|  |  |
| --- | --- |
| **Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT-20)**  **Ginebra, 1-9 de marzo de 2022** |  |
|  |  |
|  |  |
| SESIÓN PLENARIA | Addéndum 8 al Documento 37-S |
|  | **16 de septiembre de 2021** |
|  | **Original: inglés** |
|  | |
| Administraciones miembro de la Telecomunidad Asia-Pacífico | |
| PROPUESTA DE MODIFICACIÓN DE LA RESOLUCIÓN 50 | |
|  | |
|  | |

|  |  |  |
| --- | --- | --- |
| **Resumen:** | Basándose en la consideración de la importancia de crear confianza y seguridad en el uso de las TIC, se propone la revisión de la Resolución 50 de la AMNT con el fin de seguir mejorando la labor de normalización pertinente. Las principales modificaciones incluyen el fortalecimiento de las funciones de la CE 17 del UIT-T en materia de seguridad, incluida la función de coordinación de la CE 17 en materia de seguridad en el UIT-T, nuevos temas y otros cambios de redacción. | |
| **Contacto:** | Sr. Masanori Kondo Secretario General Telecomunidad Asia-Pacífico | Tel.: +66 2 5730044 Fax: +66 2 5737479 Correo-e: [aptwtsa@apt.int](mailto:aptwtsa@apt.int) |

Introducción

La seguridad adquiere cada vez más importancia en la infraestructura actual de las telecomunicaciones/TIC. Por lo tanto, la seguridad debe considerarse a lo largo de todo el ciclo de vida de un sistema/red/aplicación, ya que, de lo contrario, el sistema/red/aplicación estará lleno de vulnerabilidades de seguridad que requerirán muchos parches.

Durante las fases de diseño, desarrollo y despliegue del sistema/red/aplicación, la arquitectura de seguridad es un punto clave importante, ya que proporciona un diseño de seguridad unificado que responde a las necesidades y a los riesgos potenciales de un determinado escenario o entorno. También especifica cuándo, dónde y cómo definir/configurar y aplicar las políticas de seguridad. Además, el proceso de diseño de la arquitectura de seguridad es generalmente reproducible.

En este documento se reconoce la importancia de la seguridad en el ámbito de las TIC.

Teniendo en cuenta que las actividades de normalización de la seguridad contribuyen a la prevención de los daños resultantes de las ciberactividades malintencionadas, el trabajo en materia de seguridad debe continuar. Además, las Comisiones de Estudio del UIT-T deberían abordar las tecnologías de seguridad emergentes que se han identificado. Entre ellas se encuentran la seguridad de la conducción autónoma, la DLT, la seguridad relacionada con la IA/ML, la seguridad de las IMT 2020 (5G) OTT y las IMT 2030 (6G), los nuevos servicios y aplicaciones de TIC, como la ciudad inteligente, la fábrica inteligente, la salud inteligente, la energía inteligente, la gestión de la identidad distribuida y la seguridad con base cuántica.

La función de coordinación de la CE 17 en el UIT-T debe reforzarse para aumentar la visibilidad de los trabajos del UIT-T en el ámbito de la seguridad, lo cual resulta fundamental para que la CE 17 pueda servir de enlace o cooperar eficazmente con otras contrapartes, como el JTC 1/SC 27 de la ISO/CEI, el IETF, el ETSI y el 3GPP, y para atraer a expertos. En el próximo periodo de estudio deberían incrementarse las funciones de la CE 17 encaminadas a crear seguridad y confianza en el uso de las TIC.

Propuesta

Las administraciones miembro de la APT proponen la revisión de la Resolución 50 sobre ciberseguridad, según se indica en este documento.

MOD APT/37A8/1

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. Busán, 2014) 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 definiciones y 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 creación de una cultura mundial de la ciberseguridad;

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

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

*i)* la Resolución 70/125 de la AGNU sobre el 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 71/199 de la AGNU sobre el derecho a la privacidad en la era digital;

*k)* 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 *spam*;

*l)* la Resolución 52 (Rev. Ginebra, 2022) de esta Asamblea, Respuesta y lucha contra el *spam*;

*m)* la Resolución 58 (Rev. Dubái, 2012) 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]](#footnote-1)1;

*n)* 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);

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

considerando

*a)* la importancia vital de la infraestructura de las telecomunicaciones/TIC y sus aplicaciones para prácticamente todas 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 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 es complejo y diverso, en el que intervienen distintos actores en los planos nacional, regional y mundial, que son responsables de identificar, examinar y reaccionar a las cuestiones y ciberactividades malintencionadas 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 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 métodos de ciberataques y ciberactividades malintencionadas están aumentando día a día, y que es una tarea difícil proteger a las redes y los sistemas frente a los mismos, 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 y conexos de la Internet de las cosas (IoT) y las ciudades y comunidades inteligentes (SCC);

*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), en la Comisión de Estudio 2 del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D), incluido el informe final de la C22/1-1 de la CE 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 descripción de las tecnologías, además de 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, que la Recomendación UIT-T X.509 proporciona marcos para certificados de claves públicas y atributos 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 sobre tecnologías de la información y la comunicación (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), la alianza Fast IDentity Online (FIDO), el Grupo Especial sobre Ingeniería de Internet (IETF) y el Instituto de Ingenieros Electrotécnicos y de Electrónica (IEEE), entre otros, ya cuentan con un volumen importante de publicaciones, y que 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)* en la parte dispositiva de la Resolución 130 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios se encarga al Director de la Oficina de Normalización de las Telecomunicaciones que intensifique el trabajo de las Comisiones de Estudio existentes del UIT-T;

*b)* que la CMDT-14 aprobó la contribución al Plan Estratégico de la UIT para 2016-2019, refrendando cinco Objetivos, entre ellos el Objetivo 3 – *Mejorar la confianza y la seguridad en la utilización de las telecomunicaciones/TIC, así como la implantación de aplicaciones y servicios TIC pertinentes*, y el correspondiente Resultado 3.1: *Creación de confianza y seguridad en la utilización de TIC*, en cuyo marco de ejecución está el Programa de Ciberseguridad y la Cuestión 3/2 del UIT-D;

*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 incidencias de ciberseguridad o ciberdelitos 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 cometer ciberdelitos y difundir programas informáticos malignos basados en robot (*bot-malware*);

*c)* que en ocasiones resulta difícil identificar las fuentes de las ciberactividades malintencionadas;

*d)* que algunas ciberactividades malintencionadas son causadas por sistemas y dispositivos que están conectados a las redes de telecomunicaciones sin una autenticación adecuada;

*e)* que el acceso no autorizado a los sistemas de TIC puede reducirse mediante la introducción de tecnologías emergentes como la tecnología de libro mayor distribuido que sólo permite el acceso de cualquier dispositivo inteligente a la red tras un proceso de validación;

*f)* que amenazas críticas contra la ciberseguridad de *software* y *hardware* podrían requerir una gestión oportuna de vulnerabilidades y actualizaciones oportunas de *hardware* y *software*;

*g)* que la seguridad de los datos es un componente esencial de la ciberseguridad, ya que los datos son a menudo objeto de ciberactividades malintencionadas;

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

*i)* que la seguridad ocupa un lugar importante en todo el ciclo de vida de los sistemas/redes/aplicaciones/datos;

*j)* que es importante contar con una o varias arquitecturas de seguridad comunes, que podrían considerarse como base de la arquitectura de seguridad de diversos sistemas/redes/aplicaciones/datos,

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 (por ejemplo, computación en la nube, la tecnología de libro mayor distribuido, la seguridad de base cuántica e Internet de las cosas (IoT), que se basan en redes de telecomunicaciones/TIC), a tenor de sus mandatos 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 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 colabore estrechamente 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;

5 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;

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

7 que las Comisiones de Estudio del UIT-T sigan estableciendo relaciones de coordinación con organizaciones de normalización y otros organismos activos en este campo;

8 que se tengan en cuenta aspectos de seguridad en todos los procesos de elaboración de normas del UIT-T;

9 que se desarrollen las especificaciones y normas para probar y certificar la seguridad de los sistemas de TIC, con el fin de generar confianza entre los usuarios y de ayudar a crear bancos de prueba y laboratorios de pruebas, especialmente en los países en desarrollo;

10 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,

encarga a la Comisión de Estudio 17

1 que promueva los 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 Oficina de Normalización de las Telecomunicaciones para que mantenga la "Hoja de ruta de las normas de seguridad de las TIC", que debería incluir elementos de trabajo para hacer avanzar la labor de normalización relacionada con la seguridad, y que la comparta con los grupos pertinentes del UIT-R y del UIT-D como misión de la Comisión de Estudio rectora para las cuestiones de seguridad;

3 que cree la Actividad de Coordinación Conjunta para la seguridad (JCA Security) y coordinar las actividades de normalización de la 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 (GANT);

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/datos, de modo que pueda lograrse la consiguiente seguridad intrínseca (capacidades y características de seguridad disponibles por diseño) para los sistemas/redes/aplicaciones/datos desde el primer día;

6 que diseñe arquitectura(s) de seguridad común(es) con componentes funcionales de seguridad que puedan considerarse como base para el diseño de la arquitectura de seguridad de diversos sistemas/redes/aplicaciones/datos 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 sobre los progresos logrados en las actividades del "Plan de normalización de la seguridad de las TIC" al Consejo de la UIT;

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 prosiga la realización y el seguimiento de las actividades pertinentes de la CMSI sobre la 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 como manera de compartir a escala mundial la información 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, que entable 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 al Director de la Oficina de Desarrollo de las Telecomunicaciones a prestar asistencia a los Estados Miembros en el establecimiento de un marco adecuado entre los países en desarrollo, que permita reaccionar rápidamente en caso de 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 difunda información a todas las partes interesadas relacionadas con la ciberseguridad 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 sensibilizar y de identificar las necesidades en colaboración con la Directora de la BDT,

invita a los Estados Miembros, los Miembros del 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) de la Conferencia de Plenipotenciarios, con el fin de mejorar la confianza y seguridad en la utilización de las TIC y mitigar los ciberriesgos y las ciberamenazas;

2 a cooperar y participar activamente en la aplicación de la presente Resolución y de las medidas asociadas, incluidas la revisión y actualización del diseño de sus arquitecturas y protocolos de ciberseguridad;

3 que trabajen en actividades pertinentes de Comisiones de Estudio del UIT-T para desarrollar normas y directrices de ciberseguridad a fin de crear confianza y seguridad en la utilización de las TIC a través de la protección de los datos y de mecanismos de seguridad en el uso de las TIC;

4 que utilicen Recomendaciones y Suplementos pertinentes del UIT-T;

5 que, en el marco de las prácticas de ciberseguridad, desarrollen mecanismos de gestión de los ciberriesgos, como los ciberseguros, para recuperarse de las pérdidas y los daños causados por ciberactividades malintencionadas.

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

1. 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. [↑](#footnote-ref-1)