CUESTIÓN 3/2

Seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de la ciberseguridad

1 Exposición de la situación o el problema

La seguridad en las redes de información y comunicación y el fomento de una cultura de la ciberseguridad son hoy en día fundamentales por una serie de razones, entre las que se cuentan las siguientes:

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

b) que la ciberseguridad continúa siendo una preocupación para todos y por ello es necesario prestar asistencia a los países, en particular a los países en desarrollo, para proteger sus redes de telecomunicaciones/TIC contra ciberataques y amenazas;

c) la necesidad de esforzarse por garantizar la seguridad en 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 prácticas idóneas, normas, directrices técnicas y procedimientos para reducir las vulnerabilidades y los riesgos que pesan sobre las TIC;

e) la necesidad de tomar medidas a escala 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) el hecho de que en la Resolución 68/167 de la Asamblea General de las Naciones Unidas sobre "El derecho a la privacidad en la era digital", se afirma, entre otras cosas, que los derechos de las personas también deben estar protegidos en Internet, incluido el derecho a la privacidad;

i) 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, adoptada por la Cumbre Mundial sobre la Sociedad de la Información (CMSI) y otros instrumentos internacionales pertinentes relativos a los derechos humanos;

j) 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 la Agenda de Túnez para la sociedad de la información se reafirma la necesidad de contar con una cultura mundial de ciberseguridad, especialmente en el marco de la Línea de Acción C5 (Creación de confianza y seguridad en la utilización de las TIC);

k) que la CMSI (Túnez 2005) pidió en su Agenda a la UIT que ejerciese de facilitador/moderador principal 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 Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT) (Doha, 2006 e Hyderabad, 2010), por la Conferencia de Plenipotenciarios (Antalya, 2006 y Guadalajara, 2010) y por la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT) (Johannesburgo, 2008 y Dubái, 2012), 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;

l) que en los resultados de la CMSI, tanto de la fase de Ginebra 2003 como de la de Túnez 2005, se pide que se cree confianza y seguridad en la utilización de las TIC;

m) que la Resolución 45 (Rev. Dubái, 2014) de la CMDT refrenda mejorar la ciberseguridad entre los Estados Miembros interesados;

n) que en virtud de su mandato, el UIT-D debe desempeñar un papel fundamental para reunir a Estados Miembros, Miembros de Sector y otros expertos para que compartan experiencias sobre la seguridad en las redes TIC;

o) los excelentes resultados de la Cuestión 22-1/1 durante el último periodo de estudios, que incluyen numerosos informes y contribuciones de todo el mundo;

p) 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 en programa revisado y, en ciertos casos, por expertos de todo el mundo;

q) que los gobiernos, los proveedores de servicios y los usuarios finales, especialmente en los países menos adelantados (PMA), se enfrentan a retos peculiares a la hora de elaborar políticas y métodos de seguridad adecuados a sus circunstancias;

r) 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;

s) que el correo basura continua siendo un asunto preocupante;

t) las metodologías en constante evolución sobre pruebas de criterios comunes para las redes de telecomunicaciones;

u) la necesidad de establecer procedimientos de prueba simplificados a un nivel básico para las pruebas de seguridad de las redes de telecomunicaciones a fin de promover una cultura de seguridad.

2 Cuestión o asunto que ha de estudiarse

a) considerar enfoques y mejores prácticas para evaluar el impacto del correo basura dentro de una red, y ofrecer las medidas necesarias, tales como técnicas de mitigación, que los países en vías de desarrollo puedan utilizar, teniendo en cuenta las normas existentes y las herramientas disponibles;

b) facilitar información sobre dificultades actuales en materia de ciberseguridad que experimentan los proveedores de servicios, los organismos reguladores y otras partes interesadas;

c) continuar recabando experiencias nacionales de los Estados Miembros en ciberseguridad e identificar y analizar los temas en común entre estas experiencias;

d) seguir analizando los resultados de la encuesta de sensibilización sobre ciberseguridad realizada durante el último periodo de estudio, y distribuir una encuesta actualizada a fin de medir el progreso con el transcurso del tiempo;

e) ofrecer un compendio de las actividades de ciberseguridad en curso relevantes que estén llevando a cabo los Estados Miembros, organizaciones, el sector privado y la sociedad civil a nivel nacional, regional e internacional, en el cual podrán participar los países en desarrollo y todos los sectores, incluida la información recabada con arreglo al inciso c) anterior;

f) examinar las necesidades especiales de las personas con discapacidades de forma coordinada con otras Cuestiones relevantes;

g) examinar los medios para asistir a los países en desarrollo, haciendo hincapié en los países menos adelantados (PMA), en lo que concierne a las dificultades en materia de ciberseguridad;

h) seguir recabando experiencias y necesidades nacionales en el campo de protección de la infancia en línea, de forma coordinada con otras actividades relevantes;

i) organizar reuniones, seminarios y talleres ad hoc para intercambiar conocimientos, información y prácticas óptimas relativos a las medidas y actividades eficientes, eficaces y de utilidad para mejorar la ciberseguridad teniendo en cuenta los resultados del estudio que se celebrarán simultáneamente, en la medida de lo posible, con las

reuniones de la Comisión de Estudio 1 o las reuniones del Grupo de Relator para la Cuestión;

j) recopilar ciertas experiencias y necesidades nacionales sobre criterios comunes y pruebas de seguridad que facilitarán el desarrollo de un marco y de directrices que podrían acelerar las pruebas de seguridad de los equipos de telecomunicaciones, en colaboración con las Comisiones de Estudio del UIT-T pertinentes y otras organizaciones de normalización (SDO), llegado el caso, y teniendo en cuenta la información y materiales disponibles en esas entidades.

3 Resultados previstos

1 Informes de los Miembros sobre los temas identificados en los § 2 *a)* a 2 *j)*. 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 y la prevención y la lucha contra el correo basura. Sin embargo, las consecuencias de tales desafíos podrían mitigarse aumentando la sensibilización sobre los aspectos de la ciberseguridad, la creación de asociaciones efectivas entre el sector público y el privado, y el 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.

3 Recopilación de conocimientos, información y prácticas idóneas sobre actividades y medidas eficaces, eficientes y útiles para garantizar la ciberseguridad en los países en desarrollo como resultado de reuniones, seminarios y talleres ad hoc.

4 Plazos

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 Autores/patrocinadores de la propuesta

Comisión de Estudio 1 del UIT-D, Estados Árabes, Propuesta Interamericana, Japón, República Islámica del Irán.

6 Origen de las contribuciones

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.

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

e) Estudios, recursos en línea.

f) Expertos en el ámbito de la ciberseguridad.

g) Otras fuentes, si se estima oportuno.

7 Destinatarios

Destinatarios	Países desarrollados	Países en desarrollo[1]
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

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 utilizarse 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 reuniones, seminarios y talleres ad hoc organizados por la BDT.

8 Métodos propuestos para abordar la Cuestión o el asunto

La Cuestión se tratará en una Comisión de Estudio 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.

---

[1] El término "países en desarrollo" comprende 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.

9 Coordinación

Es necesaria la coordinación con el UIT-T, en particular con la Comisión de Estudio 17 o su sucesora, de la Cuestión 20 del UIT-D sobre las personas con discapacidad, así como con las demás organizaciones relevantes, tales como FIRST, IMPACT, APCERT, OEA, CICTE, OCDE, RIR, ONG, M3AAWG, y otras. Teniendo en cuenta el actual nivel de conocimientos técnicos sobre el tema en estos grupos, todos los documentos (cuestionarios, Informes provisionales, proyectos de Informes Finales, etc.) deben enviárseles recabando comentarios y contribuciones antes de presentar dicho documento a la CE del UIT-D para sus comentarios y aprobación.

10 Vínculo con los Programas de la BDT

El Programa de la BDT del Resultado 3.1 del Objetivo 3 facilitará el intercambio de información y utilizará las contribuciones, según corresponda, para cumplir con los objetivos del programa y las necesidades de los Estados Miembros.

11 Otra información pertinente

–