|  |  |  |
| --- | --- | --- |
| C:\Users\ponder\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\BDT-25th_anniversary_2017-Logo_411959-3_transparent.png | **Conferencia Mundial de Desarrollo de las Telecomunicaciones 2017 (CMDT-17)****Buenos Aires, Argentina, 9-20 de octubre de 2017** | C:\Users\murphy\Documents\WTDC17\bd_S_25Years_Horizontal-411959.jpg |
|  |  |
| **SESIÓN PLENARIA** | **Documento WTDC-17/36-S** |
|  | **8 de septiembre de 2017** |
|  | **Original: español** |
| Brasil (República Federativa del)/México |
| Propuestas para los trabajos de la Conferencia |
|  |
|  |
| **Área prioritaria:** - Cuestiones de las Comisiones de Estudio**Resumen:**Modificación a la Cuestión de Estudio 3/2 del UIT-D “Seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de la ciberseguridad”**Resultados previstos:**Brasil y México invitan a todas las delegaciones de la WTDC-17 para considerar el documento en la discusión de la revisión de la Cuestión de Estudio 3/2, tanto en sus fundamentos como en sus términos.**Referencias:**Cuestión 3/2 |

COMISIÓN DE ESTUDIO 2

**MOD** B/MEX/36/1

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

El uso de las telecomunicaciones y las tecnologías de la información y la comunicación han tenido invaluables usos que fomentan el desarrollo y crecimiento social y económico de manera global. A pesar de todos los beneficios y utilidades que ofrecen estas tecnologías, existen también riesgos y amenazas de seguridad. Desde las finanzas personales hasta las operaciones de negocios, las infraestructuras nacionales, los servicios públicos y privados se gestionan cada vez más a través de alguna red de información y comunicación, y por lo tanto, son más vulnerables a algún tipo de ataque.

Para la construcción de la confianza en la utilización y aprovechamiento de las telecomunicaciones/TIC para todo tipo de aplicaciones y contenidos, sobre todo para aquellos que conllevan un importante impacto positivo en los aspectos económico y social por parte de todos los actores que inciden en la privacidad, protección de datos personales, seguridad de redes, y el propio usuario de las mismas; se requiere una intensa colaboración entre autoridades nacionales, autoridades extranjeras, industria, academia y usuarios.

Con base en lo anterior, 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)la necesidad de tomar medidas a escala nacional, regional e internacional, así como el aplicar un enfoque multipartito, 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;

e)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";

f) el hecho de que en las Resoluciones 68/167, 69/166 y 71/199 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;

g) 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;

h)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);

i)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;

j) que 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 los resultados de la CMSI, afirma que fomentar la confianza y la seguridad en el uso de la información y las comunicaciones debe ser una prioridad, sobre todo teniendo en cuenta los crecientes desafíos, incluido el uso indebido de esas tecnologías para actividades nocivas, desde el acoso, la delincuencia y el terrorismo; Y debe ser coherente con los derechos humanos;

k) que de acuerdo a la Declaración de la CMSI+10 relativa a la aplicación de los resultados de la CMSI, los gobiernos y todas las partes interesadas pertinentes son conscientes de que se necesita una mayor colaboración para solventar los problemas de fiabilidad, seguridad, privacidad y protección de datos personales, seguridad y confianza en la utilización de las TIC;

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

m) que la Resolución 130 (Rev. Busán, 2014) de la PP resuelve continuar promoviendo 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;

n) que la Resolución 50 (Rev. Hammamet, 2016) de la AMNT resalta la necesidad de fortalecer y defender los sistemas de información y telecomunicaciones contra ciberamenzas y ciberataques, y se siga fomentando la cooperación entre las organizaciones internacionales y regionales correspondientes a efecto de aumentar el intercambio de información técnica en el campo de la seguridad de las redes de información y telecomunicaciones;

o) las conclusiones y recomendaciones del Reporte final de la cuestión 3/2 de la IUT-D del Grupo de estudio 2 para considerar en el siguiente estudio un ciclo de estudio sobre las amenazas en evolución y emergentes más allá del spam y el malwatre;

p)que se han desplegado importantes esfuerzos encaminados a facilitar la mejora de la seguridad de la red, como 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 el correo basura continua siendo un asunto preocupante, aunque es necesario estudiar las amenazas evolutivas y emergentes;

s) 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) fomentar la integridad de los sistemas TIC, que es esencial para su desarrollo continuo;

b) considerar enfoques y mejores prácticas para evaluar el impacto del correo basura dentro de una red, así como las amenazas en evolución y emergentes, y ofrecer las medidas y lineamientos necesarios, tales como técnicas de mitigación, legislación y medidas reglamentarias que los países en vías de desarrollo puedan utilizar, teniendo en cuenta las normas existentes y las herramientas disponibles;

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

d) continuar recabando experiencias nacionales de los Estados Miembros en ciberseguridad, privacidad y protección de la infancia en línea e identificar y analizar los temas en común entre estas experiencias y con esta información, diseñar directrices que permitan a los Estados Miembros elaborar mecanismos efectivos en materia de seguridad y privacidad en el entorno digital;

e) analizar los desafíos en ciberseguridad planteados para IoT, inteligencia artificial u otras tecnologías emergentes, así como medidas para hacer frente a dichos desafíos;

f) discutir perspectivas y mejores prácticas sobre la protección a la privacidad y datos personales;

g)promover la sensibilización y la creación de capacidades de los usuarios sobre la protección de datos, la privacidad y la ciberseguridad;

h) 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;

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

j) 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;

k) fomentar la cooperación entre los actores involucrados, con el fin de 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, aumentar la confianza y proteger los datos y la integridad de la red, considerando los riesgos actuales y potenciales para las TIC, 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;

l) trabajar 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;

m) desarrollar directrices que faciliten el establecimiento de medidas a nivel nacional, regional e internacional para combatir el envío masivo de mensajes electrónicos no solicitados;

n) recopilar las experiencias nacionales sobre la regulación y/o las políticas implementadas por la las autoridades regulatorias en telecomunicaciones con el fin de fomentar la confianza y la seguridad en el uso de las telecomunicaciones /TIC,

# 3 Resultados previstos

1) Informes de los Miembros sobre los temas identificados en los § 2 *a)* a 2 *n)*. 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) Recomendaciones que faciliten a los miembros el establecimiento de medias pertinentes para crear mayor confianza y seguridad en el uso de las TIC.

# 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) Indice Global de Seguridad Cibernética - GCI (Global Cybersecurity Index).

h) Otras fuentes, si se estima oportuno.

# 7 Destinatarios

| Destinatarios | Países desarrollados | Países en desarrollo[[1]](#footnote-1)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 |
| Academia  | 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.

# 9 Coordinación

Es necesaria la coordinación con el UIT-T, en particular con la Comisión de Estudio 17 relativa a la seguridad, encargada de la creación de confianza y seguridad en el uso de las tecnologías de la información y la comunicación, así como con las demás organizaciones relevantes, tales como FIRST, IMPACT, APCERT, OEA, CICTE, OCDE, APEC, RIR, ONG, M3AAWG, UCENET 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 enviarse al 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 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

–

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

1. 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. [↑](#footnote-ref-1)