12/2020 | *Virtual* | [C3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11727&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3468)] | Reunión intermedia del Grupo de Relator sobre la C3/17 |
| 21/12/2020a22/12/2020 | *Virtual* | [C6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11571&Group=17) [[informe de la reunión](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3463)] | Reunión intermedia del Grupo de Relator sobre la C6/17 |
| 04/01/2021a05/01/2021 | *Virtual* | [C14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11590&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3469)] | Reunión intermedia del Grupo de Relator sobre la C14/17 |
| 01/02/2021a02/02/2021 | *Virtual* | [C3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11832&Group=17) [[informe de la reunión](http://www.itu.int/md/T17-SG17-210420-TD-PLEN-3547)] | Reunión intermedia del Grupo de Relator sobre la C3/17 |
| 01/02/2021a02/02/2021 | *Virtual* | [C4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11830&Group=17) [[informe de la reunión](http://www.itu.int/md/T17-SG17-210420-TD-PLEN-3548)] | Reunión intermedia del Grupo de Relator sobre la C4/17 |
| 04/02/2021 | *Virtual* | [C6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11836&Group=17) [[informe de la reunión](http://www.itu.int/md/T17-SG17-210420-TD-PLEN-3549)] | Reunión intermedia del Grupo de Relator sobre la C6/17 |
| 17/06/2021a18/06/2021 | *Virtual* | [C15/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12574&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3876)] | Reunión intermedia del Grupo de Relator sobre la C15/17 |
| 17/06/2021a18/06/2021 | *Virtual* | [C8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12539&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3875)] | Reunión intermedia del Grupo de Relator sobre la C8/17 |
| 24/06/2021a25/06/2021 | *Virtual* | [C4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12534&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3877)] | Reunión intermedia del Grupo de Relator sobre la C4/17 |
| 24/06/2021 | *Virtual* | [C10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12575&Group=17) [[informe de la reunión](http://www.itu.int/md/T17-SG17-210824-TD-PLEN-3878)] | Reunión intermedia del Grupo de Relator sobre la C10/17 |
| 28/06/2021a29/06/2021 | *Virtual* | [C14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12592&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3879)] | Reunión intermedia del Grupo de Relator sobre la C14/17 |
| 01/07/2021a02/07/2021 | *Virtual* | [C2/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12533&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3880)] | Reunión intermedia del Grupo de Relator sobre la C2/17 |
| 05/10/2021 | *Virtual* | [C3/17 [informe de la reunión]](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4199/en) | Reunión intermedia del Grupo de Relator sobre la C3/17 |
| 19/11/2021 | *Virtual* | [C10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12744&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4178)] | Reunión intermedia del Grupo de Relator sobre la C10/17 |
| 24/11/2021a25/11/2021 | *Virtual* | [C2/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12733&Group=17) [[informe de la reunión](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4159)] | Reunión intermedia del Grupo de Relator sobre la C2/17 |
| 20/01/2022a21/01/2022 | *Virtual* | C15/17 [informe de la reunión] | Reunión intermedia del Grupo de Relator sobre la C15/17 |
| 07/02/2022 | *Virtual* | C3/17 [informe de la reunión] | Reunión intermedia del Grupo de Relator sobre la C3/17 |
| 15/02/2022 | *Virtual* | C10/17 [informe de la reunión] | Reunión intermedia del Grupo de Relator sobre la C10/17 |
| 17/02/2022 | *Virtual* | C6/17 [informe de la reunión] | Reunión intermedia del Grupo de Relator sobre la C6/17 |
| 23/02/2022a24/02/2022 | *Virtual* | C2/17 [informe de la reunión] | Reunión intermedia del Grupo de Relator sobre la C2/17 |
| ??/02/2022 | *Virtual* | C4/17 [informe de la reunión] | Reunión intermedia del Grupo de Relator sobre la C4/17 |

# 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 4 Grupos de Trabajo.En el Cuadro 2 se indica el número y título de cada Grupo de Trabajo, junto con las Cuestiones que tiene asignadas y el nombre de su Presidente y sus Vicepresidentes entre 2017 y 2020.

CUADRO 2

Organización de la Comisión de Estudio 17

| Designación | Cuestiones de estudio | Nombre del Grupo de Trabajo | Presidente y Vicepresidentes |
| --- | --- | --- | --- |
| PLEN | C1/17; |  |  |
| GT 1/17 | C2/17; C3/17; C6/17; C13/17(7); | Seguridad de las telecomunicaciones/TIC | Sr. Miyake Yutaka (Presidente)Sr. Dolmatov Vasiliy (Vicepresidente)Sr. Evren Gökhan (Vicepresidente) |
| GT 2/17 | C4/17; C5/17; C14/17(8); | Seguridad del ciberespacio | Sr. Nakao Koji (Presidente)Sra. Furey Inette (Vicepresidenta) (1) Sr. González Juan (Vicepresidente) (2) |
| GT 3/17 | C7/17; C8/17; C12/17; | Seguridad de las aplicaciones | Sr. Taddei Arnaud (Presidente)Sr. Lin Zhaoji (Vicepresidente) (3)Sra. Bai Xiaoyuan (Vicepresidenta) (4) |
| GT 4/17 | C9/17; C10/17; C11/17; | Gestión de identidades y autentificación | Sr. Li Kepeng (Presidente) (5)Sr. Nah Jae Hoon (Vicepresidente/(Copresidente) (5, 6)Sr. Lin Zhaoji (Copresidente) (6) |

Notas:

(1) Vicepresidenta hasta septiembre de 2017.

(2) Vicepresidente desde marzo de 2018.

(3) Vicepresidente hasta septiembre de 2018.

(4) Vicepresidenta desde enero de 2019.

(5) Presidente/Vicepresidente hasta septiembre de 2018.

(6) Copresidente desde enero de 2019.

(7) La C13/17 fue creada por la CE 17 en septiembre de 2017.

(8) La C14/17 fue creada por la CE 17 en marzo de 2018.

**2.1.2** Debido a la pandemia de COVID-19, la celebración de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT-20), prevista para 2020, se retrasó a 2022, y se amplió en consecuencia el periodo de estudios 2017-2020 hasta la celebración de la AMNT-20. En la reunión de agosto/septiembre de 2020, la CE 17 acordó un conjunto de 12 Cuestiones para su aprobación por la AMNT-20 (véase la sección 2.2) y decidió crear un grupo especial para la preparación del próximo periodo de estudios.

Habida cuenta del retraso de la celebración de la AMNT-20 hasta marzo de 2022, en su reunión celebrada del 11 al 18 de enero de 2021 el GANT refrendó este nuevo conjunto de Cuestiones de la CE 17 (véase la [Circular TSB 295](https://www.itu.int/md/T17-TSB-CIR-0295/es)). En su reunión celebrada del 20 al 30 de abril de 2021 la CE 17 acordó organizar dichas 12 Cuestiones conforme a una nueva estructura con cinco Grupos de Trabajo.

En el Cuadro 3 se indica el número y título de cada Grupo de Trabajo, junto con las Cuestiones que tiene asignadas y el nombre de su Presidente desde 2021.

CUADRO 3

Organización de la Comisión de Estudio 17 (2021-)

| Designación | Cuestiones de estudio | Nombre del Grupo de Trabajo | Presidente y Vicepresidentes |
| --- | --- | --- | --- |
| GT 1/17 | C1/17; C15/17 | Estrategia y coordinación de seguridad | Presidente: Sr. Dolmatov Vasily (Rusia)Vicepresidente: Sr. Kim Jonghyun (Corea) |
| GT 2/17 | C2/17; C6/17; C13/17; | Seguridad de la 5G, la IoT y los STI | Presidente: Sr. Miyake Yutaka (KDDI)Vicepresidentes: Sra. Hu Zhiyuan(Nokia Shanghai Bell)Sr. Mills Philip (Reino Unido)  |
| GT 3/17 | C3/17; C4/17;  | Ciberseguridad y gestión | Presidente: Sr. Nakao Koji (NICT)Vicepresidenta: Sra. Molinari Lia (Argentina) |
| GT 4/17 | C7/17; C8/17; C14/17 | Seguridad de servicios y aplicaciones | Presidente: Sr. Nah Jae Hoon (ETRI)Vicepresidenta: Sra. Bai Xiaoyuan (Alibaba)  |
| GT 5/17 | C10/17; C11/17 | Tecnologías de seguridad fundamentales | Presidente: Sr. Lin Zhaoji (ZTE)Vicepresidente: *Puesto vacante* |

**2.1.3** En el Cuadro 4 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‑16, en la reunión de marzo de 2017 de la CE 17, se creó el Grupo Regional de la CE 17 para los Estados Árabes (véase la sección 3.3.5).

**2.1.5** 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. se presentan los logros de la JCA-IdM.

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

En la primera reunión de la CE 17, celebrada en marzo de 2017, se decidió inactivar la Actividad Mixta de Coordinación sobre Protección de la Infancia en Línea (JCA-COP), prorrogada del periodo de estudios anterior.

**2.1.6** 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 4

Otros grupos (en su caso)

| Nombre del Grupo | Presidente | Vicepresidentes |
| --- | --- | --- |
| JCA-IdM | Copresidentes: Sr. Barbir Abbie (1),Sr. Park Keundug (1),Sr. Takechi Hiroshi (1), Sr. Youm Heung Youl (8) |  |
| JCA-COP | NA |  |
| GRCE17-AFR | Sr. Katundu Michael (2)Sra. Njiraini Mwende (3) | Sr. Elhaj Mohamed (2),Sr. Mwesigwa Patrick (2),Sr. Toure Mohamed (2) |
| GRCE17-ARB | Sra. Latrous Wala Turki (4),Sr. Al Salehi Badar Ali Said (5) | Sra. Abdelkader Manel (6),Sra. Abouche Chehrazed (6),Sra. Almansoury Laial (7) |
| Proyecto ASN.1 | Líder del proyecto: Sr. Thorpe Paul |  |
| Proyecto OID | Líder del proyecto: Sr. Dubuisson Olivier |  |

Notas:

(1) Copresidente desde marzo de 2017.

(2) Presidente/Vicepresidente hasta septiembre de 2018.

(3) Presidente desde abril de 2019.

(4) Copresidente de diciembre de 2017 a octubre de 2018.

(5) (Co)Presidente desde diciembre de 2017.

(6) Vicepresidente de diciembre de 2017 a octubre de 2018.

(7) Vicepresidente desde diciembre de 2017.

(8) Copresidente en funciones desde abril de 2021.

## 2.2 Cuestiones y Relatores

**2.2.1** La AMNT-16 asignó a la Comisión de Estudio 17 las 12 Cuestiones que figuran en el Cuadro 5, y la CE G17 nombró a lo largo de este periodo de estudios a los Relatores y los Relatores Asociados citados en el mismo.

CUaDRO 5

Comisión de Estudio 17 – Cuestiones asignadas por la AMNT-16 y Relatores (2017-2020)

| Cuestión | Nombre de la Cuestión | GT | Relator(19) |
| --- | --- | --- | --- |
| C1/17 | Coordinación de la seguridad de las telecomunicaciones/TIC | PLEN | Sra. Latrous Wala (Relatora) (13)Sr. Elhaj Mohamed M. K. (Relator) (1)Sra. Ki Juhee (Relator asociado) (2)Sr. Najarian Paul (Relator asociado) (3)Sr. Senga Wataru (Relator asociado) (3)Sra. Wang Yiwen (Relator asociado) (3) |
| C2/17 | Marco y arquitectura de seguridad | GT 1/17 | Sra. Hu Zhiyuan (Correlatora) (3)Sr. Oh Heung Ryong (Correlatora) (3)Sra. Chaabane Emna (Relator asociado) (10)Sr. Lee Jinmyung (Relator asociado) (16) |
| C3/17 | Gestión de la seguridad de las telecomunicaciones y la información | GT 1/17 | Sra. Naganuma Miho (Relatora) (3)Sr. Min Jinghua (Relator asociado) (7)Sr. Mustafa Thaib (Relator asociado) (5)Sr. Fischer Andres (Relator asociado) (4) |
| C4/17 | Ciberseguridad | GT 2/17 | Sr. Kadobayashi Youki (Relator) (6)Sr. Kim Jong-Hyun (Relator) (7)Sr. Sim Dong-Hi (Relator asociado) (2)Sr. Zhang Chen (Relator asociado) (15)Sr. Casanovas Eduardo (Relator asociado) (4) |
| C5/17 | Medios técnicos para luchar contra el spam | GT 2/17 | Sr. Zhang Yanbin (Relator) (3)Sr. Kim ChangOh (Relator asociado) (3) |
| C6/17 | Aspectos de seguridad de los servicios y redes de telecomunicaciones y de la Internet de las cosas (17)  | GT 1/17 | Sr. Baek Jonghyun (Correlator) (3)Sra. Zuo Min (Correlatora) (14)Sr. Yan Junzhi (Correlator) (8)Sr. Lee Gunhee (Relator asociado) (9)Sr. Takahashi Takeshi (Relator asociado) (3)Sr. Yu Bo (Relator asociado) (3)Sra. Pazo Robles Maria Eugenia (Relator asociado) (4) |
| C7/17 | Servicios de aplicación seguros | GT 3/17 | Sr. Nah Jae Hoon (Relator) (3)Sra. Gao Feng (Relator asociado) (7)Sr. Liu Lijun (Relator asociado) (3) |
| C8/17 | Seguridad de la computación en la nube y la infraestructura de macrodatos (18)  | GT 3/17 | Sr. Wei Liang (Relator) (3)Sr. Sang-Woo Lee (Relator asociado) (9)Sr. McFadden Mark (Relator asociado) (5) |
| C9/17 | Telebiometría | GT 4/17 | Sr. Caras John George (Relator) (3)Sr. Li Kepeng (Relator asociado) (11)Sra. Wang Mengxi (Relator asociado) (12) |
| C10/17 | Mecanismos y arquitectura de la gestión de identidades | GT 4/17 | Sr. Barbir Abbie (Relator) (3)Sr. Park Keundug (Relator asociado) (3)Sr. Takechi Hiroshi (Relator asociado) (3)Sr. Xia Junjie (Relator asociado) (3) |
| C11/17 | Tecnologías genéricas (directorio, infraestructura de clave pública (PKI), infraestructura de gestión de privilegios (PMI), sintaxis de notación abstracta uno (ASN.1), identificadores de objeto (OID)) para el soporte de aplicaciones seguras | GT 4/17 | Sr. Lemaire Jean-Paul (Relator) (3)Sra. Kaddachi Olfa (Relator asociado) (18) |
| C12/17 | Lenguajes formales para software y pruebas de telecomunicaciones | GT 3/17 | Sr. Hogrefe Dieter (Relator) (3)Sr. Mussbacher Gunter (Relator asociado) (5)Sr. Duhalde Enacom Martin (Relator asociado)(4) |

Notas:

(1) Nombramiento el 5 de septiembre de 2019

(2) Nombramiento el 30 de enero de 2019

(3) Nombramiento el 30 de marzo de 2017

(4) Nombramiento el 30 de marzo de 2017, revocación el 29 de marzo de 2018

(5) Nombramiento el 6 de septiembre de 2017

(6) Nombramiento el 30 de marzo de 2017, revocación (reasignación) el 29 de marzo de 2018

(7) Nombramiento el 29 de marzo de 2018

(8) Nombramiento el 30 de enero de 2019

(9) Nombramiento el 7 de septiembre de 2018

(10) Nombramiento el 30 de marzo de 2017, revocación el 7 de septiembre de 2018

(11) Nombramiento el 30 de marzo de 2017, dimisión el 7 de septiembre de 2018

(12) Nombramiento el 6 de septiembre de 2017, revocación el 7 de septiembre de 2018

(13) Nombramiento el 30 de marzo de 2017, revocación en enero de 2019

(14) Nombramiento el 29 de marzo de 2018, dimisión el 30 de enero de 2019

(15) Nombramiento el 7 de septiembre de 2018

(16) Nombramiento el 6 de septiembre de 2017, revocación el 7 de septiembre de 2018

(17) Se sustituyó el nombre de la C6/17, "Aspectos de seguridad de los servicios y redes de telecomunicaciones", por "Aspectos de Seguridad de los servicios y redes de telecomunicaciones y de Internet de las cosas".

(18) Se sustituyó el nombre de la C8/17, "Seguridad de la computación en la nube", por "Seguridad de la computación en la nube y la infraestructura de macrodatos".

(19) Nombramiento válido antes del 20 de abril de 2021.

**2.2.2** Habida cuenta del retraso de la celebración de la AMNT-20 hasta marzo de 2022, en su reunión celebrada del 11 al 18 de enero de 2021 el GANT refrendó el nuevo conjunto de 12 Cuestiones que se muestra en el Cuadro 5A, acordadas por la CE 17 en su reunión de agosto/septiembre de 2020 (véase la [Circular TSB 295](https://www.itu.int/md/T17-TSB-CIR-0295/en)).

Cuadro 5A

Comisión de Estudio 17 – Cuestiones refrendadas por el GANT (desde el 18 de enero de 2021)

| Nuevo número | Título de la actual Cuestión | Situación | Número anterior | Título de la anterior Cuestión | GT | Relator (1) |
| --- | --- | --- | --- | --- | --- | --- |
| 1/17 | Estrategia de normalización y coordinación de la seguridad | Continuación | 1/17 | Coordinación de la seguridad en las telecomunicaciones/TIC  | GT 1/17 | Correlatores:– Sr. Elhaj Mohamed M. K– Sra. Ki JuheeRelatores asociados:– Sr. Najarian Paul– Sr. Senga Wataru– Sra. Wang Yiwen |
| 2/17 | Arquitectura de seguridad y seguridad de red | Continuación | 2/17 | Arquitectura y marco genérico de la seguridad | GT 2/17 | Correlatores:– Sra. Hu Zhiyuan– Sr. Oh Heung Ryong |
| 3/17 | Gestión de la seguridad de la información en las telecomunicaciones y servicios de seguridad | Continuación | 3/17 | Gestión de la seguridad de la información en las telecomunicaciones | GT 3/17 | Relatora:– Sra. Naganuma MihoRelatores asociados:– Sr. Min Jinghua – Sr. Mustafa Thaib  |
| 4/17 | Ciberseguridad y lucha contra el correo basura | Continuación de las Cuestiones 4/17 y 5/17 | 4/17 | Ciberseguridad | GT 3/17 | Correlatores:– Sr. Kim Jong-Hyun– Sr. Zhang YanbinRelator asociado:– Sr. Kim ChangOh |
| 5/17 | Medios técnicos contra el correo basura |  |  |
| 6/17 | Seguridad de los servicios de telecomunicaciones e Internet de las cosas | Continuación | 6/17 | Aspectos relativos a la seguridad de los servicios de telecomunicaciones, las redes e Internet de las cosas | GT 2/17 | Correlatores:– Sr. Baek Jonghyun – Sr. Yan JunzhiRelatores asociados:– Sr. Lee Gunhee– Sr. Takahashi Takeshi– Sr. Yu Bo  |
| 7/17 | Servicios de aplicación seguros | Continuación | 7/17 | Servicios de aplicación seguros | GT 4/17 | Relator:– Sr. Nah Jae Hoon Relatores asociados:– Sra. Gao Feng– Sr. Liu Lijun |
| 8/17 | Seguridad de la infraestructura de computación en la nube y macrodatos | Continuación | 8/17 | Seguridad de la infraestructura de computación en la nube y macrodatos | GT 4/17 | Relator:– Sr. Wei LiangRelator asociado:– Sr. McFadden Mark |
| 10/17 | Arquitectura y mecanismos de gestión de identidades y telebiometría | Continuación de las Cuestiones 9/17 y 10/17 | 9/17 | Telebiometría | GT 5/17 | Correlatores:– Sr. Barbir Abbie– Sr. Caras John GeorgeRelatores asociados:– Sr. Kim Jason– Sr. Park Keundug– Sr. Takechi Hiroshi– Sr. Xia Junjie |
| 10/17 | Arquitectura y mecanismos de la gestión de identidades |  |  |
| 11/17 | Tecnologías genéricas (Directorio, PKI, Lenguajes formales e Identificadores de objeto, entre otras) para aplicaciones seguras | Continuación de las Cuestiones 11/17 y 12/17 | 11/17 | Tecnologías genéricas (Directorio, Infraestructura de clave pública (PKI), infraestructura de gestión de privilegios (PMI), Notación de sintaxis abstracta 1 (ASN.1), Identificadores de objeto (OID)) para aplicaciones seguras | GT 5/17 | Relator:– Sr. Lemaire Jean–Paul Relator asociado:– Sr. Hogrefe Dieter |
| 12/17 | Lenguajes formales para software de telecomunicaciones y pruebas |  |  |
| 13/17 | Seguridad de los sistemas de transporte inteligente | Continuación | 13/17 | Aspectos de seguridad del sistema de transporte inteligente | GT 2/17 | Relator:– Sr. Lee Sang–Woo Relator Asociado:– Sr. Park Seungwook – Sra. Zhang Yi  |
| 14/17 | Seguridad de las tecnologías de libro mayor distribuido (DTL) | Continuación | 14/17 | Aspectos de seguridad de las tecnologías de libro mayor distribuido | GT 4/17 | Correlatores:– Sr. Kadobayashi Youki– Sra. Oh Kyeong HeeRelatores asociados:– Sra. Bai Xiaoyuan– Sra. Wang Ke |
| 15/17 | Seguridad en relación con las tecnologías incipientes, en particular la seguridad cuántica | Nueva  | – | – | GT 1/17 | Relator:– Sr. Sim DongheeRelatores asociados:– Sr. Kenyoshi Kaoru– Sr. Yoon ChunSeok– Sr. Zhang Chen |

(1) Nombramiento nuevo/prolongado en la reunión de la CE 17 del 20 al 30 de abril de 2021.

**2.2.3** durante este periodo se han adoptado las Cuestiones enumeradas en el Cuadro 5b.

CUADRO 5b

Comisión de Estudio 17 – Nuevas Cuestiones adoptadas y Relatores

| Cuestión | Nombre de la Cuestión | GT | Relator |
| --- | --- | --- | --- |
| C13/17 | Aspectos de seguridad de los sistemas de transporte inteligentes **(10)**/Seguridad de los sistemas de transporte inteligentes (STI) **(11)** | GT 1/17(10)GT2/17(11) | Sr. Lee Sang-Woo (Relator) (1)Sr. Park Seungwook (Relator asociado) (1)Sra. Zhang Yi (Relatora asociada) (2) |
| C14/17 | Aspectos de seguridad de las tecnologías de libro mayor distribuido **(10)** Seguridad de las tecnologías de libro mayor distribuido (DLT) **(11)** | GT 2/17(10)GT 3/17(11) | Sr. Kadobayashi Youki (Correlator) (3)Sra. Oh Kyeong Hee (Correlatora) (3)Sra. Bai Xiaoyuan (Relatora asociada) (4)Sra. Wang Ke (Relatora asociada) (4) Sra. Zuo Min (Relatora asociada) (5) |
| C15/17 | Seguridad en relación con las tecnologías incipientes, en particular la seguridad cuántica | GT 1/17**(11)**  | Sr. Sim Dong-hi (Relator) (6)Sr. Kenyoshi Kaoru (Relator asociado) (7)Sr. Yoon Chun Seok (Relator asociado) (8)Sr. Zhang Chen (Relator asociado) (9) |

Notas:

(1) Nombramiento el 30 de marzo de 2017

(2) Nombramiento el 7 de septiembre de 2018

(3) Nombramiento el 6 de septiembre de 2017

(4) Nombramiento el 29 de marzo de 2018

(5) Nombramiento el 6 de septiembre de 2017, revocación (reasignación) el 29 de marzo de 2018

(6) Nombramiento el 20 de abril de 2021

(7) Nombramiento el 20 de abril de 2021

(8) Nombramiento el 20 de abril de 2021, responsable de la incubación

(9) Nombramiento el 20 de abril de 2021

(10) 2017-2020

(11) 2021-2022.

**2.2.4** Durante el periodo de estudios considerado se fusionaron las Cuestiones que figuran en la lista del Cuadro 6 con otras Cuestiones de la CE 17.

CUADRO 6

Comisión de Estudio 17 – Cuestiones suprimidas

| Cuestión | Título de la Cuestión | Relator | Resultados |
| --- | --- | --- | --- |
| C5/17 (suprimida) | Medios técnicos contra el correo basura | Sr. Zhang Yanbin (Relator)Sr. Kim ChangOh(Relator asociado) | La C5/17 se fusionó con la C4/17 el 18 de enero de 2021 con el beneplácito del GANT. |
| C9/17 (suprimida) | Telebiometría | Caras John George (Relator) | La C9/17 se fusionó con la C10/17 el 18 de enero de 2021 con el beneplácito del GANT. |
| C12/17 (suprimida) | Lenguajes formales para software de telecomunicaciones y pruebas | Sr. Hogrefe Dieter (Relator)Sr. Mussbacher Gunter(Relator asociado) | La C12/17 se fusionó con la C11/17 el 18 de enero de 2021 con el beneplácito del GANT. |

# 3 Resultados de los trabajos realizados durante el periodo de estudios 2017-2020

## 3.1 Generalidades

Durante el periodo de estudios considerado, y hasta su reunión virtual del 7 de enero de 2022, la Comisión de Estudio 17 examinó un gran número de contribuciones, DT y declaraciones de coordinación.

Sobre la base de esos documentos, hasta el 7 de enero de 2022, la Comisión de Estudio 17:

– elaboró 53 nuevas Recomendaciones AAP y 47 nuevas Recomendaciones TAP (3 Recomendaciones TAP determinadas);

– revisó 93 Recomendaciones AAP y 3 Recomendaciones TAP existentes;

– enmendó 4 Recomendaciones;

– elaboró 8 nuevos Suplementos, revisó un Suplemento y preparó un corrigéndum para un Suplemento existente;

– elaboró 17 Corrigenda Técnicos;

– elaboró 2 Documentos Técnicos y 6 Informes Técnicos (no se elaboró ningún Manual).

A lo largo del periodo de estudios, y hasta su reunión virtual de 7 de enero de 2022, la CE 17:

– atrajo a 2 163 participantes (2 063 + 100) (reuniones anteriores: 100, 223, 231, 91, 262, 69, 225, 206, 178, 168, 130, 134, 146);

– creó 162 nuevos temas de trabajo (reuniones anteriores: 7, 15, 0, 15, 7, 26, 13, 25, 21, 26, 7);

– recibió 1 179 contribuciones (reuniones anteriores: 1, 98, 104, 2, 110, 121, 151, 118, 144, 113, 106, 78);

– elaboró 4 220 DT (reuniones anteriores: 106, 336, 305, 44, 434, 35, 439, 508, 380, 420, 395, 426, 368);

– recibió 585 declaraciones de coordinación y envió 328 declaraciones de coordinación (reuniones anteriores: 55+1, 51+23, 36+17, 21+0, 58+32, 1+2, 77+24, 64+42, 47+30, 40+37, 46+37, 49+40, 40+38).

## 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) C1/17, Coordinación de la seguridad en las telecomunicaciones/TIC (2017‑2020)/Estrategia de normalización y coordinación de la seguridad (2021-)

La C1/17 es la coordinadora para los temas de coordinación de la seguridad en las telecomunicaciones TIC de la CE 17 con otras comisiones de Estudio y organizaciones externas. La C1/17 también elabora y actualiza diversos documentos de divulgación 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 C1/17 preparó la 7ª edición.

– El Informe Técnico *Successful Use of Security Standards* se centra en cómo aplicar satisfactoriamente las Recomendaciones UIT-T sobre seguridad aprobadas. Se consideran Recomendaciones individuales (como UIT-T X.805) y familias de Recomendaciones (como CYBEX) y se describen los beneficios que puede reportar su utilización. Durante este periodo de estudios, la C1/17 preparó la 2ª edición.

– El *Plan de Trabajo sobre Normas de Seguridad de las TIC* contiene una base de datos en línea donde se pueden consultar más de 2 600 normas sobre seguridad de las TIC aprobadas por las Comisiones de Estudio del UIT-T y otros organismos de normalización externos, incluidos 3D@home, 3GPP, 3GPP2, ATIS, ETSI, IEEE, IETF, ISO/IEC JTC 1, OASIS, oneM2M, SmartBan y TETRA. Durante este periodo de estudios, la C1/17 aprobó numerosas actualizaciones.

– El *Compendio de Recomendaciones sobre seguridad,* que contiene en su Parte I un catálogo de Recomendaciones UIT-T aprobadas que guardan relación con la seguridad en las telecomunicaciones y en su Parte II un extracto de las definiciones de seguridad aprobadas por el UIT-T. El Compendio se actualizó en cada una de las reuniones celebradas durante este periodo de estudios.

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.

La C1/17 también fomentó la celebración de talleres sobre seguridad, prestó apoyo a dos Grupos Regionales de la CE 17 (África y Estados Árabes) e hizo más eficaz el trabajo de la CE 17 creando plantillas, herramientas y procedimientos. A lo largo del periodo de estudios, la C1/17 ha contribuido a celebrar 13 talleres de la UIT hasta finales de 2021.

b) C2/17, Arquitectura y marco genérico de la seguridad (2017-2020)/Arquitectura de seguridad y seguridad de red (2021-)

La C2/17 se dedica a definir una arquitectura de seguridad global y a elaborar Recomendaciones marco para normalizar las soluciones de seguridad de las telecomunicaciones. Se trata, por ejemplo, de la seguridad de la 5G, de los marcos de seguridad para la interconexión de redes definida por software, la evolución a largo plazo y la virtualización de red.

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

– X.1011, *Directrices para la protección continua del proceso de acceso al servicio*,analiza las amenazas a la seguridad del proceso de acceso al servicio, especifica medidas de protección de la seguridad para detectar actividades anormales de acceso y presenta un mecanismo de autorización mejorado para el acceso al servicio.

– X.1040, *Arquitectura de seguridad de referencia para la gestión de la vida útil de los datos corporativos del comercio electrónico*, analiza las principales características de los ecosistemas del servicio de comercio electrónico, las amenazas que suelen afrontar, y presenta una arquitectura de referencia para la gestión de la vida útil de los datos corporativos del comercio electrónico.

– X.1041, *Marco de seguridad para la operación de redes de voz por evolución a largo plazo,* analiza las amenazas de seguridad que afrontan las redes VoLTE y recomienda a los operadores de telecomunicaciones contramedidas para garantizar un funcionamiento seguro. También se presenta un marco de seguridad de referencia para las redes VoLTE.

– X.1043, *Marco y requisitos de seguridad para el encadenamiento de funciones de servicio basado en redes definidas por software*, analiza las amenazas de seguridad y define los requisitos de seguridad para el encadenamiento de funciones de servicio basado en redes definidas por soportes lógicos (SDN). También se indican las correspondientes contramedidas de seguridad. La Recomendación X.1043 tiene por objeto facilitar la comprensión de los riesgos de seguridad que surgen al utilizar el encadenamiento de funciones de servicio basado en SDN y la implantación de cadenas de funciones seguras de servicios basadas en SDN.

– X.1044, *Requisitos de seguridad de la virtualización de la red,* se analizan los retos y amenazas de seguridad para la virtualización de redes (NV) y se especifican los requisitos de seguridad para la capa de recursos físicos, la capa de recursos virtuales y la capa de partición lógica de red aislada (LINP) en la virtualización de redes.

– X.1045, *Arquitectura de la cadena de servicios de seguridad para redes y aplicaciones,* describe la prestación de servicios de seguridad dinámicos y adaptables personalizados para redes y aplicaciones. En esta Recomendación se define la cadena de servicios de seguridad y un diseño de arquitectura para la cadena de servicios de seguridad. La presente Recomendación aplica la cadena de servicio de seguridad a las redes y aplicaciones. La presente Recomendación también permite rastrear los ataques de red a sus recursos en una red solapada de la cadena de función de servicio (SFC) de elevada calidad de funcionamiento y mitigar/impedir automáticamente dichos ataques.

– X.1046, *Marco de seguridad definida por software en redes definidas por software/redes de virtualización de las funciones de red*, especifica un marco de seguridad definida por software para redes definidas por software (SDN) y redes de virtualización de las funciones de red (NFV). En esta Recomendación se analizan los principales problemas de seguridad, incluso técnicos y operativos, de las redes SDN/NFV de los operadores. En la Recomendación se definen los requisitos de seguridad necesarios para afrontar esos problemas en las redes SDN/NFV. Se introduce el concepto de "seguridad definida por software" y se diseña un marco de "seguridad definida por software". Esta Recomendación permite la implementación de la seguridad definida por software.

– X.1047, *Requisitos y arquitectura de seguridad para la gestión y la orquestación de la segmentación de redes,* establece los requisitos y la arquitectura de seguridad para la gestión y la orquestación de la segmentación de redes, así como la creación automática de segmentos de red de extremo a extremo (E2E) con capacidades de seguridad personalizadas, a fin de desplegar a gran escala la segmentación de redes E2E para segmentos gubernamentales, empresariales y de consumo.

– X.Suppl.30, *UIT-T X.805 – Directrices de seguridad para redes móviles virtuales*, presenta directrices de seguridad para los operadores de redes móviles virtuales (MVNO). La seguridad es muy importante para los MVNO y gran parte de ellos tienen problemas de seguridad semejantes. En este Suplemento se analizan las principales características de los MVNO y las amenazas de seguridad que suelen afrontar. A partir de la estructura de los MVNO, este Suplemento define un marco de seguridad para los MVNO, incluidos sus objetivos y requisitos de seguridad.

c) C3/17, Gestión de la seguridad de la información en las telecomunicaciones (2017‑2020)/Gestión de la seguridad de la información en las telecomunicaciones y servicios de seguridad (2021-)

La C3/17 prepara Recomendaciones sobre la gestión de la seguridad de la información en las telecomunicaciones, como códigos de práctica sobre IIP, organizaciones de telecomunicaciones y organizaciones de telecomunicaciones de pequeño y mediano tamaño.

A lo largo del periodo de estudios considerado la C3/17 ha elaborado cinco nuevas Recomendaciones, un corrigéndum, tres nuevos Suplementos y dos revisados:

– Corrigéndum 1 de la 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.

– X.1052 (revisada), *Procesos de gestión de la seguridad de la información para organizaciones de telecomunicaciones,* proporciona prácticas idóneas sobre gestión de la seguridad de la información a organizaciones de telecomunicaciones con el propósito de aplicar la Recomendación UIT-T X.1051. Esta Recomendación se basa en una metodología que describe un conjunto de aspectos en materia de gestión de la seguridad a fin de facilitar directrices para que las organizaciones de telecomunicaciones cumplan los objetivos de control fijados en la Recomendación UIT-T X.1051. Los aspectos de gestión de la seguridad que se describen incluyen la gestión de activos, incidentes, riesgos y políticas con objeto de asignar los controles definidos por la Recomendación UIT-T X.1051 a las metodologías de aplicación.

– X.1053, *Código de prácticas sobre controles de seguridad de la información basada en la Recomendación UIT-T X.1051 para organizaciones de telecomunicaciones de pequeño o mediano tamaño,* establece directrices y principios generales para iniciar, aplicar, mantener y mejorar los controles de seguridad de la información en las organizaciones de telecomunicaciones de pequeño y medio tamaño, de conformidad con la Recomendación UIT-T X.1051. Esta Recomendación proporciona además 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.

– X.1058, *Tecnología de la información – Técnicas de seguridad – Código de prácticas relativo a la protección de la información de identificación personal*, establece objetivos de control, controles y directrices para la implementación de controles con la finalidad de cumplir los requisitos identificados por la evaluación de los riesgos e incidencias vinculados a la protección de la información de identificación personal (IIP). En particular, en la presente especificación se describen directrices basadas en ISO/CEI 27002, teniendo en cuenta los requisitos necesarios para el procesamiento de la IIP que puedan ser aplicables en el contexto de uno o más entornos de riesgo para la seguridad de la información de una organización.

– X.1059, *Guía de aplicación para las organizaciones de telecomunicaciones sobre la gestión de riesgos de sus activos accesibles a nivel mundial en redes basadas en el IP*, contiene orientaciones a las organizaciones de telecomunicaciones acerca la gestión de riesgos de sus activos accesibles a nivel mundial en las redes IP, activos que están expuestos directamente a piratas informáticos y a ataques. Estos activos también pueden estar conectados a los activos tradicionales (e incluso antiguos) de las redes de telecomunicaciones tradicionales, que pueden tener algunas vulnerabilidades a nivel de diseño difíciles de arreglar. Por consiguiente, resultaría práctico examinar todos los activos accesibles globalmente en las redes IP (AGIT) de una organización de telecomunicaciones en su conjunto, e introducir ciertos controles de seguridad específicos para reducir constantemente los riesgos generales y reforzar la seguridad general de los servicios y redes de telecomunicaciones.

– X.1060, *Marco para la creación y operación de un centro de ciberdefensa*, define el centro de ciberdefensa (CCD) como una entidad que desempeña un papel fundamental en toda organización para hacer frente a los riesgos de ciberseguridad. El marco describe los tres procesos que el CCD debe aplicar en la práctica, a saber, construcción, gestión y evaluación. También se indican los servicios que debe prestar la organización para aplicar medidas de ciberseguridad más específicas.

– X.1061, *Directrices para la adquisición de ciberseguros para proveedores de servicios de tecnologías de la información y la comunicación (TIC)*.En estas directrices para la adquisición de ciberseguros se explican la cobertura de los ciberseguros y los requisitos en materia de evaluación de riesgos de ciberseguridad, selección de asegurador, evaluación por el asegurador y evaluación del asegurador por las organizaciones que optan por los ciberseguros como método para hacer frente a los riesgos a fin de gestionar las consecuencias de un incidente de ciberseguridad.

– X.Suppl.13 (revisado), *UIT-T X.1051 – Guía del usuario de gestión de seguridad de la información*.

– X.Suppl.32, *UIT-T X.1058 – Código de práctica para la protección de información de identificación personal*, complementa la información presentada en UIT‑T X.1058 con orientaciones adicionales para la implementación de la protección de la información de identificación personal (IIP), que no figuran en UIT-T X.1058, pero pueden aplicar las organizaciones de telecomunicaciones para la protección de la IIP.

– X.Suppl.34, *UIT-T X.1051 – Código de práctica para controles de seguridad organizaciones de telecomunicaciones,* destaca y presenta un código de práctica para la gestión de la seguridad de la información y las redes elaborado por la industria de la información y la comunicación de Malasia sobre la base de la Recomendación
UIT-T X.1051.

– X.Suppl.36, *UIT-T X.1051 – Controles de seguridad esenciales para la gestión de la seguridad de redes e informaciones de las organizaciones de telecomunicaciones*, presenta las prácticas idóneas en materia de ciberseguridad para la gestión de la seguridad empleando controles de seguridad esenciales dentro del ámbito de aplicación de la Recomendación UIT-T X.1051. La utilización del marco de controles de seguridad esenciales (CSE) y de los correspondientes controles de seguridad esenciales es un apoyo y complemento de la Recomendación UIT-T X.1051.

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.

d) C4/17, Ciberseguridad (2017-2020)/Ciberseguridad y lucha contra el correo basura (2021-)

La C4/17 elabora Recomendaciones sobre marcos de ciberseguridad y define los requisitos que han de cumplir los proveedores de telecomunicaciones/TIC para asegurar su infraestructura y garantizar la seguridad de sus operaciones, además de intercambiar información de ciberseguridad. A lo largo de este periodo de estudios la C4/17 asumió también una función incubadora para abordar temas nuevos, como la seguridad en el entorno cuántico hasta 2020 y transfirió dicha función a la C15/17 en enero de 2021. También en enero de 2021, la C4/17 asumió las labores en curso sobre la lucha contra el correo basura, de las que hasta entonces se había ocupado la C5/17.

Durante el periodo de estudios considerado, la C4/17 ha elaborado 14 nuevas Recomendaciones, una Recomendación revisada, dos nuevas Enmiendas, dos nuevos Informes Técnicos y dos nuevos Documentos Técnicos:

– X.1212, *Consideraciones de diseño para la mejor percepción por el usuario extremo de los indicadores de fiabilidad,* describen las consideraciones de diseño para la mejor percepción por el usuario extremo de los indicadores de fiabilidad. En los apéndices se describen técnicas representativas para medir la percepción por el usuario extremo de esos indicadores*.*

– X.1213, *Capacidades de seguridad necesarias para luchar contra las redes robot en teléfonos inteligentes,* analizan el origen y las amenazas de seguridad que pueden plantear las redes robot en teléfonos móviles y se exponen las capacidades de seguridad necesarias para luchar contra ellas.

*–* X.1214, *Técnicas de evaluación de la seguridad en redes de telecomunicaciones /tecnologías de la información y la comunicación*, describe una metodología de evaluación de la seguridad de elementos de redes de telecomunicaciones/tecnologías de la información y la comunicación (TIC) basadas en software y presenta prácticas idóneas para creadores, fabricantes, operadores y expertos en seguridad del dominio de las telecomunicaciones para abordar la seguridad de sus elementos de software. Tanto las redes con conmutación de circuitos como las redes de paquetes tradicionales están expuestas a diversas amenazas y ataques, tanto internos como externos, dirigidos a diversas partes de las redes de telecomunicaciones/TIC. Para las redes de telecomunicaciones/TIC, esta Recomendación abarca tanto la detección de vulnerabilidades como la metodología de evaluación de la seguridad.

– X.1215, *Expresión estructurada de información sobre amenazas: casos de uso,* presenta varios casos de uso relativos a la manera de utilizar el lenguaje de expresión estructurada de información sobre amenazas (STIX) para la inteligencia de ciberamenazas (CTI) y la compartición de información.

– X.1216, *Requisitos para la obtención y preservación de pruebas de incidentes de ciberseguridad,* describe un procedimiento general para la investigación e intervención en caso de incidente de ciberseguridad. También se analizan las fuentes de las pruebas de incidentes de ciberseguridad y se especifican las capacidades que han de tener las herramientas empleadas para la obtención y preservación de esas pruebas durante la investigación. En esta Recomendación se especifican también requisitos de garantía de fiabilidad para esas herramientas, así como directrices para los diseñadores de herramientas para tal efecto.

– X.1217, *Directrices para la aplicación de la inteligencia sobre amenazas en la explotación de redes de telecomunicaciones*. Desde el punto de vista del operador de telecomunicaciones, por inteligencia sobre amenazas se entiende un conjunto de información organizada, analizada y depurada relativa a los ataques potenciales y reales que pueden amenazar a una organización. Esta inteligencia puede incluir también las motivaciones, intenciones, características y métodos de los atacantes, junto con su *modus operandi* o técnicas, tácticas y procedimientos. En el ámbito de la seguridad de las redes y de la información, la aparición de incidentes de ciberseguridad a gran escala e inesperados ha desencadenado la necesidad urgente de disponer de inteligencia sobre amenazas. La inteligencia sobre amenazas puede ayudar a la organización a reducir el riesgo y mejorar su seguridad general. Se ha definido una taxonomía, una gramática y una presentación unificadas de la inteligencia sobre amenazas, para que ésta pueda ser compartida por diferentes organizaciones. En esta Recomendación, tras un análisis general, se especifican directrices para aplicar la inteligencia sobre amenazas en la explotación de redes de telecomunicaciones.

– X.1218, *Requisitos y directrices para el análisis dinámico de programas malignos en un entorno aislado*. En los ataques avanzados, especialmente en las amenazas persistentes avanzadas (APT), los atacantes suelen utilizar *malware* desconocido para evitar ser detectados. Por ejemplo, un ataque específico basado en el envío de un correo electrónico de suplantación de identidad armado con *malware* desconocido puede lograr un resultado inicial satisfactorio con facilidad. Por tanto, para la detección de ataques avanzados, conviene prestar especial atención y tomar medidas de defensa que permitan detectar el *malware* desconocido. En la Recomendación UIT-T X.1218 se analizan amenazas relacionadas con el *malware* desconocido y se especifican requisitos de detección de malware desconocido partiendo de un análisis conductual dinámico.

– X.1233, *Directrices para contrarrestar los mensajes basura por mensajería instantánea,* establece directrices cuyo objetivo es ayudar a los proveedores y los usuarios de los servicios de mensajería instantánea (MI) a contrarrestar los mensajes basura por mensajería instantánea (SPIM). También se analizan supuestos de generación de mensajes basura en el ámbito de la mensajería instantánea, se especifican medidas técnicas y mecanismos que permiten a los proveedores de servicios de MI contrarrestar el SPIM y se definen medidas de supresión de emergencia para que los usuarios de MI puedan hacerle frente.

– X.1234, *Directrices para la lucha contra el spam en el servicio de mensajería multimedios,* describe directrices para la lucha contra el *spam* en el servicio de mensajería multimedios (MMS). Se analizan los casos típicos, las características y los métodos de reconocimiento del *spam* MMS, y se ofrece un marco técnico, flujos de trabajo y algunas tecnologías clave para el reconocimiento del *spam* MMS, con el fin de ayudar a los proveedores y a los usuarios del servicio MMS a luchar contra dicho *spam*.

– X.1235, *Tecnologías contra la suplantación de sitios web para las organizaciones de telecomunicaciones*, recomienda a las organizaciones de telecomunicaciones tecnologías para detectar a tiempo la suplantación de sitios web y proteger sus sitios web contra la suplantación.

– *Enmiendas* 11 y 12 de X.1500, *Aspectos generales del intercambio de información de ciberseguridad*, facilita una lista de técnicas de intercambio de información estructurada sobre ciberseguridad, que se actualizará a medida que surjan nuevas técnicas o que las ya existentes evolucionen, se amplíen o se sustituyan. La lista se ajusta a lo estipulado en el cuerpo de la Recomendación. Estas enmiendas reflejan la situación de las técnicas recomendadas en marzo de 2017 y marzo de 2018, respectivamente, e incluyen referencias bibliográficas.

– X 1541 (revisada), *Formato para el intercambio de descripciones de objetos de incidentes, versión 2*, describe el modelo de información para el formato de intercambio de descripciones de objetos de incidentes (IODEF), versión 2, y facilita un modelo de datos asociado especificado con un esquema XML. El IODEF define una representación de modelo de datos para compartir la información sobre seguridad informática u otro tipo de incidentes comúnmente intercambiada. Esto se consigue enumerando las cláusulas pertinentes de IETF RFC 7970, indicando si son de carácter normativo o informativo.

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

– X.1702, *Arquitectura de un generador de números aleatorio de ruido cuántico*, define una arquitectura funcional genérica de una fuente de entropía cuántica, un método común para estimar y validar la entropía de una fuente de ruido objeto de evaluación y un método común para especificar extractores de aleatoriedad cuando forman parte del sistema implementado.

– X.1710, *Marco de seguridad para redes de distribución de claves cuánticas*, especifica un marco que incluye requisitos y medidas para hacer frente a las amenazas de seguridad en redes de distribución de claves cuánticas (QKDN). Se establece una estructura QKDN simplificada para analizar las amenazas de seguridad pertinentes. Sobre esa base se especifican los requisitos de seguridad y las correspondientes medidas que cabe adoptar para garantizarla.

– X.1714, *Combinación de claves y suministro de claves confidenciales para redes de distribución de claves cuánticas*, describe métodos de combinación de claves para redes de distribución de claves cuánticas (QKDN) y especifica los requisitos de seguridad tanto para la combinación de claves como para el suministro de claves, que abarcan las QKDN y las aplicaciones criptográficas.

– TP.inno, *Description of the incubation mechanism and ways to improve it*, describe el mecanismo de incubación completo definido por la CE 17 y se documentan otros métodos y mecanismos utilizados por la UIT y otras organizaciones de normalización para aceptar la innovación.

– TP.sgstruct, *Strategic approaches to the transformation of security studies,* abarca los aspectos a corto, medio y largo plazo de la transformación de los estudios de seguridad.

– TR.sec-qkd, *Security considerations for quantum key distribution network,* define un marco QKD para satisfacer los requisitos desde el punto de vista de la red de telecomunicaciones.

– TR.usm, *Unified Security Model (USM) – a neutral integrated system approach to cybersecurity*, preenta una arquitectura "de seguridad global", neutra en todos sus aspectos. Ofrece la posibilidad de facilitar la interoperabilidad masiva del control de seguridad y la automatización de las intervenciones de seguridad.

Durante este periodo de estudios la C4/17 celebró, el 24 de enero de 2019, en Ginebra, un minitaller sobre comunicaciones cuánticas seguras.

e) C5/17, Medios técnicos contra el correo basura (2017-2020)

La C5/17 elabora Recomendaciones para luchar con medios técnicos contra el correo basura (spam), como el spam publicitario, el spam en mensajería instantánea, el spam publicitario en aplicaciones móviles, y definir contramedidas contra la pesca por el servicio de mensajes breves, los ataques de suplantación de identidad y los fraudes por servicio telefónico.

Durante el periodo de estudios considerado la C5/17 ha elaborado tres nuevas Recomendaciones y dos nuevos Suplementos:

– X.1232, *Marco técnico para contrarrestar el spam publicitario en la información generada por el usuario*, analiza los casos y las características del spam publicitario y se especifica un marco de referencia y flujos de procesos para ayudar a los proveedores de servicios de Internet a contrarrestar el spam*.*

– X.1248, *Requisitos técnicos para contrarrestar el spam por mensajería instantánea,* indican las características del spam por mensajería instantánea (SPIM) y se especifican los requisitos técnicos para contrarrestarlo. A medida que aumenta la popularidad de la mensajería instantánea (IM), la proliferación de SPIM se ha convertido en un problema cada vez más grave. Las características de la IM, por ejemplo que se basa en el protocolo Internet (IP) que se utiliza de manera generalizada y gratuita, hacen que potencialmente el SPIM se propague generalizada e incontroladamente. Si no se resuelven meticulosamente los problemas de SPIM, éste tendrá consecuencias negativas sobre la utilización del servicio IM propiamente dicho.

– X.1249, *Marco técnico para contrarrestar el spam publicitario en aplicaciones móviles,* describe un marco técnico para contrarrestar el spam publicitario en aplicaciones móviles. Por spam publicitario en aplicaciones móviles se entiende el envío de anuncios no solicitados que se muestran dentro de una aplicación de teléfono móvil. Esta publicidad no solicitada aparece en la pantalla del dispositivo en un cartel situado en la parte superior o inferior de la pantalla, en pantalla completa o superpuestos

– X.Supl.29, *UIT-T X.1242 – Directrices sobre contramedidas frente a ataques de suplantación de identidad por servicio de mensajes breves (SMS)*, presenta unas directrices universales sobre la pesca por el servicio de mensajes breves (SMS), que es una técnica de fraude por suplantación de identidad que utiliza la telefonía móvil para adquirir información personal a partir de los teléfonos inteligentes o permite que se apruebe el cobro de pequeñas cantidades de dinero sin que el titular sea consciente de haber dado dicha aprobación.

– X.Supl.33, *UIT-T X.1231 – Marco técnico para la lucha contra estafas en el servicio telefónico*, presenta un marco técnico, y las correspondientes prácticas idóneas, para luchar contra las estafas en el servicio telefónico. En este marco se especifican las funciones de la entidad y los procedimientos de procesamiento. Las prácticas idóneas son aquellas que han demostrado ser más eficaces a la hora de luchar contra las estafas en el servicio telefónico.

f) C6/17, Aspectos relativos a la seguridad en los servicios y redes de telecomunicaciones e Internet de las cosas (2017-2020)/Seguridad de los servicios de telecomunicaciones e Internet de las cosas (2021-)

La C6/17 elabora Recomendaciones sobre requisitos y marcos de seguridad para servicios de telecomunicaciones, redes móviles, redes de distribución eléctrica inteligentes, TVIP e Internet de las cosas.

Durante el periodo de estudios considerado, la C6/17 ha elaborado 17 nuevas Recomendaciones, una Enmienda y un Corrigéndum de un Suplemento existente:

– X.1042, *Servicios de seguridad que utilizan las redes definidas por software*, permite la protección de los recursos de red mediante la utilización de servicios de seguridad basados en las redes definidas por *software* (SDN). En la presente Recomendación se procede, en primer lugar, a la clasificación de los recursos de red para los servicios de seguridad basados en las redes SDN, a saber, la aplicación SDN, el controlador SDN, el conmutador SDN y el administrador de seguridad (SM). Después, la Recomendación UIT-T X.1042 define los servicios de seguridad basados en las SDN.

– X.1126,*Directrices para la mitigación de los efectos negativos de los terminales infectados en las redes móviles,* proporciona directrices a los operadores móviles para limitar el número de terminales infectados en las redes móviles mediante la utilización de tecnologías que protejan tanto a los abonados como a los operadores móviles.

– X.1127, *Requisitos de seguridad y arquitecturas funcionales para las medidas de lucha contra el robo de teléfonos móviles,* se centra en los requisitos funcionales de seguridad y la arquitectura funcional para los mecanismos contra el robo de teléfonos inteligentes basados en los requisitos generales descritos por la Global System Mobile Association (GSMA).

– Enmienda 1 de X.1197, *Directrices sobre criterios para la selección de algoritmos criptográficos para la protección de los servicios y contenidos de TVIP*, actualiza los Apéndices I y II para reflejar la situación a agosto de 2019 e incluye referencias bibliográficas.

– X.1331, *Directrices de seguridad para dispositivos de redes domésticas (HAN) en sistemas eléctricos inteligentes,* presenta un análisis de las amenazas a la HAN en las redes inteligentes, los requisitos de seguridad y las funciones de seguridad. Dado que cada dispositivo HAN desempeña una función y un papel diferentes, se facilitan los requisitos de seguridad y las funciones de seguridad para cada tipo de dispositivo.

– X.1332*, Directrices de seguridad para servicios de medición inteligentes en redes inteligentes,* establece directrices de seguridad para los servicios de medición inteligentes a fin de que los proveedores de servicios puedan poner en marcha medidas de seguridad adecuadas que garanticen la seguridad del servicio. Se analiza el modelo general del servicio de medición inteligente desde la perspectiva del nivel de servicio. Sobre la base del modelo general, en la Recomendación se contemplan las amenazas a la seguridad de los servicios de medición inteligentes y los métodos de ataque contra dichos servicios, y se especifican los requisitos y las capacidades en materia de seguridad para mitigar esos riesgos. Además, en esta Recomendación se introducen normas de seguridad útiles, que el proveedor de servicios podrá tomar en consideración a la hora de implementar las capacidades de seguridad.

– X.1333, *Directrices de seguridad para la utilización de herramientas de acceso remoto en sistemas de control conectados a Internet*, presenta una visión completa para la utilización segura de las HAR a efectos de supervisión, control y mantenimiento.

– X.1361, *Marco de seguridad para la Internet de las cosas basado en el modelo de pasarela,* describe un marco de seguridad para la Internet de las cosas (IoT) utilizando pasarelas de seguridad. La Internet de las cosas (IoT) es la infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) sobre la base de tecnologías de la información y comunicación compatibles existentes o en fase de desarrollo. En la presente Recomendación se analizan las amenazas y los problemas de seguridad en un entorno de Internet de las cosas y se describen las capacidades con las que se podrían abordar y reducir esas amenazas y resolver esos problemas. Se facilita una metodología marco para determinar qué capacidades de seguridad se necesitan para abordar y reducir esos problemas y amenazas en la Internet de las cosas.

– X.1362*, Procedimiento de encriptación simple para la Internet de las cosas (IoT)*,especifica la encriptación con datos de máscara asociados (EAMD) para los dispositivos de la Internet de las cosas. Además, describe la EAMD y el modo en que ésta proporciona una serie de servicios de seguridad a los efectos de tráfico de datos.

– X.1363*,* *Marco técnico para el tratamiento de la información de identificación personal en el contexto de la Internet de las cosas*, especifica un marco técnico para la gestión de la IIP en un entorno de IoT con uno o múltiples proveedores de servicios.

– X.1364*, Requisitos y marco de seguridad de la Internet de las cosas de banda estrecha*,especifica los riesgos y requisitos específicos que conlleva el despliegue de la NB-IoT y se establece un marco de seguridad que pueden aplicar los operadores para proteger las nuevas aplicaciones de la tecnología NB-IoT*.*

– X.1365*,* *Metodología de seguridad para el uso de criptografía basada en la identidad para dar soporte a servicios de Internet de las cosas mediante redes de telecomunicaciones,* proporciona una metodología de seguridad para el uso de la tecnología de clave pública IBC en apoyo de los servicios de IoT a través de las redes de telecomunicaciones, incluidos los mecanismos de gestión de identidades, la arquitectura de gestión de claves, las operaciones de gestión de claves y la autentificación.

– X.1366*, Sistemas de autentificación de mensajes combinados para la Internet de las cosas,* especifica dos sistemas de autentificación de mensajes. El primero es elsistema de autentificación de mensajes combinados (AMA) para la IoT, que es el mecanismo básico. El otro es un sistema de autentificación interactiva de mensajes combinados (IAMA), dotado de un protocolo interactivo simple y seguro. Ambos sistemas de autentificación de mensajes combinados pueden aplicarse para garantizar tanto la "autentificación (de la identidad) de las entidades", como la "autentificación de los mensajes".

– X.1367, *Formato normalizado para los registros de errores de Internet de las cosas (IoT) utilizado en las operaciones de incidentes de seguridad*, especifica un formato normalizado de registro de errores que puede utilizarse en una carga útil de protocolo, como un *syslog* (véase IETF RFC 5424) para convertir la información de un registro de errores emitida por un dispositivo periférico al formato normalizado de registro de errores. En esta Recomendación también se especifica un cuadro de códigos de error normalizados para resolver el segundo problema. De este modo se pueden gestionar de manera integral los incidentes de seguridad en las redes informáticas y en las redes de dispositivos periféricos de la IoT.

– X.1368, *Actualización segura del firmware o software para dispositivos de Internet de las cosas*. especifica: 1) modelos y procedimientos básicos para actualizar con seguridad el firmware o el software (FW/SW) de los dispositivos de Internet de las cosas (IoT), y 2) requisitos y capacidades para actualizar el FW de la IoT.

– X.1369, *Requisitos de seguridad para las plataformas del servicio IoT,* especifica los requisitos de seguridad para las plataformas del servicio de la IoT. Se analizan las amenazas y los riesgos de seguridad para las plataformas de servicio del negocio de la IoT y se describen medidas de seguridad que pueden mitigar las amenazas y los riesgos de seguridad.

– X.1453, *Amenazas y requisitos de seguridad para sistemas de gestión de vídeo,* analiza las amenazas de seguridad a VMS (sistema de gestión de vídeo) que funcionan en plataformas de servidores, a través de conexión a una red IP, y se especifican los requisitos de seguridad para hacer frente a amenazas de seguridad específicas.

– X.1811, *Directrices de seguridad para la aplicación de algoritmos de seguridad cuántica en sistemas IMT-2020,* identifica las amenazas que plantea la informática cuántica a los sistemas de telecomunicaciones móviles internacionales-2020 (IMT‑2020) mediante la evaluación del grado de seguridad de los algoritmos criptográficos utilizados actualmente. En esta Recomendación se examinan brevemente los algoritmos de seguridad cuántica, incluidos los de tipo simétrico y asimétrico, y se proporcionan directrices para aplicar los algoritmos de seguridad cuántica en los sistemas IMT-2020.

– X.Supl.26 Cor.1, *UIT-T X.1111 –* *Suplemento sobre la arquitectura funcional de seguridad para los servicios de red eléctrica inteligente que utilizan redes de telecomunicaciones*.

g) C7/17, Servicios de aplicación seguros

La C7/17 elabora Recomendaciones sobre los requisitos de seguridad de los servicios de aplicación seguros, como los servicios de valor añadido y los servicios tecnofinancieros.

Durante el periodo de estudios considerado, la C7/17 ha elaborado nueve nuevas Recomendaciones:

– X.1145, *Marco y requisitos de seguridad para las capacidades abiertas de servicios de telecomunicación*, se centra en un análisis de los requisitos de seguridad de las capacidades abiertas de servicios de telecomunicaciones y facilita un marco de seguridad.

– X.1146, *Directrices sobre garantía de protección de servicios de valor añadido prestados por operadores de telecomunicaciones*, presenta directrices de protección de seguridad para los servicios de valor añadido prestados por los operadores de telecomunicaciones. Además, de analizarse las hipótesis de servicio típicas, las amenazas de seguridad y los métodos de ataque, en esta Recomendación se ofrecen medidas técnicas para contrarrestar amenazas y ataques, lo que ayudará a los operadores a garantizar la seguridad de los servicios de valor añadido y también contribuirá a proteger los beneficios para los usuarios.

– X.1147, *Requisitos de seguridad y marco para el análisis de macrodatos en los servicios de Internet móvil,* analiza los requisitos de seguridad del análisis de macrodatos en los servicios de Internet móvil y se define un marco de seguridad.

– X.1148, *Marco del proceso de desidentificación para proveedores de servicios de telecomunicaciones*, describe un marco del proceso de desidentificación, con sus etapas operativas, y especifica los modelos de liberación de datos y las fases de datos del proceso de desidentificación para proveedores de servicios de telecomunicaciones sobre la base del modelo de vida útil de los datos y las funciones de los interesados.

– X.1149, *Marco de seguridad de una plataforma abierta para servicios de tecnología financiera,* describe una arquitectura de plataforma abierta para servicios de tecnología financiera o tecnofinancieros. También se especifican las amenazas y vulnerabilidades de la plataforma abierta y el procedimiento de uso de la API abierta para los servicios tecnofinancieros. Se especifican además los requisitos de seguridad de la plataforma abierta de servicios tecnofinancieros, desde el punto de vista de la empresa financiera y de la empresa tecnofinanciera. En el Apéndice pueden encontrarse casos de uso de la plataforma abierta propuesta.

– X.1450, *Directrices sobre autentificación híbrida y mecanismos clave de gestión en el modelo cliente-servidor,* contiene directrices para la autentificación híbrida y los mecanismos de intercambio de claves en el modelo cliente-servidor. El mecanismo subyacente sugiere la utilización de secretos compartidos y técnicas de clave pública para la autentificación y el intercambio de claves. En esta Recomendación se contemplan hipó tesis de servicio, además de amenazas de seguridad y los métodos para contrarrestar esos ataques.

– X.1451, *Identificación de riesgos para optimizar la autentificación,* especifica una función de identificación de riesgos en un sistema de servicio TIC como procesador previo, antes de invocar la función de autentificación. Ello permite al sistema de servicio de TIC optimizar la autentificación del usuario en función de los riesgos constatados. Con esta función específica de identificación de riesgos, el sistema de servicio de TIC puede escoger los mecanismos de autentificación que mejor se adapten sus usuarios y obtener múltiples beneficios, en particular: 1) mejorar la experiencia de los usuarios; 2) aumentar la capacidad y reducir el coste por transacción de la autentificación de los usuarios; 3) reducir el riesgo de falsificación de la identidad de los usuarios.

– X.1452, *Directrices sobre los servicios de seguridad prestados por operadores,* permite clasificar los posibles casos de utilización de los servicios de seguridad que prestan los operadores y analizar los requisitos específicos de dichos servicios, a fin de proporcionar directrices a los operadores para que garanticen y mejoren sus servicios de seguridad.

– X.1470, *Directrices de seguridad para el servicio de atención al cliente en línea por la web,* analiza las amenazas a la seguridad del servicio de atención al cliente en línea por la web desde tres puntos de vista: seguridad de la red, seguridad del sistema y seguridad del servicio. Se especifican las directrices de seguridad para el servicio de atención al cliente en línea por la web y sus correspondientes medidas de seguridad. También se proponen procedimientos de prueba para verificar que las medidas de seguridad satisfacen los requisitos de seguridad especificados*.*

h) C8/17, Seguridad de la infraestructura de la computación en la nube y los macrodatos

La C8/17 elabora Recomendaciones sobre las amenazas y requisitos de seguridad de la infraestructura de la computación en la nube y los macrodatos.

Durante este periodo de estudios, la C8/17 ha elaborado ocho Recomendaciones nuevas:

– X.1603, *Requisitos de seguridad de los datos para el servicio de control de la computación en la nube,* analiza los requisitos de seguridad de los datos para el servicio de control de la computación en la nube, que incluyen los requisitos de alcance de datos de control, la vida útil de los datos de control, los requisitos de seguridad de la adquisición de datos de control y los requisitos de seguridad del almacenamiento de datos de control*.*

– X.1604, *Requisitos de seguridad de la red como servicio (NaaS) en la computación en la nube,* analiza las amenazas y los problemas de seguridad para la red como servicio (NaaS) en la computación en la nube, y se especifican los requisitos de seguridad de la NaaS en los aspectos de la aplicación NaaS, la plataforma NaaS y la conectividad NaaS basados en los correspondientes tipos de capacidad en la nube.

– X.1605, *Requisitos de seguridad de la infraestructura pública como servicio (IaaS) en la computación en la nube*, pretende documentar los requisitos de seguridad de la IaaS pública a fin de ayudar a los proveedores de IaaS a mejorar la seguridad de la plataforma IaaS a lo largo de las fases de planificación, construcción y explotación.

– X.1606, *Requisitos de seguridad para el entorno de aplicación
Comunicaciones como servicio,* identifica las amenazas de seguridad y se recomiendan requisitos de seguridad para el entorno de aplicación Comunicaciones como servicio (CaaS). En esta Recomendación se describen las hipótesis de aplicación y las características de CaaS con capacidades multicomunicación. A continuación, se identifican las amenazas específicas que plantean las características únicas de CaaS y se recomiendan los requisitos de seguridad de CaaS correspondientes*.*

*–* X.1643, *Requisitos de seguridad y directrices para los contenedores de virtualización en entornos de computación en la nube,* analiza las amenazas y los desafíos de seguridad relativos a los contenedores en entornos de computación en la nube y se especifica un marco de referencia con directrices de seguridad para los contenedores de virtualización en la nube.

– X.1750, *Directrices sobre la seguridad de macrodatos como servicio
destinadas a los proveedores de servicios de macrodatos,* analiza los problemas de seguridad de macrodatos como servicio (BDaaS), se identifican las funciones y responsabilidades de seguridad para prestar el servicio BDaaS y se describe un marco de seguridad para la infraestructura de macrodatos. Asimismo, se especifican las medidas de protección de seguridad que se han de satisfacer para los servicios y componentes relacionados con el BDaaS*.*

– X.1751, *Directrices de seguridad sobre la gestión del ciclo vital de macrodatos destinadas a los operadores de telecomunicaciones*, analiza las vulnerabilidades de seguridad y se proporcionan directrices de seguridad sobre la gestión del ciclo vital de macrodatos destinadas a los operadores de telecomunicaciones. Se presentan las características específicas de los servicios de macrodatos y las categorías de datos en el ámbito de las telecomunicaciones, se analizan las vulnerabilidades de seguridad de la gestión de la vida útil de los macrodatos y especifican las directrices de seguridad para los operadores de telecomunicaciones.

– X.1752, *Directrices de seguridad para infraestructuras y plataformas de macrodatos,* analiza las amenazas y los riesgos de seguridad relativos a las infraestructuras y las plataformas de macrodatos y se especifica un marco de referencia para definir la correspondencia de las directrices de seguridad con las amenazas para dichas infraestructuras y plataformas de macrodatos.

– TR.XAASL, *Marco para la normalización de la seguridad de los servicios virtualizados,* es un documento para el debate sobre la elaboración de las premisas, requisitos y marcos de la normalización de servicios virtualizados.

i) C9/17, Telebiometría (2017-2020)

La C9/17 elabora Recomendaciones sobre telebiometría para la autentificación de los usuarios mediante telebiometría y para la protección de la información telebiométrica contra el acceso no autorizado.

Durante el periodo de estudios considerado, la C9/17 ha elaborado tres nuevas Recomendaciones, una Recomendación revisada y un Corrigéndum:

– X.1080.0 y X.1080.0 Cor.1, *Control de acceso para la protección de datos telebiométricos,* especifica cómo proteger la información telebiométrica contra el acceso no autorizado adoptando un enfoque orientado al servicio, donde sólo se facilita la información necesaria para un fin concreto, es decir, que el acceso no sólo se concede en función del derecho a saber, sino también en función de la necesidad de conocer. La piedra angular de esta Recomendación es una especificación de atributo, incluida en un certificado de atributo o certificado de clave pública, que especifica detalladamente qué privilegios posee una entidad concreta para uno o más tipos de servicios. La seguridad se da con un perfil de sintaxis de mensaje criptográfico (CMS), que garantiza la autentificación, la integridad y, cuando procede, la confidencialidad (encriptación). Este perfil está previsto para dar seguridad a las especificaciones telebiométricas en general. El perfil supone la correcta implantación de una infraestructura de clave pública (PKI) y, al mismo tiempo, depende de ella. Esta Recomendación también depende de la existencia de una infraestructura de gestión de privilegios (PMI)*.*

– X.1080.1 (revisada), *Cibersalud y telemedicinas mundiales – Protocolo de telecomunicaciones genérico*, define un marco para otras partes de la serie de Recomendaciones UIT-T 1080.x estableciendo un modelo global para los aspectos comunicativos de la telebiometría. Se establece la atribución básica de identificadores de objeto para identificar unívocamente elementos de información durante la transferencia de datos y se define un protocolo de telecomunicación genérico.
Se define una técnica para la especificación formal de objetos y se especifica un protocolo genérico que soporta las interacciones entre el centro médico local del paciente y un centro médico distante con mayor experiencia. Este protocolo se utilizará con otras partes de la serie de Recomendaciones UIT-T X.1080.x, que también podrán ampliarlo.

– X.1093, *Control de acceso telebiométrico con tarjetas e identidad inteligentes*, describe el esquema general para el control de acceso físico o lógico utilizando datos biométricos en una tarjeta. Esta Recomendación puede aplicarse al ámbito que está surgiendo recientemente empujado por la necesidad de una gestión segura del control de acceso físico y lógico.

– X.1094, *Autentificación telebiométrica mediante bioseñales*, especifica nuevos métodos de autentificación telebiométrica seguros y robustos que utilizan bioseñales.

j) C10/17, Arquitectura y mecanismos de la gestión de identidades (2017‑2020)/Arquitectura y mecanismos de gestión de identidades y telebiometría (2021-)

La C10/17 elabora Recomendaciones sobre temas relacionados con la gestión de identidades, incluidos marcos de autentificación. En enero de 2021, la C10/17 asumió los trabajos en curso sobre telebiometría de los que anteriormente se hacía cargo la C9/17.

Durante el periodo de estudios considerado, la C10/17 ha elaborado cinco nuevas Recomendaciones, dos Recomendaciones revisadas y un nuevo Suplemento:

– X.1080.2, *Protocolo biología a máquina (B2M)*, define un protocolo general para el intercambio de información biométrica entre el dispositivo del paciente y el dispositivo del médico a fin de poder controlar a los pacientes, y obtener información sobre ellos, a distancia desde los centros médicos.

– X.1252 (revisada), *Términos y definiciones de referencia para la gestión de la identidad,* contiene las definiciones de los principales términos utilizados en la gestión de la identidad (IdM). Los términos proceden de muchas fuentes y se utilizan corrientemente en el contexto de IdM. La presente Recomendación no tiene por objeto constituir un compendio exhaustivo de los términos relacionados con la IdM, sino más bien recopilar una lista básica de los términos que se consideran más importantes y que se utilizan habitualmente en el contexto de la IdM. En el Anexo A a la presente Recomendación se explican las razones por las que algunos de estos términos son tan importantes.

– X.1254 (revisada), *Marco de garantía de autentificación de entidad*, se definen tres niveles de garantía de autentificación de entidad (AAL) y los criterios y amenazas para cada uno ellos.

 Asimismo:

• se especifica un marco para la gestión de los AAL;

• se proporcionan directrices sobre las tecnologías de control que se deben utilizar para mitigar las amenazas a la autentificación, sobre la base de la evaluación de riesgos;

• se orienta sobre la correspondencia entre los tres AAL y otros planes de garantía de autentificación; y

• se facilita orientación para el intercambio de resultados de autentificación basados en los tres AAL.

– X.1276, *Protocolo y metadatos de establecimiento de autenticación, Versión 1.0*, propone patrones de arquitectura de elevación de confianza simples que exponen la utilización de la elevación de confianza en las arquitecturas de control de acceso modernas; describe los mecanismos y elementos de protocolo de un conjunto de metadatos común para el intercambio de información de elevación de confianza, y fomenta la utilización de los elementos de la elevación de confianza para facilitar su normalización en numerosas tecnologías y métodos actualmente utilizados para la reducción de riesgos de credenciales y autentificación.

– X.1277, *Marco de autentificación universal*, describe el marco de autentificación universal (UAF) FIDO que permite a los sitios web y los servicios en línea, ya sea en la Internet abierta o en de las empresas, aprovechar de manera transparente las funcionalidades de seguridad nativa de los dispositivos de computación de los usuarios finales, para una autentificación fuerte de usuario y para reducir los problemas asociados con la creación y memorización de muchas credenciales en línea.

– X.1278, *Protocolo cliente a autentificador/Marco Universal de 2 factores*, describe un protocolo de la capa de aplicación para la comunicación entre un autentificador externo y otro cliente/plataforma, así como la vinculación de ese protocolo de aplicación con varios protocolos de transporte que utilizan medios físicos diferentes.

– X.1279, *Marco de autenticación mejorada mediante telebiometría con mecanismos de detección antisuplantación,* describe un marco arquitectónico de autenticación mejorada mediante telebiometría con mecanismos de detección antisuplantación. Además, se analizan las amenazas a las soluciones tradicionales de autenticación telebiométrica y se especifican el marco arquitectónico, los flujos del proceso de autenticación y las consideraciones en materia de seguridad pertinentes para la autenticación mejorada mediante telebiometría con mecanismos de detección antisuplantación.

– X.Supl.35, *UIT-T X.1254 – Suplemento sobre casos de uso del marco de garantía de autentificación de entidades (EAA)*,contiene tres casos de uso del marco de garantía de autentificación de entidades en una implementación de seguridad y se incluyen consideraciones de seguridad pormenorizadas para la evaluación de riesgos, la elección del nivel de seguridad adecuado y la selección de tecnologías de autentificación.

En su Plenaria virtual celebrada el 29 de mayo de 2020, la CE 17 acordó asignar el número X.1261 a la Recomendación UIT-T D.1140, *Marco político con principios para la infraestructura de identidades digitales*, para su designación con doble signatura de las series D y X del UIT-T sobre gestión de identidades.

k) C11/17, Tecnologías genéricas (Directorio, infraestructura de clave pública (PKI), infraestructura de gestión de privilegios (PMI), notación de sintaxis abstracta uno (ASN.1), identificadores de objeto (OID)) para aplicaciones seguras (2017‑2020)/Tecnologías genéricas (Directorio, PKI, Lenguajes formales, Identificadores de objeto, entre otras) para aplicaciones seguras (2021-)

La C11/17 elabora Recomendaciones sobre los servicios y sistemas de directorio, incluidos los certificados de clave pública/atributos de la serie de Recomendaciones X.500. La C11/17 se encarga del mantenimiento de las Recomendaciones sobre ASN.1 y está trabajando en las Recomendaciones sobre OID, sistema mundial de identificación basado en autoridades de registro jerárquico, denominado "Árbol de identificador de objeto". En enero de 2021 la C11/17 asumió los trabajos en curso sobre lenguajes de los que anteriormente se hacía cargo la C12/17.

Durante el periodo de estudios considerado, la C11/17 ha elaborado cinco nuevas Recomendaciones, 20 Recomendaciones revisadas, una Enmienda y 14 Corrigenda técnicos a las Recomendaciones de las series X.500, X.680 y X.690 (X.680 Cor.1, X.680 Cor.2, X.680 Enm.1, X.680 Cor.3, X.681 Cor.1, X.682 Cor.1, X.682 Cor.2, X.683 Cor.1, X.693 Cor.1, X.694 Cor.1, X.696 Cor.1, X.696 Cor.2, X.696 Cor.3, X.893 Cor.1, X.894 Cor.1), un Suplemento y un nuevo Informe Técnico:

– X.500 (revisada), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Visión de conjunto de conceptos, modelos y servicios*, presenta los conceptos de directorio y de la DIB (base de información del directorio) y hace un repaso de los servicios y capacidades que se proporcionan.

– X.501 (revisada), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos*, presenta una serie de distintos modelos de directorio como marco para otras Recomendaciones UIT-T de la serie X.500. Los modelos son: general (funcional), de autoridad administrativa, genéricos de información de directorio con perspectiva de usuario de directorio y usuario administrativo sobre la información de directorio, genéricos de agente de sistema de directorio (DSA) y de información DSA, de marco operativo y de seguridad.

– Enm.1 a X.501, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos,* actualiza la cláusula 9.2 y el Anexo A.

– X.509 (revisada), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*, define un marco para los certificados de clave pública (PKI) y la infraestructura de gestión de privilegios (PMI). Introduce el concepto básico de técnica criptográfica asimétrica. Especifica los siguientes tipos de datos: certificado de clave pública, certificado de atributo, lista de revocación de certificados (CRL) y lista de revocación de certificados de atributo (ACRL). También define distintos certificados y extensiones CRL y define la información del esquema del directorio que permite almacenar los datos relacionados con PKI y PMI en el directorio. Además, define tipos de entidades, como la autoridad de certificación (CA), la autoridad de atributo (AA), la parte confiante, el verificador de privilegios, el intermediario de confianza y el ancla de confianza. Se especifican los principios de la validación de certificados, el trayecto de validación y la política de certificados, entre otras cosas. Se incluye una especificación de las listas de validación de autorización que permiten validar o restringir rápidamente las comunicaciones. Se incluyen los protocolos necesarios para el mantenimiento de las listas de validación de autorización y un protocolo para acceder al intermediario de confianza.

– Cor.1 de X.509, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*, corrige defectos en la cláusula 6.2.2 y el Anexo B.

– X.510, *Tecnología de la información – Interconexión de sistemas abiertos – El Directorio: especificación de protocolos para el funcionamiento seguro*, define un protocolo general, denominado protocolo envolvente, que se encarga de la ciberseguridad de los protocolos diseñados para la protección del protocolo envolvente mediante autentificación, integridad y, optativamente, confidencialidad (encriptación). El protocolo envolvente permite la prestación de ciberseguridad con independencia de los protocolos protegidos, lo que significa que la seguridad puede aumentarse sin menoscabo de la especificación del protocolo protegido.

– X.511 (revisada), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Definición de servicio abstracto*, define de manera abstracta los servicios exteriormente visibles que presta el directorio, incluidas las operaciones de vinculación y desvinculación, las operaciones de lectura, las operaciones de búsqueda, las operaciones de modificación, las operaciones que sustentan las políticas de contraseña y las operaciones que soportan el interfuncionamiento con LDAP. También se definen los errores.

– X.518 (revisada), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Procedimientos para operación distribuida*, especifica los procedimientos necesarios para un directorio distribuido formado por agentes del sistema de directorio (DSA) y servidores de protocolo ligero de acceso al directorio (LDAP), que interactúan para dar un servicio coherente a los usuarios, independientemente del punto de acceso utilizado. Se describen también procedimientos para la conversión de protocolo entre el protocolo de acceso al directorio/protocolo del sistema de directorio (DAP/DSP) y el protocolo LDAP.

– X.519 (revisada), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Especificaciones de protocolo*, especifica el protocolo de acceso al directorio, el protocolo de sistema del directorio, el protocolo de ocultación de información del directorio y el protocolo de gestión de la vinculación operativa del directorio, completando los servicios abstractos especificados en las Recomendaciones UIT-T X.501 | ISO/CEI 9594-2, UIT‑T X.511 | ISO/CEI 9594-3, UIT-T X.518 | ISO/CEI 9594-4 y UIT-T X.525 | ISO/CEI 9594-9. Se incluyen especificaciones para el soporte de protocolos subyacentes a fin de reducir la dependencia de especificaciones externas. Los protocolos pueden codificarse con todas las normas de codificación ASN.1 normalizadas.

– X.520 (revisada), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Tipos de atributos seleccionados*, define una serie de tipos de atributos y reglas de correspondencia que pueden ser útiles para una serie de aplicaciones del directorio. Un uso concreto de muchos de los atributos definidos es la formación de nombres, en particular para las clases de objetos definidas en la Recomendación UIT‑T X.521 | ISO/CEI 9594-7. Otros tipos de atributos, denominados atributos de notificación, ofrecen información de diagnóstico. En esta Recomendación | Norma internacional se definen tipos de contexto que ofrecen las características asociadas a los valores de atributo. Contiene además definiciones para las sintaxis LDAP pertinentes a los tipos de atributos y las reglas de correspondencia.

– X.521 (revisada), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Clases de objeto seleccionadas*, define una serie de clases de objetos y formas de nombre seleccionadas que pueden ser útiles para una serie de aplicaciones del directorio. Una definición de clase de objeto especifica los tipos de atributos pertinentes a los objetos de esa clase. Una definición de forma de nombre especifica los atributos que se utilizarán para formar los nombres de los objetos de una clase determinada.

– X.525 (revisada), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Replicación*, especifica un servicio oculto que el agente del sistema del directorio (DSA) puede utilizar para replicar la información del directorio. El servicio permite la replicación de la información del directorio entre varios DSA a fin de mejorar el servicio que se da a los usuarios, y prevé la actualización automática de esa información.

– X.676, *Marco de resolución basado en el identificador de objeto para servicios de IoT agrupados*, especifica un marco de resolución basado en el identificador de objeto (OID) para identificar diversos servicios en entornos de IoT. El OID es un identificador que denomina un objeto con un espacio nombre asignado jerárquicamente. En la Internet de las cosas (IoT) se facilitarán miles de servicios IoT basados en recursos heterogéneos como combinaciones de varios servicios. Para lograr la eficacia se necesitarán diversas tecnologías, como la vinculación de servicios, los servicios dinámicos y los servicios de cambio frecuente, además de la resolución y la identificación de servicios agrupados. En esta Recomendación se describen los conceptos de servicios IoT agrupados y las consideraciones, arquitecturas y procedimientos para un marco de resolución basado en OID para los servicios IoT agrupados.

– X.677, *Mecanismo de identificación para vehículos aéreos sin tripulante utilizando identificadores de objetos*, analiza los requisitos de gestión de la vida útil completa y el reconocimiento de la identidad operativa de aeronaves no tripuladas (ANT), habida cuenta de la seguridad. También se especifica un mecanismo de identificación de ANT mediante identificadores de objeto (OID) y se especifican detalladamente las reglas de asignación y los procedimientos de registro de los OID utilizados para los ANT.

– X.680 (revisada y su Enm.1 y Cor.1-3 previas a la revisión), *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica,* proporciona la notación denominada notación de sintaxis abstracta uno (ASN.1) para la definición de la sintaxis de datos de información. Define varios tipos de datos sencillos y especifica una notación para hacer referencia a esos tipos y especificar valores de los mismos.

– X.681 (revisada y su Cor.1 previa a la revisión), *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de objetos de información*, proporciona la notación de ASN.1 para definir y dar nombres de referencia a clases de objetos de información, así como a objetos de información individuales y conjuntos de los mismos. Una clase de objetos de información define la forma de una tabla conceptual (un conjunto de objetos de información) con una columna para cada campo de esa clase, y en el que cada fila completa define un objeto de información.

– X.682 (revisada y su Cor.2 previa a la revisión), *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de constricciones*, proporciona la notación ASN.1 para el caso general de la especificación de restricciones y excepciones que pueden limitar los valores de datos de un tipo de datos estructurado. La notación permite también señalizar si se viola una restricción y cuando se viola.

– X.683 (revisada y su Cor.1 previa a la revisión), *Tecnología de la información – Notación de sintaxis abstracta uno: Parametrización de especificaciones de notación de sintaxis abstracta uno*, define las disposiciones para nombres de referencia parametrizados y 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 pueden aplicarse a valores de tipos definidos utilizando la notación ASN.1. La aplicación de estas reglas de codificación produce una sintaxis de transferencia para estos valores. En la especificación de estas reglas de codificación está implícito que se utilizan también para la decodificación. Esta Recomendación | Norma Internacional define también un conjunto de reglas de codificación distinguida (DER) y un conjunto de reglas de codificación canónica (CER), y ambas proporcionan restricciones a las reglas de codificación básica (BER). La diferencia esencial entre ellas es que las DER utilizan la forma de longitud definida de las codificaciones, mientras que las CER utilizan la forma de longitud indefinida. Las DER son más adecuadas para los valores codificados pequeños, mientras que las CER son más adecuadas para valores grandes. En la especificación de estas reglas de codificación está implícito que se utilizan también para la decodificación.

– 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 de ASN.1 para lograr una representación mucho más compacta que la proporcionada por las reglas de codificación básicas (BER) y sus derivadas (descritas en la Recomendación UIT‑T X.690 | ISO/IEC 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 de ASN.1) que difieren de las que proporcionan las reglas de codificación normalizadas tales como las reglas de codificación básica (BER) y las reglas de codificación compactada (PER).

– X.693 (revisada y su Cor.1 previa a la revisión), *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Reglas de codificación del lenguaje de marcaje extensible*, especifica reglas para valores de la codificación de tipos de ASN.1 utilizando el lenguaje de marcaje extensible (XML, extensible markup language).

– X.694 (revisada y su Cor.1 previa a la revisión), *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 de notación de sintaxis abstracta uno (ASN.1, Abstract Syntax Notation One) con el fin de utilizar reglas de codificación ASN.1 –tales como reglas de codificación básica (BER, basic encoding rules), reglas de codificación distinguida (DER, distinguished encoding rules), reglas de codificación compactada (PER, packed encoding rules) o reglas de codificación XML (XER, XML encoding rules)– 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 paquetizada*, especifica las reglas de aplicación de las instrucciones de codificación PER (*packed encoding rules*) utilizando prefijos de tipo o una sección de control de codificación. La codificación de instrucciones es un mecanismo de modificación de las codificaciones de tipos ASN.1 para algunas reglas de codificación específicas (en este caso PER). Pueden insertarse en una especificación ASN.1 entre corchetes (como una etiqueta en las reglas de codificación básicas, BER) inmediatamente antes del tipo al que afectan (prefijos de tipo), o pueden recopilarse conjuntamente al final del módulo ASN.1 (una sección de control de codificación).

– X.696 (revisada y su Cor.1-3 previa a la revisión), *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 básicas de codificación y sus derivados (descritas en la Recomendación UIT-T X.690 | ISO/IEC 8825-1) y que las reglas de codificación compactada (descritas en la Recomendación UIT-T X.691 | ISO/IEC 8825 2).

– X.697, *Tecnología de la información – Reglas de codificación ASN.1: Especificación de las reglas de codificación de notificación de objeto de JavaScript (JER),* se define un conjunto de reglas de codificación de notificación de objeto de JavaScript (JER), que pueden utilizarse con miras a derivar una sintaxis de transferencia para los valores de los tipos definidos en las Recomendaciones UIT-T X.680 | ISO/IEC 8824-1, UIT-T X.681 | ISO/IEC 8824-2, UIT-T X.682 | ISO/IEC 8824-3 y UIT-T X.683 | ISO/IEC 8824-4. En la especificación de estas reglas de codificación está implícito que se utilizan también para la decodificación.

– Cor.1 de X.893 *Tecnología de la información – Aplicaciones genéricas de la notación de sintaxis abstracta uno: Seguridad del Infoset rápido,* contiene correcciones a los anexos informativos y a la bibliografía, en la que se suprimen las referencias al algoritmo triple DES, que ha quedado obsoleto.

– Cor.1 y Cor.2 de X.894, *Tecnología de la información – Aplicaciones genéricas de ASN.1 – Sintaxis de mensaje criptográfica,* presenta los módulos de notación de sintaxis abstracta uno (ASN.1) necesarios para utilizar la sintaxis criptográfica en las Recomendaciones UIT‑T. La sintaxis de mensaje criptográfica (CMS) ofrece los servicios de integridad de datos, confidencialidad, autenticidad del origen y no repudio necesarios para el intercambio de información fiable y la autentificación fuerte. También reúne una serie de técnicas de gestión de claves criptográficas para el soporte de mecanismos de establecimiento de claves flexibles, como la gestión de claves constructiva, el acuerdo de claves, el intercambio de claves y la encriptación por contraseña. Estas técnicas pueden emplearse para prevenir fraudes y para proteger la información de identificación personal e información sensible de otro tipo. Esta Recomendación | Norma Internacional soporta las técnicas de firma digital, encriptación y encriptación por signos basadas en la tecnología de clave pública definida en las Recomendaciones/normas multiparte de la serie UIT-T X.500 | ISO/IEC 9594. Se soportan todas las normas de codificación normalizadas para ASN.1.

– Z.161 (revisada), *Notación de pruebas y de control de prueba versión 3: Lenguaje núcleo de TTCN-3*, define la notación de pruebas y de control de pruebas 3 (TTCN-3) para la especificación de series de pruebas independientes de las plataformas, métodos de prueba, capas de protocolo y protocolos. La notación TTCN-3 puede emplearse para la especificación de todos los tipos de pruebas de sistemas reactivos en diversos puertos de comunicación.

– 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 apoyo para la configuración e implantación de TTCN-3. TTCN-3 puede emplearse para la especificación de todos los tipos de pruebas de sistemas reactivos en diversos puertos de comunicación.

– 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 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.

– 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 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.

– Z.161.7 (revisada), *Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Características orientadas a los objetos*, define el soporte de características orientadas a objetos en 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.

– Z.167 (revisada), *Notación de pruebas y de control de pruebas versión 3 (TTCN-3): Utilización de ASN.1 con TTCN-3*, define una manera normativa de utilizar ASN.1, tal como está definido en las Recomendaciones UIT-T X.680, UIT-T X.681, UIT-T X.682 y UIT-T X.683 con la TTCN-3.

– Z.168 (revisada), *Notación de pruebas y de control de pruebas versión 3: Correspondencia del lenguaje IDL con la notación TTCN-3*, define las reglas de correspondencia del lenguaje de definición de interfaz (IDL) de la arquitectura de intermediario de petición de objeto común (CORBA) con TTCN-3 (definida en la Recomendación UIT-T Z.161) para permitir la prueba de sistemas CORBA. Los principios de la correspondencia de CORBA IDL con TTCN-3 también pueden emplearse para la correspondencia de lenguajes de especificación de interfaz de otras tecnologías basadas en componentes/objetos.

– Z.169 (revisada), *Notación de pruebas y control de pruebas versión 3: Utilización de esquemas XML con TTCN-3*, define las reglas de correspondencia del Consorcio World Wide Web (W3C) con la notación TTCN-3 (Notación de pruebas y de control de pruebas 3) para poder realizar pruebas de sistemas, interfaces y protocolos basados en XML.

– Z.171 (revisada), *Notación de prueba y de control de prueba, versión 3: Utilización de JSON con TTCN-3*, se especifican las normas para definir esquemas de estructuras de datos en TTCN‑3 para permitir la prueba de sistemas, interfaces y protocolos JSON, así como las normas de conversión entre TTCN-3 y JSON para permitir el intercambio de datos TTCN-3 en formato JSON entre distintos sistemas.

– X.Supl.31, *UIT-T X.660 – Directrices sobre utilización de identificadores de objeto para Internet de las Cosas*, define directrices sobre utilización de los identificadores de objeto (OID) para identificar objetos en la Internet de las cosas (IoT). Comprende directrices sobre la estructuración de los OID, la implementación de sistemas de resolución y el establecimiento de procedimientos de gestión basados en las Recomendaciones UIT-T y otras normas internacionales existentes.

– XSTP-OID-ORS, *OID Resolution system: Problems, Requirements and Potential solutions*, identifica los problemas, requisitos y posibles soluciones de la resolución de OID. Entre los problemas se cuentan el rendimiento local y la resolución global de subárboles OID desaparecidos. También se abordan los requisitos técnicos de las posibles soluciones. Por último, se presentan las posibles soluciones técnicas y orientaciones de orden administrativo y operativo.

– Z.Imp100 (revisada), *Guía del implementador – Lenguaje de especificación y descripción – Versión 4.0.1*, recopila los defectos y problemas de mantenimiento detectados y sus correspondientes soluciones para las Recomendaciones UIT-T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.111 y Z.119 sobre el lenguaje de especificación y descripción.

l) C12/17, Lenguajes formales para software de telecomunicaciones y pruebas (2017‑2020)

La C12/17 elabora Recomendaciones sobre lenguajes formales (por ejemplo, SDL, MSC, URN) 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 prepara Recomendaciones sobre los lenguajes de prueba (por ejemplo, RRCN-3) como medio de apoyo a la interoperabilidad y la conformidad.

Durante el periodo de estudios considerado, la C12/17 ha elaborado tres nuevas Recomendaciones, 64 Recomendaciones revisadas y dos Guías del implementador revisadas:

– 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.151 (revisada), *Notación de requisitos de usuarios* *– Definición del lenguaje*, define la notación de requisitos de usuarios (URN) prevista para la obtención, análisis, especificación y validación de los requisitos. La URN combina conceptos de modelización y notaciones para objetivos (principalmente requisitos no funcionales y atributos de calidad) e hipótesis (principalmente para requisitos operativos, requisitos funcionales y el razonamiento arquitectónico y de rendimiento). La subnotación de objetivos se denomina lenguaje de requisitos orientados a objetivos (GRL) y la subnotación de hipótesis se denomina mapa de casos de uso (UCM).

– Z.161 (revisada), *Notación de pruebas y de control de prueba versión 3: Lenguaje núcleo de TTCN-3*, define la notación de pruebas y control de pruebas 3 (TTCN-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 notación TTCN-3 se puede utilizar para la especificación de todos los tipos de pruebas de sistemas reactivos en diversos puertos de comunicación. Las principales aplicaciones son las pruebas de protocolos (incluidos los protocolos móviles e Internet), las pruebas de servicios (incluidos los servicios suplementarios), las pruebas de módulos, las pruebas de plataformas basadas en la arquitectura de negociación de petición de objetos comunes (CORBA) y las pruebas de interfaces de programación de aplicaciones (API).

– 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 (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 (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 (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.161.6, (nueva y revisada), *Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3: Ajustes avanzados*, define el soporte de ajustes avanzados de la notación de pruebas y de control de pruebas 3 (TTCN-3).

– Z.161.7, (nueva y revisada), *Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN-3*: Características orientadas a los objetos, define el soporte de características orientadas a objetos en la notación de pruebas y de control de pruebas, versión 3 (TTCN-3).

– Z.164 (revisada), *Notación de pruebas y control de pruebas versión 3: Semántica operativa del TTCN-3*, define la semántica operativa de la TTCN-3 (Notación de pruebas y de control de pruebas 3). La semántica operativa es necesaria para interpretar inequívocamente las especificaciones creadas con la notación TTCN-3. Esta Recomendación utiliza el lenguaje núcleo definido de TTCN-3 en la Recomendación UIT-T Z.161. Esta revisión de la Recomendación contiene modificaciones, aclaraciones y correcciones de fondo y de forma.

– 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 interfaz de ejecución TTCN-3 (TRI) ofrece la adaptación recomendada para la temporización y la comunicación de un sistema de prueba a una plataforma de procesamiento dada y al sistema que se prueba, respectivamente. En esta Recomendación se define la interfaz como un conjunto de operaciones independientes del lenguaje objetivo.

 La interfaz está definida para ser compatible con la Resolución UIT-T Z.161. Esta Recomendación utiliza el lenguaje de definición de interfaz (ODL) de la arquitectura de negociación de petición de objetos comunes (CORBA) para especificar la TRI por completo. En las cláusulas 6, 7 y 8 de ETSI ES 201 873-5 V4.8.1 se especifican las correspondencias lingüísticas entre la especificación abstracta y los lenguajes objetivo Java y ANSI-C. Puede encontrarse un resumen de la especificación de interfaz IDL en el Apéndice A de ETSI ES 201 873-5 V4.8.1.

 Esta revisión de la Recomendación incorpora enmiendas, aclaraciones y correcciones de fondo y forma.

– Z.166 (revisada), *Notación de pruebas y de control de pruebas versión 3: Interfaz de control*, especifica las interfaces de control para las aplicaciones de notación de pruebas y de control de pruebas 3 (TTCN‑3) en sistemas de pruebas. Las interfaces de control TTCN-3 ofrecen una adaptación normalizada para la gestión, el tratamiento de componentes de pruebas y la codificación/descodificación de un sistema de pruebas con respecto a una plataforma de pruebas particular. En esta Recomendación se definen las interfaces como un conjunto de operaciones independiente del lenguaje objetivo.

 Las interfaces se han definido para ser compatibles con las normas TTCN-3 (véase la cláusula 2 de ETSI ES 201 873-6 V4.11.1). La definición de la interfaz utiliza el lenguaje de definición de interfaz (IDL de la arquitectura de negociación de petición de objetos comunes (CORBA) para especificar la TCI por completo. En las cláusulas 8, 9 y 9.7 de ETSI ES 201 873-6 V4.11.1 se presentan las correspondencias lingüísticas entre esta especificación abstracta y los lenguajes objetivo Java y ANSI C.

 Esta revisión de la Recomendación contiene enmiendas, aclaraciones y correcciones de fondo y 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. Esta Recomendación no contempla la armonización de otros lenguajes con TTCN-3.

 La primera revisión de esta Recomendación contiene enmiendas (conformidad y compatibilidad, requisitos y descripciones relacionadas con el tipo identificador de objeto se han trasladado a esta Recomendación procedentes de todas las demás Recomendaciones de la serie UIT-T 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.

 Esta revisión de la Recomendación contiene enmiendas, aclaraciones y correcciones de fondo y 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 el lenguaje de definición de interfaz (IDL) de la arquitectura de negociación de petición de objetos comunes (CORBA) y TTCN‑3 (como se define en la Recomendación UIT‑T Z.161) para permitir las pruebas en los sistemas CORBA. Los principios de correspondencia entre IDL CORBA y TTCN-3 también pueden utilizarse para establecer la correspondencia con los lenguajes de especificación de interfaz de otras tecnologías basadas en objetos/componentes. Esta revisión de la Recomendación contiene enmiendas, aclaraciones y correcciones de fondo y de forma.

– Z.169 (revisada), *Notación de pruebas y control de pruebas versión 3: Utilización de esquemas XML con TTCN-3*, define las reglas de correspondencia del Esquema W3C con la notación TTCN-3 para poder realizar pruebas de sistemas, interfaces y protocolos basados en XML. Esta revisión de la Recomendación contiene modificaciones, aclaraciones y correcciones de fondo y 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. Esta revisión de Z.170 contiene enmiendas, aclaraciones y correcciones de fondo y de forma.

– Z.171*,* (nueva y revisada), *Notación de prueba y de control de prueba, versión 3: Utilización de JSON con TTCN-3,* especifica las normas para definir esquemas de estructuras de datos JSON en TTCN‑3 para permitir la prueba de sistemas, interfaces y protocolos JSON, así como las normas de conversión entre TTCN-3 y JSON para permitir el intercambio de datos TTCN-3 en formato JSON entre distintos sistemas.

– Z.Imp100 (revisada), *Guía del implementador – Lenguaje de especificación y descripción – Versión 3.0.2*, recopila los defectos y problemas de mantenimiento detectados y sus correspondientes soluciones para las Recomendaciones UIT-T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.111 y Z.119 sobre el lenguaje de especificación y descripción.

– Z.100Imp (revisada), *Guía del implementador – Lenguaje de especificación y descripción - Versión 4.0.0*, recopila los defectos y problemas de mantenimiento detectados y sus correspondientes soluciones para las Recomendaciones UIT-T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.111 y Z.119 sobre el lenguaje de especificación y descripción.

m) C13/17, Aspectos de seguridad de los sistemas de trasporte inteligentes (2017-2020)/
Seguridad de los sistemas de transporte inteligente (2021-)

La C13/17 fue creada en septiembre de 2017 y elabora Recomendaciones sobre los aspectos de seguridad de los sistemas de transporte inteligentes (STI), incluidos diversos tipos de comunicación en vehículos, entre vehículos y entre vehículos y emplazamientos fijos.

Durante este periodo de estudios la C13/17 ha elaborado seis nuevas Recomendaciones:

– X.1371, *Amenazas a la seguridad de los vehículos conectados*, describe amenazas a la seguridad de los vehículos conectados y al ecosistema del vehículo.

– X.1372, *Directrices de seguridad para la comunicación entre el vehículo y su entorno (V2X)*, presenta directrices de seguridad para los sistemas de comunicación entre el vehículo y su entorno (V2X). Se identifican las amenazas presentes en los entornos de comunicación V2X y se especifican los requisitos de seguridad que han de cumplir los sistemas de comunicación V2X para hacer frente a esas amenazas. En esta Recomendación se presentan también casos de uso de los servicios de seguridad de la comunicación V2X.

– X.1373, *Capacidad de actualización segura de software en dispositivos de comunicación de sistemas de transporte inteligente*, proporciona procedimientos de actualización segura de software que se ejecutan entre el servidor de actualización de software y los vehículos con los controles de seguridad adecuados. Esta Recomendación puede ser de utilidad para fabricantes de automóviles y para industrias relacionadas con los STI, como conjunto de capacidades normalizadas para el desarrollo de prácticas idóneas.

– X.1374, *Requisitos de seguridad sobre interfaces y dispositivos externos con capacidad de acceso a vehículos*, analiza dos tipos de amenazas de seguridad para los vehículos conectados, a saber, las amenazas contra las interfaces que se utilizan para facilitar la comunicación de un vehículo con sus dispositivos externos y las amenazas contra dichos dispositivos externos que establecen comunicación con el vehículo. La Recomendación UIT-T X.1374 especifica los requisitos de seguridad para esas interfaces externas y los dispositivos externos con capacidad de acceso al vehículo en entornos de redes de telecomunicaciones a fin de abordar las amenazas identificadas en función de los tipos de interfaces de acceso. Las interfaces y los dispositivos externos con capacidad de acceso al vehículo incluyen, en particular, el sistema de entrada a distancia (RKE) sólo con llave inteligente, las herramientas de diagnóstico y las llaves de protección inteligente inalámbricas que utilizan el puerto de diagnóstico a bordo II (OBD‑II) y unidades de control telemático con dispositivos de comunicación inalámbricos.

– X.1375, *Directrices sobre un sistema de detección de intrusos en redes de vehículos*, establece las directrices de un sistema de detección de intrusión (IDS) para redes intravehiculares (IVN). La Recomendación hace hincapié en la forma de detectar intrusiones y actividades malignas en las IVN, en particular las que utilizan una red de área de controlador (CAN) y no pueden detectarse mediante los IDS generales desplegados en Internet. La Recomendación UIT-T X.1375 abarca varias categorías de ataques a IVN, incluido su análisis. También propone metodologías y directrices de implementación para detectar intrusiones y actividades malignas en IVN basadas en CAN que no pueden detectarse mediante IDS generales.

– X.1376, *Mecanismo de detección de conductas indebidas relacionadas con la seguridad por macrodatos para vehículos conectados,* describe un mecanismo de detección de conductas indebidas relacionadas con la seguridad para los vehículos conectados, destinado a ayudar a las partes interesadas a utilizar los datos de automoción para mejorar la seguridad de los vehículos. A medida que aumenta la conectividad de los vehículos, el número de vulnerabilidades aumenta debido al desarrollo de una tecnología compleja, estas vulnerabilidades traen consigo más amenazas para los vehículos conectados. El análisis de una gran cantidad de datos de automoción resulta de gran utilidad para evaluar la seguridad de los vehículos conectados.

Durante el periodo de estudios considerado la C13/17 celebró, el 26 de agosto de 2019 en Ginebra, un minitaller sobre problemas de ciberseguridad de la conducción automatizada.

n) C14/17, Aspectos de seguridad de las tecnologías de libro mayor distribuido (2018‑2020)/Seguridad de las tecnologías de libro mayor distribuido (DTL) (2021-)

La C14/17 fue creada en marzo de 2018 y elabora Recomendaciones sobre los aspectos de seguridad de las tecnologías de libro mayor distribuido (DLT), también conocidas como cadena de bloques, incluida la presentación de soluciones de seguridad integrales para aplicaciones y servicios DLT.

Durante este periodo de estudios la C14/17 ha elaborado nueve nuevas Recomendaciones:

– X.1400, *Términos y definiciones sobre la tecnología de libro mayor distribuido*, incluye un conjunto básico de términos y definiciones sobre la tecnología de libro mayor distribuido (DLT). Las definiciones proporcionan una caracterización básica de cada término, y en su caso, se incluye una nota aclaratoria.

– X.1401, *Amenazas a la seguridad de tecnología de libro mayor distribuido,* identifica las amenazas que pueden afrontar los diversos componentes funcionales de un sistema de libro mayor distribuido, como el protocolo, la red y los datos. Esta Recomendación podrá servir de referencia para diseñar o implementar un sistema DLT.

– X.1402, *Marco de seguridad para la tecnología de libro mayor distribuido,* describe las capacidades de seguridad que podrían atenuar las amenazas a la seguridad conexas y especifica una metodología marco de seguridad para determinar el modo en que dichas capacidades de seguridad deben utilizarse para atenuar las amenazas a la seguridad de un sistema DLT específico.

– X.1403, *Directrices de seguridad para utilizar la tecnología de libro mayor distribuido en la gestión descentralizada de identidades*. La tecnología de libro mayor distribuido (DLT) y sus aplicaciones específicas, como las cadenas de bloques, ofrecen una oportunidad sin precedentes de recurrir a una infraestructura fiable y una plataforma mediante la cual se podría crear una federación de confianza para el intercambio de atributos e información sobre identidades. En esta Recomendación se exponen las consideraciones relativas a la privacidad y seguridad específicas de las telecomunicaciones para la utilización de los datos DLT en la gestión de identidades.

– X.1404, *Garantía de seguridad para la tecnología de libro mayor distribuido*, establece tres niveles de garantía de seguridad en relación con la tecnología de libro mayor distribuido (DLT), con objeto de facilitar el diseño y el desarrollo de mecanismos que garanticen la seguridad. A tal efecto define diez componentes de garantía de seguridad y especifica varios criterios y directrices para alcanzar cada uno de los tres niveles de un componente de garantía de seguridad determinado. Por último, establece una correspondencia entre amenazas específicas y componentes de garantía de seguridad, de un lado, y de otro, entre funciones de seguridad específicas y componentes de garantía de seguridad.

– X.1405, *Amenazas y requisitos de seguridad para los servicios de pago digitales basados en la tecnología de libro mayor distribuido*, se centra en una serie de casos de uso de servicios de pago. En la Recomendación UIT-T X.1405 se describe un modelo de servicio y se analizan las amenazas a la seguridad y los desafíos conexos a partir de los que se especifican los requisitos de seguridad para contrarrestar las amenazas y los desafíos existentes.

– X.1406, *Amenazas de seguridad para la votación en línea mediante la tecnología de libro mayor distribuido*, identifica las amenazas a la seguridad de los sistemas de votación en línea que utilizan la tecnología de libro mayor distribuido (DLT) basada en la infraestructura de telecomunicaciones o de TIC. Se propone un modelo de referencia para dichos sistemas de votación en línea y analiza las amenazas a la seguridad en los procesos de votación en línea descritos en dichos modelos.

– X.1407, *Requisitos de seguridad para el servicio de validación de la integridad digital basado en la tecnología de libro mayor distribuido*, se especifican las amenazas y los requisitos de seguridad del servicio de validación de la integridad digital basado en la tecnología de libro mayor distribuido (DLT).

– X.1408, *Amenazas y requisitos de seguridad para el acceso y la compartición de datos basados en la tecnología de libro mayor distribuido*, especifica un modelo de referencia para describir el acceso y la compartición de datos basados en la tecnología de libro mayor distribuido (DLT). Se identifican las entidades y sus funciones, así como las amenazas a la seguridad del acceso y la compartición de datos basados en DLT. Además, se especifican los requisitos de seguridad para contrarrestar las amenazas a la seguridad identificadas.

o) C15/17, Seguridad en relación con las tecnologías incipientes, en particular la seguridad cuántica

La C15/17 fue creada en enero de 2021 y se ocupa de las Recomendaciones sobre seguridad en relación con las tecnologías incipientes, en particular la seguridad cuántica. La C15/17 también alberga el mecanismo de incubación (TP.inno) de la CE 17 que brinda una flexibilidad controlada en el estudio de nuevos aspectos relativos a la seguridad para proteger los nuevos servicios y aplicaciones incipientes basados en las telecomunicaciones/TIC.

Durante este periodo de estudios, la C15/17 ha elaborado dos nuevas Recomendaciones y un Corrigéndum de un Informe Técnico:

– X.1712, *Requisitos de seguridad y diseño de redes de distribución de claves cuánticas – Gestión de claves,* especifica las amenazas y requisitos de seguridad para la gestión de claves en redes de distribución de claves cuánticas (QKDN) para posteriormente especificar las medidas de seguridad de la gestión de claves que se han de aplicar para cumplir los requisitos de seguridad.

– X.1770, *Directrices técnicas para la computación multipartita segura*, especifica unas directrices técnicas para la computación multipartita (MPC) y establece la norma técnica básica para que los interesados de TIC utilicen la MPC para proteger los datos en el marco de la colaboración de datos y el análisis de macrodatos. También se describen las aplicaciones para las que puede utilizarse la MPC, y cómo se utiliza, como referencia para que los interesados de TIC elaboren aplicaciones de MPC.

– Cor.1 de TR.sec-qkd, *Consideraciones de seguridad para las redes de distribución de claves cuánticas,* modifica las expresiones correspondientes relativas a la "seguridad por TI", sustituye "qubits" por "estados cuánticos", sustituye "cofibra" por "copropagación" y modifica los contenidos conexos.

## 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 ocupan conjuntamente la C11/17 y la C12/17 hasta 2020 y la C11/17 desde 2021.

### 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‑16).

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 UIT-D (CE 1, CE 2, GADT), el UIT-R (CE 1, CE 5, CE 6, GT (4C, 5A, 5D, 6C)), la FIGI del UIT-T, diversos Grupos Temáticos del UIT-T (AI4EE, AI4H, AN, DFC, DLT, DPM, ML5G, NET2030, QIT4N, VM), diversas Actividades Conjuntas de Coordinación del UIT-T (IMT2020, IoT y SC&C, MMeS, SDN), el SCV del UIT-T, diversas Comisiones de Estudio del UIT-T (2, 3, 5, 9, 11, 12, 13, 15, 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), el BIPM, el CEN-CENELEC JTC 9, el ETSI ISG (CIM, ETI, F5G, IPE, NIN, QSC, SAI), el SAGE del ETSI, diversos comités técnicos de ETSI (CYBER, ITS, MTS), FIDO Alliance, IEEE 802.1, el IETF WG TLS, el comité técnico 307 de la ISO, diversos subcomités del JTC de la ISO/CEI (6, 27/WG 1-5, 29/WG 1), el, MEF, el NIST, OASIS, la OMA, oneM2M, el SAE y el W3C.

La CE 17 envió declaraciones de coordinación interna a la CITS de la UIT, el IPRAHG, el UIT-D (CE 1 CE 2, GADT), el UIT-R (4, 5 (GT (5A, 5D))), la FIGI del UIT-T, diversos Grupos Temáticos del UIT-T (AI4EE, DFC, DLT, NET2030, DPM, QIT4N, VM), diversas Actividades Conjuntas de Coordinación del UIT-T (IMT2020, IoT y SC&C, MMeS, SDN), el SCV del UIT-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), APT ASTAP, el BSI, el CEN-CENELEC JTC 19, el CIS, el ETSI (ISG, CIM, MEC, QKD, ZSM, SAGE), diversos comités técnicos del ETSI (CYBER, ITS, MTS, la FIDO Alliance, la GSMA (FASG, SIM), la OACI, la Blockchain Initiative del IEEE, el IETF, el IRTF, diversos comités técnicos de la ISO (12, 20, 22, 37, 204, 307), el ISO/CEI JTC1/WG9, diversos subcomités del JTC 1 de la ISO/CEI (6 (WG 10), 7, 27 (WG 1, WG 2, WG 3, WG 4, WG 5), 29, 38, 42), la Kantara Initiative, el MEF, el MITRE, el NGMN, el NIST, diversos comités técnicos de OASIS (CTI, OpenC2, Trust Elevation), la OIX, oneM2M, ONF, OPIX Foundation, RAISE Forum, SAE, la CEPE, la UPU, W3C, OMPI y OMS.

De conformidad con la Resolución 7 de la AMNT-16, *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.

La CE 17 organizó los siguientes talleres:

– [2º Taller conjunto UIT/OMS sobre el certificado COVID-19 digital](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2021/1126/Pages/default.aspx)
Virtual, 13.00-18.00 horas CEST, 26 de noviembre de 2021

– [Taller conjunto UIT/OMS sobre el certificado de vacunación digital](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2021/0811/Pages/default.aspx)
Virtual, 13.00-18.00 horas CEST, 11 de agosto de 2021

– "Identificadores descentralizados y la cadena de bloques" de la Semana de las Tecnologías Incipientes de la BDT 2021
Virtual, 14.00-15.00 horas, 8 de julio de 2021

– [Minitaller de la CE 17 sobre problemas de ciberseguridad de la conducción automatizada](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/mini-workshop_ITS.aspx)
Ginebra, 14.30-17.30 horas, 26 de agosto de 2019

– [Taller de la UIT sobre seguridad tecnofinanciera](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/mini-workshop_ITS.aspx)
Ginebra, Suiza, 26 de agosto de 2019

– [Taller de la UIT sobre tecnología de la información cuántica (TIQ) para redes](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Pages/default.aspx)
Shangái, China, 5-7 de junio de 2019

– [Minitaller de la CE 17 sobre comunicaciones cuánticas seguras](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/Secure%20quantum%20communication.aspx)
Ginebra, 14.30-17.30 horas, 24 de enero de 2019

– [Taller de la UIT sobre inteligencia artificial/aprendizaje automático y seguridad](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190121/Pages/default.aspx)
Ginebra, Suiza, 21 de enero de 2019

– [Taller de la UIT sobre ataques de ciberseguridad avanzados y Ransomware](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180828/Pages/default.aspx)
Ginebra, Suiza, 28 de agosto de 2018

– [Taller de la UIT sobre seguridad 5G](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180319/Pages/default.aspx)
Ginebra, Suiza, 19 de marzo de 2018

– [Taller de la UIT sobre aspectos de seguridad de los sistemas de transporte inteligentes](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201708/Pages/default.aspx)
Ginebra, Suiza, 28 de agosto de 2017

– [Taller de la UIT sobre aspectos de seguridad de la cadena de bloques](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201703/Pages/default.aspx)
Ginebra, Suiza, 21 de marzo de 2017

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

– la aplicación de las Resoluciones 7, 11, 18, 32, 40, 44, 50, 52, 54, 58, 64, 65, 67, 70, 73, 75, 76, 77, 78, 84, 86, 90, 92, 93, 94, 96, 97 y 98 de la AMNT-16;

– la aplicación de las Resoluciones 101, 123, 130, 136, 174, 177, 178, 179, 181, 188, 189, 197, 199, 200 y 201 de la PP-18;

– la aplicación de las Resoluciones 23, 30, 34, 45, 47, 54, 63, 67, 69 y 80 de la CMDT-17.

La Comisión de Estudio 17 elaboró un Plan de Acción para la aplicación de las Resoluciones de la PP-14/18, la AMNT-16 y la CMDT-17 que actualizó en cada una de sus reuniones. En su reunión de marzo de 2020 la CE 17 asignó un editor a esta labor para facilitar los trabajos.

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.

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.

Se publicó la 2ª edición del 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).

Se publicó la 7ª 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 CE 17) lograron los siguientes resultados en el marco de sus actividades relacionadas con las Recomendaciones sobre seguridad:

Recomendaciones aprobadas:

| CE | Recomendación | Título |
| --- | --- | --- |
| CE 9 | J.1204 | Marco de seguridad de un sistema operativo de TV inteligente |
| CE 13 | Y.2241 | Marco de servicios de apoyo para el aprendizaje ubicuo personalizado basado en objetos web |
| CE 13 | Y.2774 | Requisitos funcionales de la inspección detallada de paquetes en las redes futuras |
| CE 13 | Y.3051 | Principios básicos de entorno de confianza en la infraestructura de tecnologías de la información y la comunicación |
| CE 13 | Y.3052 | Visión general de prestación de confianza para las infraestructuras y los servicios de tecnologías de la información y la comunicación |
| CE 13 | Y.3053 | Marco de creación fiable de redes con dominios de red centrados en la confianza |
| CE 13 | Y.3054 | Marco para servicios de medios basados en la confianza |
| CE 13 | Y.3055 | Marco para la gestión de datos personales basada en la confianza |
| CE 13 | Y.3056 | Marco para la inicialización de dispositivos y aplicaciones a efectos del acceso abierto a servicios de confianza en ecosistemas distribuidos |
| CE 13 | Y.3057 | Modelo de índice de confianza para los servicios e infraestructuras de TIC |
| CE 13 | Y.3302 | Arquitectura funcional de la conexión en red definida por software |
| CE 13 | Y.3514 | Computación en la nube – Marco y requisitos de computación fiable entre nubes |
| CE 13 | Y.3516 | Arquitectura funcional de la computación entre nubes |
| CE 13 | Y.3517 | Computación en la nube – Visión general de la gestión de la confianza entre nubes |
| CE 13 | Y.3650 | Marco de creación de redes basadas en macrodatos |
| CE 13 | Y.3802 | Redes de distribución de claves cuánticas – Arquitectura funcional |
| CE 13 | Y.3803 | Redes de distribución de claves cuánticas – Gestión de claves |
| CE 13 | Y.3804 | Redes de distribución de claves cuánticas – Control y gestión |
| CE 13 | Y.3805 | Redes de distribución de claves cuánticas – Control de redes definidas por software |
| CE 13 | Y.3806 | Redes de distribución de claves cuánticas – Requisitos para garantizar la calidad del servicio |
| CE 15 | G.873.1 | Red óptica de transporte: Protección lineal |
| CE 15 | G.873.3 | Red óptica de transporte – Protección por malla compartida |
| CE 15 | G.8132/ Y.1383 (revisada) | Protección anular compartida MPLS-TP |
| CE 15 | G.9978 | Transceptores de red doméstica alámbricos de alta velocidad unificados – Admisión segura |
| CE 16 | H.248.77 | Protocolo de control de pasarela: Lote y procedimientos del protocolo de transporte en tiempo real seguro |
| CE 20 | Y.4457 | Marco arquitectónico para servicios de seguridad del transporte |
| CE 20 | Y.4808 | Marco arquitectónico de entidad digital para luchar contra la falsificación en la IoT |
| CE 20 | Y.4810 | Requisitos de seguridad de datos para dispositivos de IoT heterogéneos |

Suplementos y Apéndices acordados:

| CE | Número | Título |
| --- | --- | --- |
| CE 13 | Serie Y.3100 Suplemento 44 | Actividades de normalización y de fuente abierta relacionadas con la informatización de red de IMT-2020 |

Proyectos de Recomendación consentidos:

| CE | Número | Título |
| --- | --- | --- |
| CE 13 | Y.2086 (Y.DNI-fr) | Marco y requisitos de la infraestructura de redes fiables descentralizadas *(Consentimiento el 16/07/2021)* |
| CE 13 | Y.3807 (Y.QKDN-QoS-pa) | Redes de distribución de claves cuánticas: Parámetros de QoS *(Consentimiento el 10/12/2021)* |
| CE 13 | Y.3808 (Y.QKDN-frint) | Marco de integración de redes de distribución de claves cuánticas y redes de almacenamiento seguro*(Consentimiento el 10/12/2021)* |
| CE 13 | Y.3809 (Y.QKDN-BM) | Redes de distribución de claves cuánticas: Modelos basados en la función empresarial*(Consentimiento el 10/12/2021)* |

### 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-16).

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 CE 17) lograron los siguientes resultados en el marco de sus actividades relacionadas con las Recomendaciones sobre IdM:

Recomendaciones aprobadas:

| CE | Recomendación | Título |
| --- | --- | --- |
| CE 3CE 17 | D.1140X.1261\*\*\* | Marco político y principios para la infraestructura de identidad digital |
| CE 2 | E.217rev | Comunicaciones marítimas – Identidad de estación de barco |
| CE 11 | Q.4063 | Marco para la realización de pruebas de sistemas de identificación utilizados en Internet de las cosas |
| CE 11 | Q.5052 | Direccionamiento de dispositivos móviles mediante un identificador exclusivo duplicado |
| CE 15 | L.207 | Elementos de nodo pasivos con detección automatizada de etiqueta ID |
| CE 16 | H.273 | Puntos de código independientes de la codificación para la identificación del tipo de señal de vídeo |
| CE 17 | X.1252rev | Términos y definiciones de referencia para la gestión de la identidad |
| CE 17 | X.1403 | Directrices de seguridad para la utilización de la tecnología de libro mayor distribuido en la gestión descentralizada de identidades |
| CE 20 | Y.4805 | Requisitos de servicio de identificador para la interoperabilidad de aplicaciones de ciudades inteligentes |
| CE 20 | Y.4476 | Marco de resolución basado en los OID para las transacciones de libro mayor distribuido asignadas a recursos de IoT |
| CE 20 | Y.4809 | Identificadores de Internet de las cosas para sistemas de transporte inteligentes |
| CE 20 | Y.4811 | Marco de referencia para servicios convergentes de identificación y autentificación de dispositivos IoT en entornos descentralizados |

\*\*\* Doble signatura D.1140 (CE 3)/X.1261 (CE 17)

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-16).

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 han trabajado sobre lenguajes y técnicas de descripción para ASN.1, 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. Sigue alimentándose la [base de datos de módulos ASN.1](http://www.itu.int/ITU-T/recommendations/fl.aspx?lang=1), permitiendo así a los implementadores acceder a las especificaciones ASN.1 publicadas, en formato de lectura automática y con la sintaxis verificada. Esta base de datos contiene unos 900 módulos de más de 200 Recomendaciones UIT-T, así como los módulos de otras organizaciones de normalización a que hacen referencia.

El lenguaje de especificación y descripción (SDL‑2010) se utiliza para definir sistemas como modelos de referencia en las Recomendaciones y como implementaciones. La gramática SDL‑2010 se define en las Recomendaciones UIT-T Z.101 a Z.107 y la definición formal puede encontrarse en el Anexo F a Z.100. La Cuestión 12/17 actualizó la definición formal. Gracias a este estudio se han detectado y resuelto ambigüedades, errores e incoherencias en el texto de Z.101 a Z.107. El 5 de septiembre de 2019 recibió el consentimiento para la aprobación AAP una definición formal completamente armonizada con SDL‑2010. Al mismo tiempo recibieron el consentimiento para la aprobación AAP los textos actualizados de Z.100 a Z.107 a fin de eliminar ambigüedades, errores e incoherencias. El 5 de septiembre de 2019 se acordó la revisión de Z.Imp100, sin modificación alguna de los textos de Z.100 a Z.107 consentidos para la aprobación AAP y una lista de los anteriores textos en vigor. El resultado es un SDL‑2010 mejor definido gracias a una definición formal coherente. No se prevén más trabajos al respecto por el momento.

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 tres textos nuevos y 25 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.

### 3.3.4 Actividad Conjunta de Coordinación sobre la gestión de la identidad (JCA-IdM)

La Actividad Conjunta 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. La JCA-IdM celebró seis reuniones en paralelo a las reuniones de la CE 17 de agosto/septiembre de 2017, marzo de 2018, agosto/septiembre de 2018, agosto/septiembre de 2019, abril de 2021 y agosto/septiembre de 2021 para coordinar los trabajos sobre gestión de la identidad (IdM) del UIT-T con otros Grupos y Comisiones del UIT-T y demás organizaciones externas, por ejemplo, la Decentralized Identify Foundation, la FIDO Alliance, el ISO/CEI JTC 1/SC 27/WG 5, el ISO TC 307, la Kantara Initiative, la Mobile Driving Licence, el grupo de trabajo sobre identidades de NH-ISAC, OASIS, la OpenIdD Foundation, la Sovrin Fondation, SSI Open Standards y la UPU.

### 3.3.5 Grupo Regional para África de la Comisión de Estudio 17 (GRCE17-AFR)

El Grupo Regional de la CE 17 para África (GRCE17-AFR), creado en abril de 2015, en el anterior periodo de estudios, se prolongó durante el periodo considerado, en el que celebró una reunión en conjunción con el GRCE17-ARB los días 2 y 3 de abril de 2019.

### 3.3.6 Grupo Regional de la Comisión de Estudio 17 para los Estados Árabes(GRCE17-ARB)

En su reunión de marzo de 2017 la CE 17 creó el Grupo Regional de la CE 17 para los Estados Árabes (GRCE17-ARB). Su primera reunión se celebró en Mascate, Omán, en diciembre de 2017. Su segunda reunión se celebró en Kuwait en octubre de 2018 y la tercera se celebró en Túnez los días 2 y 3 de abril de 2019 en conjunción con el GRCE17-AFR.

En todas las reuniones de los Grupos Regionales de la CE 17 el Consejero de la CE 17 impartió formaciones de la CE 17 y sobre el cierre de la brecha de normalización. Los participantes de los países de las regiones interesadas celebraron debates abiertos sobre temas de ciberseguridad e identificaron los que despiertan un mayor interés para su estudio ulterior.

## 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 1 643 596registros inscritos al 16 de noviembre de 2021 (<http://www.oid-info.com/cgi-bin/display?a=count_nodes>) 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).

Concretamente, se aprobó la Recomendación UIT-T X.677, Mecanismo de identificación para vehículos aéreos sin tripulante utilizando identificadores de objetos, para analizar los requisitos de gestión de la vida útil completa y el reconocimiento de la identidad operativa de aeronaves no tripuladas (ANT), habida cuenta de la seguridad, y se especifica un mecanismo de identificación de ANT mediante identificadores de objeto (OID).

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 Bahréin, Benín, Ecuador, Jamaica y Viet Nam.

## 3.5 Reducción de la brecha en materia de normalización

En todas las reuniones presenciales de la CE 17 celebradas a lo largo de este periodo de estudios la TSB organizó una recepción de bienvenida y una visita de la Sede de la UIT para los nuevos participantes en la CE 17. El Presidente de la CE 17 organizó una "Sesión de orientación de la CE 17 y Diálogo con el Equipo de Gestión de la CE 17 para los nuevos participantes". En enero de 2019 el Consejero de la CE 17 organizó la "Consulta del Consejero de la CE 17" para responder a las preguntas de los delegados sobre los métodos de trabajo de la CE 17. En septiembre de 2019 la TSB organizó una "formación para equipos directivos del UIT-T" dirigida a los Relatores y Editores de la CE 17.

Entre marzo de 2017 y septiembre de 2018 la CE 17 organizó periódicamente una sesión de formación práctica para los delegados de los países en desarrollo 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.

En este periodo de estudios, la CE 17 organizó periódicamente reuniones (virtuales) informales de delegados de África y los Estados Árabes, respectivamente, en el marco de sus reuniones (virtuales) a fin de facilitar la planificación futura del GRCE17-AFR y el GRCE17-ARB.

# 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. Además, se ha creado una base sólida de Recomendaciones/normas relativas a la seguridad, se ha llegado a acuerdos de colaboración y coordinación 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, aumente y mejore, y que no se vea fragmentada.

Han de abordarse las amenazas y vulnerabilidades de seguridad existentes y futuras a fin de crear confianza y seguridad en la utilización de las TIC, habida cuenta de los nuevos servicios y aplicaciones basadas en las redes de telecomunicaciones/TIC, mediante la elaboración de Recomendaciones e Informes Técnicos. Las tecnologías de seguridad son elementos fundamentales que protegen los sistemas de TIC contra ataques o daños a su hardware, software o a su información, y también contra la interrupción o el direccionamiento indebido de los servicios que prestan.

Se necesitan nuevos enfoques y mediciones de seguridad para hacer frente adecuadamente a las amenazas y riesgos de seguridad. La Comisión de Estudio 17 tiene un papel clave que desempeñar en la elaboración de normas internacionales en materia de seguridad.

La seguridad de y para las telecomunicaciones y las TIC sigue siendo una esfera necesitada de normalización. Es de una importancia capital gestionar las nuevas amenazas a las telecomunicaciones y las TIC, incluidas las infraestructuras, sistemas, aplicaciones y servicios de red. Es imperativo crear normas y directrices de seguridad que se adapten a las necesidades de todos los países.

La gestión de las nuevas amenazas a la infraestructura de telecomunicaciones y TIC es extremadamente importante. 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 requisitos, los mecanismos, los protocolos 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 entiende que es imperativo elaborar normas y directrices en materia de seguridad aplicables que satisfagan las necesidades de todos los países.

El fortalecimiento del marco de seguridad y protección de la información de identificación personal (IIP) es un requisito previo para el desarrollo de una Sociedad de la Información muy conectada y el fomento de la confianza y la seguridad entre los usuarios de las tecnologías de la información y la comunicación (TIC). Los datos utilizados en aplicaciones y servicios se protegen mediante las tecnologías de seguridad adecuadas y la adopción de medidas físicas y organizativas. La seguridad de y por las telecomunicaciones y las TIC sigue siendo una esfera en la que se necesitarán normas de seguridad. Las nuevas tecnologías emergentes –entre ellas, la computación en nube (incluidas la computación periférica en la nube y la computación multinube), las redes eléctricas inteligentes, las fábricas inteligentes, los sistemas de transporte inteligentes, la 5ª generación de redes celulares y de otro tipo, las redes definidas por software, la virtualización de la función de red, la segmentación de red, el análisis de macrodatos, la Internet de las cosas, las tecnologías de libro mayor distribuido, los sistemas de transporte inteligentes y la seguridad cuántica– requieren medidas técnicas y de organización para hacer frente a las diversas amenazas y riesgos y proteger la IIP de los particulares, así como medidas técnicas y de organización para proteger a la infancia en línea. Además, podrían necesitarse nuevos enfoques y medidas en materia de evaluación de riesgos de seguridad para hacer frente adecuadamente a las amenazas y riesgos de seguridad. A la Comisión de Estudio 17 le aguarda un papel crucial en la elaboración de normas 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 asume su papel coordinador y 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, tecnofinancieros, OTT, 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 los trabajos sobre gestión de identidades, incluidas las identidades descentralizadas basadas en DLT, 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.

Los nuevos entornos de telecomunicaciones/TIC, véase la Internet de las cosas (IoT), los STI, las fábricas inteligentes, las ciudades/comunidades inteligentes y las redes eléctricas inteligentes, imponen nuevos requisitos al uso de la PKI. La PKI estaba pensada originalmente para garantizar la seguridad de la banca en línea y no estaba diseñada para hacer frente a entornos con entidades de baja capacidad o a 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, la seguridad de las fábricas inteligentes y las redes eléctricas inteligentes fallarán, lo cual repercutirá ampliamente en la sociedad y en la vida cotidiana al incidir en la estabilidad de gran parte de las infraestructuras esenciales. Durante el próximo periodo de estudios, cabría otorgar prioridad a los trabajos relativos a la mejora de la PKI con miras a su adaptación a estos nuevos entornos.

En aras de la seguridad, será preciso definir nuevas normas. La UIT es consciente desde hace mucho tiempo de que las herramientas 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.

# 5 Actualizaciones de la Resolución 2 de la AMNT para el periodo de estudios 2022-2024

En el Anexo 2 figuran las actualizaciones de la Resolución 2 de la AMNT propuestas por la Comisión de Estudio 17 con respecto al título, las áreas de estudio, los cometidos como Comisión de Estudio Rectora, los puntos de orientación y las Recomendaciones 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 Recomendaciones nuevas y revisadas aprobadas durante el periodo de estudios.

En ese cuadro se enumeran las **Recomendaciones, Enmiendas y Corrigenda** aprobados durante el periodo de estudios considerado hasta el 7 de enero de 2022. 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 se ordenan por la signatura (alfanumérica) de las Recomendaciones. Las Recomendaciones con doble signatura sólo aparecen una vez. Las Recomendaciones asumidas por otras Comisiones de Estudio sólo aparecerán bajo la Comisión de Estudio que la consintió o determinó.

NOTA – La última reunión a que se hace referencia en este Informe se celebró el 7 de enero de 2022.

En el Cuadro 9 figura la lista de Recomendaciones suprimidas por la Comisión de Estudio 17 durante el periodo de estudio. Los textos se ordenan por la signatura (alfanumérica) de las Recomendaciones. 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-20 para aprobación.

En el Cuadro 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 al 7 de enero de 2022.

CUADRO 7

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

| Recomendación | Aprobación | Situación | TAP/AAP | Título *(español)* |
| --- | --- | --- | --- | --- |
| [X.500](http://handle.itu.int/11.1002/1000/14031) | 14/10/2019 | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Visión de conjunto de conceptos, modelos y servicios |
| [X.501](http://handle.itu.int/11.1002/1000/14032) | 14/10/2019 | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos |
| [X.501 (2019) Enm. 1](http://handle.itu.int/11.1002/1000/14790) | 14/10/2021 | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Enmienda 1: Mejoras diversas |
| [X.509](http://handle.itu.int/11.1002/1000/14033) | 14/10/2019 | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos |
| [X.509 (2019) Cor. 1](http://handle.itu.int/11.1002/1000/14791) | 14/10/2021 | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos: Corrigéndum 1 |
| [X.510](http://handle.itu.int/11.1002/1000/14320) | 22/08/2020 | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Especificaciones de protocolo para el funcionamiento seguro |
| [X.511](http://handle.itu.int/11.1002/1000/14034) | 14/10/2019 | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Definición de servicio abstracto |
| [X.518](http://handle.itu.int/11.1002/1000/14035) | 14/10/2019 | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Procedimientos para operación distribuida |
| [X.519](http://handle.itu.int/11.1002/1000/14036) | 14/10/2019 | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Especificaciones de protocolo |
| [X.520](http://handle.itu.int/11.1002/1000/14037) | 14/10/2019 | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Tipos de atributos seleccionados |
| [X.521](http://handle.itu.int/11.1002/1000/14038) | 14/10/2019 | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Clases de objeto seleccionadas |
| [X.525](http://handle.itu.int/11.1002/1000/14047) | 14/10/2019 | En vigor | AAP | Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Replicación |
| [X.676](http://handle.itu.int/11.1002/1000/13712) | 29/11/2018 | En vigor | AAP | Marco de resolución basado en el identificador de objeto para servicios de IoT agrupados |
| [X.677](http://handle.itu.int/11.1002/1000/14039) | 08/03/2020 | En vigor | AAP | Mecanismo de identificación para vehículos aéreos sin tripulante utilizando identificadores de objeto |
| [X.680 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13257) | 14/05/2017 | Sustituida | AAP |  |
| [X.680 (2015) Cor.2](http://handle.itu.int/11.1002/1000/13361) | 14/10/2017 | Sustituida | AAP |  |
| [X.680 (2015) Cor.3](http://handle.itu.int/11.1002/1000/13598) | 14/05/2018 | Sustituida | AAP |  |
| [X.680 (2015) Enm.1](http://handle.itu.int/11.1002/1000/13597) | 14/05/2018 | Sustituida | AAP | Se abre la cláusula IMPORTACIONES a la posibilidad de importar definiciones de nuevas versiones de un módulo determinado |
| [X.680](http://handle.itu.int/11.1002/1000/14468) | 13/02/2021 | En vigor | AAP | Tecnología de la información – Notación de sintaxis abstracta uno – Especificación de la notación básica |
| [X.681 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13599) | 14/05/2018 | Sustituida | AAP |  |
| [X.681](http://handle.itu.int/11.1002/1000/14469) | 13/02/2021 | En vigor | AAP | Tecnología de la información – Notación de sintaxis abstracta uno – Especificación de objetos de información |
| [X.682 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13362) | 14/10/2017 | Sustituida | AAP |  |
| [X.682 (2015) Cor.2](http://handle.itu.int/11.1002/1000/13600) | 14/05/2018 | Sustituida | AAP |  |
| [X.682](http://handle.itu.int/11.1002/1000/14470) | 13/02/2021 | En vigor | AAP | Tecnología de la información – Notación de sintaxis abstracta uno – Especificación de constricciones |
| [X.683 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13601) | 14/05/2018 | Sustituida | AAP |  |
| [X.683](http://handle.itu.int/11.1002/1000/14471) | 13/02/2021 | En vigor | AAP | Tecnología de la información – Notación de sintaxis abstracta uno – Parametrización de especificaciones de notación de sintaxis abstracta uno |
| [X.690](http://handle.itu.int/11.1002/1000/14472) | 13/02/2021 | 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.691](http://handle.itu.int/11.1002/1000/14473) | 13/02/2021 | En vigor | AAP | Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación compactada |
| [X.692](http://handle.itu.int/11.1002/1000/14474) | 13/02/2021 | 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) Cor.1](http://handle.itu.int/11.1002/1000/13363) | 14/10/2017 | Sustituida | AAP |  |
| [X.693](http://handle.itu.int/11.1002/1000/14475) | 13/02/2021 | 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.694 (2015) Cor.1](http://handle.itu.int/11.1002/1000/14040) | 14/10/2019 | Sustituida | AAP |  |
| [X.694](http://handle.itu.int/11.1002/1000/14476) | 13/02/2021 | 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.695](http://handle.itu.int/11.1002/1000/14477) | 13/02/2021 | 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 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13258) | 14/05/2017 | Sustituida | AAP |  |
| [X.696 (2015) Cor.2](http://handle.itu.int/11.1002/1000/13364) | 14/10/2017 | Sustituida | AAP |  |
| [X.696 (2015) Cor.3](http://handle.itu.int/11.1002/1000/13602) | 14/05/2018 | Sustituida | AAP |  |
| [X.696](http://handle.itu.int/11.1002/1000/14478) | 13/02/2021 | En vigor | AAP | Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de reglas de codificación de octetos (OER) |
| [X.697](http://handle.itu.int/11.1002/1000/13365) | 14/10/2017 | Sustituida | AAP | Tecnología de la información – Reglas de codificación ASN.1: Especificación de las reglas de codificación de notificación de objeto de JavaScript (JER) |
| [X.697](http://handle.itu.int/11.1002/1000/14479) | 13/02/2021 | En vigor | AAP | Tecnología de la información – Reglas de codificación ASN.1: Especificación de las reglas de codificación de notificación de objeto de JavaScript (JER) |
| [X.893 (2007) Cor.1](http://handle.itu.int/11.1002/1000/14041) | 14/10/2019 | En vigor | AAP |  |
| [X.894](http://handle.itu.int/11.1002/1000/12848) | 14/10/2018 | En vigor | AAP | Tecnología de la información – Aplicaciones genéricas de ASN.1: Sintaxis de mensaje criptográfico |
| [X.894 (2018) Cor.1](http://handle.itu.int/11.1002/1000/13871) | 16/03/2019 | En vigor | AAP |  |
| [X.894 (2018) Cor. 2](http://handle.itu.int/11.1002/1000/14467) | 13/02/2021 | En vigor | AAP | Aplicaciones genéricas de ASN.1 – Sintaxis de mensaje criptográfico – Corrigéndum técnico |
| [X.1011](http://handle.itu.int/11.1002/1000/14793) | 29/10/2021 | En vigor | AAP | Directrices para la protección continua del proceso de acceso al servicio |
| [X.1040](http://handle.itu.int/11.1002/1000/13366) | 14/10/2017 | En vigor | AAP | Arquitectura de seguridad de referencia para la gestión de la vida útil de los datos corporativos del comercio electrónico |
| [X.1041](http://handle.itu.int/11.1002/1000/13603) | 14/05/2018 | En vigor | AAP | Marco de seguridad para la operación de redes de voz por evolución a largo plazo (VoLTE) |
| [X.1042](http://handle.itu.int/11.1002/1000/13803) | 30/01/2019 | En vigor | TAP | Servicios de seguridad que utilizan redes definidas por software |
| [X.1043](http://handle.itu.int/11.1002/1000/13872) | 16/03/2019 | En vigor | AAP | Marco y requisitos de seguridad para el encadenamiento de funciones de servicio basado en redes definidas por software |
| [X.1044](http://handle.itu.int/11.1002/1000/14042) | 29/10/2019 | En vigor | AAP | Requisitos de seguridad de la virtualización de red |
| [X.1045](http://handle.itu.int/11.1002/1000/14043) | 29/10/2019 | En vigor | AAP | Arquitectura de la cadena de servicios de seguridad para redes y aplicaciones |
| [X.1046](http://handle.itu.int/11.1002/1000/14442) | 14/12/2020 | En vigor | AAP | Marco de seguridad definida por software en redes definidas por software/redes de virtualización de las funciones de red |
| [X.1047](http://handle.itu.int/11.1002/1000/14794) | 29/10/2021 | En vigor | AAP | Requisitos y arquitectura de seguridad para la gestión y orquestación de la segmentación de red |
| [X.1051 (2016) Cor.1](http://handle.itu.int/11.1002/1000/13407) | 06/09/2017 | En vigor | Acuerdo |  |
| [X.1052](http://handle.itu.int/11.1002/1000/14044) | 29/10/2020 | En vigor | AAP | Procesos de gestión de la seguridad de la información para organizaciones de telecomunicaciones |
| [X.1053](http://handle.itu.int/11.1002/1000/13367) | 13/11/2017 | En vigor | AAP | Código de prácticas sobre controles de seguridad de la información basada en la Recomendación UIT-T X.1051 para organizaciones de telecomunicaciones de pequeño o mediano tamaño |
| [X.1058](http://handle.itu.int/11.1002/1000/13182) | 30/03/2017 | En vigor | TAP | Tecnología de la información – Técnicas de seguridad – Código de práctica para la protección de información de identificación personal |
| [X.1059](http://handle.itu.int/11.1002/1000/14045) | 29/10/2019 | En vigor | AAP | Guía de aplicación para las organizaciones de telecomunicaciones sobre la gestión de riesgos de sus activos accesibles a nivel mundial en redes basadas en el IP |
| [X.1060](http://handle.itu.int/11.1002/1000/14721) | 29/06/2021 | En vigor | AAP | Marco para la creación y operación de un centro de ciberdefensa |
| [X.1061](http://handle.itu.int/11.1002/1000/14733) | 22/08/2021 | En vigor | AAP | Directrices para la adquisición de ciberseguros |
| [X.1080.0](http://handle.itu.int/11.1002/1000/13193) | 30/03/2017 | En vigor | TAP | Control de acceso para la protección de datos telebiométricos |
| [X.1080.0 (2017) Cor.1](http://handle.itu.int/11.1002/1000/13591) | 29/03/2018 | En vigor | Acuerdo |  |
| [X.1080.1](http://handle.itu.int/11.1002/1000/13604) | 14/05/2018 | En vigor | AAP | Cibersalud y telemedicinas mundiales – Protocolo de telecomunicaciones genérico |
| [X.1080.2](http://handle.itu.int/11.1002/1000/14795) | 29/10/2021 | En vigor | AAP | Protocolo biología a máquina (B2M) |
| [X.1093](http://handle.itu.int/11.1002/1000/13725) | 13/11/2018 | En vigor | AAP | Control de acceso telebiométrico con tarjetas de identidad inteligentes |
| [X.1094](http://handle.itu.int/11.1002/1000/13873) | 16/03/2019 | En vigor | AAP | Autentificación telebiométrica mediante bioseñales |
| [X.1126](http://handle.itu.int/11.1002/1000/13194) | 30/03/2017 | En vigor | TAP | Directrices para paliar los efectos negativos de los terminales infectados en las redes móviles |
| [X.1127](http://handle.itu.int/11.1002/1000/13259) | 06/09/2017 | En vigor | TAP | Arquitectura y requisitos de seguridad funcionales para las medidas antirrobo de teléfonos móviles |
| [X.1145](http://handle.itu.int/11.1002/1000/13260) | 14/05/2017 | En vigor | AAP | Marco y requisitos de seguridad para las capacidades abiertas de servicios de telecomunicación |
| [X.1146](http://handle.itu.int/11.1002/1000/13368) | 14/10/2017 | En vigor | AAP | Directrices sobre garantía de protección de servicios de valor añadido prestados por operadores de telecomunicaciones |
| [X.1147](http://handle.itu.int/11.1002/1000/13726) | 13/11/2018 | En vigor | AAP | Requisitos de seguridad y marco para el análisis de macrodatos en los servicios de Internet móvil |
| [X.1148](http://handle.itu.int/11.1002/1000/14249) | 03/09/2020 | En vigor | TAP | Marco del proceso de desidentificación para proveedores de servicios de telecomunicaciones |
| [X.1149](http://handle.itu.int/11.1002/1000/14250) | 29/05/2020 | En vigor | AAP | Marco de seguridad de la plataforma abierta para servicios tecnofinancieros |
| [X.1197 (2012) Enm.1](http://handle.itu.int/11.1002/1000/14046) | 05/09/2019 | En vigor | Acuerdo |  |
| [X.1212](http://handle.itu.int/11.1002/1000/13195) | 30/03/2017 | En vigor | TAP | Consideraciones de diseño para la mejor percepción por el usuario extremo de los indicadores de fiabilidad |
| [X.1213](http://handle.itu.int/11.1002/1000/13261) | 06/09/2017 | En vigor | TAP | Capacidades de seguridad necesarias para luchar contra las redes robot en teléfonos inteligentes |
| [X.1214](http://handle.itu.int/11.1002/1000/13404) | 29/03/2018 | En vigor | TAP | Técnicas de evaluación de la seguridad en las redes de telecomunicaciones/tecnologías de la información y la comunicación |
| [X.1215](http://handle.itu.int/11.1002/1000/13849) | 30/01/2019 | En vigor | TAP | Expresión estructurada de información sobre amenazas: casos de uso |
| [X.1216](http://handle.itu.int/11.1002/1000/14259) | 03/09/2020 | En vigor | TAP | Requisitos para la obtención y preservación de pruebas de incidentes de ciberseguridad |
| [X.1217](http://handle.itu.int/11.1002/1000/14443) | 07/01/2021 | En vigor | TAP | Directrices para la aplicación de la información sobre amenazas en la explotación de redes de telecomunicaciones |
| [X.1218](http://handle.itu.int/11.1002/1000/14444) | 29/10/2020 | En vigor | AAP | Requisitos para el análisis dinámico de malware en entornos aislados y directrices conexas |
| [X.1232](http://handle.itu.int/11.1002/1000/14085) | 29/10/2019 | En vigor | AAP | Marco técnico para luchar contra el spam publicitario en la información generada por el usuario |
| [X.1233](http://handle.itu.int/11.1002/1000/14773) | 03/09/2021 | En vigor | TAP | Directrices para contrarrestar los mensajes basura por mensajería instantánea |
| X.1234 | 07/01/2022 | En vigor | TAP | Directrices para la lucha contra el spam en el servicio de mensajería multimedios |
| X.1235 | 07/01/2022 | En vigor | TAP | Tecnologías contra la suplantación de sitios web para las organizaciones de telecomunicaciones |
| [X.1248](http://handle.itu.int/11.1002/1000/13262) | 06/09/2017 | En vigor | TAP | Requisitos técnicos para luchar contra el spam en mensajería instantánea |
| [X.1249](http://handle.itu.int/11.1002/1000/13605) | 30/01/2019 | En vigor | TAP | Marco técnico para contrarrestar el spam publicitario en aplicaciones móviles |
| [X.1252](http://handle.itu.int/11.1002/1000/14642) | 30/04/2021 | En vigor | TAP | Términos y definiciones de referencia para la gestión de la identidad |
| [X.1254](http://handle.itu.int/11.1002/1000/14260) | 03/09/2020 | En vigor | TAP | Marco de garantía de autentificación de entidad |
| [X.1276](http://handle.itu.int/11.1002/1000/13606) | 14/05/2018 | En vigor | AAP | Protocolo y metadatos de mejora de autentificación Versión 1.0 |
| [X.1277](http://handle.itu.int/11.1002/1000/13727) | 29/11/2018 | En vigor | AAP | Marco universal de autentificación |
| [X.1278](http://handle.itu.int/11.1002/1000/13728) | 29/11/2018 | En vigor | AAP | Protocolo cliente a autentificador/Marco universal de 2 factores |
| [X.1279](http://handle.itu.int/11.1002/1000/14261) | 03/09/2020 | En vigor | TAP | Marco de autentificación mejorada mediante telebiometría con mecanismos de detección antisuplantación |
| [X.1331](http://handle.itu.int/11.1002/1000/13405) | 29/03/2018 | En vigor | TAP | Directrices de seguridad para dispositivos de redes domésticas (HAN) en sistemas eléctricos inteligentes |
| [X.1332](http://handle.itu.int/11.1002/1000/14086) | 26/03/2020 | En vigor | TAP | Directrices de seguridad para servicios de medición inteligentes en redes inteligentes |
| X.1333 | 07/01/2022 | En vigor | TAP | Directrices de seguridad para la utilización de herramientas de acceso remoto en sistemas de control conectados a Internet |
| [X.1361](http://handle.itu.int/11.1002/1000/13607) | 07/09/2018 | En vigor | TAP | Marco de seguridad para la Internet de las cosas basado en el modelo de pasarela |
| [X.1362](http://handle.itu.int/11.1002/1000/13196) | 30/03/2017 | En vigor | TAP | Procedimiento de encriptación simple para la Internet de las cosas (IoT) |
| [X.1363](http://handle.itu.int/11.1002/1000/14087) | 29/05/2020 | En vigor | TAP | Marco técnico para el tratamiento de la información de identificación personal en el contexto de la Internet de las cosas |
| [X.1364](http://handle.itu.int/11.1002/1000/14088) | 26/03/2020 | En vigor | TAP | Requisitos y marco de seguridad de la Internet de las cosas de banda estrecha |
| [X.1365](http://handle.itu.int/11.1002/1000/14089) | 26/03/2020 | En vigor | TAP | Metodología de seguridad para el uso de criptografía basada en la identidad para dar soporte a servicios de Internet de las cosas por redes de telecomunicaciones |
| [X.1366](http://handle.itu.int/11.1002/1000/14262) | 03/09/2020 | En vigor | TAP | Sistema de autentificación de mensajes combinados para la Internet de las cosas |
| [X.1367](http://handle.itu.int/11.1002/1000/14263) | 03/09/2020 | En vigor | TAP | Formato normalizado para los registros de errores de Internet de las cosas utilizado en las operaciones de incidentes de seguridad |
| [X.1368](http://handle.itu.int/11.1002/1000/14445) | 07/01/2022 | En vigor | TAP | Actualización segura de firmware/software para Internet de las cosas |
| X.1369 | 07/01/2022 | En vigor | TAP | Requisitos de seguridad para las plataformas del servicio IoT |
| [X.1371](http://handle.itu.int/11.1002/1000/14090) | 29/05/2020 | En vigor | TAP | Amenazas a la seguridad de los vehículos conectados |
| [X.1372](http://handle.itu.int/11.1002/1000/14091) | 26/03/2020 | En vigor | TAP | Directrices de seguridad para la comunicación entre el vehículo y su entorno (V2X) |
| [X.1373](http://handle.itu.int/11.1002/1000/13197) | 30/03/2017 | En vigor | TAP | Capacidad de actualización segura de software en dispositivos de comunicación de sistemas de transporte inteligentes |
| [X.1374](http://handle.itu.int/11.1002/1000/14446) | 29/10/2020 | En vigor | AAP | Requisitos de seguridad de interfaces externas y dispositivos con capacidad de acceso a vehículos |
| [X.1375](http://handle.itu.int/11.1002/1000/14447) | 29/10/2020 | En vigor | AAP | Directrices para los sistemas de detección de intrusiones en redes intravehiculares |
| [X.1376](http://handle.itu.int/11.1002/1000/14448) | 07/01/2021 | En vigor | TAP | Mecanismo de detección de conductas indebidas mediante macrodatos para vehículos conectados |
| [X.1400](http://handle.itu.int/11.1002/1000/14449) | 29/10/2020 | En vigor | AAP | Términos y definiciones utilizados en la tecnología de libro mayor distribuido |
| [X.1401](http://handle.itu.int/11.1002/1000/14092) | 29/11/2019 | En vigor | AAP | Amenazas a la seguridad de la tecnología de libro mayor distribuido |
| [X.1402](http://handle.itu.int/11.1002/1000/14251) | 21/07/2022 | En vigor | AAP | Marco de seguridad para la tecnología de libro mayor distribuido |
| [X.1403](http://handle.itu.int/11.1002/1000/14264) | 03/09/2020 | En vigor | TAP | Directrices de seguridad para el uso de sistemas de tecnología de libro mayor distribuido a efectos de la gestión descentralizada de identidades |
| [X.1404](http://handle.itu.int/11.1002/1000/14450) | 29/10/2020 | En vigor | AAP | Garantía de seguridad para la tecnología de libro mayor distribuido |
| [X.1405](http://handle.itu.int/11.1002/1000/14722) | 29/06/2021 | En vigor | AAP | Amenazas y requisitos de seguridad para los servicios de pago digitales basados en la tecnología de libro mayor distribuido |
| [X.1406](http://handle.itu.int/11.1002/1000/14734) | 14/07/2021 | En vigor | AAP | Amenazas de seguridad para la votación en línea mediante la tecnología de libro mayor distribuido |
| X.1407 | 07/01/2022 | En vigor | TAP | Requisitos de seguridad para el servicio de validación de la integridad digital basado en la tecnología de libro mayor distribuido |
| [X.1408](http://handle.itu.int/11.1002/1000/14801) | 29/10/2021 | En vigor | AAP | Amenazas y requisitos de seguridad para el acceso y la compartición de datos basados en la tecnología de libro mayor distribuido |
| [X.1450](http://handle.itu.int/11.1002/1000/13729) | 14/10/2018 | En vigor | AAP | Directrices sobre los mecanismos de autentificación híbrida y de gestión de claves en el modelo cliente-servidor |
| [X.1451](http://handle.itu.int/11.1002/1000/14252) | 29/05/2020 | En vigor | AAP | Identificación de riesgos para optimizar la autentificación |
| [X.1452](http://handle.itu.int/11.1002/1000/14451) | 29/10/2020 | En vigor | AAP | Directrices para los servicios de seguridad prestados por los operadores |
| X.1453 | 07/01/2022 | En vigor | TAP | Amenazas y requisitos de seguridad para sistemas de gestión de vídeo |
| [X.1470](http://handle.itu.int/11.1002/1000/14803) | 13/11/2021 | En vigor | AAP | Directrices de seguridad para el servicio de atención al cliente en línea por la web |
| [X.1500 (2011) Enm.11](http://handle.itu.int/11.1002/1000/13263) | 30/03/2017 | Sustituida | Acuerdo | Técnicas revisadas de intercambio de información estructurada sobre ciberseguridad |
| [X.1500 (2011) Enm.12](http://handle.itu.int/11.1002/1000/13590) | 29/03/2018 | En vigor | Acuerdo | Técnicas revisadas de intercambio de información estructurada sobre ciberseguridad |
| [X.1541](http://handle.itu.int/11.1002/1000/13264) | 06/09/2017 | En vigor | TAP | Formato para el intercambio de descripciones de objetos de incidentes Versión 2 |
| [X.1550](http://handle.itu.int/11.1002/1000/13198) | 30/03/2017 | En vigor | TAP | Modelos de control de acceso para redes de intercambio de incidentes |
| [X.1603](http://handle.itu.int/11.1002/1000/13406) | 29/03/2018 | En vigor | TAP | Requisitos de seguridad de los datos para el servicio de control de la computación en la nube |
| [X.1604](http://handle.itu.int/11.1002/1000/14093) | 26/03/2020 | En vigor | TAP | Requisitos de seguridad de la red como servicio (NaaS) en la computación en la nube |
| [X.1605](http://handle.itu.int/11.1002/1000/14094) | 26/03/2020 | En vigor | TAP | Requisitos de seguridad de la infraestructura pública como servicio (IaaS) en la computación en la nube |
| [X.1606](http://handle.itu.int/11.1002/1000/14265) | 03/09/2020 | En vigor | TAP | Requisitos de seguridad para el entorno de aplicación Comunicaciones como servicio (CaaS) |
| X.1643 | 07/01/2022 | En vigor | TAP | Requisitos de seguridad y directrices para el contenedor de virtualización en el entorno de computación en la nube |
| [X.1702](http://handle.itu.int/11.1002/1000/14095) | 13/11/2019 | En vigor | AAP | Arquitectura de un generador de números aleatorios de ruido cuántico |
| [X.1710](http://handle.itu.int/11.1002/1000/14452) | 29/10/2020 | En vigor | AAP | Marco de seguridad para redes de distribución de claves cuánticas |
| [X.1712](http://handle.itu.int/11.1002/1000/14805) | 29/10/2021 | En vigor | AAP | Requisitos y medidas de seguridad para las redes de distribución de claves cuánticas – gestión de claves |
| [X.1714](http://handle.itu.int/11.1002/1000/14453) | 29/10/2020 | En vigor | AAP | Combinación de claves y suministro de claves confidenciales en redes de distribución de claves cuánticas |
| [X.1750](http://handle.itu.int/11.1002/1000/14266) | 03/09/2020 | En vigor | TAP | Directrices sobre la seguridad de macrodatos como servicio destinadas a los proveedores de servicios de macrodatos |
| [X.1751](http://handle.itu.int/11.1002/1000/14267) | 03/09/2020 | En vigor | TAP | Directrices de seguridad para la gestión del ciclo vital de macrodatos destinadas por los operadores de telecomunicaciones |
| X.1752 | 07/01/2022 | En vigor | TAP | Directrices de seguridad para las infraestructuras y plataformas de macrodatos |
| [X.1770](http://handle.itu.int/11.1002/1000/14807) | 29/10/2021 | En vigor | AAP | Directrices técnicas para la computación multipartita segura |
| [X.1811](http://handle.itu.int/11.1002/1000/14454) | 30/04/2021 | En vigor | TAP | Directrices de seguridad para la aplicación de algoritmos de seguridad cuántica en sistemas IMT-2000 |
| [Z.100 Anexo F1](http://handle.itu.int/11.1002/1000/13732) | 13/11/2018 | Sustituido | AAP | Lenguaje de especificación y descripción – Visión general de SDL‑2010 |
| [Z.100 Anexo F2](http://handle.itu.int/11.1002/1000/13733) | 13/11/2018 | Sustituido | AAP | Lenguaje de especificación y descripción – Visión general de SDL‑2010 |
| [Z.100 Anexo F3](http://handle.itu.int/11.1002/1000/13734) | 13/11/2018 | Sustituido | AAP | Lenguaje de especificación y descripción – Visión general de SDL‑2010 |
| [Z.100](http://handle.itu.int/11.1002/1000/14048) | 14/10/2019 | Sustituida | AAP | Lenguaje de especificación y descripción – Visión general de SDL‑2010 |
| [Z.100 Anexo F2](http://handle.itu.int/11.1002/1000/14050) | 14/10/2019 | Sustituido | AAP | Lenguaje de especificación y descripción – Visión general de SDL‑2010 – Definición formal de SDL: semántica estática |
| [Z.100 Anexo F3](http://handle.itu.int/11.1002/1000/14051) | 14/10/2019 | Sustituido | AAP | Lenguaje de especificación y descripción – Visión general de SDL‑2010 – Definición formal de SDL: semántica dinámica |
| [Z.100](http://handle.itu.int/11.1002/1000/14670) | 13/16/2021 | En vigor | AAP | Lenguaje de especificación y descripción – Visión general de SDL‑2010 |
| [Z.100 Anexo F1](http://handle.itu.int/11.1002/1000/14049) | 14/10/2019 | En vigor | AAP | Lenguaje de especificación y descripción – Visión general de SDL‑2010 – Definición formal de SDL: aspectos generales |
| [Z.100 Anexo F2](http://handle.itu.int/11.1002/1000/14702) | 13/06/2021 | En vigor | AAP | Lenguaje de especificación y descripción – Visión general de SDL – Definición formal de SDL: semántica estática |
| [Z.100 Anexo F3](http://handle.itu.int/11.1002/1000/14703) | 13/06/2021 | En vigor | AAP | Lenguaje de especificación y descripción – Visión general de SDL – Definición formal de SDL: semántica dinámica |
| [Z.101](http://handle.itu.int/11.1002/1000/14052) | 14/10/2019 | Sustituida | AAP | Lenguaje de especificación y descripción – SDL-2010 básica |
| [Z.101](http://handle.itu.int/11.1002/1000/14671) | 13/06/2021 | En vigor | AAP | Lenguaje de especificación y descripción – SDL-2010 básica |
| [Z.102](http://handle.itu.int/11.1002/1000/14053) | 14/10/2019 | Sustituida | AAP | Lenguaje de especificación y descripción – SDL-2010 integral |
| [Z.102](http://handle.itu.int/11.1002/1000/14672) | 13/06/2021 | En vigor | AAP | Lenguaje de especificación y descripción – SDL-2010 integral |
| [Z.103](http://handle.itu.int/11.1002/1000/14054) | 14/10/2019 | Sustituida | AAP | Lenguaje de especificación y descripción – Notación abreviada y anotación en SDL-2010 |
| [Z.103](http://handle.itu.int/11.1002/1000/14673) | 13/06/2021 | En vigor | AAP | Lenguaje de especificación y descripción – Notación abreviada y anotación en SDL-2010 |
| [Z.104](http://handle.itu.int/11.1002/1000/14055) | 14/10/2019 | Sustituida | AAP | Lenguaje de especificación y descripción – Datos y lenguaje de acción en SDL-2010 |
| [Z.104](http://handle.itu.int/11.1002/1000/14674) | 13/06/2021 | En vigor | AAP | Lenguaje de especificación y descripción – Datos y lenguaje de acción en SDL-2010 |
| [Z.105](http://handle.itu.int/11.1002/1000/14056) | 14/10/2019 | Sustituida | AAP | Lenguaje de especificación y descripción – SDL-2010 combinado con módulos ASN.1 |
| [Z.105](http://handle.itu.int/11.1002/1000/14675) | 13/06/2021 | En vigor | AAP | Lenguaje de especificación y descripción – SDL-2010 combinado con módulos ASN.1 |
| [Z.106](http://handle.itu.int/11.1002/1000/14057) | 14/10/2019 | Sustituida | AAP | Lenguaje de especificación y descripción – Formato de intercambio común para SDL-2010 |
| [Z.106](http://handle.itu.int/11.1002/1000/14676) | 13/06/2021 | En vigor | AAP | Lenguaje de especificación y descripción – Formato de intercambio común para SDL-2010 |
| [Z.107](http://handle.itu.int/11.1002/1000/14058) | 14/10/2019 | Sustituida | AAP | Lenguaje de especificación y descripción – Datos orientados a objetos en SDL-2010 |
| [Z.107](http://handle.itu.int/11.1002/1000/14677) | 13/06/2021 | En vigor | AAP | Lenguaje de especificación y descripción – Datos orientados a objetos en SDL-2010 |
| [Z.151](http://handle.itu.int/11.1002/1000/13711) | 14/10/2018 | En vigor | AAP | Notación de los requisitos de usuario (URN) – definición del lenguaje |
| [Z.161](http://handle.itu.int/11.1002/1000/13369) | 14/10/2017 | Sustituida | AAP | Notación de prueba y de control de pruebas versión 3: Lenguaje núcleo de TTCN-3 |
| [Z.161](http://handle.itu.int/11.1002/1000/13703) | 14/10/2018 | Sustituida | AAP | Notación de prueba y de control de pruebas versión 3: Lenguaje núcleo de TTCN-3 |
| [Z.161](http://handle.itu.int/11.1002/1000/14059) | 14/10/2019 | Sustituida | AAP | Notación de prueba y de control de pruebas versión 3: Lenguaje núcleo de TTCN-3 |
| [Z.161](http://handle.itu.int/11.1002/1000/14480) | 29/10/2020 | Sustituida | AAP | Notación de prueba y de control de pruebas versión 3: Lenguaje núcleo de TTCN-3 |
| [Z.161](http://handle.itu.int/11.1002/1000/14781) | 14/10/2021 | En vigor | AAP | Notación de prueba y de control de pruebas versión 3: Lenguaje núcleo de TTCN-3 |
| [Z.161.1](http://handle.itu.int/11.1002/1000/13370) | 14/10/2017 | 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](http://handle.itu.int/11.1002/1000/13371) | 14/10/2017 | Sustituida | 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](http://handle.itu.int/11.1002/1000/13704) | 14/10/2018 | Sustituida | 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](http://handle.itu.int/11.1002/1000/14060) | 14/10/2019 | Sustituida | 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](http://handle.itu.int/11.1002/1000/14782) | 14/10/2021 | 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](http://handle.itu.int/11.1002/1000/13372) | 14/10/2017 | Sustituida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN‑3: Parametrización avanzada |
| [Z.161.3](http://handle.itu.int/11.1002/1000/14481) | 29/10/2020 | Sustituida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN‑3: Parametrización avanzada |
| [Z.161.3](http://handle.itu.int/11.1002/1000/14783) | 14/10/2021 | En vigor | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN‑3: Parametrización avanzada |
| [Z.161.4](http://handle.itu.int/11.1002/1000/13373) | 14/10/2017 | Sustituida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN‑3: Tipos de comportamiento |
| [Z.161.4](http://handle.itu.int/11.1002/1000/13705) | 14/10/2018 | Sustituida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN‑3: Tipos de comportamiento |
| [Z.161.4](http://handle.itu.int/11.1002/1000/14482) | 29/10/2020 | Sustituida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN‑3: Tipos de comportamiento |
| [Z.161.4](http://handle.itu.int/11.1002/1000/14784) | 14/10/2021 | En vigor | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN‑3: Tipos de comportamiento |
| [Z.161.6](http://handle.itu.int/11.1002/1000/13374) | 14/10/2017 | Sustituida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN‑3: Ajustes avanzados |
| [Z.161.6](http://handle.itu.int/11.1002/1000/13706) | 14/10/2018 | Sustituida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN‑3: Ajustes avanzados |
| [Z.161.6](http://handle.itu.int/11.1002/1000/14061) | 14/10/2019 | Sustituida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN‑3: Ajustes avanzados |
| [Z.161.6](http://handle.itu.int/11.1002/1000/14483) | 29/10/2020 | En vigor | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN‑3: Ajustes avanzados |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14062) | 14/10/2019 | Sustituida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN‑3: Características orientadas a objetos |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14484) | 29/10/2020 | Sustituida | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN‑3: Características orientadas a objetos |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14785) | 14/10/2021 | En vigor | AAP | Notación de prueba y de control de prueba versión 3: Ampliaciones de lenguaje TTCN‑3: Características orientadas a objetos |
| [Z.164](http://handle.itu.int/11.1002/1000/13375) | 14/10/2017 | En vigor | AAP | Notación de pruebas y de control de pruebas versión 3: Semántica operacional |
| [Z.165](http://handle.itu.int/11.1002/1000/13376) | 14/10/2017 | En vigor | AAP | Notación de pruebas y de control de pruebas versión 3: Interfaz de ejecución |
| [Z.165.1](http://handle.itu.int/11.1002/1000/14485) | 29/10/2020 | En vigor | AAP | Notación de prueba y de control de prueba versión 3: ampliaciones del lenguaje TTCN-3: Extended TRI |
| [Z.166](http://handle.itu.int/11.1002/1000/13377) | 14/10/2017 | Sustituida | AAP | Notación de pruebas y de control de pruebas versión 3: Interfaz de control |
| [Z.166](http://handle.itu.int/11.1002/1000/13707) | 14/10/2018 | Sustituida | AAP | Notación de pruebas y de control de pruebas versión 3: Interfaz de control |
| [Z.166](http://handle.itu.int/11.1002/1000/14063) | 14/10/2019 | Sustituida | AAP | Notación de pruebas y de control de pruebas versión 3: Interfaz de control |
| [Z.166](http://handle.itu.int/11.1002/1000/14486) | 29/10/2020 | En vigor | AAP | Notación de pruebas y de control de pruebas versión 3: Interfaz de control |
| [Z.167](http://handle.itu.int/11.1002/1000/13378) | 14/10/2017 | Sustituida | AAP | Notación de pruebas y de control de pruebas versión 3: Utilización de ASN.1 con TTCN-3 |
| [Z.167](http://handle.itu.int/11.1002/1000/13708) | 14/10/2018 | Sustituida | AAP | Notación de pruebas y de control de pruebas versión 3: Utilización de ASN.1 con TTCN-3 |
| [Z.167](http://handle.itu.int/11.1002/1000/14487) | 29/10/2020 | Sustituida | AAP | Notación de pruebas y de control de pruebas versión 3: Utilización de ASN.1 con TTCN-3 |
| [Z.167](http://handle.itu.int/11.1002/1000/14786) | 14/10/2021 | En vigor | AAP | Notación de pruebas y de control de pruebas versión 3: Utilización de ASN.1 con TTCN-3 |
| [Z.168](http://handle.itu.int/11.1002/1000/13379) | 14/10/2017 | Sustituida | AAP | Notación de pruebas y de control de pruebas versión 3: Correspondencia del lenguaje IDL con la notación TTCN-3 |
| [Z.168](http://handle.itu.int/11.1002/1000/14787) | 14/10/2021 | En vigor | AAP | Notación de pruebas y de control de pruebas versión 3: Correspondencia del lenguaje IDL con la notación TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/13380) | 14/10/2017 | Sustituida | AAP | Notación de pruebas y de control de pruebas versión 3: Utilización de esquemas XML con TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/13709) | 14/10/2018 | Sustituida | AAP | Notación de pruebas y de control de pruebas versión 3: Utilización de esquemas XML con TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/14064) | 14/10/2019 | Sustituida | AAP | Notación de pruebas y de control de pruebas versión 3: Utilización de esquemas XML con TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/14488) | 29/10/2020 | Sustituida | AAP | Notación de pruebas y de control de pruebas versión 3: Utilización de esquemas XML con TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/14788) | 14/10/2021 | En vigor | AAP | Notación de pruebas y de control de pruebas versión 3: Utilización de esquemas XML con TTCN-3 |
| [Z.170](http://handle.itu.int/11.1002/1000/13381) | 14/10/2017 | En vigor | AAP | Notación de pruebas y de control de pruebas versión 3: Especificación de los comentarios de documentación TTCN-3 |
| [Z.171](http://handle.itu.int/11.1002/1000/13382) | 14/10/2017 | Sustituida | AAP | Notación de pruebas y de control de pruebas versión 3: Utilización de JSON con TTCN-3 |
| [Z.171](http://handle.itu.int/11.1002/1000/13710) | 14/10/2018 | Sustituida | AAP | Notación de pruebas y de control de pruebas versión 3: Utilización de JSON con TTCN-3 |
| [Z.171](http://handle.itu.int/11.1002/1000/14789) | 14/10/2021 | En vigor | AAP | Notación de pruebas y de control de pruebas versión 3: Utilización de JSON con TTCN-3 |

CUADRO 8

Comisión de Estudio 17 – Recomendaciones consentidas/determinadas (por aprobar)

| Recomendación | Consentimiento/determinación | TAP/AAP | Título |
| --- | --- | --- | --- |
| X.672 | 03/09/2021 | AAP | Sistema de resolución de identificadores de objeto |
| Enmienda 1 de X.1246 | 03/09/2021 | TAP | Tecnologías implicadas en la lucha contra el spam vocal en organizaciones de telecomunicaciones |
| Enmienda 1 de X.1247 | 03/09/2021 | TAP | Marco técnico para la lucha contra el spam en mensajería móvil |
| Corrigéndum de X.1712 | 07/01/2022 | AAP | Requisitos y medidas de seguridad para redes de distribución de claves cuánticas – gestión de claves |
| X.1812 (X.5Gsec-t) | 03/09/2021 | TAP | Marco de seguridad basado en la relación de confianza en el ecosistema IMT-2020 |

CUADRO 9

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

| Recomendación | Última versión | Fecha de supresión | Título |
| --- | --- | --- | --- |
| Ninguna |  |  |  |

CUADRO 10

Comisión de Estudio 17 – Recomendaciones sometidas a la AMNT-20

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

CUADRO 11

Comisión de Estudio 17 – Suplementos

| Recomendación | Aprobación | Situación | Título *(español)* |
| --- | --- | --- | --- |
| [X Supl. 13](http://handle.itu.int/11.1002/1000/13730) | 07/09/2018 | En vigor | UIT-T X.1051 – Suplemento sobre la guía del usuario relativa a la gobernanza de la seguridad de la información para la Recomendación UIT-T X.1051 |
| [X Supl. 26 (2016) Cor.1](http://handle.itu.int/11.1002/1000/13592) | 29/03/2018 | En vigor |  |
| [X Supl. 29](http://handle.itu.int/11.1002/1000/13409) | 06/09/2017 | En vigor | UIT-T X.1242 – Suplemento sobre las directrices relativas a las contramedidas contra los ataques de pesca y suplantación de identidad en el servicio de mensajes breves  |
| [X Supl. 30](http://handle.itu.int/11.1002/1000/13410) | 06/09/2017 | En vigor | UIT-T X.805 – Suplemento sobre las directrices de seguridad para operadores de redes móviles virtuales |
| [X Supl. 31](http://handle.itu.int/11.1002/1000/13411) | 06/09/2017 | En vigor | UIT-T X.660 – Suplemento sobre las directrices de utilización de los identificadores de objeto para Internet de las cosas |
| [X Supl. 32](http://handle.itu.int/11.1002/1000/13593) | 29/03/2018 | En vigor | UIT-T X.1058 – Suplemento sobre el código de práctica para la protección de la información de identificación personal (PII) para organizaciones de telecomunicaciones |
| [X Supl. 33](http://handle.itu.int/11.1002/1000/13731) | 07/09/2018 | En vigor | UIT-T X.1231 – Suplemento sobre el marco técnico para la lucha contra el fraude por el servicio telefónico |
| [X Supl. 34](http://handle.itu.int/11.1002/1000/13869) | 30/01/2019 | En vigor | UIT-T X.1051 – Suplemento sobre el código de práctica para controles de seguridad de la información destinado a organizaciones de telecomunicaciones |
| [X Supl. 35](http://handle.itu.int/11.1002/1000/14066) | 05/09/2019 | En vigor | UIT-T X.1254 – Suplemento sobre casos de uso del marco de garantía de autentificación de entidades (EAA) |
| [X Supl. 36](http://handle.itu.int/11.1002/1000/14809) | 03/09/2021 | En vigor | UIT-T X.1051 – Suplemento sobre los controles de seguridad esenciales para la gestión de la seguridad de redes e informaciones de las organizaciones de telecomunicaciones |

cuadro 12

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Designación** | **Fecha** | **Título** | **Tipo de publicación** |
| [TP.inno](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15153) | 03/09/2020 | Description of the incubation mechanism and ways to improve it | Documento técnico |
| [TP.sgstruct](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15154) | 03/09/2020 | Strategic approaches to the transformation of security studies | Documento técnico |
| [TR.ors](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15256) | 26/03/2020 | OID Resolution system: Problems, Requirements and Potential solutions | Informe técnico |
| [TR.sec-manual](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14367) | 03/09/2020 | Security in telecommunications and information technology (7th edition) | Informe técnico |
| [TR.sec-qkd](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14825) | 26/03/2020 | Security considerations for quantum key distribution network | Informe técnico |
| [TR.Suss](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14370) | 03/09/2020 | Successful use of security standards (2nd edition) | Informe técnico |
| [TR.usm](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15241) | 03/09/2020 | Unified Security Model (USM) – a neutral integrated system approach to Cybersecurity | Informe técnico |
| [TR.XAASL](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16769) | 03/09/2020 | Technical Report: Framework for Security Standardization for Virtualized Services | Informe técnico |
| [XSTR-SEC-QKD Cor.1](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16969) | 30/04/2021 | Security considerations for quantum key distribution network - Corrigendum 1 | Informe técnico |
| [Z.Imp100](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16983) | 30/04/2021 | Z.100 Specification and Description Language implementer's guide - Version 4.0.1 | Guía del implementador |
| [Z.Imp100](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14424) | 07/09/2018 | Z.100 Specification and Description Language implementer's guide – Version 3.0.2 | Guía del implementador |
| [Z.Imp100rev](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14816) | 05/09/2019 | Z.100 Specification and Description Language implementer's guide – Version 4.0.0 | Guía del implementador |

CUADRO 13

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

| Recomendación | Consentimiento/Determinación | TAP/AAP | Título |
| --- | --- | --- | --- |
| Ninguna |  |  |  |

ANEXO 2

Propuesta de revisión de la Resolución 2 de la AMNT presentada por la Comisión de Estudio 17

Anexo A

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).

La seguridad de las TIC y su garantía son grandes ámbitos de estudio de la Comisión de Estudio 17, que comprenden los estudios relativos a la ciberseguridad, los servicios de seguridad gestionados, la detección y respuesta de puntos extremos, 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 seguridad cuántica, las seguridad para tecnologías de libro mayor distribuido, la seguridad de sistemas de transporte inteligentes, los aspectos de seguridad relacionados con la IA y la seguridad de las redes, aplicaciones y servicios, como Internet de las cosas (IoT) y las ciudades inteligentes, distintos tipos de redes, incluidas las redes IMT2020/5G y posteriores, la red eléctrica inteligente, el sistema de control industrial (SCI), la cadena de producción, los teléfonos inteligentes, las redes definidas por software (SDN), la virtualización de la función de red (NFV), la televisión por el protocolo Internet (TVIP), los servicios web, los servicios superpuestos (OTT), las redes sociales, la computación en la nube, el análisis de macrodatos (*big data*), los sistemas financieros digitales y la telebiometría.

La creación de confianza y seguridad en la utilización de las TIC comprende también la protección de la información de identificación personal (IIP), como los aspectos técnicos y operativos de la protección de los datos a fin de garantizar la confidencialidad, integridad y disponibilidad de la IIP.

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 los lenguajes de especificación de pruebas para pruebas de conformidad destinadas a 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 de la AMNT)

Orientaciones a las Comisiones de Estudio del UIT-T
para la elaboración del programa de trabajo posterior a 2020

…

Comisión de Estudio 17 del UIT-T

La Comisión de Estudio 17 del UIT-T se encarga de elaborar Recomendaciones técnicas clave para la creación de confianza y seguridad en el uso de las tecnologías de la información y la comunicación (TIC).

Para ello realiza 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 y la seguridad de las redes, aplicaciones y servicios, como Internet de las cosas (IoT), los sistemas de transporte inteligentes, los servicios de aplicación segura, las redes sociales, la computación en la nube, la tecnología de libro mayor distribuido 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.

El objetivo de la Comisión de Estudio 17 del UIT-T es ofrecer soluciones técnicas para la seguridad de las TIC y su garantía. En particular, se centra en estudiar la seguridad en nuevas esferas, como la seguridad de las redes IMT2020/5G y posteriores, la Internet de las cosas (IoT), las ciudades inteligentes, las tecnologías de libro mayor distribuido (DLT), la analítica de macrodatos, los sistemas de transporte inteligentes, los aspectos de seguridad relacionados con la IA y las tecnologías cuánticas. Su ámbito de estudios comprende también la gestión de la información de identificación personal (IIP), como los aspectos técnicos y operativos de la protección de datos para garantizar la confidencialidad, la integridad y la disponibilidad de la IIP.

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, como los aspectos técnicos y operativos de la protección de los datos, y la lucha contra el spam por medios técnicos.

La Comisión de Estudio 17 establece la coordinación general de los estudios sobre seguridad en el UIT‑T asumiendo su papel de Comisión de Estudio Rectora sobre seguridad, gestión de identidades y lenguajes y técnicas de descripción.

La Comisión de Estudio 17 también es responsable de la elaboración de las Recomendaciones básicas sobre seguridad de las tecnologías de libro mayor distribuido, seguridad de sistemas de transporte inteligentes, aspectos de seguridad de las aplicaciones y servicios en el área de la TVIP, diversos tipos de redes, incluidas las redes IMT2020/5G y posteriores, redes eléctricas inteligentes, sistemas de control industrial (SCI), cadenas de producción, IoT y ciudades inteligentes, SDN, NFV, redes sociales, computación en la nube, análisis de macrodatos, teléfonos inteligentes, sistemas financieros digitales 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, lo que incluye lenguajes tales como los ASN.1, SDL, MSC, URN y TTCN-3.

La Comisión de Estudio 17 coordina los trabajos sobre la seguridad de todas las Comisiones de Estudio del UIT-T. Esta labor 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 la Comisión de Estudio 20y en cooperación con ellas.

La CE 17 se ocupará de los aspectos de gestión de la identidad pertinentes en colaboración con la CE 20 y la CE 2, de acuerdo con el mandato de cada Comisión de Estudio.

…

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 2021-2024

...

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, 3, 11, 13, 15 y 16

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

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