**MOD** B/30/1

RESOLUCIÓN 45 (REV. BUENOS AIRES, 2017)

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

La Conferencia Mundial de Desarrollo de las Telecomunicaciones (Buenos Aires, 2017),

recordando

*a)* la Resolución 130 (Rev. Busán, 2014) 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 140 (Rev. Busán, 2014) de la Conferencia de Plenipotenciarios, relativa a la función de la UIT en la puesta en práctica de los resultados de la Cumbre Mundial sobre la Sociedad de la Información y en el examen general de su aplicación por parte de la Asamblea General de las Naciones Unidas;

*c)* 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;

*d)* la Resolución 179 (Rev. Busán, 2014) de la Conferencia de Plenipotenciarios, sobre el papel de la UIT en la protección de la infancia en línea;

*e)* 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;

*f)* la Resolución 50 (Rev. Hammamet, 2016) de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT) sobre ciberseguridad;

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

*h)* la Resolución 58 (Rev. Dubái, 2012) de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT) sobre fomento de la creación de equipos nacionales de intervención en caso de incidente informático (EIII), especialmente para los países en desarrollo;

*i)* la Resolución 69 (Rev. Dubái, 2014) adoptada por la Conferencia Mundial de Desarrollo de las Telecomunicaciones sobre la facilitación de la creación de equipos nacionales de intervención en caso de incidente informático, especialmente para los países en desarrollo, y la cooperación entre ellos;

*j)* la Resolución 67 (Rev. Dubái, 2014) de la Conferencia Mundial de Desarrollo de las Telecomunicaciones sobre la función del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D) en la Protección de la Infancia en Línea;

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

*l)* 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);

*m)* las disposiciones en materia de ciberseguridad del Compromiso de Túnez y la Agenda de Túnez;

*n)* la Resolución 71 (Rev. Busán, 2014) de la Conferencia de Plenipotenciarios, sobre el Plan Estratégico de la Unión para 2016-2019, que refrenda los cinco Objetivos del UIT-D, entre ellos el Objetivo D.3 - Mejorar la confianza y seguridad en la utilización de las telecomunicaciones/TIC y desplegar las aplicaciones y los servicios pertinentes, y los resultados D.3-1: Refuerzo de la capacidad de los Estados Miembros para incorporar y aplicar políticas y estrategias de ciberseguridad en los planes de TIC nacionales y en la legislación correspondiente, y D.3-2 del Objetivo: Mayor capacidad de los Estados Miembros para responder a tiempo a las ciberamenazas;

*o)* los excelentes resultados de la Cuestión 22 de la Comisión de Estudio 1 del UIT-D, en los periodos de estudios 2006-2010 y 2010-2014, que incluyen numerosos informes y contribuciones de todo el mundo y la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D en el periodo de estudios 2014-2017 que continúan las labores de la Cuestión 22;

*p)* el informe del Presidente del Grupo de Expertos de Alto Nivel (GEAN) de la Agenda sobre ciberseguridad global (GCA) 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;

*q)* que la UIT y la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) han firmado en 2011 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 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)* que en la Resolución 70/125 de la Asamblea General de las Naciones Unidas, que representa el Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información, se afirma que generar confianza y seguridad en la utilización de las tecnologías de la información y las comunicaciones para el desarrollo sostenible también debería ser una prioridad, especialmente habida cuenta de las crecientes dificultades que se presentan, como el abuso de las tecnologías de la información y las comunicaciones para actividades perniciosas, desde el acoso hasta los delitos y el terrorismo; y debería ser compatible con el respeto los derechos humanos;

*e)* la necesidad de que los Estados Miembros elaboren programas de ciberseguridad nacionales centrados en torno a un plan nacional, asociaciones entre los sectores público y privado, 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 óptimas para adoptar un enfoque nacional con respecto a la ciberseguridad: módulos esenciales para la organización de los esfuerzos nacionales en materia de ciberseguridad, elaborados durante los dos periodos de estudio de la Cuestión 22 de la Comisión de Estudio 1 del UIT‑D (2006-2010, 2010-2014) y en su continuación en la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D (2014-2017);

*f)* 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;

*g)* las razones que justifican la adopción de la Resolución 37 (Rev. Dubái, 2014) de la Conferencia Mundial de Desarrollo de las Telecomunicaciones, 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";

*h)* 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 principal para la aplicación de la Línea de Acción C5 (Creación de confianza y seguridad en la utilización de las TIC);

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

*j)* 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;

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

*l)* que los resultados de la encuesta relativa a la concienciación de la ciberseguridad realizada por la BDT y los responsables de la Cuestión 22-1/1 en el periodo de estudios 2010-2014 demuestran que los países menos adelantados tienen una notable necesidad de ayuda en esta esfera;

*m)* que la Agenda de Ciberseguridad Global (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;

*n)* que el Índice Mundial de Ciberseguridad (GCI), elaborado en el marco de ACG de la UIT, es una herramienta importante para que todos los Estados Miembros evalúen su compromiso con la ACG de la UIT e identifiquen áreas de mejora para incrementar sus propias capacidades de ciberseguridad,

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 las Resoluciones 68/167, 69/166 y 71/1999 de la Asamblea General de las Naciones Unidas 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), 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 Asamblea General de las Naciones Unidas ("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, respectando siempre los derechos humanos;

*e)* el papel de las 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 Sostenibles del Milenio;

*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 representaba 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)* 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;

*j)* la necesidad de una colaboración efectiva entre todas las actividades del UIT-D,

observando

*a*) el continuo trabajo de la Comisión de Estudio 17 (Seguridad) del Sector de Normalización de las Telecomunicaciones de la UIT (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)* las conclusiones y recomendaciones del Informe final de la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D de examinar durante el próximo periodo de estudios las amenazas que evolucionan y surgen más allá del correo basura y el malware;

*d)* que la cooperación y colaboración entre los Estados Miembros, los Miembros de Sector y las partes interesadas pertinentes son esenciales para crear y mantener una cultura de la ciberseguridad,

resuelve

1 seguir reconociendo la ciberseguridad como una de las actividades prioritarias de la UIT 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 óptimas y el desarrollo del material didáctico apropiado para promover una cultura de la ciberseguridad;

2 mejorar la colaboración y cooperación y compartir información con todas las organizaciones internacionales y regionales pertinentes en las iniciativas relacionadas con la ciberseguridad que correspondan a su 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, en colaboración con las organizaciones pertinentes, según proceda, junto con el programa sobre el Producto 3.1 del Objetivo 3, sobre la base de 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;

2 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, así como los dispositivos de IoT, la inteligencia artificial y otras tendencias emergentes, incluida la protección de niños y jóvenes;

3 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;

4 que preste asistencia a los países en desarrollo para que aumenten su grado de preparación a fin de garantizar un nivel de seguridad alto y eficiente en sus infraestructuras esenciales de telecomunicaciones/TIC, incluida la celebración de talleres;

5 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 y que proponga un plan de acción destinado a reforzar la protección en estos países, teniendo en cuenta los mecanismos y asociaciones pertinentes;

6 que recopile y difunda, junto con el trabajo de la Cuestión 3/2 de la Comisión de Estudios 2 del UIT-D, información relativa a las políticas reglamentarias elaboradas y/o aplicadas por las autoridades nacionales de reglamentación de las telecomunicaciones a fin de construir confianza y seguridad en el uso de las telecomunicaciones/TIC;

7 que aplique la presente Resolución en cooperación y colaboración con el Director de la TSB;

8 que informe acerca de los resultados de la aplicación de la presente Resolución a la próxima CMDT,

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 Memorandos de Entendimiento (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 cualquier proyecto regional o mundial de ciberseguridad como son, entre otros, IMPACT, FIRST, OAS, APCERT, y a invitar a todos los países, en especial los países en desarrollo, a participar en esas actividades,

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 procede;

2 que informe al Consejo y a la Conferencia de Plenipotenciarios de 2018 acerca de los resultados de estas actividades,

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

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

2a 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;

3a 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 ellos a fin de mejorar las soluciones para proteger la privacidad, los datos personales y la seguridad de las redes,

invita a los Estados Miembros

1 a crear un marco adecuado que permita reaccionar rápidamente en caso de incidente importante, y a proponer un plan de acción que impida y mitigue dichos incidentes;

2 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.