Cuestión 22-1/1: Garantía de seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad

1 Exposición de la situación

vistos

a) el crecimiento explosivo del desarrollo y la utilización de las redes de tecnología de la información y la comunicación (TIC);

b) que cada vez son más frecuentes los ataques contra la ciberseguridad y no hay medidas que permitan eficazmente detenerlos;

c) la necesidad de garantizar la seguridad de estas infraestructuras interconectadas mundialmente, si se desea que la sociedad de la información rinda su potencial;

d) el creciente reconocimiento en el plano nacional, regional e internacional de la necesidad de definir y promover mejores prácticas, normas, directrices técnicas y procedimientos para reducir la vulnerabilidad y los riesgos que pesan sobre las TIC;

e) la necesidad de tomar medidas a nivel nacional y de cooperar en los planos regional e internacional para constituir una cultura mundial de ciberseguridad que incluya entre otros: la coordinación nacional, las infraestructuras jurídicas nacionales adecuadas, las capacidades de vigilancia, alerta y recuperación, las asociaciones entre el gobierno y la industria, y la información ofrecida a la sociedad civil y los consumidores;

f) la necesidad de aplicar un enfoque multipartito para aprovechar las diversas herramientas disponibles a fin de aumentar la confianza en la utilización de las redes TIC;

g) que en la Resolución 57/239 de la Asamblea General de las Naciones Unidas sobre la "Creación de una cultura mundial de ciberseguridad", se invita a los Estados Miembros a "promover en todas sus sociedades una cultura de seguridad cibernética en la aplicación y utilización de las tecnologías de la información";

h) que las prácticas óptimas en ciberseguridad deben proteger y respetar los derechos de privacidad y libertad de expresión establecidos en las partes pertinentes de la Declaración Universal de Derechos Humanos, la Declaración de Principios de Ginebra y otros instrumentos internacionales pertinentes relativos a los derechos humanos;

i) que en la Declaración de Principios de Ginebra se señala que "se debe fomentar, desarrollar y poner en práctica una cultura global de la ciberseguridad, en cooperación con todas las partes interesadas y los organismos internacionales especializados", y que el Plan de Acción de Ginebra alienta a compartir las prácticas óptimas y tomar las medidas adecuadas contra el spam a nivel nacional e internacional y que en el Programa de Acciones de Túnez se reafirma la necesidad de contar con una cultura mundial de ciberseguridad, especialmente en la Línea de Acción C5 (Creación de confianza y seguridad en la utilización de las TIC);

j) Que la CMSI Túnez 2005 pidió en su Agenda a la UIT que ejerciese de facilitador/moderador único para la puesta en aplicación y el seguimiento de la Línea de Acción C5 "**Creación de confianza y seguridad en la utilización de las TIC**". Asumiendo tal responsabilidad y en respuesta a las Resoluciones pertinentes adoptadas por la CMDT (Doha, 2006), previendo que se actualizarán en Hyderabad este año, por la PP-06 (Antalya, 2006) y la AMNT-08 (Johannesburgo, 2008), el UIT-T, el UIT-R, el UIT-D y la Secretaría General han llevado a cabo numerosos estudios a fin de mejorar la ciberseguridad;

k) Los resultados de la CMSI, tanto de Ginebra 2003 como de Túnez 2005, piden que se cree confianza y seguridad en la utilización de las TIC;

l) que la Resolución 45 [(Hyderabad, 2010)] de la Conferencia Mundial de Desarrollo de las Telecomunicaciones apoya mejorar la ciberseguridad entre los Estados Miembros interesados;

m) que en coherencia con su mandato, la UIT debe desempeñar un papel fundamental para agrupar a los Estados Miembros, Miembros de Sector y otros expertos a fin de que compartan experiencias sobre la seguridad de las redes TIC;

n) Los excelentes resultados de la Cuestión 22/1 (Prácticas óptimas para la ciberseguridad), reproducidos en su Informe Final para el periodo 2006-2009, Documento 1/249(Rev.1), justifican la continuación de esta Cuestión durante un nuevo ciclo, con una orientación distinta que tenga en cuenta las necesidades de los países en desarrollo;

o) que se han desplegado importantes esfuerzos encaminados a facilitar la mejora de la seguridad de la red, incluidas la labor de los Estados Miembros y de los Miembros de Sector en las actividades de normalización en el UIT-T y en la elaboración de informes sobre prácticas óptimas en el UIT-D; la labor de la Secretaría General en relación con la Agenda sobre Ciberseguridad Global; y el trabajo realizado por el Sector de Desarrollo de la UIT en relación con sus actividades de capacitación dentro del Programa 3;

p) que los gobiernos de los países en desarrollo, los proveedores de servicios y los usuarios finales se enfrentan a retos peculiares a la hora de elaborar políticas y métodos de seguridad adecuados a sus circunstancias;

q) que los Estados Miembros y los operadores de la infraestructura se beneficiarían de Informes adicionales que detallen los diversos recursos, estrategias y herramientas disponibles para crear confianza en la utilización de las redes TIC y en el papel de la cooperación internacional a este respecto.

2 Cuestión de estudio

a) Actualizar los resultados del pasado ciclo de estudios teniendo en cuenta las necesidades de los países en desarrollo e incorporando los resultados de la UIT en su conjunto (resultados pertinentes de las CE 17 y 13 del UIT-T, del programa especial sobre ciberseguridad de la BDT, de las actividades de la Secretaría General en el seguimiento de la Línea de Acción C5 y del Grupo de Expertos de Alto Nivel (GEAN), que recibió el apoyo de todos los expertos de los países en desarrollo), así como los trabajos realizados al respecto por la ISO/CEI. Esta revisión tomará asimismo en consideración los progresos realizados por el proyecto "IMPACT", del que ya son miembros muchos países en desarrollo;

b) Durante el próximo periodo de estudios, a fin de ampliar la información contenida en el Informe de Prácticas Óptimas Fase I relativo a: 1) desarrollo de una estrategia nacional de ciberseguridad; 2) desarrollo de asociaciones públicas/privadas; 3) creación de un sistema de gestión nacional de ciberincidentes con capacidad para desarrollar mecanismos de vigilancia, alerta y respuesta a estos incidentes y mecanismos de recuperación; 4) desarrollo

de una cultura de sensibilización; y 5) identificación de las prácticas óptimas para protegerse contra el spam, el malware y otras ciberamenazas:

i) Con respecto a la elaboración de una estrategia nacional sobre ciberseguridad, (a) elaborar modelos para la gestión nacional de la ciberseguridad, (b) identificar los modelos organizativos que han seguido los países y las técnicas que han utilizado para elaborar una estrategia nacional, sacando provecho de su experiencia, en particular de los modelos empleados por la OCDE o de cualquier otro modelo recomendado en Europa.

ii) Con respecto a las asociaciones públicas/privadas, elaborar 1) los principios para establecer asociaciones sólidas del sector público/sector privado; 2) varios modelos estructurales para lograr esas asociaciones sólidas del sector público/sector privado; y 3) el concepto de reducción del riesgo con respecto a dichas asociaciones sector público/sector privado y el papel que ha de cumplir cada uno de ellos.

iii) Con respecto a la creación de una capacidad de gestión nacional de incidentes sobre ciberseguridad, elaborar el desarrollo de mecanismos de vigilancia, alerta y respuesta y recuperación, y el establecimiento de equipos nacionales de respuesta a incidentes relativos a la seguridad informática.

iv) A partir de los estudios ya realizados por la CE 17 del UIT-T sobre la ampliación de los centros nacionales para abordar todos los aspectos de la ciberseguridad en general, y no sólo Internet, así como el producto de los correspondientes programas del UIT-D relacionados con los EIII, preferiblemente ajustándose a las necesidades propias de las seis regiones de la BDT, sin olvidar que quizá la práctica idónea a este respecto sea la creación de un modelo único para todos los países en desarrollo[5].

v) Con respecto al desarrollo de una cultura de sensibilización en materia de ciberseguridad, recoger ideas de todas las fuentes sobre la forma en que los países, las empresas y los Grupos de Expertos están formando y alentando a las personas y a las entidades sobre el tema de la ciberseguridad, incluidas la protección de los niños en línea y las necesidades de las personas con discapacidad en el ámbito de la ciberseguridad.

vi) Con respecto a la identificación de las prácticas óptimas y estrategias para protegerse contra el correo basura (spam) y el software malicioso: 1) examinar e identificar los esfuerzos educativos nacionales a nivel de usuario y de empresa para ayudar a mantener la confianza del usuario mediante la prevención y reducción del spam y el software malicioso; 2) tras examinar el cometido de la organizaciones gubernamentales y no gubernamentales a la hora de promover la prevención del spam y el software malicioso, incluida la consideración de sus respectivas prácticas óptimas, directrices y códigos de conducta; 3) examinar los métodos utilizados para educar a los usuarios finales sobre los riesgos asociados a los esquemas de usurpación de identidad, redes robot (botnets), virus y otros contenidos maliciosos que puede contener el spam así como las medidas preventivas utilizadas y 4) examinar las perspectivas sobre los mecanismos empleados para mejorar la ciberseguridad e identificar la información, capacidades, herramientas y mecanismos de que se dispone para las actividades comerciales y otros usuarios finales.

---

[5] NOTA – Pendiente de la aprobación por parte de la CMDT Hyderabad 2010 de la propuesta de nueva Resolución que insta a los países en desarrollo a crear Equipos de Intervención en caso de Incidentes Informáticos (EIII) nacionales, esta Cuestión responderá a esa Resolución, de aprobarse.

vi) Llevar a cabo los estudios adecuados en las áreas definidas con objeto de identificar las medidas que deben tomar al respecto los países, las empresas y los organismos expertos.

vii) Llevar a cabo los estudios adecuados en las áreas definidas con objeto de identificar las medidas que deben tomar al respecto los países, las empresas y los organismos expertos.

viii) Como resultado de las encuestas realizadas, crear un compendio de todas las prácticas nacionales y/o regionales pertinentes al respecto, incluidas todas las respuestas e información del caso.

ix) Realizar un estudio de la situación/ejercicio de inventario para ofrecer a los Estados Miembros información que les permita contrastar y comparar las diversas políticas en vigor en los Estados Miembros de la UIT.

x) Considerar toda la información disponible sobre estos temas procedentes de una variedad de fuentes, incluidos los interesados pertinentes.

c) Utilizar el Informe de Prácticas Óptimas y otros textos adecuados para elaborar material didáctico sobre los temas identificados en los apartados 2(b)(i)-(v) anteriores a fin de ayudar en el análisis de las estrategias nacionales de ciberseguridad y en la planificación de programas de formación práctica. Este material didáctico podría utilizarse por sí mismo o como parte de talleres de expertos y otros foros.

d) A partir de las contribuciones presentadas, recopilar en un volumen los estudios de caso por país a efectos informativos, describiendo la situación de los países en términos de esfuerzos de ciberseguridad y de sus políticas de ciberseguridad.

e) Elaborar un marco para su aplicación y seguimiento en el marco del Programa 2 de la BDT a fin de sensibilizar a los países en desarrollo en lo que respecta a la ciberseguridad a escala nacional, regional e internacional, en particular:

– La función de los gobiernos, incluido el centro nacional de ciberseguridad.

– La función de los grupos intergubernamentales nacionales, regionales e internacionales.

– La función de los grupos no gubernamentales nacionales, regionales e internacionales.

– etc.

A fin de que la BDT elabore un Plan de Acción para dar a conocer la importancia de la ciberseguridad a todos los niveles en los países en desarrollo.

f) Esta Cuestión podrá participar parcialmente en la aplicación de la nueva Resolución 45 revisada[6].

3 Resultados previstos

1 Informes de los Miembros sobre los temas identificados en el punto 2(b) (i)-(v). Estos Informes reflejarán el hecho de que la seguridad de las redes de información y comunicación es parte integrante de la constitución de la sociedad de la información y del desarrollo económico y social de todas las naciones. Los retos que se plantean en el plano de la ciberseguridad incluyen el posible acceso no autorizado a las redes TIC, así como la destrucción o modificación de la información cursada a través de dichas redes. Sin embargo, las consecuencias de tales desafíos podrían mitigarse aumentando la sensibilización sobre los aspectos de la ciberseguridad y el

---

[6] NOTA – Esta cláusula depende del resultado de la revisión de la Resolución 45 en la CMDT de Hyderabad.

intercambio de las prácticas óptimas fructíferas que adoptan los responsables políticos y las empresas así como colaborando con otras partes interesadas. Asimismo, una cultura de ciberseguridad puede promover la confianza en dichas redes, estimular su utilización segura y garantizar la protección de los datos y la privacidad, sin dejar por ello de fomentar el acceso y el comercio, lo que haría posible que las naciones obtuvieran más adecuadamente los beneficios del desarrollo económico y social que entraña la sociedad de la información.

2 Material docente para su utilización en talleres, seminarios, etc.

4 Calendario

Se propone que este estudio dure cuatro años y que se preparen Informes preliminares sobre la marcha de los trabajos después de los 12, 24 y 36 meses de dicho periodo.

5 Autor de la propuesta

Comisión de Estudio 1 del UIT-D, CITEL, Estados Árabes.

6 Origen de las aportaciones

a) Estados Miembros y Miembros de Sector.

b) Trabajos sobre el particular realizados por las Comisiones de Estudio del UIT-T y del UIT-R.

c) Resultados pertinentes de las organizaciones internacionales y regionales, incluidas la ISO y la OCDE.

d) Organizaciones no gubernamentales pertinentes interesadas en la promoción de la ciberseguridad y la cultura de la seguridad.

e) Estudios, recursos en línea.

f) Otras fuentes, si se estima oportuno.

7 Destinatarios de los resultados

	Países desarrollados	**Países en desarrollo**[7]
Encargados de la formulación de políticas de telecomunicaciones	Sí	Sí
Reguladores de las telecomunicaciones	Sí	Sí
Proveedores/operadores de servicios	Sí	Sí
Fabricantes	Sí	Sí

[7] El término "países en desarrollo" incluye también a los países menos adelantados (PMA), los pequeños Estados insulares en desarrollo (PEID), los países en desarrollo sin litoral (PDSL) y los países con economías en transición.

a) Destinatarios

Formuladores de políticas nacionales y Miembros de Sector, así como otros interesados que participan en actividades de ciberseguridad o están a cargo de las mismas, especialmente de los países en desarrollo.

b) Métodos propuestos para aplicar los resultados

Puesto que el programa se consagra a reunir información y ejemplos de prácticas óptimas, tiene esencialmente un carácter informativo y puede utilizase para sensibilizar a los Estados Miembros y Miembros de Sector en materia de ciberseguridad y señalar a la atención las informaciones, instrumentos y prácticas óptimas disponibles, cuyos resultados podrán utilizarse en combinación con seminarios y talleres organizados por la BDT.

8 Métodos propuestos para abordar la Cuestión

La Cuestión se tratará en la Comisión de Estudio 1 durante un periodo de estudios de cuatro años (incluida la presentación de resultados provisionales) y será gestionada por un Relator y sus Vicerrelatores. Ello permitirá a los Estados Miembros y Miembros del Sector contribuir con sus experiencias y lecciones aprendidas con respecto a la ciberseguridad.

9 Coordinación

Es necesaria la coordinación con el UIT-T, en particular con la CE 17 o su sucesora. Teniendo en cuenta el actual nivel de conocimientos técnicos sobre el tema en la CE 17 del UIT-T, todos los documentos (cuestionarios, Informes provisionales, proyectos de Informes Finales, etc.) deben enviarse a la CE 17 recabando comentarios y contribuciones antes de presentar dicho documento a la CE del UIT-D para sus comentarios y aprobación.

10 Vínculo con el programa de la BDT

Programa 2 del UIT-D.

_____