RESOLUCIÓN 45 (Rev. Kigali, 2022)

Mecanismos para mejorar la cooperación en materia de ciberseguridad, incluida la lucha contra el correo basura

La Conferencia Mundial de Desarrollo de las Telecomunicaciones (Kigali, 2022),

recordando

a) la 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 (TIC), de la Conferencia de Plenipotenciarios;

b) la Resolución 174 (Rev. Busán, 2014), Función de la UIT respecto a los problemas de política pública internacional asociados al riesgo de utilización ilícita de las TIC, de la Conferencia de Plenipotenciarios;

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

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

e) la Resolución 45 (Rev. Dubái, 2014) de la Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT);

f) la Resolución 50 (Rev. Ginebra, 2022), Ciberseguridad, de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT);

g) la Resolución 52 (Rev. Hammamet, 2016), Respuesta y lucha contra el correo basura, de la AMNT;

h) la Resolución 58 (Rev. Ginebra, 2022), Fomento de la creación de equipos nacionales de intervención en caso de incidente informático (EIII), de la AMNT, especialmente para los países en desarrollo[1];

i) la Resolución 69 (Rev. Kigali, 2022), Creación de EIII nacionales y regionales, especialmente para los países en desarrollo, y la cooperación entre ellos, de la presente Conferencia;

---

[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.

j) la Resolución 67 (Rev. Kigali, 2022), Función del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D) en la Protección de la Infancia en Línea, de la presente Conferencia;

k) las opiniones relevantes del sexto Foro Mundial de Política de las Telecomunicaciones que se enmarcan en el mandato del UIT-D;

l) los nobles principios, finalidades y objetivos plasmados en la Carta de las Naciones Unidas y en la Declaración Universal de los Derechos Humanos;

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

n) las disposiciones en materia de ciberseguridad del Compromiso de Túnez y la Agenda de Túnez de la CMSI;

o) los objetivos establecidos en el Plan Estratégico de la Unión en vigor;

p) la cuestión de estudio del UIT-D sobre "Seguridad en las redes de información y comunicación: prácticas idóneas para el desarrollo de una cultura de ciberseguridad", en cuyo último ciclo colaboraron varios Miembros para producir informes que incluyen material didáctico destinado a los países en desarrollo, tal como un compendio de experiencias nacionales, prácticas idóneas para asociaciones públicas-privadas (APP), prácticas idóneas para constituir EIII con el correspondiente material didáctico y prácticas idóneas para la gestión de los EIII;

q) el informe del Presidente del Grupo de Expertos de Alto Nivel de la Agenda sobre Ciberseguridad Global (ACG) establecido por el Secretario General de la UIT en virtud de lo estipulado en la Línea de Acción C5 sobre la creación de confianza y seguridad en la utilización de las TIC, y de conformidad con la Resolución 140 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios sobre el cometido de la UIT como coordinador único de la Línea de Acción C5 de la CMSI y la Resolución 58 (Rev. Ginebra, 2022) de la AMNT, relativa al fomento de la creación de EIII nacionales, especialmente para los países en desarrollo;

r) que el Consejo aprobó, en su reunión de 2022, las directrices para la utilización de la ACG por la UIT en sus trabajos;

s) que la UIT y la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) han firmado un Memorando de Entendimiento (MoU) a fin de fortalecer la seguridad en el uso de las TIC,

considerando

a) el papel de las telecomunicaciones/TIC como instrumento eficaz para promover la paz, el desarrollo económico, la seguridad y la estabilidad, así como para propiciar la democracia, la cohesión social, el buen gobierno y el estado de derecho, y la necesidad de afrontar las cada vez mayores dificultades y amenazas derivadas de los abusos de estas tecnologías, incluidos los que persiguen fines delictivos y terroristas, respetando siempre los derechos humanos (§ 15 del Compromiso de Túnez);

b) la necesidad de crear confianza y seguridad en la utilización de las telecomunicaciones/TIC mediante el fortalecimiento de un marco de confianza (§ 39 de la Agenda de Túnez); y la necesidad de que los gobiernos, en cooperación con otras partes interesadas dentro de sus respectivas funciones, elaboren la legislación necesaria para investigar y perseguir la ciberdelincuencia, a nivel nacional, y cooperar en los planos regional e internacional teniendo en cuenta los marcos existentes;

c) que en la Resolución 64/211 de la Asamblea General de las Naciones Unidas (AGNU) se invita a los Estados Miembros a utilizar en sus actividades nacionales, siempre y cuando lo consideren procedente, el instrumento de autoevaluación voluntaria que figura en Anexo a dicha Resolución;

d) la necesidad de que los Estados Miembros elaboren programas de ciberseguridad nacionales centrados en torno a un plan nacional, APP, fundamentos legislativos coherentes, una gestión de incidentes, una capacidad de vigilancia, alerta, intervención y restablecimiento, y una cultura de la sensibilización, utilizando como guía los Informes sobre prácticas idóneas para adoptar un enfoque nacional con respecto a la ciberseguridad: módulos esenciales para la organización de los esfuerzos nacionales en materia de ciberseguridad;

e) que las pérdidas considerables y crecientes en que han incurrido los usuarios de sistemas de telecomunicaciones/TIC, como consecuencia del problema cada vez mayor de la ciberdelincuencia y el sabotaje deliberado en todo el mundo, alarman a todos los países desarrollados y en desarrollo sin excepción;

f) las razones que justifican la adopción de la Resolución 37 (Rev. Kigali, 2022) de la presente Conferencia, relativa a la reducción de la brecha digital, en lo que atañe a la importancia de la aplicación multipartita a nivel internacional y a las Líneas de Acción expuestas mencionadas en el § 108 de la Agenda de Túnez, incluida la "Creación de confianza y seguridad en la utilización de las TIC";

g) los resultados de diversas actividades de la UIT relacionadas con la ciberseguridad, en particular las que coordina la Oficina de Desarrollo de las Telecomunicaciones (BDT), con el fin de cumplir el mandato de la UIT en cuanto a facilitador para la aplicación de la Línea de Acción C5 (Creación de confianza y seguridad en la utilización de las TIC);

h) que un gran número de organizaciones de todos los sectores de la sociedad colaboran en la ciberseguridad de las telecomunicaciones/TIC;

i) que debido, entre otras cosas, a que las infraestructuras esenciales de telecomunicaciones/TIC están interconectadas a escala mundial, la poca seguridad en la infraestructura de un país podría aumentar la vulnerabilidad y el riesgo en otros países;

j) que numerosa información, documentación, prácticas idóneas y recursos elaborados por organizaciones nacionales, regionales e internacionales de conformidad con sus respectivas responsabilidades, están a disposición de los Estados Miembros;

k) que la ACG de la UIT fomenta la cooperación internacional con el fin de proponer estrategias que permitan mejorar la confianza y seguridad en la utilización de las telecomunicaciones/TIC;

l) que la ciberseguridad se ha convertido en un tema de suma importancia a escala internacional y que el UIT-D, en el ámbito de su mandato, puede seguir contribuyendo a la creación de confianza y seguridad en la utilización de las TIC en estos esfuerzos,

reconociendo

a) que las medidas adoptadas para asegurar la estabilidad y seguridad de las redes de telecomunicaciones/TIC, protegerse contra la ciberdelincuencia y contrarrestar el correo basura, deben proteger y respetar las disposiciones relativas a la privacidad y libertad de expresión contenidas en las partes pertinentes de la Declaración Universal de Derechos Humanos (§ 42 de la Agenda de Túnez) y del Pacto Internacional de Derechos Civiles y Políticos;

b) el hecho de que en la Resolución 68/167 de la AGNU sobre el derecho a la privacidad en la era digital, se afirma que "los derechos de las personas también deben estar protegidos en Internet, incluido el derecho a la privacidad";

c) la necesidad de tomar medidas apropiadas y preventivas, con arreglo a la legislación vigente, contra las utilizaciones abusivas de las telecomunicaciones/TIC mencionadas en el Capítulo sobre las "Dimensiones Éticas de la Sociedad de la Información", de la Declaración de Principios y el Plan de Acción de Ginebra (§ 43 de la Agenda de Túnez) de la CMSI, la necesidad de combatir el terrorismo en todas sus formas y manifestaciones en las redes de telecomunicaciones/TIC, respetando los derechos humanos y en consonancia con las obligaciones contraídas en virtud del derecho internacional, según se indica en el párrafo dispositivo 81 de la Resolución 60/1 de la AGNU ("Documento Final de la Cumbre Mundial de 2005") y la importancia de la seguridad, continuidad y estabilidad de las redes de telecomunicaciones/TIC, y la necesidad de proteger esas redes contra amenazas y vulnerabilidades (§ 45 de la Agenda de Túnez), a la vez que se garantiza el respeto por la privacidad y la protección de la información y los datos personales mediante la adopción de legislaciones, la aplicación de marcos de colaboración, prácticas idóneas y medidas tecnológicas y de autorreglamentación por las empresas y los usuarios (§ 46 de la Agenda de Túnez);

d) la necesidad de afrontar eficazmente las dificultades y amenazas que representa la utilización de las telecomunicaciones/TIC para fines que son incompatibles con los objetivos de mantener la estabilidad y la seguridad internacionales y que podrían menoscabar la integridad de las infraestructuras nacionales, en detrimento de su seguridad, y que es necesario cooperar para evitar el abuso de las tecnologías y de los recursos de la información con fines delictivos y terroristas, respetando siempre los derechos humanos;

e) el papel de las telecomunicaciones/TIC en la protección y el fomento del desarrollo de los niños, y que es necesario reforzar las medidas de protección de la infancia contra cualquier tipo de abuso y en defensa de sus derechos en el contexto de las telecomunicaciones/TIC, insistiendo en que el interés de los niños es un factor primordial;

f) la voluntad y el compromiso de todas las partes involucradas de construir una sociedad de la información centrada en la persona, abierta a todos y orientada al desarrollo, con arreglo a los objetivos y a los principios de la Carta de las Naciones Unidas, el derecho internacional y el multilateralismo, y en el respeto y la defensa total de la Declaración Universal de Derechos Humanos, a fin de que todos los pueblos del mundo puedan crear, consultar, utilizar y compartir la información y el conocimiento con plena seguridad para desarrollar su pleno potencial y alcanzar las metas y los objetivos de desarrollo acordados internacionalmente, entre ellos los Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas;

g) lo dispuesto en los § 4, 5 y 55 de la Declaración de Principios de Ginebra, y que la libertad de expresión y la libre circulación de información, ideas y conocimientos son beneficiosos para el desarrollo;

h) que la fase de Túnez de la CMSI representó una oportunidad excepcional de aumentar la sensibilización sobre las ventajas que las telecomunicaciones/TIC pueden aportar a la humanidad y de la manera en que pueden transformar las actividades y la vida de las personas, así como su interacción, despertando así una mayor confianza en el futuro, que depende de la seguridad en la utilización de las telecomunicaciones/TIC, como ha quedado demostrado en la aplicación de los resultados de la Cumbre;

i) que el correo basura (spam) constituye un problema mundial, con distintas características en cada región, y es necesario un enfoque de colaboración multipartito para luchar contra él;

j) la necesidad de resolver eficazmente el problema cada vez más importante que plantea el correo basura, conforme a lo estipulado en el § 41 de Agenda de Túnez, y otros problemas como la ciberdelincuencia, los virus, los gusanos y los ataques de denegación del servicio;

k) la necesidad de una colaboración efectiva en el UIT-D,

observando

a) el continuo trabajo de la Comisión de Estudio 17 (Seguridad) del UIT-T y otras organizaciones de normalización sobre diversos aspectos de la seguridad de las telecomunicaciones/TIC;

b) que el correo basura es un problema considerable y sigue suponiendo una amenaza para los usuarios, las redes e Internet en general, y de que se deben abordar los problemas de la ciberseguridad a nivel nacional, regional e internacional, según proceda;

c) que la cooperación y colaboración entre los Estados Miembros, los Miembros de Sector y las partes interesadas pertinentes contribuyen a crear y mantener una cultura de la ciberseguridad,

resuelve

1 seguir reconociendo la ciberseguridad como una de las actividades prioritarias de la UIT, teniendo en cuenta los servicios y las tecnologías de telecomunicaciones/TIC nuevas e incipientes, y seguir abordando, en el contexto de su ámbito de competencia fundamental, la cuestión de crear seguridad y confianza en la utilización de las telecomunicaciones/TIC a través de la sensibilización, la identificación de prácticas idóneas, la prestación de asistencia para la implementación de medidas técnicas y el desarrollo de herramientas y materiales didácticos apropiados para promover una cultura de ciberseguridad;

2 mejorar la colaboración y cooperación y compartir información con todas las organizaciones internacionales y regionales pertinentes en ciberseguridad incluidas las iniciativas relacionadas con la ciberresiliencia que correspondan al ámbito de competencia de la UIT, teniendo en cuenta la necesidad de prestar asistencia a los países en desarrollo,

encarga al Director de la Oficina de Desarrollo de las Telecomunicaciones

1 que promueva una cultura en cuyo marco la seguridad se considere un proceso continuo e iterativo, integrado en los productos desde el principio y durante toda su vida útil, de forma accesible y comprensible para los usuarios;

2 que, en colaboración con las organizaciones pertinentes, según proceda, teniendo en cuenta las contribuciones de los Miembros, siga organizando, en cooperación con el Director de la Oficina de Normalización de las Telecomunicaciones (TSB), reuniones de Estados Miembros, Miembros de Sector y otras partes interesadas para estudiar las diversas maneras de mejorar la ciberseguridad;

3 que, en colaboración con las organizaciones y partes interesadas pertinentes, siga realizando estudios sobre el fortalecimiento de la ciberseguridad en países en desarrollo a escala regional e internacional, basados en la determinación clara de sus necesidades, en particular las relativas a la utilización de las telecomunicaciones/TIC, con inclusión de la lucha contra el correo basura y de los servicios y tecnologías de telecomunicaciones/TIC nuevas e incipientes, así como de la protección en línea de niños y jóvenes y de las personas vulnerables;

4 que considere los resultados del Índice de Ciberseguridad Global (ICG) a fin de orientar las iniciativas de la BDT relacionadas con la ciberseguridad, teniendo especialmente en cuenta las carencias identificadas a través del proceso del ICG;

5 que cambie la forma de presentar los resultados del ICG para que los países estén representados por niveles en lugar de una clasificación individual, con el fin de reflejar con mayor precisión el desarrollo de la ciberseguridad de los Estados Miembros;

6 que determine y documente medidas prácticas para ayudar a los países en desarrollo a crear capacidades y competencias en materia de ciberseguridad, teniendo en cuenta los retos específicos que afrontan;

7 que apoye las iniciativas de los Estados Miembros, especialmente en los países en desarrollo, relacionadas con los mecanismos para mejorar la cooperación en materia de ciberseguridad, incluida la lucha contra el correo basura;

8 que difunda entre los países en desarrollo información sobre las Directrices, Recomendaciones, Informes Técnicos y prácticas idóneas relacionados con la ciberseguridad elaborados por las Comisiones de Estudio del UIT-T, en colaboración con el Director de la TSB;

9 que ayude a los Estados Miembros, en particular a los países en desarrollo, proporcionando orientaciones y prácticas idóneas, a superar los retos en materia de ciberseguridad y correo basura que plantean las tecnologías nuevas e incipientes;

10 que preste asistencia a los países en desarrollo para que aumenten su grado de preparación a fin de garantizar un nivel alto y eficiente de ciberseguridad, incluyendo la ciberresiliencia, en sus infraestructuras esenciales de telecomunicaciones/TIC, mediante, entre otros, la organización de talleres y formación para promover una cultura de ciberhigiene;

11 que ayude a los Estados Miembros a establecer un marco adecuado entre los países en desarrollo que permita reaccionar rápidamente en caso de incidentes importantes, incluso mediante la promoción de intercambios voluntarios de información entre las administraciones interesadas, y que proponga un plan de acción destinado a reforzar la protección en estos países y reforzar su ciberresiliencia, teniendo en cuenta los mecanismos y asociaciones pertinentes;

12 que recopile de los Estados Miembros y comparta, junto con los trabajos de la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D, información relativa a las reglamentaciones, las políticas y otros enfoques destinados a crear confianza y seguridad en la utilización de las telecomunicaciones/TIC, que hayan sido desarrollados y/o aplicados por las autoridades nacionales de reglamentación de las telecomunicaciones u otras organizaciones interesadas;

13 que facilite que las Comisiones de Estudio del UIT-D pertinentes examinen las investigaciones en materia de seguridad de ciberseguridad, en colaboración con diferentes partes interesadas;

14 que anime a todas las partes interesadas a participar en las actividades de los Centros de Formación de la Academia de la UIT para formar, educar y sensibilizar sobre cuestiones de ciberseguridad, en el marco de la ACG;

15 que ayude a los Estados Miembros mejorando el intercambio de información actualizada sobre cuestiones y prácticas idóneas de ciberseguridad para su consideración por los Estados Miembros;

16 que ayude a los países en desarrollo a mejorar el desarrollo de sus capacidades mediante la celebración de talleres, seminarios o eventos, en el marco de los pilares de la ACG, sobre medidas de organización y técnicas, en colaboración con el Director de la TSB;

17 que informe acerca de los resultados de la aplicación de la presente Resolución a la próxima CMDT;

18 que siga consultando a los Estados Miembros sobre la mejora del proceso del ICG, incluyendo el debate de la metodología, la estructura, la ponderación y las preguntas, utilizando el Grupo de Expertos ICG según corresponda, y teniendo en cuenta las implicaciones financieras,

invita al Secretario General en coordinación con los Directores de la Oficina de Radiocomunicaciones, la Oficina de Normalización de las Telecomunicaciones y la Oficina de Desarrollo de las Telecomunicaciones

1 a informar sobre los MoU entre los países, así como sobre las modalidades de cooperación existentes ofreciendo un análisis sobre su situación, 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;

2 a brindar su apoyo a las Iniciativas Regionales y mundiales de ciberseguridad y a invitar a todos los países, en especial los países en desarrollo, a participar en esas actividades;

3 a seguir movilizando el conocimiento especializado en materia de desarrollo de la UIT, con miras a reforzar la ciberseguridad nacional, regional e internacional para apoyar los ODS, trabajando con otros organismos/entidades de las Naciones Unidas y otros organismos internacionales pertinentes, teniendo en cuenta los mandatos específicos y los ámbitos de conocimiento de estos diferentes organismos, y siendo conscientes, al mismo tiempo, de la necesidad de evitar duplicidades de los trabajos entre organizaciones y entre las Oficinas y la Secretaría General,

pide al Secretario General

1 que presente esta Resolución a la consideración de la próxima Conferencia de Plenipotenciarios para que tome las medidas correspondientes, si corresponde;

2 que informe a las reuniones del Consejo y las Conferencias de Plenipotenciarios posteriores acerca de los resultados de estas actividades, según corresponda,

invita a los Estados Miembros, Miembros de Sector, Asociados e Instituciones Académicas

1 a que presten el apoyo necesario y se impliquen activamente en la aplicación de la presente Resolución y las acciones que de ella se desprendan;

2 a que consideren prioritario el tema de la ciberseguridad y la lucha contra el correo basura, y a que tomen las medidas adecuadas y contribuyan a la creación de confianza y seguridad en la utilización de las telecomunicaciones/TIC en el plano nacional, regional e internacional;

3 a que insten a los proveedores de servicio a protegerse contra los riesgos identificados, a esforzarse por garantizar la continuidad de los servicios que ofrecen y a notificar los atentados a la seguridad;

4 a que colaboren entre sí a nivel nacional, con el objetivo de mejorar las soluciones encaminadas a proteger la ciberseguridad y la resiliencia de las redes;

5 a que informen a la UIT sobre los marcos de cooperación existentes entre los Miembros y con otros organismos y entidades, regionales o internacionales, en el plano bilateral,

invita a los Estados Miembros

1 a colaborar estrechamente para reforzar la cooperación regional e internacional con el fin de abordar los problemas actuales y futuros relacionados con la ciberseguridad y el correo basura;

2 a crear un marco adecuado que permita reaccionar rápidamente en caso de incidente importante, y a proponer un plan de acción para impedir y mitigar dichos incidentes y recuperarse de ellos;

3 a establecer estrategias y capacidades a nivel nacional para asegurar la protección de las infraestructuras públicas esenciales, incluida la mejora de la resiliencia de las infraestructuras de telecomunicaciones/TIC;

4 a fomentar el intercambio de información sobre ciberseguridad a nivel nacional, regional e internacional.