ITUPublications
Resoluciones

Unión Internacional de Telecomunicaciones
Sector de Normalización

ASAMBLEA MUNDIAL DE NORMALIZACIÓN DE LAS TELECOMUNICACIONES
Nueva Delhi, 15-24 de octubre de 2024

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. Nueva Delhi, 2024)

Ciberseguridad

(Florianópolis, 2004; Johannesburgo, 2008; Dubái, 2012; Hammamet, 2016; Ginebra, 2022; Nueva Delhi, 2024)

La Asamblea Mundial de Normalización de las Telecomunicaciones (Nueva Delhi, 2024),

recordando

a) la Resolución 130 (Rev. Bucarest, 2022) de la Conferencia de Plenipotenciarios, sobre el fortalecimiento del 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. Bucarest, 2022) 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 64/211 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 76/19 de la AGNU, sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional y promoción del comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones;

j) 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;

k) la Resolución 45 (Rev. Kigali, 2022) 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. Nueva Delhi, 2024) de la presente Asamblea, sobre la respuesta y la lucha contra el *spam*;

m) la Resolución 58 (Rev. Nueva Delhi, 2024) de la presente Asamblea, sobre el fomento y mejora de la creación de equipos nacionales de intervención en caso de incidente informático (EIII), especialmente para los países en desarrollo[1];

n) que la UIT es el principal facilitador de la Línea de Acción C5 de la Cumbre Mundial sobre la Sociedad de la Información (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 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 telecomunicaciones/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 todas las telecomunicaciones/TIC;

j) que garantizar la seguridad y protección de las nuevas telecomunicaciones/TIC es vital para un ciberespacio seguro, por lo que la elaboración de normas de seguridad para ellas es fundamental;

---

[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.

k) 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;

l) 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), y en el marco del Plan de Acción de Kigali adoptado por la CMDT (Kigali, 2022);

m) que el UIT-T tiene una función que desempeñar en el marco de su mandato y competencias en lo que respecta al *considerando k)* de la presente Resolución,

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, 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 que, al utilizar las telecomunicaciones/TIC, la seguridad se aborde como un proceso iterativo y continuo que se integra en los productos desde el principio y que continúa durante todas las etapas de su vida útil;

e) que la adopción de un método iterativo basado en los riesgos en el que se combinen criterios tecnológicos, operativos y humanos es fundamental para reforzar la seguridad y la resiliencia en la utilización de las telecomunicaciones/TIC, propiciando la creación y aplicación de prácticas de ciberseguridad de la forma necesaria para hacer frente a las amenazas y vulnerabilidades en constante evolución, y respaldando también la innovación y las telecomunicaciones/TIC incipientes,

reconociendo

a) que, en la parte dispositiva de la Resolución 130 (Rev. Bucarest, 2022), 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. Bucarest, 2022), la Conferencia de Plenipotenciarios adoptó el Plan Estratégico para 2024-2027, incluida la Meta Estratégica 1 (Conectividad universal: Permitir y fomentar el acceso universal a unas telecomunicaciones/TIC asequibles, seguras y de alta calidad), en virtud de la cual la Unión se centrará en lograr que la infraestructura, los servicios y las aplicaciones de telecomunicaciones/TIC sean universalmente accesibles, asequibles, interoperables, seguros y de alta calidad;

c) que las normas son un componente esencial del Pilar 2 (Medidas técnicas y de procedimiento) de la Agenda sobre Ciberseguridad Global (ACG), que 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 telecomunicaciones/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 crear la confianza y la seguridad en la utilización de las telecomunicaciones/TIC,

reconociendo además

a) que los ciberataques que están apareciendo, como la pesca (*phishing*), el redireccionamiento fraudulento (*pharming*), el rastreo/intrusión, la denegación de servicio distribuidos, la sustitución de páginas web (*web-facements*) y el acceso no autorizado, son cada vez más numerosos y variados y tienen consecuencias importantes;

b) que se pueden utilizar diferentes vectores 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, actualizaciones puntuales del *hardware* y el *software* y una asignación adecuada de derechos de acceso para prevenir los ataques;

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 un elemento fundamental para crear confianza y seguridad en el uso de las telecomunicaciones/TIC;

g) el acceso cada vez más generalizado a las telecomunicaciones/TIC en todo el mundo, y en particular a Internet, así como su utilización por menores de edad,

observando

a) la pujante actividad y el interés de la Comisión de Estudio 17 del UIT-T, 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, en el desarrollo de normas y Recomendaciones UIT-T 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) que, al margen de otras ciberamenazas, los aspectos de la protección de datos y la información de identificación personal (IIP) relacionados con la ciberseguridad suponen un reto importante para los Estados Miembros;

d) 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 telecomunicaciones/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 telecomunicaciones/TIC en los planos nacional, regional e internacional;

2 que las Comisiones de Estudio del UIT-T sigan evaluando las Recomendaciones UIT-T existentes y en curso de elaboración, conforme a los mandatos definidos para ellas en la Resolución 2 (Rev. Nueva Delhi, 2024) de la presente Asamblea y remitan los problemas de seguridad a la Comisión de Estudio 17 del UIT-T para su examen, en lo que se refiere a la robustez de su diseño y su funcionamiento, y a su posible explotación por grupos malintencionados, y que tengan en cuenta los servicios y tecnologías de telecomunicaciones/TIC nuevos e incipientes que debe soportar la infraestructura mundial de telecomunicaciones/TIC;

3 que el UIT-T siga sensibilizando a la población mundial sobre la seguridad de las telecomunicaciones/TIC, mediante la elaboración, en el marco de su mandato y competencias, de Recomendaciones UIT-T e Informes técnicos que respalden los procedimientos de ciberseguridad, las políticas técnicas y los marcos normativos, en lo que respecta a la importancia de proteger las telecomunicaciones/TIC contra las ciberamenazas y ciberactividades malintencionadas, a fin de mejorar el fomento de las capacidades de seguridad del personal institucional, 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 las telecomunicaciones/TIC, con el objetivo de gestionar los riesgos de ciberseguridad y proteger las telecomunicaciones/TIC;

4 que el UIT-T tenga en cuenta las necesidades de los usuarios y desarrolladores al preparar productos que podrían utilizarse para promover la ciberseguridad de las tecnologías incipientes relacionadas con las telecomunicaciones/TIC;

5 que el UIT-T tenga en cuenta la importancia de la capacitación para facilitar la adopción de normas en favor de la ciberseguridad, en particular para los países en desarrollo, pero no exclusivamente para ellos;

6 que el UIT-T se coordine y colabore con el UIT-D a este respecto, tanto en el contexto de la Cuestión 3/2 (Garantías de seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad) en lo relativo a la labor de creación de capacidad de la Oficina de Desarrollo de las Telecomunicaciones (BDT);

7 que las Comisiones de Estudio pertinentes del UIT-T se mantengan al día de la evolución de las tecnologías y servicios de telecomunicaciones/TIC nuevos e incipientes, a tenor de sus mandatos, para señalar a la Comisión de Estudio 17 los aspectos que podrían requerir nuevas Recomendaciones UIT-T, Suplementos e Informes técnicos a fin de abordar las dificultades relacionadas con la ciberseguridad y los aspectos conexos de la protección de datos y la IIP;

8 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";

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

10 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 telecomunicaciones/TIC;

11 que los aspectos relativos a la seguridad se tengan en cuenta en todos los procesos de elaboración de normas del UIT-T;

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

13 que la ciberresiliencia de las redes y los sistemas de telecomunicaciones/TIC se considere una prioridad en el desarrollo de redes, infraestructuras y aplicaciones de telecomunicaciones/TIC,

encarga a la Comisión de Estudio 17 del Sector de Normalización de las Telecomunicaciones de la UIT

1 que promueva la realización de estudios sobre ciberseguridad, incluidos los aspectos de la protección de datos y la IIP para los servicios y tecnologías de telecomunicaciones/TIC nuevos e incipientes, a fin de contrarrestar las vulnerabilidades asociadas a la utilización de la infraestructura mundial de telecomunicaciones/TIC, mediante la elaboración de Recomendaciones UIT-T, Suplementos e Informes técnicos, según corresponda;

2 que ayude al Director de la TSB en el mantenimiento del 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 ciberseguridad, y los correspondientes aspectos de la protección de datos y la IIP, además de un Compendio de Seguridad que incluya la lista de Recomendaciones UIT-T y los términos y definiciones, y que comparta todo ello con los grupos pertinentes del Sector de Radiocomunicaciones de la UIT y del UIT-D, en calidad de Comisión de Estudio rectora para las cuestiones de seguridad;

3 que dirija las Actividades Conjuntas de Coordinación en materia de confianza y seguridad entre todas las Comisiones de Estudio de la UIT y otras organizaciones de normalización, según corresponda;

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 abordar las cambiantes amenazas y vulnerabilidades de seguridad a fin de fomentar la resiliencia de las redes de telecomunicaciones/TIC frente a los ciberataques, y siga presentando informes periódicos sobre la seguridad de las telecomunicaciones/TIC al Grupo Asesor de Normalización de las Telecomunicaciones;

5 que continúe definiendo un conjunto general/común de capacidades de seguridad en cada fase del ciclo de desarrollo (requisitos, diseño, aplicación, verificación, publicación y mantenimiento) de los sistemas de información/redes/aplicaciones/productos de servicio, incluido el fomento de las capacidades de seguridad del personal institucional, 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 continúe diseñando uno o varios marcos de seguridad o arquitecturas de referencia con componentes funcionales de seguridad, incluida una posible interoperabilidad en materia de seguridad entre diferentes tipos de sistemas 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 UIT-T en materia de seguridad y facilitar referencias para el diseño de la seguridad de posibles aplicaciones de la infraestructura mundial de telecomunicaciones/TIC;

7 que siga realizando y respaldando los análisis de ciberseguridad cooperativos y las herramientas para la gestión de incidentes, a fin de apoyar la labor de los EIII, en particular en los países en desarrollo;

8 que considere cumplir los requisitos, en su forma actual, para elaborar normas técnicas en apoyo de las iniciativas encaminadas a mejorar la ciberseguridad de los menores;

9 que tenga en cuenta la constante evolución de las telecomunicaciones/TIC y examine y revise periódicamente las Recomendaciones UIT-T existentes sobre seguridad de las redes a fin de adaptarlas a los nuevos requisitos de seguridad y responder a las nuevas amenazas a la seguridad de las redes;

10 que defina las prácticas idóneas para evaluar y mejorar la ciberseguridad, incluidos los aspectos conexos de la protección de datos y la IIP, en el marco de una infraestructura de telecomunicaciones/TIC en evolución;

11 que lleve a cabo una evaluación de las repercusiones de las telecomunicaciones/TIC nuevas e incipientes, desde la perspectiva de la ciberseguridad, localizando las carencias y recomendando estrategias para una adopción y utilización seguras,

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 telecomunicaciones/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 telecomunicaciones/TIC, según lo dispuesto en la Resolución 130 (Rev. Bucarest, 2022) 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 telecomunicaciones/TIC;

4 que siga reconociendo el papel que desempeñan otras organizaciones con experiencia y competencia técnica en el ámbito de las normas sobre ciberseguridad, incluidos los aspectos conexos de la protección de datos y la IIP, 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 telecomunicaciones/TIC, en colaboración con otros Sectores de la UIT y en cooperación con otras organizaciones y todas 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 al Director de la BDT a supervisar la preparación de Recomendaciones UIT-T y, cuando proceda, de otras herramientas que puedan utilizar los Estados Miembros, en particular los países en desarrollo, para anticipar respuestas rápidas en caso de incidentes importantes, y a colaborar con esos organismos para proponer planes de acción utilizando un marco adecuado, según corresponda y previa solicitud, para reforzar la protección en estos países, teniendo en cuenta los mecanismos y asociaciones existentes;

8 que ayude en las actividades pertinentes de la Comisión de Estudio 17 del UIT-T relacionadas con el fortalecimiento y la creación de confianza y seguridad en la utilización de las telecomunicaciones/TIC, y que coordine estos trabajos con las Comisiones de Estudio del UIT-D y las actividades del programa pertinentes;

9 que facilite información en materia de ciberseguridad a todas las partes interesadas y mejore su entendimiento sobre este asunto, mediante la organización de programas de formación, foros, talleres, seminarios, etc., según corresponda, sobre las Recomendaciones UIT-T y las directrices de ejecución, destinados a los responsables políticos, los organismos reguladores, los operadores y otras partes interesadas, en particular de países en desarrollo, con el fin de crear conciencia y detectar las necesidades existentes en colaboración con el Director de la BDT;

10 que colabore con las organizaciones regionales de telecomunicaciones para proporcionar conocimientos teóricos y prácticos a una población más amplia y de la manera más eficaz;

11 que, siempre que sea posible, considere la posibilidad de crear conciencia a través de talleres organizados en paralelo a las reuniones de los Grupos Regionales de las Comisiones de Estudio del UIT-T competentes, o de eventos organizados en coordinación y colaboración con el Director de la BDT y las Oficinas Regionales de la UIT en paralelo a dichas reuniones,

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 y el apoyo regionales e internacionales, habida cuenta de la Resolución 130 (Rev. Bucarest, 2022), con el fin de mejorar la confianza y seguridad en la utilización de las telecomunicaciones/TIC y mitigar los riesgos y responder a 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 telecomunicaciones/TIC;

4 a utilizar las Recomendaciones, los Informes técnicos 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 riesgos vinculados a la ciberseguridad y la ciberdefensa, dentro del ámbito de competencia de la UIT;

6 a seguir apoyando iniciativas para fomentar la participación activa de las mujeres en las actividades y funciones directivas del UIT-T relacionadas con la ciberseguridad;

7 a adoptar y apoyar la aplicación de medidas de ciberseguridad para las telecomunicaciones/TIC nuevas e incipientes dentro de sus jurisdicciones, garantizando un entorno seguro y resiliente para todos los usuarios.