|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | **Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT-16)**  **Hammamet, 25 de octubre - 3 de noviembre de 2016** | | CCITT/ITU-T 60th Anniversary logo |
|  | |  | |
|  | |  | |
| SESIÓN PLENARIA | | **Addéndum 13 al Documento 44-S** | |
|  | | **3 de octubre de 2016** | |
|  | | **Original: inglés** | |
|  | | | |
| Administraciones miembro de la Telecomunidad Asia-Pacífico | | | |
| PROPUESTA DE MODIFICACIÓN DE LA RESOLUCIÓN 50  DE LA AMNT-12 – Ciberseguridad | | | |
|  | | | |
|  | | | |

|  |  |
| --- | --- |
| **Resumen:** | En este documento las Administraciones de la Telecomunidad Asia-Pacífico proponen modificaciones a la Resolución 50. |

Introducción

Desde la AMNT-12 el UIT-T ha avanzado en las actividades relacionadas con la ciberseguridad. Se han producido cambios en el panorama de las amenazas a la ciberseguridad. En el próximo periodo de estudios (2017-2020) es necesario reforzar sus actividades y estudiar los problemas incipientes de seguridad.

Es preciso actualizar la Resolución 50 para incorporar los cambios y la evolución producidos desde 2012.

Propuesta

Las Administraciones miembro de la APT proponen modificaciones de la Resolución 50 relativa a la ciberseguridad, como se indican en el Anexo.

MOD APT/44A13/1

RESOLUCIÓN 50 (Rev. HAMMAMET, 2016)

Ciberseguridad

(Florianópolis, 2004; Johannesburgo, 2008; Dubái, 2012, Hammamet, 2016)

La Asamblea Mundial de Normalización de las Telecomunicaciones (Hammamet, 2016),

recordando

*a)* la Resolución 130 (Busán, 2014) de la Conferencia de Plenipotenciarios, sobre el 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 181 (Guadalajara, 2010) de la Conferencia de Plenipotenciarios, sobre definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las TIC;

*c)* las Resoluciones pertinentes de la Asamblea General de las Naciones Unidas, en particular la Resolución 57/239, la Resolución 58/199 y la Resolución 64/211, sobre creación de una cultura mundial de la ciberseguridad y la protección de la infraestructura de la información esencial;

*d)* las partes pertinentes de 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;

*e)* la Resolución 52 (Rev. Dubái, 2012) de esta Asamblea, Respuesta y lucha contra el correo basura;

*f)* la Resolución 58 (Rev. Dubái, 2012) de esta Asamblea, Fomento de la creación de equipos nacionales de intervención en caso de incidente informático, especialmente para los países en desarrollo[[1]](#footnote-1)1,

considerando

*a)* la importancia vital de la infraestructura de TIC y sus aplicaciones para prácticamente todas los tipos de actividades sociales y económicas, en particular los nuevos adelantos como la cuarta revolución industrial (CRI) e Internet de las Cosas;

*b)* 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;

*c)* que la seguridad es una cuestión intersectorial y que el panorama de la ciberseguridad es complejo y disperso, en el que intervienen 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;

*d)* 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;

*e)* el Informe final sobre la Cuestión 22-1/1 (Garantías de seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad) del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D);

*f)* los trabajos de normalización sobre cuestiones de seguridad relacionadas con Internet de las Cosas (IoT) y las aplicaciones de ciudades y comunidades inteligentes (C+CI) que afectan a la seguridad de los usuarios de Internet;

*g)* que, a fin de proteger las infraestructuras mundiales de telecomunicaciones/TIC de 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 y que el papel del UIT-T es importante en este campo, con arreglo a su mandato y ámbito de competencias;

*h)* la naturaleza dinámica de la economía mundial cuando el suministro de equipos electrónicos e informáticos que constituyen el ecosistema del vendedor es muy disperso y esencial para gestionar las amenazas a la seguridad;

*i*) los trabajos realizados y en curso en la UIT, en particular en la Comisión de Estudio 17 del UIT-T, en la Comisión de Estudio 2 del UIT-D y en el marco del Plan de Acción de Dubái adoptado por la CMDT (Dubái, 2014);

*j)* que el Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) tiene una función que desempeñar en el marco de su mandato y competencias en la creación de confianza y seguridad en la utilización de las TIC y en lo que respecta al *considerando g)*,

considerando además

*a)* que la Recomendación UIT-T X.1205 ofrece una definición y descripción de las tecnologías, además de los principios de protección de las redes;

*b)* que la Recomendación UIT-T X.805 establece un marco sistemático para la identificación de fallos de seguridad y que la Recomendación UIT-T X.1500 establece el modelo para el intercambio de información sobre ciberseguridad (CYBEX) y aborda técnicas que podrían utilizarse para facilitar el intercambio de información sobre ciberseguridad; y

*c)* que el UIT-T y el Comité Técnico Mixto sobre tecnologías de la información y la comunicación (JTC 1) de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI) ya cuentan con un volumen importante de publicaciones, y que están realizando estudios directamente relacionados con este tema, que se han considerar,

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. Dubái, 2012), así como las Resoluciones 45 y 69 (Rev. Dubái, 2014);

*c)* 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, de conformidad con lo dispuesto en la Resolución 58 (Rev. Dubái, 2012),

reconociendo

*a)* los resultados de la Cumbre Mundial sobre la Sociedad de la Información que identifican a la UIT como facilitador y moderador para la Línea de Acción C5 (Creación de confianza y seguridad en la utilización de las TIC), que fue reafirmada en diciembre 2015 por la reunión de alto nivel Asamblea General de las Naciones Unidas sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información;

*b)* que la ciberseguridad es uno de los aspectos fundamentales para la creación de confianza y seguridad en la utilización de las telecomunicaciones/TIC;

*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,

reconociendo además

*a)* que la naturaleza y el tipo de incidentes de ciberseguridad son muchos y diversos (por ejemplo, ataques de ingeniería social, amenazas persistentes avanzadas, etc.), y siguen evolucionando con el transcurso del tiempo, y que el origen de los ataques a la ciberseguridad resulta a veces difícil de identificar;

*b)* que las amenazas a la ciberseguridad se producen por vulnerabilidades en el código, el software y el hardware que puede resultar esencial para la infraestructura nacional e incluso perjudicial para la vida humana, por lo que se requiere una gestión oportuna de las vulnerabilidades y la distribución, en su caso, de parches de software/hardware;

*c)* que los datos se están convirtiendo en un activo fundamental de las redes de la información y la comunicación, así como el principal objetivo de los ataques a la ciberseguridad,

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 identidades, 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)* la necesidad de armonizar en la medida de lo posible las estrategias e iniciativas nacionales, regionales e internacionales a fin de evitar la duplicación y optimizar la utilización de los recursos;

*c)* que el UIT-D puede ayudar a los países en desarrollo en actividades de capacitación relativa a la ciberseguridad que se adapte a las condiciones y necesidades concretas de cada país;

*d)* que la cooperación y la colaboración entre organizaciones en materia de seguridad puede propiciar adelantos en esta esfera y contribuir a crear y mantener una cultura de la ciberseguridad,

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 que todas las Comisiones de Estudio del UIT‑T sigan evaluando las Recomendaciones existentes y nuevas en lo que respecta a su robustez de diseño y posible explotación por partes maliciosas, en particular la nueva infraestructura de servicios y aplicaciones (por ejemplo, analítica de datos masivos, computación en la nube, ciudades inteligentes, servicios financieros digitales, computación en el límite de la red móvil, computación cuántica, redes móviles de 5ª generación, cibersalud, Internet de la Cosas, redes definidas por software, virtualización de la función de red, Internet industrial, distribución eléctrica inteligente y sistemas de transporte inteligentes, que se basan en las redes de telecomunicaciones/TIC tales como las IMT-2020) que se basarán en la infraestructura mundial de telecomunicaciones/TIC, y que informe al GANT según proceda;

3 que el UIT-T comience a investigar sobre normas relacionadas con la seguridad de los datos masivos, especialmente sobre normas y prácticas para la evaluación de la seguridad de los datos y la protección de los datos durante toda su vida útil;

4 que el UIT-T siga desempeñando, en el marco de su mandato y competencias, su labor de sensibilización respecto de la necesidad de defender los sistemas de información y telecomunicaciones contra la amenaza de ciberataques, 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;

5 que el UIT-T colabore estrechamente 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 el UIT-T siga trabajando en la elaboración y el perfeccionamiento de términos y definiciones relacionados con la creación de confianza y seguridad en el uso de las telecomunicaciones/TIC, incluido el término ciberseguridad;

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

8 que la Comisión de Estudio 17, en estrecha colaboración con todas las demás Comisiones de Estudio del UIT-T definan un plan de acción para evaluar las Recomendaciones UIT-T, actuales, modificadas y nuevas en cuanto a las vulnerabilidades de seguridad y sigan presentando informes periódicos sobre seguridad de las telecomunicaciones/TIC al Grupo Asesor de Normalización de las Telecomunicaciones (GANT);

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, como el JTC 1 de la ISO/CEI, la Organización de Cooperación y Desarrollo Económicos (OCDE), la Cooperación Económica Asia-Pacífico sobre Telecomunicaciones e Información (APEC-TEL) y el Grupo Especial sobre Ingeniería de Internet (IETF); y

10 que las Comisiones de Estudio del UIT-T aborden el tema de la gestión de amenazas de seguridad que cubra las funciones y responsabilidades de los proveedores de equipos, de software y de servicios, así como de los usuarios finales, con el fin de garantizar que la gestión de ciberamenazas sea eficaz y ofrezca una clara responsabilidad multipartita en la mitigación de las amenazas a la cibersiguridad;

11 que la Comisión de Estudio 17 prosiga su labor respecto de los medios técnicos para la seguridad de las redes TIC, en particular las cuestiones pertinentes planteadas en la Resolución 130 (Rev. Busán, 2014),

encarga al Director de la Oficina de Normalización de las Telecomunicaciones

1 que prepare, 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 dirigidas a fomentar, en la medida de lo posible, la armonización a escala mundial de las estrategias y enfoques adoptados en esta esfera fundamental;

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 TIC, como se especifica en la Resolución 130 (Rev. Busán, 2014);

3 que publique el informe anual sobre los progresos logrados en las actividades del "Plan de normalización de la seguridad de las TIC" al Consejo de la UIT como se especifica en la Resolución 130 (Rev. Busán, 2014) y evalúe la eficacia de los trabajos en curso y planifique los futuros trabajos, orientación u hoja de ruta;

4 que siga reconociendo el papel que desempeñan otras organizaciones con experiencia y competencia técnica en el ámbito de las normas sobre seguridad, y se coordine con ellas según proceda;

5 que prosiga la realización y el seguimiento de las actividades pertinentes de la CMSI sobre la creación de confianza y seguridad en el uso de las TIC, en colaboración con otros Sectores de la UIT y en cooperación con las partes interesadas correspondientes como manera de compartir a escala mundial la información sobre iniciativas de ciberseguridad nacionales, regionales, internacionales y no discriminatorias; y

6 que coopere con la BDT en relación con cualquier tema que afecte a la ciberseguridad, en particular en la aplicación lo dispuesto en la Resolución 45 (Rev.Dubái, 2014);

7 que continúe colaborando con la Agenda sobre Ciberseguridad Global (GCA) (GCA), según proceda, que entable relaciones y asociaciones, con diversas organizaciones e iniciativas regionales e internacionales referentes a la ciberseguridad;

8 que fomente la colaboración con el UIT-D en el desarrollo de principios y un marco de gestión de la ciberseguridad que sirvan de referencia a los Estados Miembros;

9 identifique y documente las medidas prácticas para fortalecer la seguridad en la utilización de las TIC a nivel internacional, sobre la base de prácticas, directrices y recomendaciones ampliamente aceptadas, que los Estados Miembros pueden optar por aplicar para mejorar su capacidad para combatir las ciberamenazas y los ciberataques, 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,

invita a los Estados Miembros, los Miembros del 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. Busán, 2014) de la Conferencia de Plenipotenciarios, con el fin de mejorar la confianza y seguridad en la utilización de las TIC, a fin de mitigar los riesgos y las amenazas;

2 a cooperar y participar activamente en la aplicación de la presente Resolución y de las medidas asociadas;

3 que trabajen de consuno en la elaboración de normas y directrices sobre la protección contra ciberataques;

4 que utilicen las Recomendaciones UIT-T pertinentes, en particular las Recomendaciones UIT-T y Suplementos de la serie X.

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

1. 1 Este término incluye 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)