Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

ASAMBLEA MUNDIAL DE NORMALIZACIÓN DE LAS TELECOMUNICACIONES

Ginebra, 1-9 de marzo de 2022

Resolución 50 – Ciberseguridad

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

RESOLUCIÓN 50 (Rev. Ginebra, 2022)

Ciberseguridad

(Florianópolis, 2004; Johannesburgo, 2008; Dubái, 2012; Hammamet, 2016; Ginebra, 2022)

La Asamblea Mundial de Normalización de las Telecomunicaciones (Ginebra, 2022),

recordando

a) la Resolución 130 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios, sobre el papel de la UIT en la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación (TIC);

b) la Resolución 174 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios, sobre la función de la UIT respecto a los problemas de política pública internacional asociados al riesgo de utilización ilícita de las TIC;

c) la Resolución 179 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios, sobre el papel de la UIT en la protección de la infancia en línea;

d) la Resolución 181 (Guadalajara, 2010) de la Conferencia de Plenipotenciarios, sobre las definiciones y la terminología relativas a la creación de confianza y seguridad en la utilización de las TIC;

e) las Resoluciones 55/63 y 56/121 de la Asamblea General de las Naciones Unidas (AGNU), por las que se instituyó el marco jurídico para la lucha contra la utilización indebida de las tecnologías de la información con fines delictivos;

f) la Resolución 57/239 de la AGNU, sobre la creación de una cultura mundial de la ciberseguridad;

g) la Resolución 58/199 de la AGNU, sobre la creación de una cultura mundial de la ciberseguridad y la protección de las infraestructuras de información esenciales;

h) la Resolución 41/65 de la AGNU, sobre los principios relativos a la teledetección de la Tierra desde el espacio exterior;

i) la Resolución 70/125 de la AGNU, relativa al documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información;

j) la Resolución 45 (Rev. Dubái, 2014) de la Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT), sobre los mecanismos para mejorar la cooperación en materia de ciberseguridad, incluida la lucha contra el correo basura;

k) la Resolución 52 (Rev. Hammamet, 2016) de la Asamblea Mundial de Normalización de las Telecomunicaciones, sobre la respuesta y la lucha contra el *spam*;

l) la Resolución 58 (Rev. Ginebra, 2022) de la presente Asamblea, sobre el fomento de la creación de equipos nacionales de intervención en caso de incidente informático, especialmente para los países en desarrollo[1];

m) que la UIT es el principal facilitador de la Línea de Acción C5 de la CMSI en la Agenda de Túnez para la Sociedad de la Información (Crear confianza y seguridad en la utilización de las TIC);

n) las disposiciones de los resultados de la CMSI relacionadas con la ciberseguridad,

---

[1] Este término comprende los países menos adelantados, los pequeños Estados insulares en desarrollo, los países en desarrollo sin litoral y los países con economías en transición.

considerando

a) la importancia vital de la infraestructura de las telecomunicaciones/TIC y sus aplicaciones para prácticamente todos los tipos de actividades sociales y económicas;

b) que la red telefónica pública conmutada heredada tiene un determinado nivel intrínseco de propiedades de seguridad, debido a su estructura jerárquica y a los sistemas de gestión incorporados;

c) que, si no se tiene el debido cuidado en el diseño y la gestión de la seguridad, las redes basadas en el protocolo Internet (IP) ofrecen una separación limitada entre los componentes de usuario y los componentes de red;

d) que, si no se tiene especial cuidado en el diseño y la gestión de la seguridad, las redes heredadas y las redes IP convergentes son potencialmente más vulnerables a la intrusión;

e) que la seguridad es una cuestión intersectorial y que el panorama de la ciberseguridad, además de ser complejo y diverso, abarca distintos actores en los planos nacional, regional y mundial, que son responsables de identificar, examinar y reaccionar a las cuestiones relacionadas con la creación de confianza y seguridad en la utilización de las TIC;

f) que las pérdidas considerables y crecientes en que han incurrido los usuarios de los sistemas de telecomunicaciones/TIC, a consecuencia del problema cada vez mayor de la ciberseguridad, alarman a todos los países desarrollados y en desarrollo sin excepción;

g) que debido, entre otras cosas, a que las infraestructuras esenciales de telecomunicaciones/TIC están interconectadas a escala mundial, la seguridad insuficiente de la infraestructura de un país podría aumentar la vulnerabilidad y el riesgo en otros países, por lo que la cooperación es importante;

h) que el número y las modalidades de las ciberamenazas y los ciberataques están aumentando, del mismo modo que la dependencia de Internet y otras redes que son necesarias para acceder a servicios e información;

i) que las normas pueden dar soporte a los aspectos de seguridad de la Internet de las cosas (IoT) y las ciudades y comunidades inteligentes;

j) que, a fin de proteger las infraestructuras mundiales de telecomunicaciones/TIC contra las amenazas y los peligros del cambiante panorama de la ciberseguridad, es necesario tomar medidas coordinadas a escala nacional, regional e internacional, que sirvan para prevenir, preparar, responder y recuperarse de incidentes de seguridad;

k) los trabajos realizados y en curso en la UIT, en particular en la Comisión de Estudio 17 del Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) y en la Comisión de Estudio 2 del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D), incluido el informe final de la Cuestión 22/1-1 de la Comisión de Estudio 1 del UIT-D, y en el marco del Plan de Acción de Dubái adoptado por la CMDT (Dubái, 2014);

l) que el UIT-T tiene una función que desempeñar en el marco de su mandato y competencias en lo que respecta al *considerando j)*,

considerando además

a) que la Recomendación UIT-T X.1205 ofrece una definición y una descripción de las tecnologías, además de especificar los principios de protección de las redes;

b) que la Recomendación UIT-T X.805 establece un marco sistemático para la identificación de fallos de seguridad, y que la Recomendación UIT-T X.1500 establece el modelo para el intercambio de información sobre ciberseguridad (CYBEX) y aborda técnicas que podrían utilizarse para facilitar el intercambio de información sobre ciberseguridad;

c) que el UIT-T y el Comité Técnico Mixto para las tecnologías de la información (JTC 1) de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI), así como varios consorcios y organismos de normalización tales como el Consorcio World Wide Web (W3C), la Organización para el progreso de los estándares de información estructurada (OASIS), el Grupo Especial sobre Ingeniería de Internet (IETFI) y el Instituto de Ingenieros Electrotécnicos y de Electrónica (IEEE), entre otros, ya cuentan con un volumen importante de publicaciones y están realizando estudios directamente relacionados con este tema, que se han considerar;

d) la importancia de los trabajos que se están realizando sobre la arquitectura de seguridad de referencia para la gestión de la vida útil de los datos corporativos del comercio electrónico,

reconociendo

a) que, en la parte dispositiva de la Resolución 130 (Rev. Dubái, 2018), se encarga al Director de la Oficina de Normalización de las Telecomunicaciones (TSB) que intensifique el trabajo de las Comisiones de Estudio existentes del UIT-T;

b) que, en virtud de su Resolución 71 (Rev. Dubái, 2018), la Conferencia de Plenipotenciarios adoptó el Plan Estratégico para 2020-2023, incluida la Meta Estratégica 3 (Sostenibilidad: Gestionar los riesgos, los retos y las oportunidades que plantee el rápido crecimiento de las telecomunicaciones/TIC), en virtud de la cual la Unión se centrará en mejorar la calidad, la fiabilidad, la sostenibilidad y la resiliencia de las redes y los sistemas, así como en fomentar la confianza y la seguridad en el uso de las telecomunicaciones/TIC;

c) que la Agenda sobre Ciberseguridad Global (ACG) fomenta la cooperación internacional dirigida a la formulación de propuestas estratégicas para la mejora de la confianza y la seguridad en la utilización de las TIC, teniendo en cuenta los aspectos de seguridad a lo largo de todo el proceso de normalización;

d) las dificultades que tienen los Estados, en particular los de los países en desarrollo, para desarrollar la confianza y la seguridad en la utilización de las TIC,

reconociendo además

a) que están apareciendo ciberataques, como la peska (*phishing*), el redireccionamiento fraudulento (*pharming*), el rastreo/intrusión, la denegación de servicio distribuidos, la sustitución de páginas web (*web-facements*), el acceso no autorizado, etc., que tienen graves consecuencias;

b) que las redes robot (*botnet*) se utilizan para realizar ciberataques y difundir programas informáticos malignos basados en robots (*bot-malware*);

c) que, en ocasiones, resulta difícil identificar las fuentes de los ataques;

d) que las amenazas críticas contra la ciberseguridad del *software* y el *hardware* podrían requerir una gestión oportuna de las vulnerabilidades y actualizaciones puntuales del *hardware* y el *software*;

e) que la seguridad de los datos es un componente esencial de la ciberseguridad, ya que los datos son a menudo objeto de ciberataques;

f) que la ciberseguridad es uno de los elementos que permiten crear confianza y seguridad en el uso de las telecomunicaciones/TIC,

observando

a) la pujante actividad y el interés de la Comisión de Estudio 17, Comisión de Estudio Rectora en materia de seguridad y gestión de identidad, y de otros órganos de normalización, incluido el Grupo de Cooperación en materia de Normas Mundiales (GSC, *Global Standards Collaboration Group*), en el desarrollo de normas y Recomendaciones sobre seguridad de las telecomunicaciones/TIC;

b) la necesidad de armonizar en la medida de lo posible las estrategias e iniciativas nacionales, regionales e internacionales, a fin de evitar la duplicación y optimizar la utilización de los recursos;

c) la considerable labor de colaboración de los gobiernos, el sector privado, la sociedad civil, la comunidad técnica y el mundo académico, con miras a crear confianza y seguridad en la utilización de las TIC,

resuelve

1 seguir atribuyendo gran prioridad a esta actividad en la UIT, de conformidad con sus competencias y conocimientos técnicos, en particular mediante la promoción del entendimiento común entre los gobiernos y otras partes interesadas acerca de la creación de confianza y seguridad en la utilización de las TIC en los planos nacional, regional e internacional;

2 que todas las Comisiones de Estudio del UIT-T sigan evaluando las Recomendaciones existentes y en curso de elaboración, en lo que se refiere a la robustez de su diseño y a su posible explotación por grupos malintencionados, y tengan en cuenta los nuevos servicios y aplicaciones que debe soportar la infraestructura mundial de telecomunicaciones/TIC (incluidos, entre otros, la computación en la nube y la IoT, que se basan en redes de telecomunicaciones/TIC), a tenor de sus mandatos definidos en la Resolución 2 (Rev. Ginebra, 2022) de la presente Asamblea;

3 que el UIT-T siga, en el marco de su mandato y competencias, con su labor de sensibilización respecto de la necesidad de fortalecer y defender los sistemas de información y telecomunicaciones contra las ciberamenazas y ciberactividades malintencionadas, y siga fomentando la cooperación entre las organizaciones internacionales y regionales correspondientes a efectos de aumentar el intercambio de información técnica en el campo de la seguridad de las redes de información y telecomunicaciones;

4 que el UIT-T debería sensibilizar a la opinión pública mundial sobre la seguridad en las TIC mediante la elaboración de Recomendaciones e informes técnicos que sustenten los procedimientos, las políticas técnicas y los marcos normativos en materia de ciberseguridad;

5 que el UIT-T debería colaborar con el UIT-D, en especial en lo tocante a la Cuestión 3/2 (Garantías de seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad);

6 que las Comisiones de Estudio pertinentes del UIT-T deberían mantenerse al día de la evolución de las tecnologías nuevas y emergentes, a tenor de sus mandatos, para elaborar Recomendaciones, Suplementos e informes técnicos que ayuden a superar las dificultades relacionadas con la seguridad;

7 que el UIT-T siga trabajando en la elaboración y el perfeccionamiento de términos y definiciones relacionados con la creación de confianza y seguridad en el uso de las telecomunicaciones/TIC, incluido el término ciberseguridad;

8 que se fomente la adopción de procesos compatibles y coherentes a escala mundial para el intercambio de información sobre respuesta a incidentes;

9 que las Comisiones de Estudio del UIT-T sigan estableciendo relaciones de coordinación con organizaciones de normalización y otros organismos activos en este campo y fomenten la participación de expertos en las actividades de la UIT relativas a la creación de confianza y seguridad en la utilización de las TIC;

10 que los aspectos relativos a la seguridad deberían tenerse en cuenta en todos los procesos de elaboración de normas del UIT-T;

11 que se desarrollen y mantengan redes y servicios de telecomunicaciones/TIC seguros, fiables y resilientes para aumentar la confianza en el uso de las TIC;

12 que la Comisión de Estudio 17 necesita desarrollar marcos cooperativos de análisis de seguridad y gestión de incidentes;

13 que la resiliencia de las redes y los sistemas de TIC debería considerarse una prioridad en el desarrollo de redes e infraestructuras,

encarga a la Comisión de Estudio 17

1 que promueva la realización de estudios sobre ciberseguridad, incluida la seguridad de los nuevos servicios y aplicaciones emergentes que se apoyarán en la infraestructura mundial de telecomunicaciones/TIC;

2 que preste apoyo al Director de la TSB para que mantenga el Plan de normalización de la seguridad de las TIC, que debería incluir elementos de trabajo para hacer avanzar la labor de normalización relacionada con la seguridad, y que comparta todo ello con los grupos pertinentes del Sector de Radiocomunicaciones de la UIT (UIT-R) y del UIT-D, en calidad de Comisión de Estudio rectora para las cuestiones de seguridad;

3 que promueva Actividades Conjuntas de Coordinación en materia de seguridad entre todas las Comisiones de Estudio y Grupos Temáticos pertinentes de la UIT y de otras organizaciones de normalización;

4 que colabore estrechamente con todas las demás Comisiones de Estudio del UIT-T, establezca un plan de acción para evaluar las Recomendaciones del UIT-T existentes, en evolución y nuevas para contrarrestar las vulnerabilidades de seguridad, y siga presentando informes periódicos sobre la seguridad de las telecomunicaciones/TIC al Grupo Asesor de Normalización de las Telecomunicaciones;

5 que defina un conjunto general/común de capacidades de seguridad para cada fase del ciclo de vida de los sistemas de información/redes/aplicaciones, de modo que pueda lograrse la consiguiente seguridad intrínseca (capacidades y características de seguridad disponibles por diseño) para los sistemas/redes/aplicaciones desde el primer día;

6 que diseñe uno o varios marcos de referencia de la arquitectura de seguridad con componentes funcionales de seguridad que puedan considerarse como base para el diseño de la arquitectura de seguridad de diversos sistemas/redes/aplicaciones, con el fin de mejorar la calidad de las recomendaciones en materia de seguridad,

encarga al Director de la Oficina de Normalización de las Telecomunicaciones

1 que siga manteniendo, a partir de la información asociada con el Plan de Normalización de Seguridad de las TIC y los trabajos del UIT-D en materia de ciberseguridad, y con la asistencia de otras organizaciones pertinentes, un inventario de iniciativas y actividades nacionales, regionales e internacionales dirigidas a fomentar, en la medida de lo posible, la armonización a escala mundial de las estrategias y enfoques adoptados en esta esfera fundamental, incluido el desarrollo de enfoques comunes en el ámbito de la ciberseguridad;

2 que contribuya a los informes anuales al Consejo de la UIT relativos a la creación de confianza y seguridad en la utilización de las TIC, según lo dispuesto en la Resolución 130 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios;

3 que informe al Consejo de la UIT sobre los progresos logrados en el marco de las actividades del Plan de normalización de la seguridad de las TIC;

4 que siga reconociendo el papel que desempeñan otras organizaciones con experiencia y competencia técnica en el ámbito de las normas sobre seguridad, y se coordine con ellas según proceda;

5 que siga velando por la realización y el seguimiento de las actividades pertinentes de la CMSI sobre creación de confianza y seguridad en el uso de las TIC, en colaboración con otros Sectores de la UIT y en cooperación con las partes interesadas correspondientes, con el objetivo de compartir a escala mundial la información y las prácticas idóneas sobre iniciativas de ciberseguridad nacionales, regionales, internacionales y no discriminatorias;

6 que coopere con la ACG del Secretario General y con otros proyectos mundiales o regionales de ciberseguridad, según proceda, para promover la capacitación y entablar relaciones y asociaciones, según el caso, con diversas organizaciones e iniciativas regionales e internacionales referentes a la ciberseguridad, e invite a todos los Estados Miembros, en especial a los países en desarrollo, a que tomen parte en las actividades, garantizando la cooperación y coordinación entre estas diversas actividades;

7 que ayude a la Directora de la Oficina de Desarrollo de las Telecomunicaciones (BDT) a prestar asistencia a los Estados Miembros en el establecimiento de un marco adecuado entre los países en desarrollo, que permita reaccionar rápidamente ante incidentes importantes, y que proponga un plan de acción destinado a reforzar la protección en estos países, teniendo en cuenta los mecanismos y asociaciones pertinentes;

8 que ayude en las actividades pertinentes de las Comisiones de Estudio del UIT-T relacionadas con el fortalecimiento y la creación de confianza y seguridad en la utilización de las TIC;

9 que facilite información en materia de ciberseguridad a todas las partes interesadas, mediante la organización de programas de formación, foros, talleres, seminarios, etc., destinados a los responsables políticos, los organismos reguladores, los operadores y otras partes interesadas, especialmente de los países en desarrollo, con el fin de crear conciencia y detectar las necesidades existentes en colaboración con la Directora de la BDT,

invita a los Estados Miembros, los Miembros de Sector, los Asociados y las Instituciones Académicas, según corresponda

1 a colaborar estrechamente en el fortalecimiento de la cooperación regional e internacional, habida cuenta de la Resolución 130 (Rev. Dubái, 2018), con el fin de mejorar la confianza y seguridad en la utilización de las TIC y mitigar los riesgos y las amenazas;

2 a cooperar y participar activamente en la aplicación de la presente Resolución y de las medidas asociadas;

3 a participar en las actividades pertinentes de las Comisiones de Estudio del UIT-T para desarrollar normas y directrices de ciberseguridad y, de esta forma, crear confianza y seguridad en la utilización de las TIC;

4 a utilizar las Recomendaciones y los Suplementos pertinentes del UIT-T;

5 a seguir contribuyendo a los trabajos de la Comisión de Estudio 17 sobre los métodos de gestión de los ciberriesgos.