Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

ASAMBLEA MUNDIAL DE NORMALIZACIÓN DE LAS TELECOMUNICACIONES

Dubai, 20-29 de noviembre de 2012

Resolución 50 – Ciberseguridad

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

RESOLUCIÓN 50 (REV. DUBAI, 2012)

Ciberseguridad

(Florianópolis, 2004; Johannesburgo, 2008; Dubai, 2012)

La Asamblea Mundial de Normalización de las Telecomunicaciones (Dubai, 2012),

recordando

a) la Resolución 130 (Guadalajara, 2010) 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 174 (Guadalajara, 2010) de la Conferencia de Plenipotenciarios, sobre la función de la UIT respecto a los problemas de política pública internacional asociados al riesgo de utilización ilícita de las TIC;

c) la Resolución 179 (Guadalajara, 2010) de la Conferencia de Plenipotenciarios, sobre el papel de la UIT en la protección de la infancia en línea;

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

e) las Resoluciones 55/63 y 56/121 de la Asamblea General de las Naciones Unidas, por las que se instituyó el marco jurídico para la lucha contra la utilización indebida de las tecnologías de la información con fines delictivos;

f) la Resolución 57/239 de la Asamblea General de las Naciones Unidas sobre creación de una cultura mundial de la ciberseguridad;

g) la Resolución 58/199 de la Asamblea General de las Naciones Unidas, sobre creación de una cultura mundial de la ciberseguridad y protección de las infraestructuras de información esenciales;

h) la Resolución 41/65 de la Asamblea General de las Naciones Unidas, sobre principios relativos a la teledetección de la Tierra desde el espacio exterior;

i) las partes pertinentes de la Resolución 45 (Rev. Hyderabad, 2010) de la Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT);

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

k) la Resolución 58 (Rev. Dubai, 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],

[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.

considerando

a) la importancia vital de la infraestructura de TIC para prácticamente todas los tipos de actividades sociales y económicas;

b) que la red telefónica pública conmutada (RTPC) heredada tiene un determinado nivel intrínseco de propiedades de seguridad debido a su estructura jerárquica y a los sistemas de gestión incorporados;

c) que si no se tiene el debido cuidado en el diseño y la gestión de la seguridad, las redes IP ofrecen una separación limitada entre los componentes de usuario y los componentes de red;

d) que si no se tiene especial cuidado en el diseño y la gestión de la seguridad, las redes heredadas y las redes IP convergentes son potencialmente más vulnerables a la intrusión;

e) que los incidentes cibernéticos provocados por ciberataques, por ejemplo las intrusiones malintencionadas o en busca de emociones realizadas utilizando programas informáticos dañinos (como gusanos o virus), se distribuyen por distintos medios, a saber, a través de la web y ordenadores infectados por robots;

f) 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 para protegerse contra distintos efectos adversos y luchar contra ellos; y

g) 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 lo que respecta al *considerando f)*,

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,

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);

b) el *resuelve* de la Resolución 130 (Rev. Guadalajara, 2010) 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, y el encargo de intensificar el trabajo de las Comisiones de Estudio del UIT-T, atribuyéndole gran prioridad;

c) que el Programa 2, sobre ciberseguridad, aplicaciones TIC y cuestiones relacionadas con las redes IP, adoptado por la CMDT-10 (Hyderabad, 2010) incluye la ciberseguridad como una de las actividades prioritarias y principales de las que debe ocuparse la Oficina de Desarrollo de las Telecomunicaciones (BDT), que la Cuestión 22/1 del Sector de Desarrollo de las Telecomunicaciones (UIT-D) trata de la garantía de seguridad en las redes de información y comunicación mediante la identificación de prácticas idóneas para el desarrollo de una cultura de ciberseguridad, y que se adoptó la Resolución 45 (Hyderabad, 2010) de la CMDT, sobre los mecanismos para mejorar la cooperación en materia de ciberseguridad, incluida la lucha contra el correo basura; y

d) 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 están apareciendo ciberataques, como suplantación de identidad (*phishing*), redireccionamiento fraudulento (*pharming*), rastreo/intrusión, ataques de denegación de servicio distribuidos, sustitución de páginas web (*web-facements*), acceso no autorizado, etc., que tienen graves consecuencias;

b) que las redes robot (*botnet*) se utilizan para realizar ciberataques y difundir programas informáticos malignos basados en robot (*bot-malware*);

c) que en ocasiones resulta difícil identificar las fuentes de los ataques (por ejemplo, los ataques realizados desde direcciones IP de origen falsificadas);

d) que la ciberseguridad es uno de los elementos que permiten crear confianza y seguridad en el uso de las telecomunicaciones/TIC;

e) que, conforme a lo dispuesto en la Resolución 181 (Guadalajara, 2010) de la Conferencia de Plenipotenciarios, se reconoce que es importante estudiar la cuestión de la terminología relacionada con la creación de confianza y seguridad en el uso de las TIC, que esta cuestión básica ha de incluir otras importantes además de la ciberseguridad, y que tal vez sea necesario modificar cada cierto tiempo la definición de ciberseguridad para tomar en consideración los cambios en las políticas;

f) que en la Resolución 181 (Guadalajara, 2010) se decidió tener en cuenta la definición del término ciberseguridad aprobado en la Recomendación UIT-T X.1205 para emplearla en las actividades de la UIT relacionadas con la creación de confianza y seguridad en el uso de las TIC;

g) que, tal y como se reconoce en la Resolución 181 (Guadalajara, 2010), la Comisión de Estudio 17 del UIT-T se encarga de elaborar las principales Recomendaciones sobre seguridad de las telecomunicaciones y las TIC,

observando

a) la pujante actividad y el interés de la Comisión de Estudio 17, Comisión de Estudio Rectora en materia de seguridad, 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 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; y

d) que, como se reconoce en la Resolución 130 (Rev. Guadalajara, 2010), la Comisión de Estudio 17 está examinando la creación de un centro de seguridad de las redes IP públicas nacionales para los países en desarrollo, y se han completado algunos trabajos al respecto, incluidas las Recomendaciones de la serie UIT-T X.800 – X.849 y sus Suplementos,

resuelve

1 que todas las Comisiones de Estudio del UIT-T sigan evaluando las Recomendaciones existentes y en curso de elaboración, y especialmente las Recomendaciones sobre señalización y protocolos de telecomunicaciones, en lo que se refiere a la robustez de su diseño y a su posible explotación por grupos malintencionados con el fin de interferir destructivamente en su implantación en la infraestructura mundial de información y las telecomunicaciones, elaboren Recomendaciones sobre nuevas cuestiones de seguridad y tengan en cuenta los nuevos servicios y aplicaciones que debe soportar la infraestructura mundial de telecomunicaciones/TIC (por ejemplo, computación en la nube, redes eléctricas inteligentes y sistemas de transporte inteligentes, que se basan en redes de telecomunicaciones/TIC);

2 que el UIT-T siga, en su esfera de operación e influencia, con 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;

3 que el UIT-T colabore estrechamente con el UIT-D, en especial en lo tocante a la Cuestión 22/1;

4 que se tomen en consideración y se apliquen, cuando sea necesario, las Recomendaciones UIT-T, incluidas las Recomendaciones de la serie UIT-T X y sus Suplementos, entre otras la UIT-T X.805, la UIT-T X.1205 y la UIT-T X.1500, las normas de la ISO/CEI y cualquier otro producto pertinente de otras organizaciones, a la hora de evaluar las vulnerabilidades de seguridad de las redes y los protocolos, y facilitar el intercambio de información sobre ciberseguridad;

5 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;

6 que se invite a las partes concernidas a trabajar de consuno en la elaboración de normas y directrices sobre la protección contra ciberataques, y para facilitar el rastreo del origen de un ataque;

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 todas las Comisiones de Estudio del UIT-T sigan presentando informes periódicos sobre seguridad de las telecomunicaciones/TIC al Grupo Asesor de Normalización de las Telecomunicaciones (GANT) sobre la evolución de la evaluación de las Recomendaciones nuevas, existentes y en curso de elaboración;

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 la Comisión de Estudio 17 prosiga su labor respecto de las cuestiones planteadas en la Resolución 130 (Rev. Guadalajara, 2010), así como de las Recomendaciones de la serie UIT-T X, incluidos los Suplementos, según proceda,

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 informe cada año al Consejo de la UIT, según lo dispuesto en la Resolución 130 (Rev. Guadalajara, 2010) de la Conferencia de Plenipotenciarios, sobre los progresos en la aplicación de las medidas señaladas; y

3 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,

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

1 que prosiga el seguimiento de las actividades de la CMSI sobre la creación de confianza y seguridad en el uso de las TIC, 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

2 que coopere con la BDT en relación con cualquier tema que afecte a la ciberseguridad, de conformidad con lo dispuesto en la Resolución 45 (Rev. Hyderabad, 2010);

3 que continúe cooperando con la Agenda sobre Ciberseguridad Global (GCA) del Secretario General (GCA) y con UIT-IMPACT, FIRST y otros proyectos mundiales o regionales de ciberseguridad, según proceda, que entable relaciones y asociaciones, según el caso, con diversas organizaciones e iniciativas regionales e internacionales referentes a la ciberseguridad, e invite a todos los Estados Miembros, en especial a los países en desarrollo, a que tomen parte en las actividades, garantizando la cooperación y coordinación entre estas diversas actividades; y

4 que, teniendo en cuenta la Resolución 130 (Rev. Guadalajara, 2010), trabaje en colaboración con los Directores de las demás Oficinas para apoyar al Secretario General en la preparación de un documento relativo a un posible Memorándum de Entendimiento (MoU) (de conformidad con lo dispuesto en la Resolución 45 (Rev. Hyderabad, 2010) entre los Estados Miembros interesados para fortalecer la ciberseguridad y combatir las ciberamenazas con objeto de proteger a los países en desarrollo y a cualquier país interesado en adherirse a este posible MoU,

invita a los Estados Miembros, los Miembros del Sector, los Asociados y las instituciones académicas, según corresponda

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