|  |  |  |
| --- | --- | --- |
|  | **Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT-24)**Nueva Delhi, 15-24 de octubre de 2024 |  |
|  |
|  |  |
| SESIÓN PLENARIA | Addéndum 10 alDocumento 37-S |
|  | 22 de septiembre de 2024 |
|  | Original: inglés |
|  |
| Administraciones miembros de la Telecomunidad Asia-Pacífico |
| PROPUESTA DE MODIFICACIÓN DE LA RESOLUCIÓN 50 |
|  |
|  |

|  |  |
| --- | --- |
| **Resumen:** | El presente documento contiene una propuesta de modificación de la Resolución 50 de la AMNT, relativa a la ciberseguridad. |
| **Contacto:** | Sr. Masanori Kondo Secretario GeneralTelecomunidad Asia-Pacífico | Correo-e: aptwtsa@apt.int |

Introducción

La seguridad reviste una importancia cada vez mayor para la infraestructura actual de telecomunicaciones/TIC. Al UIT-T le corresponde un papel propio en la elaboración de Recomendaciones técnicas clave para la creación de confianza y seguridad en la utilización de las TIC. El uso de las TIC para proporcionar seguridad y la garantía de seguridad de las TIC integran dos ámbitos de estudio importantes.

Conviene tener en cuenta la seguridad a lo largo de todo el ciclo de vida de los sistemas, redes y aplicaciones, pues, de lo contrario, estos últimos estarán plagados de vulnerabilidades para las que se requerirán numerosos parches.

Habida cuenta de que las actividades encaminadas a la normalización de la seguridad contribuyen a la prevención de los daños causados por las ciberactividades maliciosas, dicha labor debe continuar. Además, las Comisiones de Estudio del UIT-T, en especial la CE 17, deberían abordar nuevos ámbitos tecnológicos relacionados con la seguridad, como pueden ser la seguridad de la IA, la seguridad metaverso, la seguridad de confianza cero, la seguridad de la cadena de suministro de software, etc.

El principal objetivo de esta propuesta de modificación es aclarar y reforzar la función de la CE 17 como Comisión de Estudio rectora sobre seguridad.

Propuesta

Dadas las consideraciones que anteceden, las Administraciones miembros de la APT proponen que la AMNT-24 considere la posibilidad de revisar su Resolución 50 sobre ciberseguridad.

MOD APT/37A10/1

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. 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. 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 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 68/167 de la AGNU, sobre el derecho a la privacidad en la era digital, en la que se afirma, entre otras cosas, "que los derechos de las personas también deben estar protegidos en Internet, incluido el derecho a la privacidad";

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

*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. 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;

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

*m)* 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]](#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 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, incluidos los aspectos de seguridad de las tecnologías nuevas y emergentes;

*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 en aras de la ciberseguridad;

*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 establece los 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 la Recomendación UIT-T X.1060 brinda a las organizaciones un marco para la creación y operación de un centro de ciberdefensa, que les permita garantizar su seguridad, evaluar su grado de eficacia en la implementación de servicios de seguridad y abordar los riesgos a los que se enfrentan en términos de ciberseguridad;

*d)* 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), la alianza Fast IDentity Online (FIDO), 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;

*e)* 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. 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 debe esforzarse por lograr que las infraestructuras, los servicios y las aplicaciones de telecomunicaciones/TIC sean universalmente accesibles, asequibles, interoperables, seguros y de alta calidad;

*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 países en desarrollo, para crear confianza y seguridad en la utilización de las TIC, y la Resolución 44 (Rev. Ginebra, 2022) de la AMNT, sobre la reducción de la brecha de normalización entre los países en desarrollo y desarrollados;

*e)* las dificultades que tienen los Estados Miembros, en particular los países en desarrollo, para crear infraestructuras y aplicaciones de telecomunicaciones/TIC fiables y seguras, especialmente, en lo que respecta a los aspectos técnicos y operativos de la protección de datos y la información de identificación personal (IIP),

reconociendo además

*a)* el advenimiento de ciberataques como la peska (*phishing*), el envío de correo basura (*spam*), el redireccionamiento fraudulento (*pharming*), el rastreo/intrusión, la denegación de servicio distribuida, la amenaza persistente avanzada, la sustitución de páginas web (*web-facements*), el acceso no autorizado, el *software* malicioso (*malware*), la alteración de datos, la usurpación de identidad (*spoofing*), 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*, así comouna asignación adecuada de derechos de acceso para prevenir los ataques a los dispositivos finales;

*e)* que los ataques mediante software de extorsión (*ransomware*) siguen aumentando;

*f)* que la aplicación de las nuevas tecnologías, unida a la constante evolución de la infraestructura mundial de telecomunicaciones/TIC, plantea desafíos inéditos y conlleva mayores requisitos en lo que respecta a la seguridad de las telecomunicaciones/TIC y a los aspectos técnicos y operativos de la protección de datos y la IIP, lo que puede afectar a la arquitectura de seguridad de las redes;

*g)* la evolución de las tecnologías en el ámbito de la gestión de las amenazas a la ciberseguridad y la protección de las telecomunicaciones/TIC;

*h)* el necesario desarrollo de las capacidades relacionadas con la seguridad, incluidas las capacidades de los profesionales para gestionar los riesgos a la seguridad y las tecnologías conexas;

*i)* que la seguridad de los datos y la infraestructura de macrodatos reviste una importancia crucial para la ciberseguridad, ya que los datos son a menudo el objetivo de los ciberataques y que la aplicación generalizada de la tecnología de macrodatos hace de este un riesgo omnipresente en los comportamientos de red actuales;

*j)* que la ciberseguridad es un elemento clave para la creación de confianza y seguridad en el uso de las telecomunicaciones/TIC;

*k)* que la seguridad desempeña un papel importante en todo el ciclo de vida de los sistemas, redes, aplicaciones y datos;

*l)* que la arquitectura y el marco de seguridad son importantes y podrían considerarse la base para el diseño de la arquitectura de seguridad de diversos sistemas, redes, aplicaciones y 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)* que conviene evaluar los aspectos relativos a la interoperabilidad y la seguridad de las infraestructuras de red en evolución y la rápida innovación en el desarrollo de infraestructuras de red abiertas;

*c)* que, al margen de otras ciberamenazas, los aspectos técnicos y operativos de la protección de datos y la IIP suponen un desafíos importante para los Estados Miembros;

*d)* 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;

*e)* 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, conforme a los mandatos definidos en la Resolución 2 (Rev. Ginebra, 2022) de la presente Asamblea y teniendo presentes las cuestiones relacionadas con la seguridad a lo largo de todo el proceso de elaboración de normas del UIT-T, en lo que se refiere a la robustez de su diseño y su funcionamiento, así como a su posible explotación por grupos malintencionados, y tengan en cuenta los servicios y tecnologías de telecomunicaciones/TIC nuevos y emergentes 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);

3 que el UIT-T siga, en el marco de su mandato y competencias, con su labor mundial de sensibilización con respecto a la seguridad de las TIC, mediante la elaboración de Recomendaciones e informes técnicos que sustenten los procedimientos, las políticas técnicas y los marcos de ciberseguridad, así como a la necesidad de fortalecer y defender los sistemas de información y telecomunicaciones contra las ciberamenazas y ciberactividades malintencionadas, en aras del desarrollo de las capacidades de los profesionales en el ámbito de la seguridad, 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 crear conciencia a escala 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 de ciberseguridad, con el objetivo de gestionar mejor los riesgos relacionados con la ciberseguridad y proteger sus redes de información y telecomunicaciones;

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, a fin de señalar a la atención de la CE 17 ámbitos en los que pudiera requerirse la elaboración de Recomendaciones, Suplementos e informes técnicos para superar dificultades relacionadas con la seguridad y los aspectos técnicos y operativos de la protección de datos y la IIP;

7 que el UIT-T siga trabajando en la elaboración y el perfeccionamiento de términos y definiciones relacionados con la creación de confianza (incluso mediante la protección de datos y la IIP) y seguridad en el uso de las telecomunicaciones/TIC, incluida la 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 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;

11 que la Comisión de Estudio 17 necesita desarrollar marcos cooperativos de análisis de la ciberseguridad y gestión de incidentes;

12 que la resiliencia de las redes y los sistemas de TIC debería considerarse una prioridad en el desarrollo de infraestructuras y aplicaciones de redes de telecomunicaciones/TIC,

encarga a la Comisión de Estudio 17

1 que promueva la realización de estudios sobre ciberseguridad, incluida la seguridad y los aspectos técnicos y operativos de la protección de datos y la IIP para servicios y tecnologías nuevos y emergentes, a fin de contrarrestar las vulnerabilidades vinculadas al uso de la infraestructura mundial de telecomunicaciones/TIC, mediante la elaboración de Recomendaciones, Suplementos e informes técnicos, según proceda;

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 los aspectos técnicos y operativos de la protección de datos y la IIP, así como un compendio de seguridad, que debería incluir una lista de Recomendaciones y términos, junto con su definición, 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 relacionadas con la confianza y la seguridad entre todas las Comisiones de Estudio y Grupos Temáticos pertinentes de la UIT y de otras organizaciones de normalización, incluida la Actividad Conjunta de Coordinación sobre Protección de la Infancia en Línea y su análisis de deficiencias;

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 y abordar así las cuestiones relacionadas con la seguridad, las amenazas y las vulnerabilidades en constante evolución, a fin de garantizar la resiliencia de las redes 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 siga trabajando en la definición de un conjunto general/común de capacidades de seguridad para cada fase del ciclo de vida de los sistemas de información/redes/aplicaciones, incluido el desarrollo de las capacidades de los profesionales en el ámbito de la seguridad, 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 siga trabajando en el diseño de uno o varios marcos de seguridad o arquitecturas de referencia conexas con componentes funcionales de seguridad, incluida una posible colaboración en pos de la 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 en materia de seguridad y facilitar referencias para el diseño de la seguridad de posibles aplicaciones de nuevas tecnologías en el marco de la infraestructura mundial de telecomunicaciones/TIC;

7 que tenga en cuenta la constante evolución de la tecnología y el sector comercial de las TIC, revise periódicamente las Recomendaciones sobre seguridad de las redes y examine las Recomendaciones existentes a fin de adaptarlas a los nuevos requisitos de seguridad y responder a las nuevas amenazas a la seguridad de las redes;

8 que defina las mejores prácticas para evaluar y mejorar la seguridad y los aspectos técnicos y operativos de la protección de datos y la IIP en el marco de unas infraestructuras de telecomunicaciones/TIC en evolución,

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 la seguridadde 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 seguridad, protección de datos e 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 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 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 relacionada con la ciberseguridad a todas las partes interesadas y amplíe sus conocimientos en la materia, mediante la organización de programas de formación, foros, talleres, seminarios, etc., según proceda, sobre las Recomendaciones y las directrices de aplicación del UIT-T, para responsables políticos, organismos reguladores, operadores y otras partes interesadas, especialmente de países en desarrollo;

10 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 regional e internacional, 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, mitigar los riesgos y abordar 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, los informes técnicos y los Suplementos pertinentes del UIT-T;

5 a seguir contribuyendo a los trabajos de la Comisión de Estudio 17 sobre métodos de gestión de los riesgos vinculados a la ciberseguridad y la ciberdefensa.

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

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)