# RESOLUCIÓN 130 (REV. DUBÁI, 2018)

## 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

La Conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones (Dubái, 2018),

*recordando*

*a)* la Resolución 68/198 de la Asamblea General de las Naciones Unidas (AGNU) sobre las tecnologías de la información y la comunicación (TIC) para el desarrollo;

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

*c)* la Resolución 68/243 de la AGNU sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional;

*d)* la Resolución 57/239 de la AGNU sobre la creación de una cultura mundial de seguridad cibernética;

*e)* la Resolución 64/211 de la AGNU sobre la creación de una cultura mundial de ciberseguridad y el registro de las acciones nacionales para proteger las infraestructuras de información críticas;

*f)* la Declaración de la CMSI+10 relativa a la aplicación de los resultados de la Cumbre Mundial de la Sociedad de la Información (CMSI) y la Perspectiva para la CMSI después de 2015, adoptadas en el Evento de Alto Nivel CMSI+10 coordinado por la UIT (Ginebra, 2014) y basado en el proceso de la Plataforma Preparatoria Multipartita (PPM), junto con otros organismos de Naciones Unidas e incluyendo a todas las partes interesadas de la CMSI, y refrendadas por la Conferencia de Plenipotenciarios (Busán, 2014) y sometidas al examen general de la AGNU;

*g)* la Resolución 70/125 de la AGNU sobre el documento final de la reunión de alto nivel de la AGNU sobre el examen general de la aplicación de los resultados de la CMSI;

*h)* 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;

*i)* la Resolución 179 (Rev. Dubái, 2018) de la presente Conferencia sobre la función de la UIT en la protección de la infancia en línea;

*j)* la Resolución 181 (Rev. Guadalajara, 2010) de la Conferencia de Plenipotenciarios sobre definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación;

*k)* la Resolución 196 (Rev. Dubái, 2018) de la presente Conferencia sobre la protección del usuario/consumidor de servicios de telecomunicaciones;

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

*m)* la Resolución 140 (Rev. Dubái, 2018) de la presente Conferencia sobre la función de la UIT en la puesta en práctica de los resultados de la CMSI y en el examen general de su aplicación por parte de la AGNU;

*n)* la Resolución 58 (Rev. Dubái, 2012) de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT) sobre el fomento de la conformación de equipos nacionales de respuesta a incidentes informáticos (EIII), en particular para los países en desarrollo[1];

*o)* la Resolución 67 (Rev. Buenos Aires, 2017) de la CMDT sobre la función del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D) en la protección de la infancia en línea;

*p)* la Resolución 69 (Rev. Buenos Aires, 2017) de la CMDT sobre la creación de EIII, especialmente para los países en desarrollo, y cooperación entre los mismos;

---

[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.

*q)* que el Consejo de la UIT adoptó en su reunión de 2009 la Resolución 1305, en la que se determina que la seguridad, la protección, la continuidad, la sostenibilidad y la solidez de Internet son cuestiones de política pública que corresponden al ámbito de competencia de la UIT,

*considerando*

*a)* que el Evento de Alto Nivel de la CMSI+10 coordinada por la UIT reafirmó la importancia de la creación de confianza y seguridad en la utilización de las TIC, como se menciona en los párrafos pertinentes de los documentos finales de la CMSI+10 (Ginebra, 2014);

*b)* la importancia decisiva de las infraestructuras de la información y la comunicación y sus aplicaciones en prácticamente todas las formas de actividades sociales y económicas;

*c)* las disposiciones en materia de ciberseguridad del Compromiso de Túnez y la Agenda de Túnez y el documento de resultados de la reunión de alto nivel de la AGNU sobre el examen general de la aplicación de los resultados de la CMSI;

*d)* que, debido a la aplicación y al desarrollo de las TIC, han surgido nuevas amenazas de diversos orígenes, que han tenido repercusiones sobre la confianza y la seguridad en la utilización de las TIC por parte de todos los Estados Miembros, los Miembros de Sector y otras partes interesadas, incluidos todos los usuarios de dichas tecnologías, y que pueden afectar además al mantenimiento de la paz y al desarrollo económico y social de todos los Estados Miembros, y que, por otra parte, esas amenazas y la vulnerabilidad de las infraestructuras, las redes y los dispositivos siguen planteando a todos los países, en particular a los países en desarrollo, problemas de seguridad cada vez más acuciantes que rebasan las fronteras nacionales, observando al mismo tiempo en este contexto el fortalecimiento del papel de la UIT en la creación de confianza y seguridad en la utilización de las TIC y la necesidad de reforzar la cooperación internacional y la capacitación, y de elaborar los mecanismos nacionales, regionales e internacionales existentes (por ejemplo, acuerdos, prácticas idóneas o memorandos de entendimiento, etc.);

*e)* que se ha invitado al Secretario General de la UIT a brindar su apoyo a otros proyectos mundiales o regionales sobre ciberseguridad, según proceda, y que se ha invitado a todos los países, en particular los países en desarrollo, a participar en las actividades que revistan interés para la UIT;

*f)* la Agenda sobre Ciberseguridad Global (ACG) de la UIT que alienta la cooperación internacional orientada a proponer estrategias para soluciones que aumenten la confianza y la seguridad en la utilización de las telecomunicaciones/TIC;

*g)* que la protección de esas infraestructuras y las respuestas para afrontar esos problemas y esas amenazas requieren la adopción de medidas coordinadas a escala nacional, regional e internacional en lo que concierne a la prevención de los incidentes, la preparación ante ellos, las respuestas a dar y el restablecimiento de la situación a causa de incidentes informáticos, por parte de las autoridades gubernamentales a escala nacional (incluida la creación de EIII) y subnacional, del sector privado y de los ciudadanos y usuarios, teniendo en cuenta la cooperación y coordinación internacional y regional, y que la UIT desempeña una función esencial en el marco de su mandato y sus competencias en la materia;

*h)* que la adopción de un enfoque de ciberseguridad iterativo y basado en los riesgos permite elaborar y aplicar prácticas de ciberseguridad de la forma necesaria para hacer frente a una serie de amenazas y vulnerabilidades en constante evolución, y que la seguridad es un proceso continuo e iterativo que debe integrarse en las fases de desarrollo e implantación de las tecnologías y sus aplicaciones desde el principio y durante toda su vida útil;

*i)* la necesidad de que las nuevas tecnologías evolucionen de manera constante con miras a la detección temprana de eventos o incidentes, y la respuesta coordinada y oportuna frente a eventos o incidentes que ponen en peligro la seguridad informática, o incidentes contra la seguridad de la red informática que podrían poner en peligro la disponibilidad, integridad y confidencialidad de infraestructuras esenciales en los Estados Miembros de la UIT, así como la necesidad de contar con estrategias que reduzcan al mínimo las consecuencias de dichos incidentes y atenúen los riesgos y amenazas cada vez mayores a que están expuestas esas plataformas;

*j)* que en la Resolución 70/125 de la AGNU, Documento Final de la reunión de alto nivel de la AGNU relativo al examen general de la aplicación de los resultados de la CMSI, se reconocen los problemas que los Estados, en particular los países en desarrollo, afrontan a la hora de crear confianza y seguridad en la utilización de las TIC, y se pide recentrar la atención en la capacitación, la educación, el intercambio de conocimientos y las prácticas reglamentarias, promoviendo la cooperación multipartita a todos los niveles y la sensibilización de los usuarios de las TIC, en particular entre los más pobres y los más vulnerables;

*k)* que el número de ciberamenazas y de ciberataques está aumentando, al mismo tiempo que nuestra dependencia de Internet y otras redes que son indispensables para acceder a los servicios y la información;

*l)* que el Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) ha aprobado alrededor de 300 normas relativas a la creación de confianza y seguridad en la utilización de las TIC;

*m)* el Informe final sobre la Cuestión 3/2 del UIT-D sobre Seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad;

*n)* que la naturaleza del panorama de las normas de ciberseguridad exige la cooperación entre la UIT y otras organizaciones nacionales, regionales, mundiales y sectoriales;

*o)* que muchos países en desarrollo se hallan en fase de elaboración o aplicación de estrategias nacionales de ciberseguridad;

*p)* que la seguridad se ha convertido en un tema de suma importancia a escala internacional y que, por lo tanto, la función y la implicación de las Naciones Unidas y de sus organismos especializados pertinentes, como la UIT, en la creación de confianza y seguridad en la utilización de las TIC son cada vez más importantes;

*q)* las distintas funciones y responsabilidades de todas las partes interesadas para garantizar la confianza y la seguridad en la utilización de las TIC;

*r)* que algunas pequeñas y medianas empresas (PYME) se enfrentan a retos adicionales en la aplicación de prácticas de ciberseguridad,

*reconociendo*

*a)* que la ciberseguridad es un elemento fundamental para la seguridad de las infraestructuras de las telecomunicaciones/TIC, y una base fundamental para el desarrollo económico y social;

*b)* que el desarrollo de las TIC ha sido y sigue siendo decisivo para el crecimiento y el desarrollo de la economía mundial, incluida la economía digital, sobre una base de seguridad y confianza;

*c)* que en la CMSI se afirmó la importancia de la creación de confianza y seguridad en la utilización de las TIC y la importancia fundamental de la aplicación multipartita en el plano internacional, y se estableció la Línea de Acción C5 (Creación de confianza y seguridad en la utilización de las TIC), de la Agenda de Túnez para la Sociedad de la Información, siendo la UIT, según se estipula en dicha Agenda, el facilitador/moderador de esa Línea de Acción, y que la Unión ha llevado a cabo esta tarea en los últimos años, por ejemplo, por medio de la ACG;

*d)* que la CMDT-17 adoptó el Plan de Acción de Buenos Aires y su Objetivo 2, concretamente su Resultado 2.2, consistente en mejorar la confianza y la seguridad en la utilización de las TIC, en el cual se identifica la ciberseguridad como una actividad prioritaria de la Oficina de Desarrollo de Telecomunicaciones (BDT) y se definen las principales áreas de trabajo que deberá emprender dicha Oficina; y que la CMDT-14 adoptó la Resolución 45 (Rev. Dubái, 2014), Mecanismos para mejorar la cooperación en materia de ciberseguridad, incluida la lucha contra el correo indeseado y los medios para contrarrestarlo, en la que se pide al Secretario General que presente la Resolución a la consideración de la próxima Conferencia de Plenipotenciarios para que tome las medidas oportunas y que informe al Consejo y a la Conferencia de Plenipotenciarios de 2018 acerca de los resultados de estas principales áreas de trabajo, en su caso; y que la CMDT-17 adoptó la Resolución 69 (Rev. Buenos Aires, 2017) sobre facilitación de la creación de EIII nacionales, especialmente para los países en desarrollo, y cooperación entre los mismos;

*e)* que en la Declaración de Buenos Aires adoptada por la CMDT-17 se declara que la creación de confianza y seguridad en la utilización de las telecomunicaciones/TIC, así como la protección de los datos personales, son una prioridad, por lo que es necesaria la cooperación y coordinación internacional entre gobiernos, organizaciones pertinentes, entidades y empresas privadas en la capacitación e intercambio de prácticas óptimas para el desarrollo de las correspondientes políticas públicas y de medidas de índole jurídica, reglamentaria y técnica que aborden, entre otras cosas, la protección de los datos personales, y que las partes interesadas deben trabajar conjuntamente para garantizar la fiabilidad y seguridad de las redes y servicios de las TIC;

*f)* que, con el fin de promover la creación EIII nacionales en los Estados Miembros que carecen y tienen necesidad de dichos equipos, la AMNT-16 adoptó la Resolución 58 (Rev. Dubái, 2012), fomento de la creación de equipos nacionales de intervención en caso de incidente informático, especialmente para los países en desarrollo, y la CMDT-17 adoptó la Resolución 69 (Rev. Buenos Aires, 2017) sobre facilitación de la creación de EIII nacionales, incluidos EIII encargados de la cooperación entre gobiernos, especialmente para los países en desarrollo, y cooperación entre los mismos, y la importancia de la coordinación entre las organizaciones pertinentes;

*g)* el § 15 del Compromiso de Túnez, en el cual se indica que "Reconociendo los principios de acceso universal y sin discriminación a las TIC para todas las naciones, la necesidad de tener en cuenta el nivel de desarrollo social y económico de cada país, y respetando la orientación hacia el desarrollo de la Sociedad de la Información, subrayamos que las TIC son un instrumento eficaz para promover la paz, la seguridad y la estabilidad, así como para propiciar la democracia, la cohesión social, la buena gobernanza y el estado de derecho, en los planos regional, nacional e internacional. Se pueden utilizar las TIC para promover el crecimiento económico y el desarrollo de las empresas. El desarrollo de infraestructuras, la creación de capacidades humanas, la seguridad de la información y la seguridad de la red son decisivos para alcanzar esos objetivos. Además, reconocemos la necesidad de afrontar eficazmente las dificultades y amenazas que representa la utilización de las TIC para fines que no corresponden a los objetivos de mantener la estabilidad y seguridad internacionales y podrían afectar negativamente a la integridad de la infraestructura dentro de los Estados, en detrimento de su seguridad. Es necesario evitar que se abuse de las tecnologías y de los recursos de la información para fines delictivos y terroristas, respetando

siempre los derechos humanos"; y reconociendo también que desde la celebración de la CMSI han seguido aumentando los problemas causados por dicha utilización indebida de los recursos de las TIC;

*h)* que el Evento de Alto Nivel CMSI+10 coordinado por la UIT identificó varios problemas para la aplicación de las Líneas de Acción de la CMSI que siguen existiendo y tendrán que resolverse después de 2015;

*i)* que, al elaborar medidas legislativas apropiadas y viables en relación con la protección contra las ciberamenazas a escala nacional, regional e internacional, los Estados Miembros, y en particular los países en desarrollo, pueden necesitar asistencia de la UIT para establecer medidas técnicas y de procedimiento destinadas a garantizar la seguridad de las infraestructuras TIC nacionales, a petición de esos Estados Miembros, al tiempo que se observa que existen varias iniciativas regionales e internacionales que podrían ayudar a esos países a elaborar esas medidas legislativas;

*j)* la Opinión 4 del Foro Mundial de Política de las Telecomunicaciones/TIC (FMPT) (Lisboa, 2009) sobre estrategias de colaboración para la creación de confianza y seguridad en la utilización de las TIC;

*k)* los resultados pertinentes de la AMNT, en particular:

i) la Resolución 50 (Rev. Hammamet, 2016) – Ciberseguridad;

ii) la Resolución 52 (Rev. Hammamet, 2016) – Respuesta y lucha contra el correo basura;

*l)* que las redes seguras y fiables propician la confianza y alientan el intercambio y la utilización de la información y los datos;

*m)* que el desarrollo de competencias y la capacitación son fundamentales para mejorar la protección de las redes de información;

*n)* que los Estados Miembros hacen esfuerzos por mejorar sus entornos institucionales;

*o)* que los análisis y evaluaciones de los riesgos permiten comprender mejor los riesgos en materia de ciberseguridad a los que se enfrentan las organizaciones y la forma de atenuarlos,

*consciente*

*a)* de la que la UIT y otras organizaciones internacionales realizan diversas actividades y están examinando asuntos relacionados con la creación de confianza y seguridad en la utilización de las TIC, incluida la estabilidad, así como las medidas encaminadas a combatir el correo indeseado, los programas informáticos malignos, etc., sin olvidar la protección de los datos personales ni la privacidad;

*b)* de que la Comisión de Estudio 17 del UIT-T, las Comisiones de Estudio 1 y 2 del UIT-D y otras Comisiones de Estudio pertinentes de la UIT siguen trabajando sobre los medios técnicos para la seguridad de las redes de la información y la comunicación, de conformidad con las Resoluciones 50 y 52 (Rev. Hammamet, 2016), así como las Resoluciones 45 (Rev. Dubái, 2014) y 69 (Rev. Buenos Aires, 2017);

*c)* de que la UIT ha de desempeñar una función esencial en la creación de confianza y seguridad en la utilización de las TIC;

*d)* de que la Comisión de Estudio 2 del UIT-D sigue llevando a cabo los estudios en el marco de la Cuestión 3/2 del UIT-D (Garantías de seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad) la cual ha quedado reflejada en la Resolución 64/211 de la AGNU;

*e)* de que la UIT también brinda asistencia a los países en desarrollo en este ámbito y respalda la creación de EIII y apoya el establecimiento de esos EIII, incluido los encargados de la cooperación entre gobiernos y la importancia de la coordinación entre las organizaciones pertinentes;

*f)* de que con arreglo a la Resolución 1336, adoptada por el Consejo en su reunión de 2011, se creó un Grupo de Trabajo del Consejo sobre cuestiones de política pública internacional relacionadas con Internet (GTC-Internet), cuyo mandato consiste en identificar, estudiar y elaborar temas en torno a cuestiones de política pública internacional relacionadas con Internet, incluidas las enunciadas en la Resolución 1305 (2009) del Consejo, como la seguridad, la protección, la continuidad, la sostenibilidad y la solidez de Internet;

*g)* de la Resolución 80 (Buenos Aires, 2017) de la CMDT sobre el establecimiento y promoción de marcos de información fiables en los países en desarrollo para facilitar y fomentar el intercambio electrónico de información financiera entre socios económicos;

*h)* del Artículo 6, relativo a la seguridad y la robustez de las redes, y el Artículo 7, relativo al envío masivo de mensajes no solicitados, del Reglamento de las Telecomunicaciones Internacionales, aprobados por la Conferencia Mundial de Telecomunicaciones Internacionales (Dubái, 2012),

*observando*

*a)* que, como organización intergubernamental que cuenta con la participación del sector privado, la UIT está en buenas condiciones para desempeñar una función importante, junto con otros organismos y organizaciones internacionales pertinentes, para afrontar las amenazas y vulnerabilidades que inciden en la creación de confianza y seguridad en la utilización de las TIC;

*b)* los § 35 y 36 de la Declaración de Principios de Ginebra y el § 39 de la Agenda de Túnez para la Sociedad de la Información, sobre la creación de confianza y seguridad en la utilización de las TIC;

*c)* que, aunque no existen definiciones universalmente aceptadas de correo indeseado y otros términos afines, la Comisión 2 del UIT-T, en su reunión de junio de 2006, indicó que la expresión "correo indeseado" era utilizada habitualmente para describir el envío masivo de mensajes no solicitados por correo electrónico o por sistemas de mensajería móvil (SMS o MMS), cuyo propósito es, en general, vender productos o servicios comerciales;

*d)* las iniciativas de la Unión encaminadas a la cooperación con el Foro de los equipos de respuesta en caso de incidentes de seguridad (FIRST),

*teniendo en cuenta*

los trabajos de la UIT consignados en las Resoluciones 50 y 52 (Rev. Hammamet, 2016), la Resolución 58 (Rev. Dubái, 2012); la Resolución 45 (Rev. Dubái, 2014) y la Resolución 69 (Rev. Buenos Aires, 2017); el Objetivo 2 del Plan de Acción de Buenos Aires; las cuestiones de estudio pertinentes del UIT-T sobre aspectos técnicos de la seguridad de las redes de información y comunicación; y la Cuestión 3/2 del UIT-D,

*resuelve*

1 seguir atribuyendo gran prioridad a esta actividad en la UIT, teniendo en cuenta su competencia y conocimientos técnicos, lo que incluye promover el 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 atribuir una alta prioridad en la UIT a los trabajos descritos en el *teniendo en cuenta* anterior, de conformidad con sus conocimientos técnicos y ámbitos de competencia y seguir colaborando estrechamente, según proceda, con otros órganos/agencias de las Naciones Unidas y otros organismos internacionales, habida cuenta de sus mandatos específicos y los ámbitos de competencia de los diversos organismos, teniendo presente la necesidad de evitar la duplicación de trabajos entre las organizaciones y entre las Oficinas de la UIT, o la Secretaría General;

3 que la UIT centre sus recursos y programas en aquellos ámbitos nacionales, regionales e internacionales de la ciberseguridad que se corresponden con su mandato fundamental y su ámbito de competencia, y más concretamente en las esferas técnica y del desarrollo, excluyendo las áreas relacionadas con la aplicación de principios legales o políticos por parte de los Estados Miembros en relación con la defensa nacional, la seguridad nacional, los contenidos y el ciberdelito, que corresponden a sus derechos soberanos; no obstante, ello no excluye que la UIT cumpla con su mandato relativo a la elaboración de recomendaciones técnicas destinadas a reducir las vulnerabilidades de la infraestructura de TIC; tampoco excluye que la UIT preste toda su asistencia acordada en la CMDT-17, incluida la prevista en el Objetivo 2 y las actividades de la Cuestión 3/2;

4 promover una cultura en cuyo marco la seguridad se vea como un proceso continuo e iterativo, integrado en los productos desde el principio y durante toda su vida útil, y accesible y comprensible para los usuarios;

5 promover una mayor sensibilización de los Miembros de la UIT sobre las actividades llevadas a cabo en el seno de la UIT y de otras entidades pertinentes que participan en el fortalecimiento de la ciberseguridad, incluida la capacitación, y sensibilizar a dichas entidades sobre los obstáculos concretos a los que se enfrentan los países en desarrollo para crear confianza y seguridad en el uso de las TIC;

6 que la UIT contribuya a seguir fortaleciendo el marco de confianza y seguridad en consonancia con su función de facilitador principal de la Línea de Acción C5 de la CMSI, teniendo en cuenta la Resolución 140 (Rev. Dubái, 2018);

7 seguir 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 destinadas a fomentar la elaboración de enfoques comunes en el ámbito de la ciberseguridad;

8 elaborar estudios de caso sobre acuerdos institucionales relacionados con la ciberseguridad en colaboración con los Miembros y las organizaciones pertinentes;

9 examinar los retos concretos en materia de ciberseguridad a los que se enfrentan las PYME e integrar sus consideraciones al respecto en las actividades llevadas a cabo por la UIT en el ámbito de la creación de confianza y seguridad en la utilización de las TIC;

10 tener en cuenta las repercusiones de la implantación de nuevas tecnologías en la esfera de la ciberseguridad e integrar sus consideraciones al respecto en las actividades llevadas a cabo por la UIT en el ámbito de la creación de confianza y seguridad en la utilización de las TIC;

11 apoyar el desarrollo de la infraestructura en que se basa la transformación digital en curso de la economía mundial mediante de la creación de confianza y seguridad en la utilización de las TIC, en particular para hacer frente a las amenazas actuales y futuras, en el marco del mandato de la UIT;

12 utilizar el marco de la ACG de la UIT para seguir encauzando la labor de la Unión en sus esfuerzos por crear confianza y seguridad en la utilización de las TIC,

*encarga al Secretario General y a los Directores de las Oficinas*

1 que sigan examinando:

i) los trabajos realizados hasta la fecha en los tres Sectores de la UIT, en la ACG de la UIT y en otras organizaciones competentes así como en las iniciativas encaminadas a responder a las amenazas existentes y futuras y a reforzar la protección contra las mismas, con miras a crear confianza y seguridad en la utilización de las TIC;

ii) con ayuda de los Grupos Asesores, de conformidad con las disposiciones del Convenio y la Constitución de la UIT, los avances logrados en la aplicación de la presente Resolución y la conveniencia de que la UIT siga cumpliendo una función destacada como moderadora/facilitadora de la Línea de Acción C5 de la CMSI;

iii) los resultados de los trabajos realizados hasta ahora para ayudar, en particular a los países en desarrollo, en la creación de capacidad y competencias en ciberseguridad, con el fin de asegurar que la UIT está dedicando sus recursos de manera efectiva a responder a los retos del desarrollo;

2 que, con arreglo a la Resolución 45 (Rev. Dubái, 2014), informe al Consejo sobre las actividades dentro de la UIT y otras organizaciones y entidades pertinentes para mejorar la cooperación y la colaboración, a nivel regional y mundial, a fin de fortalecer la creación de confianza y seguridad en la utilización de las TIC de los Estados Miembros, en particular, los países en desarrollo, teniendo en cuenta toda la información proporcionada por los Estados Miembros, incluida la información sobre las situaciones dentro de su propia jurisdicción que pudieran afectar esta cooperación;

3 que, con arreglo a la Resolución 45 (Rev. Dubái, 2014), informen sobre los Memorandos de Entendimiento (MoU) entre los países, así como sobre las modalidades de cooperación existentes, y faciliten un análisis relativo a la situación, el alcance y las aplicaciones de estos mecanismos cooperativos para reforzar la ciberseguridad y luchar contra las ciberamenazas, con el fin de permitir a los Estados Miembros determinar si se requieren nuevos memorandos o mecanismos;

4 que den a conocer las actividades de la UIT y de otras entidades relevantes involucradas en el fortalecimiento de la ciberseguridad, incluida la capacitación, y los desafíos concretos que afrontan los países en desarrollo en la creación de confianza y seguridad en la utilización de las TIC, en consonancia con el *resuelve* 5;

5 que, teniendo presentes las disposiciones de la CMSI sobre el acceso universal y no discriminatorio a las TIC para todas las naciones, faciliten el acceso a los instrumentos y recursos necesarios, según las disponibilidades del presupuesto, para aumentar la confianza y la seguridad de todos los Estados Miembros en la utilización de las TIC;

6 que sigan intercambiando conocimientos e información sobre iniciativas existentes y futuras, nacionales, regionales e internacionales relativas a la ciberseguridad en todo el mundo a través de la página web de la UIT sobre ciberseguridad y aliente a todas las partes interesadas a contribuir a estas actividades, teniendo en cuenta los portales existentes;

7 que presenten todos los años un informe al Consejo sobre estas actividades y formulen las propuestas del caso;

8 que intensifiquen aún más la coordinación entre las Comisiones de Estudio y los programas correspondientes,

*encarga al Director de la Oficina de Normalización de las Telecomunicaciones*

1 que intensifique los trabajos en el marco de las Comisiones de Estudio existentes del UIT-T con objeto de:

i) analizar las amenazas y vulnerabilidades existentes y futuras, que afectan a los esfuerzos destinados a crear confianza y seguridad en la utilización de las TIC, habida cuenta de los nuevos servicios y aplicaciones basados en las redes de telecomunicaciones/TIC, mediante la elaboración, en su caso, de informes o Recomendaciones con la finalidad de aplicar las Resoluciones de la AMNT, en particular las Resoluciones 50 y 52 (Rev. Hammamet, 2016) y la Resolución 58 (Rev. Dubái, 2012), permitiendo la iniciación de los trabajos antes de la aprobación de una Cuestión;

ii) buscar la manera de mejorar el intercambio de información técnica en la materia, fomentar la adopción de protocolos y normas que aumentan la seguridad e impulsar la cooperación internacional entre las entidades apropiadas;

iii) facilitar proyectos derivados de los resultados de la AMNT, en particular:

- la Resolución 50 (Rev. Hammamet, 2016) sobre ciberseguridad;
- la Resolución 52 (Rev. Hammamet, 2016) sobre respuesta y lucha contra el correo basura;

2 que examine en el UIT-T la promoción de una cultura en la que la seguridad se considere un proceso continuo e iterativo, y presente propuestas al Consejo, según proceda;

3 que siga colaborando con las organizaciones competentes con miras a intercambiar prácticas óptimas y difundir información mediante, como talleres mixtos, reuniones de capacitación y grupos mixtos de coordinación, e invitando a las organizaciones interesadas a formular contribuciones por escrito,

*encarga al Director de la Oficina de Desarrollo de las Telecomunicaciones*

1 que teniendo en cuenta los resultados de la CMDT-17 y, de conformidad con las Resoluciones 45 (Rev. Dubái, 2014) y 69 (Rev. Buenos Aires, 2017), la Resolución 80 (Buenos Aires, 2017) y el Objetivo 2 del Plan de Acción de Buenos Aires, apoye los proyectos regionales y mundiales en curso sobre la ciberseguridad y aliente a todos los países a participar en esas actividades;

2 que, previa solicitud, brinde apoyo a los Estados Miembros de la UIT en sus actividades de capacitación de la siguiente manera: facilitar el acceso de los Estados Miembros a recursos desarrollados por otras organizaciones internacionales que trabajan en la elaboración de una legislación nacional para combatir el ciberdelito; respaldar los esfuerzos regionales y nacionales de los Estados Miembros de la UIT para la capacitación con miras a la protección contra las ciberamenazas y el ciberdelito, en colaboración recíproca; en armonía con la legislación nacional de los Estados Miembros indicada anterior, ayudar a los Estados Miembros, en particular a los países en desarrollo, a elaborar medidas jurídicas viables y apropiadas contra las ciberamenazas en los planos nacional, regional e internacional; establecer medidas técnicas y de procedimiento destinadas a la protección de infraestructuras nacionales de las TIC, teniendo en cuenta la labor de las correspondientes Comisiones de Estudio del UIT-T y, llegado el caso, de otras organizaciones pertinentes; establecer estructuras orgánicas, como los EIII, para identificar, gestionar y dar respuesta a las ciberamenazas, así como mecanismos de cooperación a escala regional e internacional;

3 que, en el límite de los recursos existentes, proporcione el apoyo financiero y administrativo necesario para estos proyectos y que procure conseguir recursos adicionales (en efectivo o en especie) para su ejecución mediante acuerdos de colaboración;

4 que garantice la coordinación de los trabajos de estos proyectos en el marco de las actividades globales que la UIT lleva a cabo como moderador/facilitador de la Línea de Acción C5 de la CMSI y elimine la duplicación de tareas sobre este tema importante con la Secretaría General y el UIT-T;

5 que coordine los trabajos de estos proyectos con los de las Comisiones de Estudio del UIT-D sobre este asunto, con las actividades del programa correspondiente y con la Secretaría General;

6 que siga colaborando con las organizaciones competentes con miras a intercambiar prácticas idóneas y difundir información mediante, por ejemplo, talleres mixtos y reuniones de capacitación;

7 que apoye la labor de la Comisión de Estudio 17 y de otras Comisiones de Estudio del UIT-T promoviendo y facilitando la aplicación de las Recomendaciones del UIT-T aprobadas en materia de seguridad en los Estados Miembros y Miembros de Sector de la UIT, en particular en los países en desarrollo;

8 que apoye a los Estados Miembros de la UIT para la formulación de sus estrategias de ciberseguridad nacionales y/o regionales, para fortalecer la capacidad nacional dirigida a la protección frente a las ciberamenazas y la respuesta a las mismas, y con arreglo a los principios de la cooperación internacional en consonancia con el Objetivo 2 del Plan de Acción de Buenos Aires de la CMDT;

9 que preste apoyo a los Miembros en el desarrollo de competencias y capacitación con miras a mejorar la ciberseguridad;

10 que preste apoyo a los Miembros en la realización de actividades de evaluación de riesgos relacionadas con la ciberseguridad;

11 que presente todos los años un informe al Consejo sobre estas actividades y formule las propuestas del caso,

*encarga además al Director de la Oficina de Normalización de las Telecomunicaciones y al Director de la Oficina de Desarrollo de las Telecomunicaciones*

que, cada uno de ellos, en el ámbito de sus responsabilidades:

1 aplique las Resoluciones pertinentes de la AMNT-16 y la CMDT-17, incluido el Resultado 2.2 del Objetivo 2 del Plan de Acción de Buenos Aires, prestando especial atención a las necesidades de los países en desarrollo en su labor para aumentar la ciberseguridad y crear confianza y seguridad en la utilización de las TIC;

2 identifique y fomente la disponibilidad de información sobre la creación de confianza y seguridad en la utilización de las TIC, incluida la información relativa a la infraestructura de las TIC, para los Estados Miembros, los Miembros de Sector y las organizaciones pertinentes;

3 sin duplicar las tareas correspondientes a la Cuestión 3/2 del UIT-D, siga identificando prácticas óptimas relacionadas con la Cuestión 3/2, incluida la creación de EIII, y revise la guía de referencia para los Estados Miembros y, llegado el caso, aporte contribuciones a la Cuestión 3/2;

4 coopere con las organizaciones correspondientes y con expertos internacionales y nacionales, si procede, para identificar prácticas óptimas en la creación de confianza y seguridad en la utilización de las TIC, incluida la creación de EIII;

5 adopte medidas para que las nuevas Cuestiones relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación sean examinadas por las Comisiones de Estudio en los Sectores;

6 identifique y documente las medidas prácticas para respaldar a los países en desarrollo a crear capacidad y competencias en ciberseguridad, teniendo en cuenta los retos específicos que afrontan;

7 tenga en cuenta los retos que afrontan todas las partes interesadas, en particular en los países en desarrollo, para crear confianza y seguridad en la utilización de las TIC e identifique medidas que pueden ayudar a darles respuesta;

8 identifique y documente las medidas prácticas para fortalecer la seguridad en la utilización de las TIC a nivel internacional, incluido el concepto de que la seguridad se ve como un proceso continuo e iterativo, sobre la base de prácticas, directrices y recomendaciones ampliamente aceptadas, que los Estados Miembros y otras partes interesadas pueden optar por aplicar para mejorar su capacidad para combatir las ciberamenazas y los ciberataques, incluido un enfoque dinámico, iterativo y basado en el riesgo que refleje el carácter cambiante de las amenazas y las vulnerabilidades y para fortalecer la cooperación internacional en la creación de la confianza y seguridad en la utilización de las TIC, teniendo en cuenta la ACG de la UIT y dentro de los recursos financieros disponibles;

9 respalde las estrategias, la organización, la sensibilización, la cooperación, la evaluación y el desarrollo de aptitudes;

10 proporcione el apoyo técnico y financiero necesario, dentro de las restricciones de los recursos presupuestarios actuales, de conformidad con la Resolución 58 (Rev. Dubái, 2012);

11 aliente la participación de expertos en las actividades de la UIT en el ámbito de la creación de confianza y seguridad en la utilización de las TIC;

12 movilice los recursos extrapresupuestarios suficientes fuera del presupuesto ordinario de la Unión para la aplicación de la presente Resolución con miras a prestar ayuda a los países en desarrollo;

13 que apoye y preste asistencia a los países en desarrollo en la promoción y facilitación de la aplicación de las Recomendaciones del UIT-T relacionadas con la seguridad,

*encarga al Secretario General*

de conformidad con su iniciativa en esta materia:

1 que informe al Consejo, teniendo en cuenta las actividades de los tres Sectores, de la aplicación y eficacia de un plan de acción para fortalecer el papel de la UIT en la creación de confianza y seguridad en la utilización de las TIC;

2 que coopere con las organizaciones internacionales pertinentes, incluso a través de la adopción de MoU, sujeta a la aprobación del Consejo al respecto, con arreglo a la Resolución 100 (Minneápolis, 1998) de la Conferencia de Plenipotenciarios,

*pide al Consejo*

que incluya el informe del Secretario General en los documentos enviados a los Estados Miembros de conformidad con el número 81 del Convenio,

*invita a los Estados Miembros*

1 a considerar su participación en iniciativas internacionales y regionales adecuadas y competentes para mejorar los marcos legislativos nacionales relativos a la seguridad de la información y de las redes de comunicación;

2 a colaborar estrechamente en el fortalecimiento de la cooperación regional e internacional, teniendo en cuenta la Resolución 45 (Rev. Dubái, 2014), con el fin de aumentar la confianza y la seguridad en la utilización de las TIC, con el fin de mitigar los riesgos y amenazas;

3 a apoyar las iniciativas de la UIT sobre ciberseguridad, incluido el Índice de Ciberseguridad Global, con el fin de promover las estrategias gubernamentales y el intercambio de información acerca de los esfuerzos en todas las industrias y sectores;

4 a informar al Secretario General sobre las actividades pertinentes relacionadas con la presente Resolución en relación con la confianza y la seguridad en la utilización de las TIC;

5 a aprovechar los recursos, el apoyo y las prácticas idóneas de las iniciativas nacionales, regionales e internacionales relacionadas con la ciberseguridad en todo el mundo a través de la página web de la UIT sobre ciberseguridad;

6 a colaborar con las organizaciones pertinentes, mediante el intercambio de prácticas idóneas en la creación de confianza y seguridad en la utilización de las TIC incluido el desarrollo y creación de los EIII nacionales;

7 a seguir sensibilizando mediante la difusión de prácticas idóneas y políticas implementadas con el fin de incrementar la capacidad de elaborar políticas adecuadas relativas a la protección de los usuarios, a fin de aumentar la confianza en la utilización de las telecomunicaciones/TIC,

*invita a los Estados Miembros, Miembros de Sector y Asociados*

1 a contribuir a esta tarea en las Comisiones de Estudio pertinentes de la UIT en todas las demás actividades en las que la UIT asume su responsabilidad;

2 a contribuir a crear confianza y seguridad en la utilización de las TIC en los ámbitos nacional, regional e internacional, emprendiendo las actividades descritas en los documentos finales de la CMSI, la Declaración de la CMSI+10 relativa a la aplicación de los resultados de la CMSI y la Perspectiva de la CMSI+10 para la CMSI después de 2015, el documento final de la reunión de alto nivel de la AGNU sobre el examen general de la aplicación de los resultados de la CMSI, y a participar en la preparación y aplicación de esas actividades;

3 a sensibilizar todas las partes interesadas, incluidas las organizaciones y los usuarios individuales de la importancia de fortalecer la ciberseguridad, incluida la adopción de protecciones básicas;

4 a fomentar la elaboración de programas de educación y capacitación para dar mejor a conocer al usuario los riesgos en el ciberespacio y las medidas que los usuarios pueden adoptar para protegerse;

5 a incorporar un enfoque dinámico, iterativo y basado en el riesgo, para hacer frente a las amenazas y vulnerabilidades en constante cambio y a fomentar una cultura en la que la seguridad se considere un proceso continuo e iterativo, que debe integrarse, en las fases de desarrollo e implantación de las tecnologías y sus aplicaciones desde el principio y durante toda su vida útil, en su labor de creación de confianza y seguridad en la utilización de las TIC;

6 a colaborar, según proceda, para abordar y prevenir los problemas que socavan la confianza y la seguridad en la utilización de las telecomunicaciones/TIC.

*(Marrakech, 2002) – (Rev. Antalya, 2006) – (Rev. Guadalajara, 2010) – (Rev. Busán, 2014) – (Rev. Dubái, 2018)*