|  |  |  |
| --- | --- | --- |
| ITU Logo | UNIÓN INTERNACIONAL DE TELECOMUNICACIONES**SECTOR DE NORMALIZACIÓNDE LAS TELECOMUNICACIONES**PERIODO DE ESTUDIOS 2017-2020 | TSAG – R21 – S |
| **TSAG** |
| **Original: inglés** |
| **Cuestión(es):** | N/A | Virtual, 11-18 de enero de 2021 |
| **INFORME** |
| **Origen:** | GANT |
| **Título:** | Informe de la séptima reunión del GANT (virtual, 11-18 de enero de 2021) – Cuestiones refrendadas en relación con la Comisión de Estudio 17 |
| **Objeto:** | Administrativo |
| **Contacto:** | Secretaría del GANT  | Correo-e: tsbtsag@itu.int |

|  |  |
| --- | --- |
| **Palabras clave:** | GANT; Actualización de Cuestiones |
| **Resumen:** | El presente Informe contiene el texto definitivo relativo a las Cuestiones acordadas por la Comisión de Estudio 17, para su presentación a la AMNT, que se refrendaron en la reunión virtual del GANT celebrada del 11 al 18 de enero de 2021. Dichas Cuestiones son aplicables desde su entrada en vigor, el 18 de enero de 2021, hasta el final del periodo de estudios. |

ÍNDICE

 Página

[1 Introducción 4](#_Toc67427796)

[2 Texto de las Cuestiones 6](#_Toc67427797)

[A Cuestión 1/17 – Estrategia de normalización y coordinación de la seguridad 6](#_Toc67427798)

[A.1 Motivación 6](#_Toc67427799)

[A.2 Cuestión 7](#_Toc67427800)

[A.3 Tareas 8](#_Toc67427801)

[A.4 Relaciones 9](#_Toc67427802)

[B Cuestión 2/17 – Arquitectura de seguridad y seguridad de red 10](#_Toc67427803)

[B.1 Motivación 10](#_Toc67427804)

[B.2 Cuestión 11](#_Toc67427805)

[B.3 Tareas 12](#_Toc67427806)

[B.4 Relaciones 12](#_Toc67427807)

[C Cuestión 3/17 – Gestión de la seguridad de la información en las telecomunicaciones y servicios de seguridad 13](#_Toc67427808)

[C.1 Motivación 13](#_Toc67427809)

[C.2 Cuestión 13](#_Toc67427810)

[C.3 Tareas 14](#_Toc67427811)

[C.4 Relaciones 15](#_Toc67427812)

[D Cuestión 4/17 – Ciberseguridad y lucha contra el correo basura 16](#_Toc67427813)

[D.1 Motivación 16](#_Toc67427814)

[D.2 Cuestión 17](#_Toc67427815)

[D.3 Tareas 19](#_Toc67427816)

[D.4 Relaciones 21](#_Toc67427817)

[E Cuestión 6/17 – Seguridad de los servicios de telecomunicaciones e Internet de las cosas 22](#_Toc67427818)

[E.1 Motivación 22](#_Toc67427819)

[E.2 Cuestión 23](#_Toc67427820)

[E.3 Tareas 23](#_Toc67427821)

[E.4 Relaciones 24](#_Toc67427822)

[F Cuestión 7/17 – Servicios de aplicación seguros 26](#_Toc67427823)

[F.1 Motivación 26](#_Toc67427824)

[F.2 Cuestión 27](#_Toc67427825)

[F.3 Tareas 27](#_Toc67427826)

[F.4 Relaciones 28](#_Toc67427827)

[G Cuestión 8/17 – Seguridad de la infraestructura de computación en la nube y macrodatos 29](#_Toc67427828)

[G.1 Motivación 29](#_Toc67427829)

[G.2 Cuestión 30](#_Toc67427830)

[G.3 Tareas 31](#_Toc67427831)

[G.4 Relaciones 31](#_Toc67427832)

[H Cuestión 10/17 – Arquitectura y mecanismos de gestión de identidades y telebiometría 33](#_Toc67427833)

[H.1 Motivación 33](#_Toc67427834)

[H.2 Cuestión 34](#_Toc67427835)

[H.3 Tareas 35](#_Toc67427836)

[H.4 Relaciones 36](#_Toc67427837)

[I Cuestión 11/17 – Tecnologías genéricas (Directorio, PKI, Lenguajes formales e Identificadores de objeto, entre otras) para aplicaciones seguras 38](#_Toc67427838)

[I.1 Motivación 38](#_Toc67427839)

[I.2 Cuestión 41](#_Toc67427840)

[I.3 Tareas 42](#_Toc67427841)

[I.4 Relaciones 44](#_Toc67427842)

[J Cuestión 13/17 – Seguridad de los sistemas de transporte inteligente 45](#_Toc67427843)

[J.1 Motivación 45](#_Toc67427844)

[J.2 Cuestión 45](#_Toc67427845)

[J.3 Tareas 46](#_Toc67427846)

[J.4 Relaciones 47](#_Toc67427847)

[K Cuestión 14/17 – Seguridad de las tecnologías de libro mayor distribuido (DTL) 48](#_Toc67427848)

[K.1 Motivación 48](#_Toc67427849)

[K.2 Cuestión 48](#_Toc67427850)

[K.3 Tareas 49](#_Toc67427851)

[K.4 Relaciones 49](#_Toc67427852)

[L Cuestión 15/17 – Seguridad en relación con las tecnologías incipientes, en particular la seguridad cuántica 51](#_Toc67427853)

[L.1 Motivación 51](#_Toc67427854)

[L.2 Cuestión 52](#_Toc67427855)

[L.3 Tareas 53](#_Toc67427856)

[L.4 Relaciones 53](#_Toc67427857)

# 1 Introducción

El presente documento contiene el texto definitivo relativo a las Cuestiones acordadas por la Comisión de Estudio 17, para su presentación a la AMNT, que se refrendaron en la reunión virtual del GANT celebrada del 11 al 18 de enero de 2021. Dichas Cuestiones son aplicables desde su entrada en vigor, el 18 de enero de 2021, hasta el final del periodo de estudios.

En el Cuadro 1 figuran las Cuestiones que se refrendaron y su relación con las que estaban en vigor. Cabe señalar que se han suprimido las Cuestiones 5/17, 9/17 y 12/17, y que los demás temas de estudio y tareas se han transferido a otras Cuestiones, con arreglo a lo especificado en el Cuadro 1.

Cuadro 1 – Cuestiones en vigor relativas a la CE 17 con respecto a las anteriores Cuestiones (las Cuestiones refrendadas figuran a la izquierda y las anteriores a la derecha)

| Nuevo número | Título de la actual Cuestión  | Situación | Número anterior | Título de la anterior Cuestión  |
| --- | --- | --- | --- | --- |
| 1/17 | Estrategia de normalización y coordinación de la seguridad | Continuación | 1/17 | Coordinación de la seguridad en las telecomunicaciones/TIC  |
| 2/17 | Arquitectura de seguridad y seguridad de red | Continuación | 2/17 | Arquitectura y marco genérico de la seguridad |
| 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 |
| 4/17 | Ciberseguridad y lucha contra el correo basura | Continuación de las Cuestiones 4/17 y 5/17 | 4/17 | Ciberseguridad |
| 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 |
| 7/17 | Servicios de aplicación seguros | Continuación | 7/17 | Servicios de aplicación seguros |
| 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 |
| 10/17 | Arquitectura y mecanismos de gestión de identidades y telebiometría | Continuación de las Cuestiones 9/17 y 10/17 | 9/17 | Telebiometría |
| 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 |
| 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 |
| 14/17 | Seguridad de las tecnologías de libro mayor distribuido (DTL) | Continuación | 14/17 | Aspectos de seguridad de las tecnologías de libro mayor distribuido |
| 15/17 | Seguridad en relación con las tecnologías incipientes, en particular la seguridad cuántica | Nueva  | – | – |

# 2 Texto de las Cuestiones

## A Cuestión 1/17 – Estrategia de normalización y coordinación de la seguridad

(Continuación de la Cuestión 1/17)

### A.1 Motivación

Las amenazas a la seguridad a las telecomunicaciones, a las tecnologías de la información y la comunicación (TIC) y a la infraestructura siguen siendo cada vez más complejas. Los esfuerzos desplegados a lo largo de los años para proteger la infraestructura han sido fragmentarios y conservadores por lo que, hasta el momento, no se ha alcanzado el nivel de protección deseado contra dichas amenazas de manera oportuna. Las repercusiones económicas de dichos ataques y amenazas han sido inmensas, dando lugar a diversas financieras y orgánicas para gobiernos y entidades. Resulta por tanto esencial desplegar esfuerzos de manera intensiva, continua y centrada para combatir estas amenazas.

Esta tarea es compleja y requiere la participación de un gran número de organizaciones que se ocupan de diversos aspectos de la seguridad, cada una dentro de su esfera de especialización y su mandato. A tal efecto, es indispensable la coordinación, colaboración y cooperación entre los diversos interesados, lo que constituye una ardua y difícil tarea.

La seguridad es un tema muy amplio, puesto que puede aplicarse a prácticamente todos los aspectos de las TIC y las redes. Existen diversas formas de abordar los requisitos de seguridad, a saber:

– El enfoque ascendente, en el que los expertos en distintas esferas determinan las medidas de seguridad necesarias para reforzar y proteger su dominio particular de la red utilizando para ello técnicas y contramedidas específicas tales como la biometría y la criptografía. Éste es el enfoque más ampliamente adaptado, pero es fragmentario y sus resultados desiguales en cuanto a la determinación y aplicación de medidas de seguridad.

– El enfoque descendente, que es una manera estratégica y compleja de abordar la seguridad, por cuanto se requiere un conocimiento global del tema. Por esa razón es el enfoque más difícil de adoptar, puesto que resulta mucho más complicado encontrar expertos que conozcan detalladamente todas y cada una de las partes de la red, y por tanto, sus requisitos de seguridad, que encontrar expertos en determinados aspectos de uno o dos campos específicos.

– Otra alternativa es combinar ambos enfoques y realizar un trabajo de coordinación para aunar los distintos saberes. Se ha demostrado con frecuencia que este enfoque es difícil de aplicar al variar los intereses y disponibilidades de los expertos en cuestión.

Esta Cuestión produce muchos resultados que el UIT-T considera fundamentales para promover su labor y sus productos. También proporcionan valiosos recursos a la UIT y a organizaciones externas. Entre los ejemplos cabe citar la hoja de ruta sobre normas de seguridad de las TIC, el manual de seguridad, los compendios de seguridad y la utilización satisfactoria de las normas de seguridad. En esta Cuestión se elaborará un planteamiento y se propondrá la arquitectura orgánica de la CE 17. El estudio de esta Cuestión se seguirá centrando en la coordinación y organización de toda la serie de actividades del UIT-T relativas a la seguridad de las telecomunicaciones/TIC y se continuará el desarrollo y actualización de la documentación para la coordinación y las actividades de divulgación. Se adoptará un enfoque descendente y se colaborará con otras Comisiones de Estudio y organizaciones de normalización. El objetivo de este proyecto es concentrar aún más los esfuerzos a nivel de proyecto y estratégico, tanto dentro como fuera de la CE 17. En el marco de esta Cuestión se apoyarán las actividades de la CE 17 para garantizar que constituyan un proceso eficiente capaz de elaborar normas de telecomunicaciones/TIC de alta calidad, oportunas y orientadas al mercado. En esta Cuestión también se estudian las necesidades de los países en desarrollo y de las Comisiones de Estudio Regionales mediante la aplicación de la Resolución 44 de la AMNT relativa a la reducción de la brecha de normalización.

La estrategia de normalización de la seguridad es uno de los temas más importantes de todas las Cuestiones de la CE 17. En necesario que la CE 17 considere cómo la arquitectura y el diseño de la normalización de la seguridad pueden mejorar el desarrollo de los temas de estudio presentes y futuros en materia de seguridad.

Los trabajos de la CE 17 en materia de seguridad tiene en cuenta las Resoluciones 7, 11, 40, 44, 45, 50, 52, 58, 64, 65, 67, 70, 73, 75, 76, 78, 84, 87, 89, 90, 94, 96, 97 y 98 de la AMNT; las Resoluciones 101, 123, 130, 136, 174, 175, 177, 178, 179, 180, 181; 188, 189, 196, 197, 199, 200, 201, 204 y 206 de la PP; y las Resoluciones 21, 23, 34, 45, 47, 54, 58, 59, 63, 64, 67, 69, 78, 79, 80 y 84 de la CMDT.

La CE 17 también respalda la Línea de Acción C5 de la CMSI "Creación de confianza y seguridad en la utilización de las TIC" y el Objetivo 2 del Plan de Acción de Buenos Aires adoptado en la Conferencia Mundial de Desarrollo de las Telecomunicaciones de 2017, "Infraestructura de telecomunicaciones/TIC moderna y segura: Fomentar el desarrollo de la infraestructura y los servicios, incluida la instauración de la confianza y seguridad en el uso de las telecomunicaciones/TIC".

Informes técnicos relativos a esta Cuestión al 3 de septiembre de 2020: TR.sec-manual, XSTR‑SUSS.

Textos en preparación: TP.sec-arch y X.arch-design.

### A.2 Cuestión

Los temas de estudio que se han de considerar son, entre otros:

a) ¿Cuáles son los resultados previstos de esta Cuestión?

b) ¿Qué procesos, temas, métodos y calendario son necesarios para alcanzar estos resultados?

c) ¿Qué documentos de divulgación (hoja de ruta, compendio sobre seguridad, informes técnicos, folletos, páginas web, etc.) habrá de preparar y mantener actualizados la UIT?

d) ¿Qué talleres sobre seguridad será necesario celebrar y cómo pueden organizarse?

e) ¿Qué se necesita para establecer relaciones efectivas con otros organismos de normalización con el fin de adelantar los trabajos en materia de seguridad?

f) ¿Cuáles son los puntos esenciales, los criterios para obtener buenos resultados y las correspondientes métricas del rendimiento?

g) ¿Cómo se puede estimular y mantener constante el interés de los Miembros de Sector y las Administraciones por las actividades relativas a la seguridad?

h) ¿Qué puede hacerse para que el mercado se interese más por las funciones de seguridad de las telecomunicaciones/TIC?

i) ¿Cómo se puede lograr que los gobiernos y el sector privado sean conscientes de la enorme importancia que reviste la seguridad y de la necesidad urgente de proteger los intereses de la economía mundial, que dependen de una infraestructura de telecomunicaciones/TIC robusta y segura?

j) ¿Qué actividades en materia de seguridad están llevándose a cabo en otras Comisiones de Estudio de la UIT y organizaciones de normalización?

k) ¿Cómo atender las necesidades de los países en desarrollo y de las Comisiones de Estudio Regionales en la aplicación de la Resolución 44 de la AMNT?

l) ¿Cuál es la estrategia de normalización que contribuye a obtener una solución de seguridad de las telecomunicaciones exhaustiva y coherente?

m) ¿Cómo debe la estrategia de normalización incorporar las Recomendaciones existentes en materia de seguridad?

### A.3 Tareas

Las tareas son, entre otras:

a) Actuar como grupo de referencia en la CE 17 para asuntos relativos a coordinación de la seguridad en las telecomunicaciones/TIC.

b) Desarrollar y mantener actualizada una hoja de ruta de arquitectura orgánica, a fin de proporcionar una noción y un plan detallado que determine el nivel y el alcance del dominio de seguridad para su estudio. La hoja de ruta identificará todos los componentes conexos (estructura, procesos) y sus interrelaciones, las organizaciones participantes y las funciones. Es necesario diferenciar entre los sistemas/redes incipientes y los sistemas/redes existentes.

c) Mantener actualizada la hoja de ruta sobre normas de seguridad.

d) Mantener actualizado el Compendio sobre seguridad del UIT-T.

e) Prestar asistencia y aportar contribuciones a la TSB en relación con el mantenimiento del Manual sobre seguridad publicado como el Informe técnico "Seguridad en la esfera de las tecnologías de la información y la comunicación".

f) Mantener actualizado el Informe técnico sobre la utilización satisfactoria de las normas de seguridad.

g) Prestar asistencia en la aplicación de normas de seguridad en las telecomunicaciones/TIC.

h) Promover la cooperación y la colaboración de los grupos de trabajo encargados de la elaboración de normas relativas a la seguridad en las telecomunicaciones/TIC.

i) Examinar las Recomendaciones y los documentos de coordinación de otras Comisiones de Estudio y organismos de normalización, según el caso, para evaluar las repercusiones de la coordinación en materia de seguridad.

j) Ayudar en las tareas destinadas a garantizar una coordinación eficaz de la seguridad, cuando sea necesario.

k) Facilitar la coordinación entre grupos externos y las Comisiones de Estudio correspondientes de la UIT.

l) Tomar la iniciativa de organizar y planificar talleres y seminarios sobre seguridad en la UIT, según convenga.

m) Garantizar la participación eficaz en las actividades de coordinación de la seguridad con otras organizaciones.

n) Contribuir a aumentar la eficiencia de la labor de la CE 17 (por ejemplo, mediante el desarrollo de plantillas, herramientas, procedimientos y métricas del rendimiento).

o) Alentar a las autoridades y operadores nacionales de los países en desarrollo de las regiones a que colaboren y refuercen su contribución en lo concerniente a las actividades de la CE 17 del UIT-T en consonancia con el mandado de dicha Comisión de Estudio, y la aplicación de las Recomendaciones sobre seguridad de la CE 17.

p) Prestar asistencia a la CE 17 para reducir la disparidad en materia de normalización en apoyo a la Res. 44 de la AMNT, la Res. 123 de la PP y la Res. 47 de la CMDT.

q) Lograr una participación efectiva y eficiente en los esfuerzos de coordinación de la seguridad dentro de la CE 17 para garantizar que el programa de trabajo de la CE 17 refleje las actividades en curso de la CE 17 en el ámbito de la seguridad y responda a las inquietudes de los Miembros del UIT-T.

r) Elaboración de un conjunto exhaustivo de documentos sobre estrategias de normalización de la seguridad, en particular documentos sobre la arquitectura, a fin de contribuir a la normalización de soluciones de seguridad en colaboración con otras organizaciones de normalización y otras Comisiones de Estudio del UIT-T.

En el programa de trabajo de la Comisión de Estudio 17 se indica el estado actual del estudio de esta Cuestión (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

### A.4 Relaciones

Líneas de Acción de la CMSI

C5.

Objetivos de Desarrollo Sostenible

–

Recomendaciones

Serie X y otras relacionadas con la seguridad en las telecomunicaciones/TIC.

Cuestiones

Cuestiones 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 y 15/17 del UIT‑T.

Comisiones de Estudio

UIT‑D; UIT‑R; CE 2, 3, 5, 9, 11, 13, 15, 16 y 20 del UIT‑T; GANT, comprendidos los GT y JCA pertinentes.

Entidades de normalización

Alliance of Telecommunications Industry Solutions (ATIS); Cloud Security Alliance (CSA); Instituto Europeo de Normas de Telecomunicación (ETSI); Instituto de Ingenieros Eléctricos y Electrónicos (IEEE); Grupo Especial sobre Ingeniería de Internet (IETF); JTC 1/SC 6 y SC 27 de ISO/CEI, ISO TC 292, ISO TMB; Organización para el Desarrollo de Normas relativas a la Información Estructurada (OASIS); Proyecto común de tecnologías inalámbricas de la tercera generación (3GPP); Proyecto común de tecnologías inalámbricas de la tercera generación 2 (3GPP2); Programa de Normalización de la Telecomunidad Asia-Pacífico (ASTAP).

Otras entidades

Organismo Europeo para la Seguridad de la Información y las Redes (ENISA); National Institute of Standards and Technology (NIST); one M2M; Foro de intercambio de seguridad de la información en la Región de Asia (RAISE).

## B Cuestión 2/17 – Arquitectura de seguridad y seguridad de red

(Continuación de la Cuestión 2/17)

### B.1 Motivación

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

Hay que proseguir este trabajo para mantener y ampliar estas Recomendaciones sobre seguridad con el fin de satisfacer las necesidades de las nuevas tecnologías (por ejemplo, las redes de la próxima generación (NGN), los aspectos de seguridad de las redes definidas por *software* (SDN)/virtualización de funciones de red (NFV), segmentación de red (NS), cadena de función de servicio (SFC), computación periférica multiacceso (MEC), evolución a largo plazo/evolución de la arquitectura del sistema (LTE/SAE), red IMT-2020/5G y posteriores, marco y arquitectura de seguridad común para los servicios/aplicaciones, fundamentos de la inteligencia artificial (IA)/aprendizaje automático (ML) para crear confianza y seguridad en la utilización de las TIC, orientaciones para la aplicación técnica de sistemas que proporcionan comunicaciones de extremo a extremo y las redes basadas en el protocolo Internet). Los resultados de este trabajo se consignan en las Recomendaciones X.1035 y X.1036 que describen en detalle el protocolo de intercambio de claves con autentificación mediante contraseña y la distribución y aplicación de políticas de seguridad, X.1037 que contiene directrices de seguridad IPv6, X.1038, X.1042, X.1043 y X.1044 que describe los requisitos de seguridad, etc., sobre redes definidas por *software* (SDN) y virtualización de funciones de red (NFV), X.1045 que describe los servicios de seguridad personalizados basados en la cadena de funciones de servicio (SFC).

Con la llegada de la convergencia y la movilidad, los operadores de telecomunicaciones y sus redes y sistemas informáticos se ven expuestos a nuevos tipos de amenazas a la seguridad. Los agresores consiguen llegar a niveles cada vez más profundos y sin ser expertos logran causar daños más graves. Los virus, el pirateo informático y los ataques de denegación de servicio están a la orden del día y afectan negativamente tanto a los elementos de red como a sus sistemas.

Las industrias de las telecomunicaciones y la tecnología de la información buscan soluciones de seguridad integrales y rentables que sean independientes de la tecnología y protejan un amplio espectro de redes, servicios y aplicaciones. Para poder encontrar soluciones de este tipo en un entorno constituido por dispositivos de diversos fabricantes, la seguridad de la red debe diseñarse y optimizarse en torno a arquitecturas y tecnologías de seguridad normalizadas. Es necesario definir requisitos y soluciones de seguridad teniendo presente las amenazas a la seguridad que acechan el entorno de las telecomunicaciones y los últimos adelantos en materia de seguridad para contrarrestarlas. Así pues, se necesitan nuevas Recomendaciones que expliquen cómo integrar las normas de tecnología y los marcos de seguridad para lograr la seguridad integral de las redes, servicios y aplicaciones incipientes.

Las Recomendaciones y los Suplementos relacionados con el estudio de esta Cuestión son, al 3 de septiembre de 2020, los siguientes: X.800, X.802, X.803, X.805, X.810, X.811, X.812, X.813, X.814, X.815, X.816, X.830, X.831, X.832, X.833, X.834, X.835, X.841, X.842, X.843, X.1031, X.1032, X.1033, X.1034, X.1035, X.1036, X.1037, X.1038, X.1039, X.1040, X.1041, X.1042, X.1043, X.1044, X.1045, y los Suplementos X.Supl.2, X.Supl.3, X.Supl.15, X.Supl.16, X.Supl.23 y X.Supl.30.

Textos en preparación: X.nsom-sec, X.rf-csap, X.SDsec (X.1046), X.5GSec-ecs, X.5GSec-guide, X.5Gsec-netec, X.5Gsec-q (X.1811), X.5Gsec-ssl y X.5Gsec-t, X.5Gsec-vs.

### B.2 Cuestión

Los temas de estudio que se han de considerar son, entre otros:

a) ¿Cómo debe definirse una solución completa y coherente de la seguridad en las comunicaciones?

b) ¿Cuál es la arquitectura más adecuada para lograr una solución completa y coherente de la seguridad?

c) ¿Cuál es el marco de aplicación de la arquitectura de seguridad con objeto de crear una solución para la seguridad?

d) ¿Cuál es el marco de aplicación de la arquitectura de seguridad para evaluar (y consiguientemente mejorar) la solución de seguridad existente?

e) ¿Cuáles son los fundamentos de la arquitectura de seguridad?

i) ¿Qué arquitectura garantiza la seguridad extremo a extremo?

ii) ¿Cuál es la arquitectura de seguridad de los sistemas abiertos?

iii) ¿Cuál es la arquitectura de seguridad en el entorno móvil?

iv) ¿Cuál es la arquitectura de seguridad para las redes evolutivas?

v) ¿Cuál es la arquitectura de seguridad para servicios de aplicaciones en colaboración con la Cuestión C7/17?

f) ¿Qué Recomendaciones nuevas sobre el marco y la arquitectura de seguridad se requieren para proporcionar soluciones de seguridad en el entorno cambiante?

g) ¿Cómo estructurar las normas relativas a la arquitectura con respecto a las Recomendaciones sobre seguridad existentes?

h) ¿Cómo organizar las normas relativas a la arquitectura con respecto a las actuales tecnologías avanzadas en materia de seguridad?

i) ¿Cómo modificar las Recomendaciones que definen el marco de seguridad para adaptarlas a las nuevas tecnologías, y qué nuevas Recomendaciones marco se requieren?

j) ¿Cómo se aplican los servicios de seguridad para suministrar soluciones de seguridad?

k) ¿Cómo se supervisa la infraestructura de telecomunicaciones/TIC para suministrar soluciones de seguridad?

l) ¿Cuáles son los fundamentos de la inteligencia artificial/aprendizaje automático (IA/ML) para fomentar la creación de confianza y seguridad en la utilización de las TIC?

m) ¿Cuáles son los nuevos retos y amenazas de seguridad generados por las tecnologías de red incipientes (por ejemplo, SDN, NFV, división de redes, SFC, MEC, LTE/SAE, red IMT-2020/5G y posteriores, etc.)?

n) ¿Cuáles son los requisitos de seguridad de las redes IMT-2020/5G y posteriores, y cómo puede abordarlos la CE 17?

o) ¿Cuáles son los mecanismos de seguridad comunes para las tecnologías de redes incipientes?

### B.3 Tareas

Las tareas son, entre otras:

a) Elaborar un conjunto completo de Recomendaciones que proporcionen soluciones normalizadas de seguridad para las telecomunicaciones en colaboración con otros organismos de normalización y las Comisiones de Estudio del UIT‑T.

b) Estudiar y elaborar Recomendaciones sobre la arquitectura de red de telecomunicaciones fiable que integre tecnologías de seguridad avanzadas.

c) Estudiar y elaborar Recomendaciones sobre los fundamentos de IA/ML para fomentar la confianza y la seguridad en la utilización de las TIC.

d) Mantener actualizadas y mejorar las Recomendaciones y los Suplementos de las series X.800 y X.103.x.

e) Estudiar y elaborar Recomendaciones sobre la seguridad de redes comunes.

f) Estudiar los requisitos de seguridad de las redes IMT-2020/5G y posteriores, coordinar los trabajos conexos en diversas Cuestiones de la CE 17, ser el coordinador único para los aspectos relativos a la seguridad de las redes IMT-2020/5G y posteriores en la CE 17, y dirigir la investigación y el desarrollo de normas sobre los aspectos relativos a la seguridad de las redes IMT-2020/5G y posteriores.

En el programa de trabajo de la Comisión de Estudio 17 se indica el estado actual del estudio de esta Cuestión (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

### B.4 Relaciones

Líneas de Acción de la CMSI

C5.

Objetivos de Desarrollo Sostenible

–

Recomendaciones

Serie X y otras relativas a la seguridad.

Cuestiones

Cuestiones 1/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 y 15/17 del UIT‑T.

Comisiones de Estudio

CE 2 del UIT-D; GT 6B del UIT-R; CE 2, 9, 11, 13, 15, 16 y JCA-IMT2020 del UIT‑T.

Entidades de normalización

Alliance of Telecommunications Industry Solutions (ATIS); Instituto Europeo de Normas de Telecomunicación (ETSI); Asociación GSM (GSMA); Forum for the International Irregular Network Access (FIINA); JTC 1/SC 27 y SC 37 de ISO/CEI; TC 25 de la CEI; TC 12 de la ISO; Grupo Especial sobre Ingeniería de Internet (IETF); Proyecto común de tecnologías inalámbricas de la tercera generación (3GPP).

## C Cuestión 3/17 – Gestión de la seguridad de la información en las telecomunicaciones y servicios de seguridad

(Continuación de la Cuestión 3/17)

### C.1 Motivación

La información y los procesos relacionados con ella, las instalaciones de telecomunicaciones, las redes y las líneas son activos comerciales importantes de los organismos de telecomunicaciones. Para que estos organismos puedan gestionar adecuadamente dichos activos y proseguir adecuadamente sus actividades, es extremadamente necesario gestionar la seguridad de la información. Por ese motivo se elaboró la Recomendación UIT-T X.1051 con el fin de proporcionar un código de prácticas para los controles de seguridad de la información destinados a las organizaciones de telecomunicaciones.

A partir del código de prácticas, se ha elaborado un Suplemento que contiene esferas de gestión detalladas y específicas, incluidos los riesgos, los activos, la gobernanza, el marco de gestión y los incidentes, junto con una introducción a las prácticas óptimas. Asimismo, habrá que estudiar nuevos temas relativos a la Recomendación UIT-T X.1051. Entretanto la serie de Recomendaciones se ha de mantener actualizada con las cuestiones más recientes en materia de gestión de seguridad de la información. El objetivo es elaborar en el UIT‑T un conjunto de Recomendaciones sobre gestión de la seguridad basadas en la Recomendación UIT-T X.1051.

Además de elaborar Recomendaciones para ámbitos de gestión detallados y específicos basados en la Recomendación UIT-T X.1051, deben considerarse los nuevos ámbitos de los servicios de seguridad de las telecomunicaciones y las TIC, por ejemplo, los servicios del Centro de Ciberdefensa (CDC), incluidos los servicios del Centro de Operaciones de Seguridad (SOC), los servicios de gestión de la seguridad (SMS) y los servicios de los equipos de intervención en caso de incidentes informáticos (EIII), la gestión del ciclo de vida de los controles de seguridad y la gestión eficaz de los riesgos, así como la gestión de la información de identificación personal que requiera medidas de respuesta nuevas y globales. Esas esferas no se refieren solamente a la seguridad de la información, sino que también abarcan aspectos de la ciberseguridad. Por consiguiente, los estudios deberían centrarse especialmente en los aspectos relativos a la gestión de las nuevas esferas mencionadas de la seguridad de la información y la ciberseguridad.

Durante la realización de estos estudios, UIT‑T y el JTC 1 de ISO/CEI seguirán colaborando plenamente con el fin de garantizar la mayor compatibilidad posible de las soluciones de seguridad. El éxito comercial de las soluciones elaboradas como normas nacionales en muchos países también ha de tenerse en cuenta.

Esta Cuestión difiere de las asignadas a la Comisión de Estudio 2 en que se estudia el intercambio de información de gestión de red entre elementos de red y sistemas de gestión, por una parte, y entre sistemas de gestión, por la otra, en el entorno de la RGT. En cambio, esta Cuestión versa principalmente sobre la protección de activos empresariales, en particular la información y los procesos, con miras a la gestión de la seguridad de la información.

Las Recomendaciones y los Suplementos relacionados con el estudio de esta Cuestión son, al 3 de septiembre de 2020, los siguientes: E.409 (junto con la CE 2), X.1051, X.1052, X.1053, X.1054, X.1055, X.1056, X.1057, X.1058, X.1059 y los Suplementos X.Supl.13, Supl.27, Supl.32 y Supl.34.

Textos en preparación: X.1051rev2, X.1052-rev, X.1054-rev, X.ciag, X.fram-cdc y X.sup-csc.

### C.2 Cuestión

Los temas de estudio que se han de considerar son, entre otros:

a) ¿Cómo determinar los problemas específicos de gestión de la seguridad en las organizaciones de telecomunicaciones?

b) ¿Cómo determinar y gestionar la forma de medir la gestión de la seguridad en las telecomunicaciones?

c) ¿Cómo asignar e integrar los objetivos y controles de control en la gestión orgánica y los aspectos operativos de las organizaciones de telecomunicaciones?

d) ¿Cómo aplicar los conceptos y principios para la gestión de la seguridad de la información, mediante los cuales las organizaciones pueden evaluar, dirigir, supervisar y comunicar las actividades relacionadas con la seguridad de la información dentro de la organización?

e) ¿Cómo adoptar la opción de tratamiento de riesgos para gestionar el impacto de un incidente de seguridad?

f) ¿Cómo aplicar las prácticas idóneas que ofrecen orientación sobre los servicios de seguridad, por ejemplo, los servicios CDC, incluidos los servicios SOC, SMS y servicios de los EIII?

g) ¿Cómo implantar la gestión de la seguridad de la información para los operadores de telecomunicaciones que sea compatible con las normas existentes (de ISO/CEI y el UIT-T)?

h) ¿Cómo gestionar de manera efectiva la información personal de identificación?

i) ¿Qué revisiones de las Recomendaciones existentes o qué nuevas Recomendaciones han de adoptarse para atenuar los efectos directos o indirectos de las telecomunicaciones/TIC y de otras industrias sobre el cambio climático (por ejemplo, el ahorro de energía, la reducción de las emisiones de gases con efecto invernadero, la utilización de sistemas de supervisión, etc.)?

### C.3 Tareas

Las tareas son, entre otras:

a) Estudiar y elaborar un marco de las funciones de gestión de la seguridad de la información descritas en la Recomendación UIT-T X.1051.

b) Estudiar y elaborar una metodología para implantar la gestión de la seguridad de la información destinada a organizaciones de telecomunicaciones basada en las normas existentes (en particular ISO/CEI y UIT-T).

c) Estudiar y elaborar marcos/directrices para servicios de seguridad, por ejemplo, servicios CDC, en particular SOC, MSS y EIII.

d) Estudiar y elaborar directrices para la gestión de la vida útil en el ámbito de controles de seguridad.

e) Estudiar y elaborar directrices para la gestión eficaz de riesgos, por ejemplo, la adquisición de ciberaseguradoras de riesgo para el tratamiento de riesgos.

f) Estudiar y elaborar directrices para la gestión de la información de identificación personal.

g) Proponer una descripción de las nuevas Recomendaciones.

h) Evaluar los resultados de las actividades mencionadas con miras a su aplicación a instalaciones y servicios de telecomunicaciones.

i) Preparar proyectos de Recomendaciones.

j) Actualizar y mejorar las Recomendaciones de la serie X.105x.

En el programa de trabajo de la Comisión de Estudio 17 se indica el estado actual del estudio de esta Cuestión (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

### C.4 Relaciones

Líneas de Acción de la CMSI

C5.

Objetivos de Desarrollo Sostenible

–

Recomendaciones

Series X.800, X.1000, X.1100, X.1200 y X.1300.

Cuestiones

Cuestiones 1/17, 2/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17, 15/17 y 14/15 del UIT‑T.

Comisiones de Estudio

UIT-D; UIT-R; CE 2, 9, 11, 13, 15, 16 y 20 del UIT-T.

Entidades de normalización

Programa de Normalización de la Telecomunidad Asia-Pacífico (ASTAP); Instituto Europeo de Normas de Telecomunicación (ETSI); JTC 1/SC 27 de ISO/CEI; JTC 1/SC 40 de ISO/CEI; ISO TC 68, ISO TC 215, ISO TC 307; National Institute of Standards and Technology (NIST); Comité de Tecnología de Telecomunicaciones (TTC); Proyecto común de tecnologías inalámbricas de la tercera generación (3GPP); Foro sobre los equipos de seguridad y respuesta ante incidentes (FIRST).

## D Cuestión 4/17 – Ciberseguridad y lucha contra el correo basura

(Continuación de las Cuestiones 4/17 y 5/17)

### D.1 Motivación

El panorama de las telecomunicaciones varía constantemente y, por ende, los correspondientes requisitos de la seguridad de las telecomunicaciones/TIC. Así, las amenazas y los ataques a las telecomunicaciones/TIC evolucionan constantemente en el ciberentorno, siendo cada vez más sofisticados y específicos y causa un complejo abanico de problemas a los usuarios, los proveedores de servicios, los operadores y las redes. Resulta indispensable elaborar marcos y requisitos de ciberseguridad, es decir, un conjunto de recomendaciones y prácticas idóneas para ayudar a las organizaciones a gestionar los riesgos de la ciberseguridad.

Los marcos y requisitos de ciberseguridad contra las amenazas y ataques consisten en un conjunto de componentes destinados a identificar, proteger, detectar, responder y recuperar. La lucha contra los ciberataques por medios técnicos exige un planteamiento global para mitigar los riesgos, detectar y responder sin dilación a los incidentes y recuperarse de sus efectos; intercambiar información sobre ciberseguridad como las técnicas de intercambio de información sobre ciberseguridad (CYBEX) y la expresión estructurada de la información sobre amenazas (STIX); así como proteger los protocolos, infraestructuras y aplicaciones que se utilizan en nuestras comunicaciones cotidianas.

La inteligencia artificial y el aprendizaje automático se aplican más ampliamente que nunca en todas las industrias y aplicaciones. Los medios técnicos que propicia la inteligencia artificial y el aprendizaje automático deberían mejorar la calidad y la eficiencia de las actividades técnicas contra las amenazas y los ataques. Los servicios de seguridad gestionados (MSS) son servicios que han sido subcontratados a un proveedor de servicios. Los servicios de seguridad administrados tienen dos aspectos: técnico y de gestión.

Las tecnologías de ciberseguridad implican la prestación de asistencia técnica para los servicios de seguridad gestionados, la detección y respuesta en los puntos extremos, la prevención y detección de intrusiones y la identificación de la fuente de los atacantes a fin de proteger los servicios y la información personal, incluida la información de identificación personal, así como la facilitación de garantías de información entre las entidades que interactúan.

El intercambio de información sobre seguridad cibernética mediante técnicas CYBEX (marco de intercambio de información sobre ciberseguridad) y la inteligencia sobre ciberamenazas son esenciales para proteger la infraestructura de telecomunicaciones/TIC y mejorar la ciberseguridad para los proveedores de telecomunicaciones/TIC.

Por otra parte, el ritmo vertiginoso al que evolucionan las ciberamenazas exige examinar los aspectos técnicos para dar soporte a los procedimientos, políticas y marcos técnicos de la ciberseguridad. Resulta difícil lograr un nivel mínimo de armonización, por cuanto la ciberseguridad exige la colaboración de todas las partes interesadas.

En lo que respecta a los problemas de ciberseguridad, el correo basura también se ha convertido en un problema generalizado que causa pérdidas económicas a los proveedores de servicios de Internet, los operadores de telecomunicaciones, los operadores de telecomunicaciones móviles y los usuarios comerciales de todo el planeta. Además, el correo basura crea problemas de seguridad en las redes de la información y la telecomunicación cuando se utilizan como vehículo para *peskar* datos (*phishing*) y difundir virus, gusanos y otras formas de *software* maligno, etc. Por ese motivo, en la Resolución 52 de la AMNT se encarga a las Comisiones de Estudio pertinentes, en particular la Comisión de Estudio 17, que prosigan la labor en curso relacionada con la lucha contra el correo basura y aceleren sus trabajos al respecto a fin de contrarrestar, según proceda y dentro de las posibilidades y conocimientos técnicos del UIT-T, las amenazas existentes y futuras. También se les encarga que sigan colaborando con las organizaciones pertinentes para seguir elaborando con carácter urgente Recomendaciones técnicas con el objetivo de intercambiar prácticas idóneas y divulgar la información a través de talleres conjuntos, sesiones de formación, etc.; y encarga asimismo a la Comisión de Estudio 17 que informe periódicamente al Grupo Asesor de Normalización de las Telecomunicaciones sobre la puesta en aplicación de dicha Resolución.

Con la rápida expansión de Internet móvil y la convergencia de las TIC, el correo basura resulta cada vez más peligroso y presenta nuevas características. Los principales componentes del correo basura han evolucionado considerablemente, pasando de los anuncios tradicionales y el fraude a *software* malicioso convergente, como exigir el pago de rescates y ataques selectivos. La nueva generación de correo basura, aparte de que sigue siendo no solicitado y acosa a los consumidores de los servicios TIC, causa daños aún más graves que el correo basura tradicional. Los ataques dirigidos suelen recurrir a la *peska específica*, un tipo de ingeniería social, para obtener acceso a las redes a través de medios legítimos como el correo electrónico. El *software* de secuestro es un tipo de *software* malicioso que amenaza con publicar los datos de la víctima o bloquear perpetuamente el acceso a ellos a menos que se pague un rescate. Algunos programas maliciosos, especialmente la mayoría del *software* de secuestro, pueden propagarse en archivos adjuntos de correo electrónico maliciosos y sitios web infectados. Con la evolución de la inteligencia artificial y la tecnología de aprendizaje automático (IA/ML), las máquinas, en lugar de personas, pueden iniciar comunicaciones, como las llamadas robot, el chat de robots, los mensajes de texto automáticos, etc. Los algoritmos de IA/ML también aprovechan la información personal con mayor precisión para encontrar víctimas de correo basura comercial a gran escala o incluso correo basurafraudulento.

El amplio despliegue de las IMT-2020, la Internet de las cosas y otras tecnologías de telecomunicaciones/TIC, ha dado lugar a que el correo basura también empiece a afectar gradualmente a los sistemas industriales.

Es de sobra conocido que el correo basura es un problema de alcance mundial que se ha de abordar desde múltiples ángulos y de manera exhaustiva. En su calidad de Comisión de Estudio rectora sobre seguridad en las telecomunicaciones y en aplicación de la Resolución 52 de la AMNT, la Comisión de Estudio 17 reúne las condiciones idóneas para estudiar toda la gama de medidas técnicas posibles para combatir el correo basura, en la medida en que afecta a la estabilidad y la robustez de la red de telecomunicaciones. Por otra parte, se ha creado una estructura técnica para las Recomendaciones presentes y futuras relativas a la lucha contra el correo basura por medios técnicos con el fin de facilitar la preparación de las mismas. Además, se habrán de publicar nuevas Recomendaciones sobre las nuevas formas de correo basura.

Las Recomendaciones y los Suplementos relacionados con el estudio de esta Cuestión son, al 3 de septiembre de 2020, los siguientes: X.1205, X.1206, X.1207, X.1208, X.1209, X.1210, X.1211, X.1212, X.1213, X.1214, X.1215, X.1216, X.1231, X.1232, X.1240, X.1241, X.1242, X.1243, X.1244, X.1245, X.1246, X.1247, X.1248, X.1249, X.1303, X.1303*bis*, X.1500, X.1500.1, X.1520, X.1521, X.1524, X.1525, X.1526, X.1528, X.1528.1, X.1528.2, X.1528.3, X.1528.4, X.1541, X.1542, X.1544, X.1546, X.1550, X.1570, X.1580, X.1581, X.1582 y los Suplementos X.Supl.6, X.Supl.8, X.Supl.9, X.Supl.10, X.Supl.11, X.Supl.12, X.Supl.14, X.Supl.18, X.Suppl.20, X.Suppl.25 y X.Supl.29 y el Informe técnico TR.usm.

Textos en preparación: X.1246rev, X.1247rev, X.arc-ev, X.fgati (X.1217), X.gcims, X.ics-schema, X.tf-mpc, X.rdmase (X.1218), X.tecwes, X,tfcmms, X.tsfpp, TR.cs-ml y TR.sgfdm.

### D.2 Cuestión

Los temas de estudio que se han de considerar en el contexto de redes y sistemas de telecomunicaciones/TIC son, entre otros:

a) ¿Cómo deben los proveedores de telecomunicaciones/TIC proteger su infraestructura, efectuar operaciones seguras y utilizar mecanismos que garanticen la seguridad?

b) ¿Cuáles son los requisitos de seguridad que los ingenieros y fabricantes de *software*, protocolos de telecomunicaciones y sistemas de comunicaciones han de tomar en consideración al diseñar, desarrollar e intercambiar prácticas idóneas en el ciberentorno?

c) ¿Cuál es la forma más eficaz de compartir la información acerca de las vulnerabilidades, puntos débiles y medidas contra ataques para ayudar en los procesos mientras persista la vulnerabilidad?

d) ¿Qué requisitos y soluciones son necesarios para asegurar la resistencia, seguridad e integridad de los sistemas modulares de telecomunicaciones/TIC?

e) ¿Qué requisitos y soluciones son necesarios para la responsabilidad en materia de telecomunicaciones/TIC, la respuesta a incidentes, los servicios de seguridad gestionados, la atribución de ciberataques, la supervisión de amenazas y la comunicación de riesgos?

f) ¿Qué mecanismo se requiere para el intercambio de información sobre seguridad y garantía de la misma en relación con los cibersistemas, incluidos los sistemas basados en la nube, integrados y modulares?

g) ¿Cómo se pueden utilizar la inteligencia artificial y el aprendizaje automático para determinar y analizar rápidamente las nuevas amenazas y vulnerabilidades?

h) ¿Cómo deberían los proveedores de telecomunicaciones/TIC utilizar la inteligencia sobre amenazas para mejorar sus actividades de seguridad?

i) ¿Cómo pueden utilizarse las redes para prestar servicios esenciales, como la utilización de un protocolo de alerta común, de manera segura en caso de emergencia nacional?

j) ¿Qué conjunto de componentes del marco de ciberseguridad puede utilizar una organización para hacer frente a los riesgos?

k) ¿Qué directrices y prácticas idóneas en materia de seguridad son necesarias para identificar y mitigar las ciberamenazas, incluido el *software* maligno (*malware*), la denegación de servicio distribuido y la ingeniería social, y reducir sus consecuencias?

l) ¿Qué tipo de informes técnicos y recomendaciones pueden elaborarse para respaldar los procedimientos, políticas y marcos técnicos de ciberseguridad?

m) ¿Cómo se puede comprender e identificar el correo basura?

n) ¿Cuáles son las nuevas formas de correo basura en las redes presentes y futuras?

o) ¿Qué efectos graves puede tener el correo basura?

p) ¿Qué factores técnicos contribuyen dificultar la identificación del origen del correo basura?

q) ¿De qué manera las nuevas tecnologías, servicios y aplicaciones, como la mensajería instantánea, las redes sociales, las aplicaciones móviles, los servicios de voz por evolución a largo plazo (VoLTE)/Rich Communication Suite (RCS), etc., aumentan las oportunidades para crear y difundir correo basura?

r) ¿Cómo se pueden identificar las rutas, las fuentes y los volúmenes de correo basura para contrarrestarlo y combatirlo?

s) ¿Cómo se puede aplicar la seguridad de la mensajería?

t) ¿Cómo se puede evitar la distribución de *software* malicioso y *software* malignoa través del correo electrónico?

u) ¿Cómo se pueden identificar las rutas, las fuentes y los volúmenes del correo basura y calcular la cuantía de la inversión en instalaciones y otros medios técnicos necesaria para contrarrestar y combatir dicho correo basura?

v) ¿Cómo se pueden impedir los ataques dirigidos que utiliza la *peska* específica?

w) ¿Cómo se pueden impedir los ataques mediante *software* de secuestro por correo electrónico?

x) ¿Cómo se puede identificar e impedir la comunicación de correo basura mediante IA/ML?

y) ¿Cómo se puede proteger la información personal con la adopción de la tecnología IA/ML para evitar la propagación de mensajes correo basura?

z) ¿Qué tareas técnicas se están llevando a cabo en el IETF, 3GPP, GSMA, M3AAWG y otros foros, así como por entidades del sector privado, para resolver el problema del correo basura?

aa) ¿Qué actividad de normalización de las redes de telecomunicaciones se requiere eventualmente para combatir de manera eficaz el correo basura en la medida en que afecta a la estabilidad y la robustez de las redes de telecomunicaciones?

bb) ¿Cuáles son las soluciones efectivas y eficaces contra el correo basura?

cc) ¿Cómo se pueden determinar los requisitos genéricos y específicos para compartir información sobre la lucha contra el correo basura?

dd) ¿Cuáles son las prácticas idóneas para luchar contra el correo basura?

### D.3 Tareas

Las tareas que se han de considerar en el contexto de los sistemas y redes de telecomunicaciones/TIC son, entre otras:

a) Colaborar con las Comisiones de Estudio del UIT-T, ETSI, FIRST, IETF, IEEE, JTC 1 de ISO/CEI, OASIS, OMA, TCG, 3GPP, 3GPP2, y otras entidades de normalización en el ámbito de la ciberseguridad.

b) Estudiar marcos y Recomendaciones sobre la manera en que los proveedores de telecomunicaciones/TIC pueden proteger su infraestructura, efectuar operaciones seguras e intercambiar información sobre ciberseguridad.

c) Elaborar un conjunto de Recomendaciones que faciliten soluciones de seguridad para la responsabilidad y garantía en materia de telecomunicaciones/TIC y la respuesta y recuperación en caso de incidente, comprendidos los aspectos técnicos de los servicios de seguridad gestionados.

d) Estudiar y especificar las capacidades y técnicas de seguridad para que los proveedores de servicios coordinen e intercambien información sobre vulnerabilidades, plataformas y ciberataques.

e) Estudiar y especificar el marco de ciberseguridad integrado por un conjunto de componentes que sirvan para identificar, proteger, detectar, responder y recuperar.

f) Especificar cómo utilizar la inteligencia artificial y el aprendizaje automático para identificar y analizar rápidamente las nuevas amenazas y vulnerabilidades.

g) Especificar cómo emplear el mecanismo de responsabilidad, garantía y respuesta en caso de incidente en las redes de telecomunicaciones/TIC.

h) Elaborar directrices y técnicas para proteger la información personal y la información personal de identificación (PII) utilizando técnicas CYBEX, STIX y TAXII y otras herramientas de seguridad pertinentes.

i) Estudiar y desarrollar una guía técnica para apoyar la gestión de las amenazas en términos de identificación de la fuente de los ciberataques.

j) Prestar asistencia a otras Comisiones de Estudio del UIT-T en la aplicación de las Recomendaciones sobre ciberseguridad a determinadas soluciones de seguridad.

k) Elaborar prácticas idóneas y directrices para el intercambio de información sobre vulnerabilidades y la aplicación de soluciones que sirvan de ayuda en los procesos mientras persista la vulnerabilidad.

l) Colaborar con otras organizaciones de normalización (por ejemplo, OASIS para adoptar STIX y TAXII en los documentos de la UIT).

m) Elaborar Recomendaciones e Informes técnicos sobre cómo abordar los problemas de ciberseguridad.

n) Actuar de Comisión rectora del UIT‑T en materia de medios técnicos para combatir el correo basura, según define este término la Comisión de Estudio 2.

o) Identificar y examinar los riesgos de seguridad en las redes de telecomunicaciones (marginales y centrales) resultantes del carácter permanentemente cambiante del correo basura.

p) Identificar las rutas, las fuentes y los volúmenes de correo basura y estimar el monto de las inversiones en instalaciones y otros medios técnicos para contrarrestar y combatir dicho correo basura.

q) Elaborar una lista de recursos, completa y actual, de las medidas técnicas existentes para combatir el correo basura en las redes de telecomunicaciones que se utilizan o están en fase de desarrollo.

r) Elaborar nuevas Recomendaciones para contrarrestar las formas existentes y nuevas de correo basura.

s) Elaborar un conjunto de medidas técnicas para reforzar la seguridad de la mensajería.

t) Elaborar nuevas Recomendaciones para impedir la distribución de *software* malicioso y el *software* malignoa través del correo electrónico.

u) Preparar un conjunto de soluciones para impedir los ataques selectivos mediante el uso de la *peska* específica a través del correo electrónico.

v) Elaborar nuevas Recomendaciones para impedir la distribución de *software* de secuestro a través del correo electrónico.

w) Elaborar requisitos genéricos y específicos para compartir información sobre la lucha contra el correo basura.

x) Determinar si la adopción de nuevas Recomendaciones o la revisión de las existentes relativas a métodos para combatir el envío de correo electrónico no solicitado, *software* maligno y otro contenido pernicioso y para protegerse contra los equipos de red infectados, como las redes zombi, favorecería los esfuerzos desplegados para combatir eficazmente el correo basura en lo que se refiere a la estabilidad y la robustez de las redes de telecomunicaciones.

y) Desarrollar un conjunto de soluciones o nuevas Recomendaciones para contrarrestar el correo basura de tipo comunicación IA/ML.

z) Informar periódicamente de las novedades al Grupo Asesor de Normalización de las Telecomunicaciones y al Director de la Oficina de Normalización de las Telecomunicaciones, para que las incluyan en el Informe anual al Consejo.

En el programa de trabajo de la Comisión de Estudio 17 se indica el estado actual del estudio de esta Cuestión (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

### D.4 Relaciones

Líneas de Acción de la CMSI

C5.

Objetivos de Desarrollo Sostenible

–

Recomendaciones

Serie X y otras relacionadas con la seguridad.

Cuestiones

Cuestiones 1/17, 2/17, 3/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 y 15/17 del UIT‑T.

Comisiones de Estudio

CE 1 y CE 2 del UIT-D; CE 2, 9, 11, 13, 16 y 20 del UIT-T.

Entidades de normalización

Instituto Europeo de Normas de Telecomunicación (ETSI); Instituto de Ingenieros Eléctricos y Electrónicos (IEEE); Grupo Especial sobre Ingeniería de Internet (IETF); TC 57 de la CEI, TC 292 de la CEI, TC 65/GT 10 de la CEI; JTC 1/SC 27 de ISO/CEI; National Institute of Standards and Technology (NIST); Organización para el Desarrollo de Normas relativas a la Información Estructurada (OASIS); Alianza móvil abierta (OMA); Grupo Abierto; Grupo de gestión de objetos (OMG); Proyecto común de tecnologías inalámbricas de la tercera generación (3GPP); Proyecto común de tecnologías inalámbricas de la tercera generación 2 (3GPP2); Trusted Computing Group (TCG).

Otras entidades

Grupo de Trabajo contra la suplantación de identidad (APWG); CERT/CC; Agencia Europea de Seguridad de las Redes y la Información (ENISA); Asociación GSM (GSMA); Grupo de Trabajo contra el abuso de mensajería, incluida la móvil, y el *software* maligno (M3AAWG); Foro sobre los equipos de seguridad y respuesta ante incidentes (FIRST); National Institute of Standards and Technology (NIST); Organización para la Cooperación y el Desarrollo Económicos (OCDE).

## E Cuestión 6/17 – Seguridad de los servicios de telecomunicaciones e Internet de las cosas

(Continuación de la Cuestión 6/17)

### E.1 Motivación

En la Recomendación UIT-T X.1101 se especifican los requisitos de seguridad y el marco para la comunicación multidifusión. En las Recomendaciones UIT-T X.1111, X.1112, X.1113 y X.1114 se describe el marco de seguridad para las redes domésticas, incluidos los perfiles de certificado de dispositivo, los mecanismos de autentificación y el marco de autorización. En las Recomendaciones UIT-T X.1121, X.1122, X.1123, X.1124 y X.1125 se especifica de manera exhaustiva la seguridad en redes móviles. En los proyectos de Recomendación X.1171, X.1311 y X.1312 se especifica, respectivamente, el marco general de la privacidad para servicios NID móviles, el marco de seguridad de la USN (red de sensores ubicua), las directrices de seguridad del *software* intermedio de la USN y los requisitos de seguridad para el encaminamiento en la red de sensores inalámbrica. En las Recomendaciones UIT-T X.1191, X.1192, X.1193, X.1194, X.1195, X.1196, X.1197 y X1198 se describe un conjunto completo de requisitos, mecanismos y marco de seguridad de los servicios de TVIP. En los Suplementos X.Supl.19 y X.Supl.24 del UIT-T se indican los aspectos relacionados con la seguridad de los teléfonos móviles. Las Recomendaciones UIT-T X.1331, X.1332 y el Suplemento UIT-T X.Suppl.26 describen los aspectos relativos a la seguridad de la red inteligente. Las Recomendaciones UIT-T X.1361, X.1362, X.1363, X.1364 y X.1365 proporcionan requisitos, mecanismos y marcos de seguridad relacionados con la IoT. Es indispensable proseguir el mantenimiento y mejora de estas Recomendaciones y Suplementos de seguridad para satisfacer las necesidades de las nuevas tecnologías y servicios.

Por servicios de telecomunicaciones, redes e IoT se entiende el servicio que permite al usuario acceder a cualquier información deseada de manera fácil, en cualquier momento y dondequiera que se encuentre, utilizando todo tipo de dispositivos. El sector de las telecomunicaciones ha experimentado un crecimiento exponencial en el ámbito de los servicios de telecomunicaciones basados en la tecnología móvil. Para que prosiga el desarrollo ulterior de la industria, los operadores de redes y los proveedores de servicio, resulta especialmente crucial la seguridad de los servicios y redes de telecomunicaciones de dominio específico entre dispositivos heterogéneos para las tecnologías de nivel de aplicación, como la IoT y las ciudades inteligentes (incluidas la máquina a máquina (M2M), la RFID, la comunicación de campo cercano (NFC) y la red de sensores), la red doméstica, los sistemas de control industrial (por ejemplo, la fábrica inteligente), la red inteligente, el módulo de identidad del abonado integrado (eSIM), los teléfonos inteligentes y las redes de TVIP, etc., son cruciales para el desarrollo ulterior de la industria, los operadores de redes y los proveedores de servicios.

Para los operadores de red y proveedores de servicio que desempeñan actividades en el entorno internacional de telecomunicaciones con dispositivos de diversos fabricantes resulta indispensable la normalización de las mejores soluciones de seguridad integrales. Dadas algunas características inherentes del entorno IoT (por ejemplo, la limitada potencia de cálculo y el reducido tamaño de la memoria de los dispositivos móviles pequeños, la prolongada vida útil, los sistemas operativos y *software* personalizados), proporcionar seguridad y protección de la información de identificación personal (PII) es una tarea especialmente difícil que merece especial atención y estudio.

Las Recomendaciones y los Suplementos relacionados con el estudio de esta Cuestión son, al 3 de septiembre de 2020, los siguientes: X.1101, X.1111, X.1112, X.1113, X.1114, X.1121, X.1122, X.1123, X.1124, X.1125, X.1126, X.1127, X.1171, X.1191, X.1192, X.1193, X.1194, X.1195, X.1196, X.1197, X.1198, X.1311, X.1312, X.1313, X.1314, X.1331, X.1332, X.1361, X.1362, X.1363, X.1364, X.1365, X.1366, X.1367 y los Suplementos X.Supl.19, X.Supl.24 y X.Supl.26.

Textos en preparación: X.iotsec-4, X.sc-iot, X.secup-iot (X.1368), X,sg-rat, X.ssp-iot, X.strvms y X.ztd-iot.

### E.2 Cuestión

Los temas de estudio que se han de considerar son, entre otros:

a) ¿Cómo identificar y definir los aspectos relativos a la seguridad de los servicios de telecomunicaciones e IoT en las telecomunicaciones móviles?

b) ¿Cómo identificar y tratar las amenazas que acechan a los servicios de telecomunicaciones e IoT?

c) ¿Cuáles son las tecnologías de seguridad que pueden utilizarse en los servicios de telecomunicaciones e IoT?

d) ¿Cómo ha de efectuarse y mantenerse la interconexión segura de los servicios de telecomunicaciones e IoT?

e) ¿Cómo se han de estudiar y desarrollar las tecnologías de seguridad que utilizan tecnologías basadas en la IA/ML para los servicios de telecomunicaciones y la IoT?

f) ¿Qué técnicas, mecanismos y protocolos de seguridad son necesarios para los nuevos servicios de telecomunicaciones e IoT, en particular para los servicios incipientes de protección del contenido digital?

g) ¿Cuáles son las soluciones de seguridad globales para los servicios de telecomunicaciones e IoT (por ejemplo, los servicios para ciudades inteligentes, la red de distribución de energía eléctrica inteligente e ICS (por ejemplo, fábricas inteligentes) basados en redes de telecomunicaciones/TIC)?

h) ¿Cuáles son las directrices o prácticas idóneas para los servicios de telecomunicaciones e IoT?

i) ¿Qué revisiones de las Recomendaciones existentes o qué nuevas Recomendaciones han de adoptarse para atenuar los efectos directos o indirectos de las telecomunicaciones/TIC y de otras industrias sobre el cambio climático (por ejemplo, el ahorro de energía, la reducción de las emisiones de gases con efecto invernadero, la utilización de sistemas de supervisión, etc.)?

j) ¿Qué mecanismos de protección y gestión de la PII (información de identificación personal) son necesarios a los efectos de seguridad de los servicios de telecomunicaciones e IoT?

### E.3 Tareas

Las tareas son, entre otras:

a) En colaboración con otras Comisiones de Estudio del UIT-T y otras organizaciones de normalización, en particular el IETF, los JTC 1/SC 6, 25, 27, 31 y 41 de ISO/CEI, preparar un conjunto de Recomendaciones que proporcionen soluciones de seguridad completas para los servicios de telecomunicaciones e IoT seguros.

b) Examinar las Recomendaciones del UIT-T y las normas de ISO/CEI existentes en el ámbito de las redes domésticas, la red de distribución de energía eléctrica inteligente, la seguridad de los teléfonos inteligentes, la IoT y la red de sensores ubicuos con el fin de determinar servicios y redes de telecomunicaciones seguros.

c) Proseguir los estudios destinados a definir aspectos relativos a la seguridad en los servicios de telecomunicaciones e IoT para un entorno de telecomunicaciones internacional con dispositivos de diversos fabricantes, y para los nuevos servicios (por ejemplo, los relativos a ciudades inteligentes, redes de distribución de energía eléctrica inteligentes e ICS (por ejemplo, fábricas inteligentes) basados en redes de telecomunicaciones/TIC).

d) Estudiar y solucionar los problemas de seguridad y las amenazas en los servicios de telecomunicaciones e IoT.

e) Estudiar y elaborar mecanismos de seguridad para los servicios de telecomunicaciones e IoT seguros.

f) Estudiar y elaborar mecanismos de interconexión para los servicios y las redes de telecomunicaciones seguros en un entorno de telecomunicaciones de uno o varios fabricantes.

g) Estudiar y determinar los problemas y las amenazas en materia de protección de PII en servicios y redes de telecomunicaciones seguros.

h) Estudiar y elaborar mecanismos de protección y gestión en materia de PII para los servicios de telecomunicaciones e IoT.

i) Estudiar y desarrollar tecnologías de seguridad utilizando tecnologías basadas en la IA/ML para los servicios de telecomunicaciones seguras e IoT.

En el programa de trabajo de la Comisión de Estudio 17 se indica el estado actual del estudio de esta Cuestión (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

### E.4 Relaciones

Líneas de Acción de la CMSI

C5.

Objetivos de Desarrollo Sostenible

–

Recomendaciones

Serie X y otras relacionadas con la seguridad.

Cuestiones

Cuestiones 1/17, 2/17, 3/17, 4/17, 7/17, 8/17, 10/17, 11/17, 13/17 y 14/17 y 15/17 del UIT-T.

Comisiones de Estudio

UIT-R; CE 9, 11, 13, 15, 16 y 20 del UIT-T; JCA-IoT, y SC&C.

Entidades de normalización

Grupo Especial sobre Ingeniería de Internet (IETF); IEC SEG 6 (microrred eléctrica), SMB GT 3 de la CEI, TC 57 y 65 de la CEI; JTC 1/SC 6, 25, 27, 31 y 41 de ISO/CEI; Alianza móvil abierta (OMA); Proyecto común de tecnologías inalámbricas de la tercera generación (3GPP); Proyecto común de tecnologías inalámbricas de la tercera generación 2 (3GPP2).

Otras entidades

Alliance of Telecommunications Industry Solutions (ATIS); Asociación de Normalización de las Comunicaciones de China (CCSA); Instituto Europeo de Normas de Telecomunicación (ETSI), Asociación GSM (GSMA); Alianza M2M; Foro NFC; National Institute of Standards and Technology (NIST); oneM2M; Comité Tecnológico de Telecomunicaciones (TTC); Asociación para las Tecnologías de las Telecomunicaciones (TTA); Universal Plug and Play (UPnP).

## F Cuestión 7/17 – Servicios de aplicación seguros

(Continuación de la Cuestión 7/17)

### F.1 Motivación

Las Recomendaciones UIT-T X.1141, X.1142, X.1143, X.1144, X.1145, X.1146 y X.1147 constituyen un conjunto de Recomendaciones sobre llaves de seguridad para la autentificación/autorización y arquitecturas de seguridad para mensajes en servicios de red. En las Recomendaciones UIT-T X.1151, X.1152, X.1153, X.1154, X1155, X.1156, X.1157, X.1158 y X.1159 se especifican las directrices para la autentificación segura mediante contraseña e intercambio de claves y para diversos servicios de terceros fiables (TTP). En las Recomendaciones UIT-T X.1161, X.1162, X.1163 y X.1164 se especifican los mecanismos y un marco exhaustivo para la seguridad de servicios entre entidades pares (P2P). Es preciso seguir adelante con las actividades destinadas a mantener actualizadas y mejorar estas Recomendaciones sobre seguridad a fin de satisfacer las necesidades de los nuevos servicios y tecnologías.

El sector de las telecomunicaciones ha experimentado un crecimiento exponencial en el ámbito de los servicios TTP (terceros fiables). Para la expansión del sector resultan particularmente importantes los servicios de aplicación basados en telecomunicaciones, incluidos el servicio de redes sociales y los servicios P2P y TTP. Los protocolos de aplicación seguros desempeñan un papel importantísimo para suministrar un servicio de aplicación seguro. La normalización de las mejores soluciones integrales de seguridad es fundamental para la industria, los operadores de red y los proveedores de servicio que operan a escala internacional con dispositivos de diversos fabricantes. También es necesario estudiar y desarrollar otros tipos de servicios de aplicaciones en plataformas seguras, como los servicios de estampación de fecha y hora, servicios notariales seguros, servicios FinTech seguros (banca abierta, préstamos entre pares, remesas, monedero móvil, seguros), servicios OTT (Over The Top) seguros, y réplicas digitales; utilización de asertos de seguridad en lugar de certificados en protocolos basados en PKI y servicios de aplicaciones de PKI, etc. Las tecnologías de seguridad de los servicios web, tales como el aserto de seguridad y el aserto del control de acceso son ahora esenciales en las redes de telecomunicaciones.

A medida que las telecomunicaciones y las TIC desarrollan servicios de aplicaciones, se enfrentan a dos nuevos horizontes que es preciso estudiar: las aplicaciones generan y procesan cada vez más datos y, por ese motivo, requieren ahora inteligencia artificial. Es necesario ampliar los servicios de aplicaciones seguras para que abarquen la amplia investigación y el mercado necesarios para estudiar toda la gama de los aspectos operativos y técnicos de la protección de datos, que se basa en la labor existente sobre los servicios de análisis de datos.

En cuanto a la inteligencia artificial, los proveedores de servicios se enfrentan a varios retos, en particular la selección, incorporación e integración de docenas, si no cientos, de componentes de IA de código abierto y de la industria, que deben agrupar en diversos factores de forma (aplicaciones integradas de IA, IA como plataformas más genéricas, IA como plataforma como servicio, etc.) en diversas infraestructuras (en instalaciones, en nubes privadas, en nubes híbridas o en nubes públicas). Al igual que cuando surgieron los macrodatos, la IA crea nuevos problemas de interoperabilidad en materia de seguridad, así como los relativos a garantizar la confidencialidad, integridad y disponibilidad de datos para entrenar la IA y de datos procesados por la IA. Todo esto forma una nueva superficie de ataque para la inteligencia artificial que se ha de estudiar y desarrollar. Una vez más puede basarse en el trabajo inicial existente sobre los servicios de análisis de datos.

Las Recomendaciones y los Suplementos relacionados con el estudio de esta Cuestión son, al 3 de septiembre de 2020, los siguientes: X.1141, X.1142, X.1143, X.1144, X.1145, X.1146, X.1147, X.1148, X.1149, X.1151, X.1152, X.1153, X.1154, X.1155, X.1156, X.1157, X.1158, X.1159, X.1161, X.1162, X.1163, X.1164, X.1450, X.1451 y los Suplementos X.Supl.17, X.Supl.21 y X.Supl.22.

Textos en preparación: X.rdda, X.scpa, X.sec-grp-mov, X.sgos, X,sles, X.smdtsc, X.smsrc, X.tfss (X.1452), X.websec-7 y TR.cta.

### F.2 Cuestión

Los temas de estudio que se han de considerar son, entre otros:

a) ¿Cómo identificar y tratar las amenazas que acechan a los servicios de aplicación seguros?

b) ¿Cuáles son las técnicas de seguridad necesarias para los servicios de aplicación seguros?

c) ¿Cómo pueden mantenerse la interconexión segura entre servicios de aplicación?

d) ¿Qué técnicas de seguridad o protocolos son necesarios para los servicios de aplicación seguros?

e) ¿Qué técnicas de seguridad o protocolos son necesarios para los nuevos servicios de aplicación seguros, en particular la plataforma de servicios, los servicios FinTech y los servicios OTT?

f) ¿Cuáles son las soluciones globales para los servicios de aplicación seguros y sus aplicaciones?

g) ¿Cómo definir una estrategia de protección de datos operativos y técnicos para los servicios de aplicación?

h) ¿Cómo definir una estrategia de protección de la superficie de ataque de la inteligencia artificial?

### F.3 Tareas

Las tareas son, entre otras:

a) En colaboración con otras Comisiones de Estudio del UIT-T y otras organizaciones de normalización, en particular el JTC 1/SC 27 de ISO/CEI, preparar un conjunto de Recomendaciones que proporcionen soluciones de seguridad completas para los servicios de aplicaciones seguros.

b) Examinar las Recomendaciones UIT-T y las normas ISO/CEI relativas a los servicios de aplicación seguros.

c) Proseguir los estudios encaminados a definir los aspectos relativos a la seguridad para los servicios de aplicación seguros y los nuevos servicios, como los servicios FinTech y OTT.

d) Estudiar y solucionar los problemas de seguridad y las amenazas en los servicios de aplicación seguros.

e) Estudiar y elaborar mecanismos de interconectividad para servicios de aplicación seguros.

f) Estudiar y elaborar estrategias y Recomendaciones sobre los aspectos operativos y técnicos de la protección de datos para los servicios de aplicaciones.

g) Estudiar y elaborar estrategias y Recomendaciones para la protección de la superficie de ataque de la inteligencia artificial.

En el programa de trabajo de la Comisión de Estudio 17 se indica el estado actual del estudio de esta Cuestión (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

### F.4 Relaciones

Líneas de Acción de la CMSI

C5.

Objetivos de Desarrollo Sostenible

–

Recomendaciones

Serie X.800 y otras relacionadas con la seguridad.

Cuestiones

Cuestiones 1/17, 2/17, 3/17, 4/17, 6/17, 8/17, 10/17, 11/17, 14/17, 15/17, 7/13 y 13/17 del UIT‑T.

Comisiones de Estudio

CE 2, 9, 11, 13, 16 y 20 del UIT-T.

Entidades de normalización

Grupo Especial sobre Ingeniería de Internet (IETF); Instituto Europeo de Normas de Telecomunicación (ETSI); Asociación GSM (GSMA); JTC 1/SC 27 de ISO/CEI; JTC 1/SC 42 de ISO/CEI; ISO/TC 68; ISO/TC 307; Iniciativa Kantara; Organización para el Desarrollo de Normas relativas a la Información Estructurada (OASIS); Alianza móvil abierta (OMA); Consorcio WWW (W3C).

Otras entidades

Consejo de Europa (COE); Agencia Europea de Seguridad de las Redes y la Información (ENISA); Alianza "Fast Identity Online" (FIDO); Alianza Internacional Multilateral contra las Ciberamenazas (IMPACT).

## G Cuestión 8/17 – Seguridad de la infraestructura de computación en la nube y macrodatos

(Continuación de la Cuestión 8/17)

### G.1 Motivación

La computación en la nube es un modelo que permite ofrecer al usuario de servicio un acceso ubicuo, práctico, por demanda y a través de la red a un conjunto compartido de recursos informáticos configurables (como, por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser suministrados y liberados rápidamente con una labor de gestión mínima o una interacción mínima con el proveedor de servicio. El modelo de computación en la nube tiene cinco características esenciales (por demanda, suministro a través de un amplio acceso a la red, agrupación de recursos, elasticidad rápida, autoservicio y servicios medidos), cinco categorías de servicios de computación en la nube, a saber, *software* como servicio (SaaS, *software as a service*), comunicación como servicio (CaaS, *communication as a service*), plataforma como servicio (PaaS, *platform as a service*), infraestructura como servicio (IaaS, *infrastructure as a service*) y red como servicio (NaaS, *network as a service*), y de diferentes modelos de despliegue (público, privado, híbrido...), así como ampliación flexible de tipos de suministro de servicios (central, regional, periférico...). El hecho de que la computación en la nube se haya convertido en la opción preferida para el descubrimiento, la externalización, la composición y la reutilización del servicio en los flujos de trabajo, las aplicaciones y las aplicaciones de comunicaciones pone de manifiesto la necesidad de que sea segura.

Entre los beneficios que se prevé reportará la computación en la nube se cuentan la configuración flexible y dinámica de recursos y la administración más simple y automatizada de la infraestructura de TI. La virtualización permite compartir recursos prácticamente ilimitados con mejoras progresivas y una reducción masiva de los costos de gestión de la infraestructura. La introducción de la computación periférica permite distribuir las capacidades de la nube en la periferia de la red. Así se logran implementaciones de servicios en la nube que tienen una latencia baja y determinista y una alta fiabilidad. Sin embargo, los sistemas abiertos, los recursos compartidos y el interfuncionamiento inherente de la nube y la periferia suscitan inquietudes de seguridad, probablemente el más importante obstáculo a la adopción de la computación en la nube. Pasar a la nube implica dejar atrás los sistemas de TI propios, tradicionales y seguros para pasar a infraestructuras abiertas de tipo nube y no seguras. Es, por tanto, necesario un replanteamiento total de la seguridad.

Durante años la computación en la nube fue considerada una tecnología de la información centrada en el servicio y controlada por los actores de Internet. Sin embargo, los actores de telecomunicaciones cumplen una importante función en el mercado y ecosistema emergentes de la computación en la nube. Dado que los servicios en nube se entregan a través de las redes de telecomunicaciones, los actores de telecomunicaciones deben garantizar un alto nivel de seguridad. Una protección de seguridad fuerte, pero flexible, será fundamental para habilitar todo el ecosistema y el mercado de la nube, especialmente cuando la computación periférica brinda una distribución más local de los recursos de la nube. Así se complican las relaciones entre las implementaciones periféricas, regionales y centrales de la nube.

Además, la utilización flexible de grandes recursos en el entorno de computación en la nube hará posibles nuevos servicios de seguridad que las actuales defensas no pueden ofrecer (por ejemplo, servicios *anti-malware* como servicio en nube).

Se entiende por macrodatos las tecnologías, el conjunto de herramientas, los datos y los análisis utilizados en el procesamiento de grandes volúmenes de datos. A medida que el volumen de datos crece exponencialmente y se convierte en un activo esencial de las redes de telecomunicaciones/TIC, los conjuntos de datos masivos se analizan con la ayuda de la computación en la nube a fin de determinar patrones y relaciones que de otro modo permanecerían ocultos. Los procesos básicos de los macrodatos, como la recopilación, el almacenamiento, el análisis, la gestión y la visualización de los mismos, se consigue gracias a la computación en la nube, ya que los grandes datos no podrían transferirse y analizarse rápidamente utilizando las tecnologías tradicionales (por ejemplo, los macrodatos como servicio). Por consiguiente, es necesario estudiar qué tipo de medidas de seguridad la computación en la nube podrá ofrecer en un futuro próximo. En las Recomendaciones UIT-T X.1601, X.1602 y X.1631 se formulan una serie de Recomendaciones relativas al servicio de seguridad en el marco general de la seguridad en nube, la arquitectura y el marco general, la seguridad en nube entre capas y la seguridad específica de los servicios de red. Hoy en día resulta fundamental dar seguridad a los servicios de voz, multimedios e identidad, los servicios de garantía de la información, los servicios de identidad y datos y los servicios de emergencia disponibles en la computación en la nube. Con esta Cuestión se pretenden elaborar nuevas Recomendaciones, basadas en la parte 5 del Informe técnico del Grupo Temático sobre computación en la nube, sobre:

– elaboración de directrices y prácticas idóneas sobre cómo proporcionar seguridad en un entorno de computación en la nube;

– definición de amenazas y requisitos de seguridad, y aclaración de las responsabilidades que incumben a cada uno de los actores principales y sus correspondientes funciones en el ecosistema de la computación en la nube;

– arquitectura de seguridad basada en la arquitectura de referencia definida por la C18/13;

– gestión de seguridad y tecnologías de auditoria para la gestión de confianza.

La Cuestión 8/17 colaborará con Cuestiones afines, como 2/17, 3/17, 4/17, 7/17, 10/17 y 11/17, para elaborar Recomendaciones sobre seguridad en la computación en la nube.

Recomendaciones bajo la responsabilidad de esta Cuestión al 3 de septiembre de 2020: X.1601, X.1602, X.1603, X.1606, X.1631, X.1641, X.1642, X.1750 y X.1751.

Textos en preparación: X.BaaS-sec, X.sgBDIP, X.sgcc, X.sr-cphr, X.sgdc, X.sgmc, X.nssa-cc y TR.fssvs.

### G.2 Cuestión

Los temas de estudio son, aunque no exclusivamente, los siguientes:

a) ¿Qué nuevas Recomendaciones u otro tipo de documentos conviene elaborar para los principales actores, como proveedores de servicios, usuarios de servicios y asociados en los servicios, así como otras partes interesadas de la industria, a fin de promover la seguridad de todo el ecosistema de computación en la nube, incluida la seguridad de la computación en la nube, la seguridad de la computación periférica, la seguridad del interfuncionamiento, etc.?

b) ¿Qué nuevas Recomendaciones se han de elaborar sobre la arquitectura de seguridad y la organización de las funcionalidades de seguridad de acuerdo con la arquitectura de referencia?

c) ¿Qué nuevas Recomendaciones se han de elaborar sobre los mecanismos de garantía, las tecnologías de auditoría y la evaluación de riesgos conexos para crear confianza entre los diferentes actores?

d) ¿Qué nuevas Recomendaciones se han de elaborar sobre soluciones de seguridad, prácticas idóneas o directrices para la seguridad de la plataforma de macrodatos e infraestructura?

e) ¿Con qué otras Cuestiones, Comisiones de Estudio y organismos de normalización será necesario colaborar para minimizar la duplicación de esfuerzos?

f) ¿Cómo se debe desarrollar la seguridad como servicio para proteger los sistemas de telecomunicaciones/TIC?

### G.3 Tareas

Las tareas que se han de realizar son, aunque no exclusivamente, las siguientes:

a) Elaborar Recomendaciones o documentos de otro tipo para avanzar en la seguridad de la computación en la nube.

b) Elaborar Recomendaciones para identificar las amenazas y requisitos de seguridad para los servicios de computación en la nube basándose en los requisitos generales de la computación en la nube especificados por la Comisión de Estudio 13 del UIT-T.

c) Elaborar Recomendaciones para definir la arquitectura de seguridad y organizar las funciones de seguridad de acuerdo con la arquitectura de referencia especificada por la Comisión de Estudio 13 del UIT-T.

d) Elaborar Recomendaciones para definir una arquitectura de seguridad fuerte, flexible y elástica y su aplicación a los sistemas de computación en la nube.

e) Elaborar Recomendaciones para identificar los mecanismos de garantía, las tecnologías de auditoria, la evaluación de riesgos a fin de lograr relaciones de confianza en el ecosistema de la computación en la nube.

f) Estudiar y elaborar Recomendaciones sobre la seguridad de las plataformas e infraestructuras de macrodatos en consonancia con la arquitectura de referencia especificada por la Comisión de Estudio 13 del UIT-T.

g) Asumir todas las actividades de la Comisión de Estudio 17 relativas a la seguridad de la computación en la nube y a la seguridad de las plataformas e infraestructuras de macrodatos.

h) Representar el trabajo de la Comisión de Estudio 17 en relación con la seguridad de la computación en la nube dentro de la Actividad de Coordinación Conjunta sobre computación en la nube.

En el programa de trabajo de la Comisión de Estudio 17 se indica el estado actual del estudio de esta Cuestión (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

### G.4 Relaciones

Recomendaciones

Recomendaciones de la serie Y sobre computación en la nube.

Cuestiones

Cuestiones 1/17, 2/17, 3/17, 4/17, 7/17, 10/17, 11/17 y 15/17 del UIT-T.

Comisiones de Estudio

CE 2, 13, 16 y 20 del UIT-T.

Organismos de normalización

Grupo Especial sobre Ingeniería de Internet (IETF); JTC 1/SC 27 y SC 38 de ISO/CEI; Organización para el Desarrollo de Normas relativas a la Información Estructurada (OASIS); y otros organismos pertinentes que se puedan identificar.

Otras entidades

Cloud Security Alliance (CSA); Grupo especial de gestión distribuida (DMTF).

## H Cuestión 10/17 – Arquitectura y mecanismos de gestión de identidades y telebiometría

(Continuación de las Cuestiones 9/17 y 10/17)

### H.1 Motivación

La biometría está ganando aceptación en las aplicaciones que realizan, entre otras cosas, la verificación de la identidad, como el comercio electrónico, la telemedicina y la cibersalud. Los sistemas de aplicaciones biométricas presentan diversos problemas relacionados con la protección de datos operativos y técnicos, la fiabilidad y la seguridad de los datos biométricos para aplicaciones de bioseguridad y bioprotección.

La autenticación biométrica en el servidor se hace más complicada y exigente cuando se adopta la autenticación biométrica en un entorno de red abierto. Las aplicaciones de telecomunicaciones (como la telebiometría) que utilizan terminales móviles y servicios de Internet exigen métodos de autenticación muy seguros y fáciles de utilizar. Es necesario especificar los requisitos para la utilización segura de los datos telebiométricos, y con una mayor protección operativa y de los datos.

Por gestión de identidades (IdM) se entiende la gestión de la vida útil y utilización (creación, mantenimiento, utilización y revocación) de credenciales, identificadores, atributos y pautas que definen a entidades (por ejemplo, proveedores de servicios, usuarios finales, organizaciones, dispositivos de red, aplicaciones y servicios) con cierto nivel de confianza. Dependiendo del contexto, una misma entidad puede tener varias identidades para distintos requisitos de seguridad y en varias ubicaciones. En función del modelo de identidad, el control de las identidades puede ser centralizado o descentralizado o una combinación de ambos. En las redes públicas, la IdM permite intercambiar información fiable entre entidades autorizadas. El intercambio se basa en la afirmación de identidades a través de sistemas distribuidos de múltiples proveedores de servicios. El intercambio también puede basarse en diversos entornos de servicios, como la nube y los 5G. La IdM también mejora la protección de la información privada y, dependiendo del modelo de confianza, puede garantizar que sólo se difunda información autorizada.

La IdM es un componente fundamental de las redes, servicios y productos de telecomunicaciones/TIC, ya que su función es la de establecer y mantener comunicaciones de confianza. Además de servir para la autentificación de la identidad de entidades, también permite la autorización de privilegios y su fácil intercambio cuando varía la función que desempeña una determinada entidad, y para la delegación, la itinerancia y otros servicios importantes basados en la identidad.

La IdM también es esencial para gestionar la seguridad en las redes dado que mejora el acceso nómada y por solicitud a redes y ciberservicios corrientes hoy en día. Utilizada junto con otros mecanismos de defensa, la IdM ayuda a impedir el fraude y el robo de identidad y, por ende, aumenta el grado de confianza de los usuarios en cuanto a la seguridad y fiabilidad de las transacciones electrónicas. Como la IdM funciona de manera recíproca, aumenta el nivel de confianza tanto para el usuario como para el proveedor de servicios.

Existen especificaciones y soluciones nacionales y regionales de la IdM, las cuales seguirán evolucionando. Es importante establecer fundamentos que permitan armonizar soluciones. Además de estudiar la telebiometría, en el estudio de esta Cuestión se tratará de forjar un enfoque común y coordinar y organizar todas las actividades del UIT-T en materia de IdM. Se adoptará un enfoque descendente en colaboración con otras Comisiones de Estudio y otras organizaciones de normalización. Se reconoce que determinados aspectos de la IdM (tales como protocolos, requisitos e identificadores de dispositivos de red) se estudiarán también en el marco de otras Cuestiones.

Las Recomendaciones y Suplementos relacionadas con el estudio de esta Cuestión son, al 3 de septiembre de 2020, las siguientes: X.1080.0, X.1080.1, X.1081, X.1082, X.1083, X.1084, X.1085, X.1086, X.1087, X.1088, X.1089, X.1090, X.1091, X.1092, X.1093, X.1094, X.1250, X.1251, X.1252, X.1253, X.1254, X.1255, X.1256, X.1257, X.1258, X.1275, X.1276, X.1277, X.1278, X.1279, y Suplementos X.Supl.7 y X.Supl.35.

Textos en preparación: X.1250rev, X.1252rev, X.b2m, X.gpwd, X.pet\_auth, X.tas, X.tec-idms, y X.upu.

### H.2 Cuestión

Los temas de estudio que se han de considerar son, entre otros:

a) ¿Cómo pueden mejorarse las Recomendaciones existentes para ampliar su ámbito de aplicación y utilización?

b) ¿Cuáles son los requisitos para la autentificación biométrica en redes de alta funcionalidad?

c) ¿Cómo evaluar las contramedidas de seguridad para determinadas aplicaciones de la telebiometría?

d) ¿Cómo diseñar los sistemas y funcionalidades de biometría para que se ajusten a los requisitos de seguridad de cualquier aplicación de la telebiometría, incluidos los servicios de computación en la nube?

e) ¿Cómo mejorar la identificación y la autenticación de los usuarios en los aspectos relativos a la seguridad y protección mediante la utilización de modelos interoperables en la telebiometría?

f) ¿Qué mecanismos son necesarios para garantizar la manipulación segura de los datos biométricos en cualquier aplicación de telebiometría, por ejemplo, la cibersalud, la telemedicina, comercio electrónico, servicios bancarios en línea, vídeo vigilancia?

g) ¿Cómo desarrollar los sistemas y operaciones biométricos a fin de que sean acordes con los requisitos funcionales para la autenticación de entidades de animales de compañía mediante la telebiometría?

h) ¿Cuáles son los conceptos funcionales para una infraestructura común de la gestión de identidades (IdM)?

i) ¿Qué modelo de IdM resulta adecuado que sea independiente de la tecnología de red, permita la participación del usuario, la identidad basada en la nube, modelos de identidad descentralizados y favorezca el intercambio seguro de información IdM entre entidades comunicantes (por ejemplo, usuarios, partes fiables y proveedores de identidad) basado en el consentimiento y políticas conexas?

j) ¿Cuáles son los componentes de un marco genérico y los requisitos para la IdM?

k) ¿Cuáles son los requisitos en materia de IdM específicos de los proveedores de servicio?

l) ¿Cuáles son los requisitos, capacidades y posibles estrategias para lograr la interoperabilidad entre diferentes sistemas IdM (por ejemplo, garantías de identidad, interfuncionamiento?

m) ¿Cuáles son los aspectos que hay que tomar en consideración para sustentar la identidad en las tecnologías de libro mayor distribuido, incluidas el monedero, los identificadores descentralizados y las credenciales verificables?

n) ¿Cuáles son los posibles mecanismos para la interoperabilidad de la IdM que permitan identificar y definir perfiles aplicables y minimicen así los problemas de interoperabilidad?

o) ¿Cuáles son los requisitos y mecanismos para la protección y divulgación de la información de identificación personal (PII)?

p) ¿Cómo puede una entidad controlar su relación cuando interviene en relaciones e interacciones basadas en identidad?

q) ¿Cuáles son los requisitos para la protección de sistemas IdM contra ciberataques?

r) ¿Qué capacidades de la IdM pueden utilizarse contra los ciberataques?

s) ¿Cómo ha de integrarse la IdM en las tecnologías de seguridad avanzadas?

t) ¿Cómo se puede realizar la autenticación sin compartir secretos?

u) ¿Puede realizarse la autenticación basada en la KPI de manera compatible y segura?

v) ¿Puede utilizarse la biometría en una capa de confianza y autenticación fuerte para permitir interacciones fiables a través de una red?

w) ¿Cuáles son los requisitos específicos del sistema de gestión de la identidad basado en el consumidor en lo que respecta a la verificación de la identidad y la recuperación de cuentas sin depender de contraseñas?

x) ¿Cómo recurrir a la confianza y la relación para mejorar la recuperación de cuentas, la seguridad del usuario y la experiencia al tratar con partes fiables?

### H.3 Tareas

Las tareas son, entre otras:

a) Mejorar y revisar las Recomendaciones existentes sobre autentificación telebiométrica.

b) Examinar las similitudes y las diferencias entre las Recomendaciones del UIT-T y las normas ISO/CEI existentes relativas a la telebiometría.

c) Estudiar y elaborar los requisitos de seguridad y las directrices para cualquier aplicación de la telebiometría, utilizando para ello las arquitecturas y marcos tales como los resultantes de la Cuestión 2/17.

d) Estudiar y elaborar requisitos para evaluar las técnicas de seguridad y de protección de datos operativas y técnicas en cualquier aplicación de la telebiometría.

e) Estudiar y elaborar requisitos para aplicaciones de telebiometría en redes de alta funcionalidad.

f) Estudiar y elaborar marcos integrados y requisitos de arquitecturas de aplicaciones de telebiometría para entornos de computación en la nube y almacenamiento de datos.

g) Estudiar y elaborar requisitos de autentificación biométrica para el marco de identidad fiable.

h) Estudiar y elaborar requisitos para los protocolos genéricos adecuados que proporcionen protección, seguridad, protección de datos técnicos y autoricen el "empleo de datos biométricos" en cualquier aplicación de telebiometría, por ejemplo, cibersalud, telemedicina, comercio electrónico, servicios bancarios en línea, pagos electrónicos y vídeo vigilancia.

i) Estudiar y desarrollar protocolos de Sistema biológico-a-máquina (B2M) para la transmisión de datos métricos biológicos que interactúen con protocolos de Máquina a máquina (M2M).

j) Estudiar y desarrollar aplicaciones telebiométricas mediante señales biológicas para aplicaciones que incluyen, en particular, autenticación, identificación y supervisión de datos sanitarios.

k) Estudiar y desarrollar servicios de autenticación de entidades para mascotas basados en telebiometría.

l) Especificar un marco general necesario para la IdM que permita gestionar la detección, el modelo de política y confianza, la autentificación y la autorización, los asertos y el periodo de validez de las credenciales.

m) Definir conceptos arquitectónicos funcionales de la IdM para establecer un nexo entre redes y sistemas IdM habida cuenta de las tecnologías de seguridad avanzadas.

n) Especificar los requisitos (y proponer mecanismos) para la protección de la identidad y la compatibilidad/interfuncionamiento entre los diferentes métodos de protección de la identidad que pudieran adoptarse en las distintas redes. En este contexto, la protección de la identidad incluye pautas de identidad y reputación.

o) Definir interfaces para la interoperabilidad de los sistemas IdM.

p) Definir los requisitos (y proponer mecanismos) para proteger y revelar la información personal de identificación (PII).

q) Definir los requisitos (y proponer mecanismos) para proteger los sistemas IdM, en particular cómo pueden los proveedores de servicio utilizar las capacidades IdM como mecanismo para coordinar e intercambiar información relativa a los ciberataques.

r) Mantener actualizada y coordinar la terminología y definiciones de la IdM y proseguir la labor en curso.

s) Estudiar y definir los riesgos y amenazas a la seguridad en la IdM.

t) Estudiar y desarrollar sistemas descentralizados de gestión de la identidad con soporte para el control por el usuario de sus identidades.

u) Dar soporte a sistemas de gestión de identidades de confianza que puedan federarse entre sistemas, servicios, dispositivos, IoT y aplicaciones.

v) Dar soporte a sistemas de gestión de identidades que proporcionen gestión de identidades como un servicio para los agentes de la nube, las redes 5G y los dispositivos móviles.

w) Especificar los requisitos y proponer mecanismos para garantizar la identidad para la autentificación y la federación. Establecer criterios para la compatibilidad/interfuncionamiento entre los diferentes métodos de protección de la identidad que pudieran adoptarse en las distintas redes. En este contexto, la protección de la identidad incluye pautas de identidad y reputación.

En el programa de trabajo de la Comisión de Estudio 17 se indica el estado actual del estudio de esta Cuestión (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

### H.4 Relaciones

Líneas de Acción de la CMSI

C5.

Objetivos de Desarrollo Sostenible

–

Recomendaciones

Series X e Y

X.200, X.273, X.274, X.509, X.680, X.805 y X.1051.

Cuestiones

Cuestiones 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 11/17, 15/17, 7/13 y 14/15 del UIT‑T.

Comisiones de Estudio

CE 1 y CE 2/2 del UIT-D; CE 7 del UIT-R; CE 2, 5, 9, 11, 13, 15, 16 y 20 del UIT-T.

Entidades de normalización

TC 25 de la CEI, IEC/TC 25/JWG 1; Instituto de Ingenieros Eléctricos y Electrónicos (IEEE); Grupo Especial sobre Ingeniería de Internet (IETF); JTC 1/SC 17, 27 y 37 de ISO/CEI; TC 12, 68, 215 y 307 de la ISO; 12/JWG 20 de ISO/TC; ETSI; OASIS; Kantara Initiative; 3GPP; 3GPP2.

Otras entidades

Oficina Internacional de Pesos y Medidas (BIPM); Comisión Internacional sobre Unidades y Mediciones de Radiación (ICRU); Fast Identity Online (FIDO) Alliance; DID Alliance; Oficina Internacional del Trabajo (OIT); Organización Mundial de la Salud (OMS).

## I Cuestión 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)

### I.1 Motivación

En esta Cuestión se prosigue el desarrollo de diversas tecnologías genéricas que se utilizan ampliamente en aplicaciones seguras, entre las que se cuentan:

– servicios de directorio (serie X.500)

– infraestructuras de clave pública (PKI – X.509)

– comunicación segura (X.510)

– infraestructura de gestión de privilegios (PMI – X.509)

– notación de sintaxis abstracta Uno (ASN.1)

– identificadores de objeto y sus autoridades de registro

– notación de pruebas y de control de pruebas versión 3 (TTCN-3)

– mantenimiento de lenguajes formales:

• lenguaje de especificación y descripción (SDL)

* diseño de perfiles de lenguaje de modelización unificado (UML)

• gráficos de secuencias de mensajes (MSC)

• notación de requisitos de usuario (URN)

• CHILL, Lenguaje de programación del UIT-T

– mantenimiento de OSI y ODP.

#### I.1.1 Motivos de los trabajos sobre directorios, KPI y PMI

Las Recomendaciones UIT-T de la serie X.500 tienen una incidencia considerable en la industria, por cuanto constituyen componentes importantes de tecnologías ampliamente utilizadas, tales como la infraestructura de clave pública (PKI) y el protocolo ligero de acceso al directorio (LDAP), tecnologías que tienen aplicación en ámbitos diversos, por ejemplo, finanzas, medicina y derecho. Cuando se requieren servicios de directorio con seguridad alta, por ejemplo, en aplicaciones militares, la única opción es la X.500.

La Recomendación X.500 proporciona un control minucioso de acceso y protección de la privacidad de los datos. Se trata de una especificación abierta que puede adaptarse a diferentes aplicaciones. Se puede ampliar para satisfacer los requisitos que se hayan de cumplir en el futuro. El muy utilizado LDAP se basa en el modelo de directorio de la X.500 del UIT-T. La Recomendación UIT-T X.500 incluye capacidades para el interfuncionamiento con LDAP. Las soluciones de directorio UIT-T X.500 y LDAP son una parte importante de la gestión de identidad (IdM).

La Recomendación UIT-T X.509 reviste una importancia considerable, dado que los certificados de clave pública se utilizan de manera generalizada.

Además de ser un componente importante en el comercio electrónico, la banca electrónica y la cibersalud, actualmente también se utiliza en otras aplicaciones caracterizadas por grandes redes con comunicación máquina a máquina y entidades restringidas, por ejemplo, Internet de las cosas (IoT) y redes eléctricas inteligentes (red inteligente).

También se utilizan certificados de clave pública para varias especificaciones del IETF, por ejemplo, en la seguridad de la capa de transporte (TLS).

Los certificados de atributos proporcionan un método seguro para transferir privilegios importantes para el control de acceso. Las especificaciones SAML de OASIS se basan en los certificados de atributo de la Recomendación UIT-T X.509. Éstos se utilizan también en los sistemas eléctricos y son especialmente útiles cuando los privilegios los asignan autoridades distintas de las que emiten los certificados de clave pública.

En colaboración con otros grupos, es necesario que la Recomendación UIT-T X.509 evolucione y se mantenga actualizada para que responda y aproveche las experiencias obtenidas en los campos de la infraestructura de clave pública (PKI) y de la infraestructura de gestión de privilegios (PMI). Debe mejorarse a tenor de los nuevos requisitos, como las comunicaciones entre máquinas, la seguridad de las redes inteligentes, la seguridad de Internet de las cosas, los algoritmos de seguridad cuántica y las tecnologías de libro mayor distribuido. Se está elaborando un mecanismo descentralizado de PKI que utiliza cadenas de bloques.

Las Recomendaciones relacionadas con el estudio de esta Cuestión son, al 3 de septiembre de 2020, las siguientes: E.104 (en colaboración con la CE 2), E.115 (en colaboración con la CE 2), F.500, F.510, F.511, F.515, X.500, X.501, X.509, X.510, X.511, X.518, X.519, X.520, X.521, X.525, X.530 y X.1341.

Textos en preparación: X.510 Amd.1, X.pki-em.

#### I.1.2 Motivos de los trabajos relativos a ASN.1

Se elaborarán, si procede, nuevas Recomendaciones para integrar los adelantos tecnológicos y las nuevas necesidades de los usuarios de la notación ASN.1, sus reglas de codificación.

La ASN.1 ha demostrado ser la notación predilecta de muchos grupos de normalización del UIT‑T, muchos de los cuales siguen solicitando la corrección de ciertas ambigüedades y una mayor claridad.

Hay una demanda continua de asistencia y asesoramiento por parte de otras Comisiones de Estudio, organizaciones de normalización externas y países sobre asuntos relativos a la notación ASN.1.

Las Recomendaciones relacionadas con el estudio de esta Cuestión son, al 3 de septiembre de 2020, las siguientes: X.680, X.681, X.682, X.683, X.690, X.691, X.692, X.693, X.694, X.695, X.696, X.697, X.891, X.892, X.893 y X.894.

Textos en preparación: X.680-690 series-rev, X.894 Cor.2.

#### I.1.3 Motivos de los trabajos sobre identificadores de objeto y sus autoridades de registro

Los identificadores de objeto (OID) se han convertido en un espacio de nombres muy popular basado en una estructura arborescente de autoridades de registro jerárquicas que se identifican mediante un número entero. Su reciente ampliación a OID internacionales, que permite la identificación mediante etiquetas Unicode, también es objeto de demanda para diversas aplicaciones y es probable que surjan nuevos requisitos en los desarrollos y ampliaciones futuros.

Hay una demanda continua de asistencia y asesoramiento por parte de otras Comisiones de Estudio, organizaciones de normalización externas y países sobre asuntos relativos a la gestión del espacio de nombres OID. Se prevé que esta demanda de asistencia y asesoramiento aumentará con la introducción de los OID internacionales y que los países en desarrollo utilizarán más las autoridades de registro de país. Por consiguiente, para prestar dicha asistencia y asesoramiento sigue siendo necesario un "proyecto sobre OID" en el UIT-T y nombrar a un director encargado del mismo.

Cualquier utilización innovadora de identificadores de objeto debe desarrollarse junto con la Comisión de Estudio 2 del UIT-T.

Las Recomendaciones y artículos técnicos relacionados con el estudio de esta Cuestión son, al 3 de septiembre de 2020, las siguientes: X.660, X.662, X.665, X.666, X.667, X.668, X.669, X.670, X.671, X.672, X.674, X.675, X.676, X677 y el artículo técnico XSTP-OID-ORS.

Textos en preparación: X.672rev.

#### I.1.4 Motivos de los trabajos sobre TTCN-3

La notación de pruebas y control de pruebas versión 3 (TTCN-3) permite especificar pruebas de funcionalidad y compatibilidad de sistemas y escribir conjuntos de pruebas genéricas. La TTCN-3 se utiliza en pruebas relativas a las Recomendaciones del UIT-T elaboradas por las Comisiones de Estudio pertinentes del UIT-T, en particular la CE 11, como Comisión de Estudio Rectora sobre especificaciones de prueba y pruebas de conformidad y compatibilidad. El UIT-T elabora una gran variedad de Recomendaciones. A los efectos de compatibilidad, es indispensable que las aplicaciones de esas Recomendaciones se ajusten a las Recomendaciones.

Las Recomendaciones relacionadas con el estudio de esta Cuestión son, al 3 de septiembre de 2020, las siguientes: X.292, Z.161, Z.161.1, Z.161.2, Z.161.3, Z.161.4, Z.161.5, X.161.6, Z.161.7, Z.162, Z.163, Z.164, Z.165, Z.165.1, Z.166, Z.167, Z.168, Z.169, Z.170 y Z.171.

Textos en preparación: ninguno.

#### I.1.5 Motivos de los trabajos sobre mantenimiento del lenguaje formal

No se espera evolución alguna en los siguientes lenguajes formales:

– lenguaje de especificación y descripción (SDL);

– perfil del lenguaje de modelización unificado (UML);

– gráfico de secuencia de mensajes (MSC);

– notación de requisitos de usuario (URN);

– CHILL, el lenguaje de programación del UIT-T.

No obstante, es necesario seguir realizando un mantenimiento.

Las Recomendaciones relacionadas con el estudio de esta Cuestión son, al 3 de septiembre de 2020, las siguientes: Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.110, Z.111, Z.119, Z.120, Z.121, Z.150, Z.151, Z.200, Z.450 y Suplementos Z.Suppl.1 y Z.Imp100.

#### I.1.6 Motivos de los trabajos relativos al mantenimiento de OSI

El estudio de las Recomendaciones básicas sobre interconexión de sistemas abiertos (OSI) ha terminado. La realización de sistemas basados en las Recomendaciones sobre OSI puede abarcar un periodo de tiempo relativamente prolongado y la experiencia práctica de la aplicación puede llevar a detectar errores técnicos o a la necesidad de ampliar dichas Recomendaciones. Se requiere por lo tanto seguir manteniendo actualizadas las Recomendaciones sobre OSI de la serie X.

Las Recomendaciones y las Guías del implementador relacionadas con el estudio de esta Cuestión son, al 3 de septiembre de 2020: F.400, F.401, F.410, F.415, F.420, F.421, F.423, F.435, F.440, F.471, F.472, X.200, X.207, X.210, X.211, X.212, X.213, X.214, X.215, X.216, X.217, X.217*bis*, X.218, X.219, X.220, X.222, X.223, X.224, X.225, X.226, X.227, X.227*bis*, X.228, X.229, X.233, X.234, X.235, X.236, X.237, X.237*bis*, X.245, X.246, X.247, X.248, X.249, X.255, X.256, X.257, X.260, X.263, X.264, X.273, X.274, X.281, X.282, X.283, X.284, X.287, X.400, X.402, X.404, X.408, X.411, X.412, X.413, X.419, X.420, X.421, X.435, X.440, X.445, X.446, X.460, X.462, X.467, X.481, X.482, X.483, X.484, X.485, X.486, X.487, X.488, X.610, X.612, X.613, X.614, X.622, X.623, X.625, X.630, X.633, X.634, X.637, X.638, X.639, X.641, X.642, X.650, X.851, X.852, X.853, X.860, X.861, X.862, X.863, X.880, X.881, X.882 y X.ImpOSI.

#### I.1.7 Motivos de los trabajos relativos al mantenimiento de ODP

Un aspecto importante en el desarrollo de sistemas de telecomunicaciones es la disponibilidad de *software* que permita el procesamiento distribuido abierto (ODP). Para facilitar el ODP se requiere la normalización de modelos de referencia, arquitecturas, funciones, interfaces y lenguajes para su especificación (serie X.900 del UIT-T).

Las Recomendaciones relacionadas con el estudio de esta Cuestión son, al 3 de septiembre de 2020, las siguientes: X.901, X.902, X.903, X.904, X.906, X.910, X.911, X.920, X.930, X.931, X.950, X.952 y X.960.

### I.2 Cuestión

Los temas de estudio que se han de considerar son, entre otros:

#### I.2.1 Temas de estudio relacionados con los trabajos relativos a directorios, PKI y PMI

En relación con los servicios de directorio:

a) ¿Qué nuevas definiciones de servicio o modificaciones hay que introducir en las Recomendaciones de la serie F para especificar cómo utilizar las capacidades existentes y cuáles son los nuevos requisitos de la X.500 del UIT-T?

b) ¿Qué mejoras es preciso introducir en las Recomendaciones de la serie E para atender las nuevas necesidades del servicio?

c) ¿Qué mejoras se han de introducir en el directorio para integrar los nuevos requisitos de PKI?

d) ¿Cuáles son las nuevas necesidades en lo que concierne a la seguridad y privacidad de la información del directorio?

e) ¿Qué otras reglas de codificación de la X.500 del UIT-T, tales como XML, pueden emplearse para mejorar la utilidad de la X.500 del UIT-T?

f) ¿Qué otras ampliaciones de los certificados de clave pública y de atributos se requieren para permitir su utilización en diversos entornos, tales como los entornos de recursos limitados, las comunicaciones de máquina a máquina y las redes amplias?

g) ¿Qué otras mejoras es necesario introducir en los certificados de clave pública y de atributos para aumentar su utilidad en ámbitos tales como la biometría, la autentificación, el control de acceso y el comercio electrónico?

h) ¿Qué cambios es preciso introducir en la Recomendación UIT-T X.509 para dar soporte a los algoritmos de seguridad cuántica y las tecnologías de libro mayor distribuido?

Los trabajos se realizarán en colaboración con el JTC 1/SC 6 de ISO/CEI en lo que respecta a la ampliación de la norma ISO/CEI 9594. Se cooperará con el IETF especialmente en el ámbito de LDAP y PKI.

#### I.2.2 Temas de estudio relacionados con los trabajos relativos a ASN.1

a) ¿Qué mejoras requiere la notación de sintaxis abstracta uno (ASN.1) y sus reglas de codificación para atender las necesidades de las futuras aplicaciones?

b) ¿Qué tipo de colaboración, aparte de los acuerdos vigentes, se requiere con otras entidades encargadas *de jure* o *de facto* de la elaboración de normas, para que la labor del UIT‑T sobre la ASN.1 siga siendo una referencia en el campo de las notaciones para la definición de protocolos?

Los trabajos se realizarán en colaboración con el JTC 1/SC 6 de ISO/CEI.

#### I.2.3 Temas de estudio relacionados con los trabajos relativos al mantenimiento de identificadores de objetos y sus autoridades de registro

a) ¿Qué actividad didáctica se requiere para fomentar la utilización de OID en diversos entornos?

b) ¿Qué otras autoridades de registro, o sus procedimientos, se necesitan para el estudio de ésta y otras Cuestiones?

c) ¿Qué tipo de colaboración, aparte de los acuerdos vigentes, se requiere con otras entidades encargadas *de jure* o *de facto* de la elaboración de normas, para que la labor del UIT‑T sobre OID siga siendo una referencia en el campo de la denominación inequívoca?

Los trabajos se realizarán en colaboración con el JTC 1/SC 6 de ISO/CEI.

#### I.2.4 Temas de estudios relacionados con los trabajos sobre TTCN

¿Qué mejoras es necesario introducir en la TTCN-3 para satisfacer las necesidades de las aplicaciones futuras?

Estos trabajos se realizarán en colaboración con ETSI TC MTS.

#### I.2.5 Mantenimiento de los idiomas oficiales

Mantenimiento continuo de las Recomendaciones sobre SDL, el perfil UML, MSC, URN y CHILL.

#### I.2.6 Mantenimiento de OSI

Seguir manteniendo actualizadas las Recomendaciones sobre arquitectura OSI y sus distintas capas para efectuar toda ampliación necesaria y subsanar los defectos comunicados. Seguir manteniendo actualizados los servicios y sistemas de tratamiento de mensajes, transferencia fiable, funcionamiento a distancia, CCR y procesamiento de transacciones para realizar toda ampliación necesaria y subsanar los defectos comunicados.

Es muy conveniente establecer una estrecha colaboración y coordinación con otras Comisiones de Estudio y otros grupos internacionales encargados de OSI para asegurar la más amplia aplicabilidad de las Recomendaciones resultantes.

Esta labor se realizará en colaboración con JTC 1 de ISO/CEI y sus subcomités.

#### I.2.7 Mantenimiento de ODP

Seguir manteniendo las Recomendaciones sobre ODP.

Es muy conveniente establecer una estrecha colaboración y coordinación con otras Comisiones de Estudio y otros grupos internacionales encargados de ODP para asegurar la más amplia aplicabilidad de las Recomendaciones resultantes.

Esta labor se realizará en colaboración con JTC 1/SC 7/GT 19 de ISO/CEI.

### I.3 Tareas

Las tareas son, entre otras:

#### I.3.1 Tareas relacionadas con los trabajos relativos a directorios, PKI y PMI

a) Mantener actualizado el directorio mediante informes sobre defectos y corrigenda técnicos.

b) Determinar los nuevos requisitos del directorio relativos a las tecnologías nuevas y existentes.

c) Preparar la novena edición de las Recomendaciones UIT-T de la serie X.500.

d) Mejorar la Recomendación UIT.T X.509, X.510 y X.pki-em a tenor de los nuevos requisitos.

#### I.3.2 Tareas relacionadas con los trabajos relativos a ASN.1

a) Actualizar las Recomendaciones de las series UIT-T X.680, X.690 y X.890 durante el periodo de estudios para atender las necesidades de los usuarios y, si procede, publicar nuevas ediciones de las mismas.

b) Prestar asistencia, cuando se requiera mejorar la transferencia de datos, en el estudio de otras Cuestiones en todas las Comisiones de Estudio en lo que respecta al suministro de módulos ASN.1 equivalentes a las estructuras XML definidas en las Recomendaciones del UIT-T (existentes o en fase de desarrollo), en particular en los casos de pequeña anchura de banda.

c) Supervisar y ayudar en la publicación de Recomendaciones | Normas Internacionales y corrigenda técnicos aprobados.

d) Resolver todos los informes sobre defectos y avanzar los corrigenda técnicos, según proceda.

e) Garantizar que toda coordinación de los trabajos en materia de ASN.1 de manera adecuada y oportuna.

f) Preparar tutoriales adicionales o páginas web que probablemente ayuden a los usuarios de ASN.1.

#### I.3.3 Tareas relacionadas con los trabajos relativos a identificadores de objetos y sus Autoridades de Registro

a) Actualizar las Recomendaciones de las series UIT-T X.660 y X.670 durante el periodo de estudios para atender las necesidades de los usuarios y, si procede, publicar nuevas ediciones de las mismas.

b) Supervisar y ayudar en la publicación de Recomendaciones | Normas Internacionales y corrigenda técnicos aprobados.

c) Resolver todos los informes sobre defectos y avanzar los corrigenda técnicos, según proceda.

d) Garantizar que toda coordinación de los trabajos en materia de OID de manera adecuada y oportuna.

e) Preparar tutoriales adicionales o páginas web que probablemente ayuden a los usuarios de OID.

f) Obtener acuerdo entre JTC 1/SC 6 de ISO/CEI y la CE 17 sobre toda atribución adicional de OID que se considere necesaria.

g) Bajo la responsabilidad del director del proyecto OID:

• prestar asesoramiento general a los usuarios de los OID;

• promover la utilización de los OID internacionales en otras Comisiones de Estudio y organismos de normalización externos;

• prestar asistencia a los países en la creación y gestión de autoridades de registro de OID (incluidos los OID internacionales).

#### I.3.4 Tareas relacionadas con los trabajos sobre TTCN

a) Mantener actualizadas las Recomendaciones relacionadas con esta Cuestión.

b) Promover la utilización de TTCN en otras Comisiones de Estudio y organizaciones de normalización externas.

#### I.3.5 Tareas relacionadas con los trabajos sobre el mantenimiento de lenguajes formales

Corregir y mejorar, en caso necesario, las Recomendaciones relacionadas con SDL, el perfil UML, MSC, URN y CHILL. Mantener actualizada la Guía del implementador de SDL.

#### I.3.6 Tareas relacionadas con los trabajos relativos al mantenimiento de OSI

Introducir modificaciones o mejoras en las Recomendaciones sobre OSI en función de las necesidades señaladas en las contribuciones recibidas y resolver todos los defectos notificados. Mantener actualizadas las Guías del implementador de OSI.

#### I.3.7 Tareas relacionadas con los trabajos relativos al mantenimiento de ODP

Introducir modificaciones o mejoras en las Recomendaciones sobre ODP en función de las necesidades señaladas en las contribuciones recibidas y resolver todos los defectos notificados.

En el programa de trabajo de la Comisión de Estudio 17 se indica el estado actual del estudio de esta Cuestión (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

### I.4 Relaciones

Líneas de Acción de la CMSI

C5.

Objetivos de Desarrollo Sostenible

–

Recomendaciones

Serie H.200, H.323, serie H.350, T.120 y las series X.600-X.609, X.700, X.800-X.849 y Z.

Cuestiones

Todas las Cuestiones del UIT-T relacionadas con las Recomendaciones mencionadas y la Cuestión 14/17 relacionada con la PKI distribuida.

Comisiones de Estudio

Comisiones de Estudio 2, 9, 11, 13, 15, 16, 20 del UIT-T y todas las que utilizan o necesitan el ASN.1, OID, pruebas de conformidad e interoperabilidad.

Entidades de normalización

Grupo de Dirección de Ingeniería Internet (IESG); Grupo Especial sobre Ingeniería de Internet (IETF); TC 57 de la CEI; JTC 1/SC 6, 7, 27 y 31 de la ISO/CEI; ISO TC 68, 204; Organización para el Desarrollo de Normas relativas a la Información Estructurada (OASIS); Grupo de gestión de objetos (OMG); Consorcio WWW (W3C); Instituto Europeo de Normas de Telecomunicación (ETSI) (TC MTS); JTC 1 de ISO/CEI y sus subcomités que utilizan los lenguajes de la UIT de diseño de sistemas.

Otras entidades

Unión Postal Universal (UPU); SDL Forum Society.

## J Cuestión 13/17 – Seguridad de los sistemas de transporte inteligente

(Continuación de la Cuestión 13/17)

### J.1 Motivación

Los sistemas de transporte inteligentes (STI), incluidos los sistemas de conducción autónomos, ofrecen diversos tipos de aplicaciones para aumentar la seguridad vial, reducir la huella ambiental del transporte, mejorar la gestión del tráfico y maximizar los beneficios del sector del transporte para los usuarios públicos y comerciales.

Los STI consisten en diversos tipos de comunicaciones en vehículos (por ejemplo, de vehículo a dispositivo nómada), entre vehículos (por ejemplo, de vehículo a vehículo (V2V)) y entre vehículos y posiciones fijas (por ejemplo, de vehículo a infraestructura (V2I)), es decir, comunicaciones de vehículo y su entorno (V2X). Las tecnologías de la información y la comunicación (TIC) se utilizan para aplicar los STI, incluidos el transporte por carretera, ferrocarril, marítimo y aéreo, y los sistemas de navegación.

Los sistemas de conducción automatizada y asistida constan de diversos componentes de sistemas en los que son la electrónica y la maquinaria las que se ocupan de la percepción, la toma de decisiones y la conducción del automóvil, en lugar de un conductor humano, y constituyen los albores de la automatización en el tráfico vial.

En el entorno de los sistemas de conducción autónoma y asistida, las vulnerabilidades de un vehículo pueden propagarse a otros vehículos, ya que los vehículos están conectados entre sí. Por consiguiente, las vulnerabilidades de los sistemas de comunicación V2X de un vehículo se deben gestionar y controlar para que no influyan demasiado los numerosos otros vehículos.

Los dispositivos eléctricos dentro de un vehículo, como las unidades de control electrónico (ECU) y los dispositivos de peaje eléctrico (ETC) son cada vez más sofisticados. En consecuencia, los módulos de *software* integrados en esas entidades deben estar lo debidamente actualizados para mejorar el rendimiento y la seguridad.

La Recomendación UIT-T X.1373 aprobada en marzo de 2017 describe la capacidad de actualización segura de *software* para los dispositivos de comunicación de los STI. Actualmente la Recomendación UIT-T X.1373 está en revisión.

La normalización de las soluciones integrales de seguridad más idóneas resulta fundamental en el contexto de los STI. Las características específicas de las comunicaciones vehiculares hacen que la seguridad sea una tarea especialmente difícil que es preciso estudiar.

Las Recomendaciones relacionadas con el estudio de esta Cuestión son, al 3 de septiembre de 2020: X.1371, X.1372 y X.1373.

Textos en preparación: X.1373rev, X.edrsec, X.eivnsec, X.evtol-sec, X.fstiscv, X.ipscv, X.itssec-3 (X.1374), X.itssec-4 (X.1375), X.itssec-5, X.mdcv (X.1376), X.rsu-sec y X.srcd.

### J.2 Cuestión

Los temas de estudio que se han de considerar son, entre otros:

a) ¿Cómo identificar y definir los aspectos relativos a la seguridad (por ejemplo, la arquitectura y los subsistemas de seguridad) en el entorno de los STI y de los sistemas de conducción autónomos y asistidos?

b) ¿Cómo identificar y gestionar las amenazas y vulnerabilidades en los servicios y redes de los STI y de los sistemas de conducción autónomos y asistidos?

c) ¿Cuáles son los requisitos de seguridad (por ejemplo, los de identificación y autenticación) para mitigar las amenazas en el entorno de los STI y de los sistemas de conducción autónomos y asistidos?

d) ¿Qué tecnologías de seguridad sirven para sustentar los servicios y redes de los STI?

e) ¿Cómo ha de mantenerse la interconectividad segura entre las entidades del entorno de los STI y de los sistemas de conducción autónomos y asistidos?

f) ¿Qué técnicas, mecanismos y protocolos de seguridad se necesitan para los STI y los servicios y redes de los sistemas de conducción autónomos y asistidos?

g) ¿Cuáles son las soluciones de seguridad convenidas a escala mundial para los STI y los servicios y redes de sistemas de conducción autónomos y asistidos que se basan en las redes de telecomunicaciones/TIC?

h) ¿Cuáles son las prácticas idóneas o directrices para la seguridad de los STI y los sistemas de conducción autónoma y asistida?

i) ¿De qué manera pueden utilizarse las tecnologías de IA/ML para brindar seguridad y confianza al STI y al sistema de conducción autónoma y asistida?

j) ¿Qué mecanismos de protección y gestión de la información de identificación personal (PII) se necesitan para los servicios de los STI?

### J.3 Tareas

Las tareas son, entre otras:

a) Elaborar un conjunto de Recomendaciones que ofrezcan soluciones integrales de seguridad para los STI y los sistemas de conducción autónoma y asistida.

b) Proseguir los estudios para definir los aspectos de seguridad de los STI y los servicios y redes de sistemas de conducción autónomos y asistidos, que se basan en las redes de telecomunicaciones/TIC.

c) Estudiar y determinar los problemas y amenazas de seguridad de los STI y del sistema de conducción autónoma y asistida.

d) Estudiar y determinar los requisitos y los casos de utilización de los servicios y aplicaciones específicas de los STI y de los sistemas de conducción autónoma y asistida.

e) Estudiar y elaborar mecanismos, protocolos y tecnologías de seguridad para los STI y los sistemas de conducción autónoma y asistida.

f) Estudiar y elaborar perfiles de seguridad, un plan jerárquico para la autenticación y un mecanismo para servicios y aplicaciones específicos de los STI y de los sistemas de conducción autónoma y asistida.

g) Estudiar y desarrollar aplicaciones con algoritmos eficientes de cifrado y descifrado para nodos de red que se mueven rápidamente y topologías de red que cambian dinámicamente.

h) Estudiar y desarrollar las tecnologías de registro de datos de sucesos en el contexto de los STI y los sistemas de conducción autónoma y asistida.

i) Estudiar y desarrollar mecanismos de interconexión seguros para los STI y los sistemas de conducción autónoma y asistida en el contexto de las telecomunicaciones.

j) Estudiar y determinar los problemas de protección de la información de identificación personal y los peligros en los STI y los sistemas de conducción autónoma y asistida.

k) Estudiar y elaborar mecanismos de protección y gestión de la PII para los STI y los sistemas de conducción autónoma y asistida.

l) Estudiar y desarrollar STI seguros y sistemas de conducción autónoma y asistida basados en tecnologías IA/ML.

m) Estudiar y desarrollar el proyecto de Recomendación X.1373rev, X.itssec-3, X.itssec-4, X.itssec-5, X.mdcv, X.srcd, X.edrsec, X.eivnsec, X.fstiscv, X.ipscv, X.rsu-sec.

n) Colaborar con las organizaciones de normalización afines para elaborar Recomendaciones de consuno.

En el programa de trabajo de la Comisión de Estudio 17 se indica el estado actual del estudio de esta Cuestión (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

### J.4 Relaciones

Líneas de Acción de la CMSI

C5.

Objetivos de Desarrollo Sostenible

–

Recomendaciones

Series X y otras relacionadas con la seguridad.

Cuestiones

Cuestiones 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17 y 15/17 del UIT-T.

Comisiones de Estudio y Grupos Temáticos

CE 11, 13, 16 y 20 del UIT-T; GT 5A del UIT-R; Colaboración sobre normas de comunicación en los STI (CITS); GT-VM del UIT-T (multimedios en vehículos.).

Entidades de normalización

TC 22 y 204 de la ISO; JTC 1/SC 6 y 27 de la ISO/CEI; IETF WG ITS; IEEE 802.11 WG y 1609 WG; SAE International (por ejemplo, Vehicle Cybersecurity Systems Engineering Committee, Connected Vehicles Steering Committee, y DSRC Technical Standard Committee); TC ITS del ETSI; W3C Automotive WG.

Otras entidades

GSMA; ATIS; CCSA; TIA; TTA; TTC; Grupo de Trabajo 29 de la UNECE (Comisión Económica de Naciones Unidas para Europa) y órganos subsidiarios (por ejemplo, Taskforce on cyber security (TFCS)); AGL (Automotive Grade Linux).

## K Cuestión 14/17 – Seguridad de las tecnologías de libro mayor distribuido (DTL)

(Continuación de la Cuestión 14/17)

### K.1 Motivación

Las tecnologías de libro mayor distribuido (DLT), cuya implementación más destacada es la cadena de bloques (*Blockchain*), son un nuevo tipo de registros seguros que se comparten, replican y sincronizan en un sistema distribuido. El control de los datos en los libros mayores distribuidos lo efectúan múltiples partes.

Siendo una tecnología específica de base de datos distribuida, las DLT son intrínsecamente resistentes a la modificación de los datos: una vez registrados, los datos de un bloque ya no pueden alterarse retroactivamente. Esta característica prominente de la DLT es bien conocida después del éxito que han recabado sus primeras aplicaciones a la criptomoneda digital, conocida como *bitcoin*.

La DLT se ha convertido en una de las tecnologías perturbadoras con gran potencial para cambiar nuestra economía, cultura y sociedad. La DLT permite aplicaciones innovadoras descentralizadas financieras o de otro tipo que eliminan la necesidad de terceros intermediarios. Las DLT consisten en una nueva infraestructura de gestión de datos que acelerará la revolución de los servicios en ciertas industrias (por ejemplo, la banca y las finanzas, el gobierno, la atención sanitaria y la superlogística) basadas en las telecomunicaciones.

Las tecnologías de libro mayor distribuido tendrán una profunda repercusión para los usuarios y las industrias de telecomunicaciones, incluidos los proveedores de servicios de telecomunicaciones.

Es necesario identificar las funciones y responsabilidades de los usuarios, operadores y proveedores de servicios de telecomunicaciones en lo que respecta a los aspectos de seguridad en el entorno de las DLT.

La normalización de las mejores soluciones de seguridad integral resulta fundamental para las DLT, cuyas aplicaciones son innumerables para todos los sectores, incluido el de las telecomunicaciones. Debido a las características específicas de la DLT, la seguridad se convierte en un reto especialmente difícil que es preciso estudiar.

Las Recomendaciones relacionadas con el estudio de esta Cuestión son, al 3 de septiembre de 2020: X.1401, X.1402 y X.1403.

Textos en preparación: X.dlt-td (X.1400), X.das-mgt, X.sa-dlt (X.1404), X.sc-dlt, X.srip-dlt, X.srscm-dlt, X.sa-dsm, X.ss-dlt, X.stov, X.str-dlt, X.tf-spd-dlt y TR.qs-dlt.

### K.2 Cuestión

Los temas de estudio que se han de considerar son, entre otros:

a) ¿Cómo identificar y definir los aspectos de seguridad (por ejemplo, la arquitectura y los subsistemas) a partir de los fundamentos (términos y definiciones, conceptos y taxonomía, casos de utilización) en el entorno DLT?

b) ¿Cómo han de tratarse las amenazas y vulnerabilidades de las aplicaciones y servicios basados en DLT?

c) ¿Cuáles son los requisitos de seguridad para mitigar las amenazas en un entorno DLT?

d) ¿Cuáles son las tecnologías de seguridad para dar soporte a las aplicaciones y servicios basados en DLT?

e) ¿Cómo se ha de conservar y mantener la interconectividad segura entre entidades en el entorno DLT?

f) ¿Qué técnicas, mecanismos y protocolos de seguridad se necesitan para las aplicaciones y servicios basados en DLT?

g) ¿Qué soluciones de seguridad son aceptables a escala mundial para las aplicaciones y servicios basados en DLT, que utilizan las redes de telecomunicaciones/TIC?

h) ¿Cuáles son las prácticas idóneas o las directrices de seguridad para las aplicaciones y servicios basados en DLT?

i) ¿Qué protección de la PII (información de identificación personal) y gestión de la seguridad de la información se necesitan para aplicaciones y servicios basados en DLT?

j) ¿Cómo puede utilizarse la DLT para fomentar la seguridad?

k) ¿Cómo se puede valorar, evaluar y garantizar la seguridad de DLT?

l) ¿Con qué partes interesadas debería colaborar la CE 17?

### K.3 Tareas

Las tareas son, entre otras:

a) Realizar un análisis de las deficiencias de los trabajos en curso en materia de seguridad en otras organizaciones en el campo de la tecnología de libro mayor distribuido.

b) Proseguir los estudios para definir los aspectos relativos a la seguridad de las aplicaciones y servicios basados en DLT, que utilizan las redes de telecomunicaciones/TIC.

c) Estudiar los fundamentos, tales como términos y definiciones, conceptos y taxonomía, y casos de utilización, que guarden relación con la seguridad y protección de la PII en las redes DLT.

d) Estudiar e identificar los problemas y amenazas de seguridad en las aplicaciones y servicios basados en DLT.

e) Estudiar y desarrollar mecanismos, protocolos y tecnologías de seguridad para aplicaciones y servicios basados en DLT.

f) Estudiar y desarrollar mecanismos de interconexión seguros para aplicaciones y servicios basados en DLT.

g) Estudiar e identificar problemas y amenazas de protección de la PII en aplicaciones y servicios basados en la DLT.

h) Estudiar y desarrollar un sistema de gestión de la información para las entidades que proporcionan aplicaciones y servicios basados en DLT.

i) Estudiar y elaborar orientaciones sobre la utilización de DLT para fomentar la seguridad.

j) Estudiar y desarrollar orientaciones para la evaluación, valoración y garantía de la seguridad de DLT.

k) Elaborar un conjunto de Recomendaciones para ofrecer soluciones de seguridad íntegras para aplicaciones y servicios basados en DLT.

En el programa de trabajo de la Comisión de Estudio 17 se indica el estado actual del estudio de esta Cuestión (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

### K.4 Relaciones

Líneas de Acción de la CMSI

C5.

Objetivos de Desarrollo Sostenible

–

Recomendaciones

Serie X y otras relacionadas con la seguridad.

Cuestiones

Cuestiones 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17 y 15/17 del UIT-T.

Comisiones de Estudio

CE 5, 11, 13, 16 y 20 del UIT-T.

Entidades de normalización

TC 307 de la ISO;

JTC 1/SC 27 de la ISO/CEI.

Otras entidades

GSMA, W3C, IEEE;

UNECE (Comisión Económica de Naciones Unidas para Europa); FIGI;

ATIS; CCSA; TIA; TTA; TTC.

## L Cuestión 15/17 – Seguridad en relación con las tecnologías incipientes, en particular la seguridad cuántica

(Nueva Cuestión)

### L.1 Motivación

La CE 17 reconoce que el carácter dinámico de los estudios relativos a la seguridad depende sobremanera de cómo evolucionen las herramientas de ataque y defensa, así como del efecto en cadena de las innovaciones que se aprovechan para esos fines. Esta coyuntura genera una cadencia de adelantos tecnológicos en materia de seguridad, algunos de los cuales se han de normalizar a escala mundial.

Dada su naturaleza, resulta imposible prever cuáles serán las innovaciones y cuándo se producirán, por lo que la CE 17 ha establecido y dirige proactivamente un mecanismo de incubación (TP.inno) 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.

Este mecanismo de incubación permite a la CE 17 introducir nuevos temas de estudio de manera eficiente en los nuevos ámbitos y promover textos no normativos (Documentos técnicos e Informes técnicos), práctica ésta de eficacia probada por cuanto permite dar tiempo a la comunidad de la CE 17 para familiarizarse con estos nuevos ámbitos y, a los recién incorporados, para familiarizarse con los procedimientos y el contexto de la CE 17 y el UIT-T. Al preparar nuevos temas de estudio, se repara a veces en que las características de la tecnología de seguridad incipiente se parecen a las que se examinan en otra Cuestión existente y, en consecuencia, el tema de estudio se transmite a dicha Cuestión para maximizar la coherencia, eficiencia y calidad de los trabajos de la CE 17.

Por otra parte, este mecanismo de incubación permite identificar las tendencias de las tecnologías de seguridad incipientes que se están desarrollando en el marco de esta Cuestión. Algunas tecnologías incipientes derivan de:

– la naturaleza incipiente del tema considerado, por ejemplo, la seguridad cuántica, la computación segura multipartita, el homomorfismo o la seguridad potencialmente identificable para la robótica, etc.;

– el tema no es incipiente pero no se había normalizado antes a escala mundial, por ejemplo, análisis de *software* maligno, prevención de la pérdida de datos, etc.;

– las lagunas de la arquitectura de seguridad operativa que no encajan en ninguna Cuestión, por ejemplo, el producto de seguridad propiamente dicho;

– los grandes problemas de integración y composición que muestran nuevas soluciones transversales incipientes, planes de datos de seguridad, etc.

Uno de los campos incipientes identificados mediante el mecanismo de incubación es la seguridad cuántica. La aparición de los computadores cuánticos de gran escala causará probablemente perturbaciones importantes en los sistemas convencionales de telecomunicaciones basados en las TIC y, por añadidura, planteará importantes riesgos para la seguridad.

En efecto, la seguridad de la criptografía actual se basa en problemas de cálculo difíciles: un problema logarítmico discreto y un problema de factorización de enteros. Se considera que son difíciles de resolver dentro un plazo razonable, utilizando las arquitecturas actuales de los computadores disponibles hoy en día y a medio plazo. No obstante, la criptografía de clave pública que utiliza claves asimétricas es la piedra angular de la autenticación en las redes públicas. Ahora bien, por su naturaleza, los computadores cuánticos pueden resolver problemas de factorización de números enteros y logaritmos discretos en un tiempo relativamente rápido y, por ende, son capaces, de destruir los cimientos sobre los que se construye actualmente la criptografía, poniendo en peligro la piedra angular existencial de la vida cibernética y la digitalización de hoy en día.

La distribución de clave cuántica (QKD) permite a dos partes generar una clave secreta aleatoria compartida que sólo ellos conocen y que puede utilizarse para encriptar y desencriptar mensajes mediante algoritmos criptográficos convencionales. La QKD tiene dos límites que causan problemas de topología e integración de la red: a) es punto a punto y sólo puede aplicarse a dos partes, A y B; y b) presenta límites de distancia en las redes terrenales. Para superar estas dos limitaciones, se ha introducido en la industria el concepto de redes QKD que consiste en 1) un conjunto de nodos vinculados entre sí mediante sistemas QKD que funcionan punto a punto; y 2) un sistema de gestión que comparte y tiene integrado cada uno de los nodos QKD. Este sistema de gestión tiene por objeto distribuir claves secretas entre dos o más nodos dentro de la misma red QKD que podrían no estar directamente vinculados. Actualmente, los sistemas QKD comerciales son lo suficientemente estables y consolidados como para comenzar a planificar redes QKD a gran escala. Existen diversas iniciativas de empresas/instituciones para desarrollar redes QKD, sin embargo, no existe una norma ampliamente aceptada sobre lo que constituye un sistema QKD.

Además, los números aleatorios son un elemento fundamental en la ingeniería con importantes aplicaciones en la criptografía. La aleatoriedad inherente en el núcleo de la mecánica cuántica hace que los sistemas cuánticos sean una fuente perfecta de entropía. La generación de números aleatorios cuánticos es una de las tecnologías cuánticas más consolidadas y existen muchos métodos de generación alternativos.

En resumen, la seguridad cuántica garantiza una comunicación que no es vulnerable a los ataques de los computadores cuánticos. La implementación de la seguridad cuántica requiere varios elementos esenciales, en particular la distribución de claves cuánticas y el generador de números aleatorios cuánticos (QRNG). Además, la interoperabilidad en los elementos y funcionalidades esenciales de la QKD y del QRNG es importante para que puedan utilizarse ampliamente en las redes de telecomunicaciones reales.

A su vez, es muy necesario que la CE 17 estudie una seguridad cuántica que sea resistente a los ataques cuánticos.

Las Recomendaciones e Informes técnicos relacionados con el estudio de esta Cuestión son, al 3 de septiembre de 2020: X.1702 y TP.inno, TP.sgstruct, y TR.sec-qkd.

Textos en preparación: X.cf-QKDN (X.1714), X.sec\_QKDN\_intrq, X.sec-QKDN-km, X.sec‑QKDN-ov (X.1710), y X.sec-QKDN-tn, X.rdmase, X.icd-schemas, X.tf-mpc, TR.sgfdm.

### L.2 Cuestión

Los temas de estudio que se han de considerar son, entre otros:

a) ¿Cuáles son las nuevas tecnologías de seguridad incipientes?

b) ¿Cuáles son las categorías de las nuevas tecnologías de seguridad incipientes?

c) ¿Cómo desarrollar con seguridad las nuevas tecnologías de seguridad incipientes?

d) ¿Qué mecanismos son los más eficaces para poner en práctica el mecanismo de incubación?

e) ¿Cuáles serán los efectos y los retos de las comunicaciones convencionales cuando surjan los computadores cuánticos a gran escala?

f) ¿Cuáles son los elementos fundamentales para construir la seguridad cuántica?

g) ¿Cuál es la estrategia de transición para construir la seguridad cuántica?

h) ¿Cómo se deberían tratar las amenazas y vulnerabilidades en la seguridad cuántica?

i) ¿Cuáles son los requisitos de seguridad para mitigar las amenazas en la seguridad cuántica?

j) ¿Cuáles son las tecnologías de seguridad para lograr la seguridad cuántica?

k) ¿Cómo mantener y conservar la interconectividad segura entre entidades que emplean la seguridad cuántica?

l) ¿Qué requisitos, técnicas, mecanismos y protocolos de seguridad se necesitan para la seguridad cuántica?

m) ¿Qué soluciones de seguridad podrían acordarse a escala mundial para la seguridad cuántica, que se basa en las comunicaciones de telecomunicaciones/TIC?

n) ¿Cuáles son las prácticas idóneas o directrices en materia de seguridad para la seguridad cuántica?

### L.3 Tareas

Las tareas son, entre otras:

a) Determinar nuevas tecnologías de seguridad incipientes.

b) Determinar nuevas categorías de tecnologías de seguridad incipientes para afianzar la estrategia de la Cuestión M.

c) Reasignar eventualmente los nuevos temas de estudio a otra Cuestión cuando su evolución indique que encajan mejor en una Cuestión existente.

d) Incorporar un mecanismo de incubación para examinar las nuevas esferas que surjan en la CE 17 del UIT-T.

e) Producir un conjunto de Recomendaciones técnicas que ofrezcan soluciones de seguridad completas para crear la seguridad cuántica.

f) Estudiar la definición de los aspectos relativos a seguridad de la seguridad cuántica, que se basa en la infraestructura de las telecomunicaciones/TIC.

g) Estudiar e identificar los aspectos relativos a la seguridad y las amenazas en la seguridad cuántica.

h) Estudiar y desarrollar los requisitos, mecanismos, protocolos y tecnologías de seguridad para la seguridad cuántica.

i) Estudiar y desarrollar mecanismos de interconexión segura para la seguridad cuántica.

k) Estudiar y desarrollar un sistema de gestión de la información para las entidades que proporcionan seguridad cuántica.

En el programa de trabajo de la Comisión de Estudio 17 se indica el estado actual del estudio de esta Cuestión (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

### L.4 Relaciones

Líneas de Acción de la CMSI

C5.

Objetivos de Desarrollo Sostenible

–

Recomendaciones Recomendaciones

Serie X y otras relacionadas con la seguridad.

Cuestiones

Cuestiones 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17 y 14/17 del UIT-T.

Comisiones de Estudio

CE 2, 3, 5, 9, 11, 12, 13, 15, 16 y 20 del UIT-T.

Entidades de normalización

TC Cyber de la ETSI, ISG-QKD; JTC 1/SC 27 de la ISO/CEI; OASIS; IETF.

Otras entidades

GSMA; ATIS; CCSA; TIA; TTA; TTC.

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