|  |  |  |  |
| --- | --- | --- | --- |
|  | **Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT-24)**  Nueva Delhi, 15-24 de octubre de 2024 | |  |
|  | | | |
|  | |  | |
| SESIÓN PLENARIA | | Addéndum 13 al Documento 37-S | |
|  | | 22 de septiembre de 2024 | |
|  | | Original: inglés | |
|  | | | |
| Administraciones miembros de la Telecomunidad Asia-Pacífico | | | |
| PROPUESTA DE MODIFICACIÓN DE LA rESOLUCIÓN 58 | | | |
|  | | | |
|  | | | |

|  |  |  |
| --- | --- | --- |
| **Resumen:** | Dado que las ciberamenazas y los ciberataques a las infraestructuras mundiales de telecomunicaciones/TIC no cesan de crecer y evolucionar, es necesario contar con capacidades adecuadas de respuesta ante emergencias de ciberseguridad en todos los países. En consecuencia, el papel de los equipos de intervención en caso de incidente informático (EIII) ha adquirido una importancia sin precedentes. El presente documento contiene una propuesta de modificación de la Resolución 58 de la AMNT. | |
| **Contacto:** | Sr. Masanori Kondo  Secretario General Telecomunidad Asia-Pacífico | Correo-e: [aptwtsa@apt.int](mailto:aptwtsa@apt.int) |

Introducción

Las ciberamenazas y los ciberataques evolucionan al ritmo de los servicios y las tecnologías de la infraestructura de telecomunicaciones/TIC. Las ciberamenazas no sólo pueden propagarse a través de ordenadores, sino también de dispositivos móviles, servidores, redes e incluso tecnología operativa. Por su parte, los ciberataques se centran cada vez más en infraestructuras de telecomunicaciones/TIC críticas y datos importantes.

Con el rápido aumento del volumen, la gravedad y la sofisticación de las ciberamenazas y los ciberataques, el tema de la seguridad sigue suscitando preocupación en todo el mundo y es necesario ayudar a los países, en particular a los países en desarrollo, a proteger sus redes de telecomunicaciones/TIC contra esos ciberataques y ciberamenazas. La labor de los equipos de intervención en caso de incidente informático (EIII) es fundamental para responder a los incidentes de forma adecuada y debería reforzarse. Sin embargo, muchos países siguen adoleciendo de un bajo nivel de preparación frente a incidentes de ciberseguridad, véanse en especial los países en desarrollo. De ahí la importancia de crear EIII a escala nacional y fomentar el intercambio de información y la colaboración entre los gobiernos y otras partes interesadas para dar respuesta a estos incidentes de ciberseguridad. Con miras a facilitar la creación de EIII y promover el marco operativo correspondiente, podrían elaborarse Recomendaciones y Suplementos de la índole de la Recomendación UIT-T X.1060, relativa al marco para la creación y operación de un centro de ciberdefensa, que ofrece directrices encaminadas a garantizar que las organizaciones cuenten con las capacidades de ciberdefensa necesarias, así como con unos servicios de seguridad eficaces, incluida la respuesta a incidentes de ciberseguridad.

La AMNT-20 actualizó la Resolución 58, en la que se aborda la apremiante necesidad de crear EIII nacionales en todos los países, poniendo especial atención a la reducción de la brecha de ciberseguridad entre los países desarrollados y en desarrollo. Esta Resolución pretende reflejar la última revisión de la Resolución 130 (Rev. Bucarest, 2022) de la Conferencia de Plenipotenciarios en lo que respecta a la promoción y el marco operativo de los EIII.

El objetivo principal de esta propuesta de modificación de la Resolución 58 es contribuir a la mejora de la capacidad de respuesta ante emergencias de ciberseguridad a escala mundial.

Propuesta

Las Administraciones miembros de la APT proponen revisar la Resolución 58 de la AMNT.

MOD APT/37A13/1

RESOLUCIÓN 58 (Rev. Nueva Delhi, 2024)

Fomento de la creación de equipos nacionales de intervención  
en caso de incidente informático, especialmente  
para los países en desarrollo[[1]](#footnote-1)1

(Johannesburgo, 2008; Dubái, 2012; Ginebra, 2022; Nueva Delhi, 2024)

La Asamblea Mundial de Normalización de las Telecomunicaciones (Nueva Delhi, 2024),

considerando

*a)* la Resolución 130 (Rev. Bucarest, 2022) 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 (TIC);

*b)* que la Resolución 123 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios encarga al Secretario General y a los Directores de las tres Oficinas que colaboren estrechamente en la aplicación de iniciativas que contribuyan a reducir la brecha de normalización entre los países en desarrollo y los desarrollados,

considerando además

que la Recomendación UIT-T X.1060 proporciona un marco para la creación y operación de un centro de ciberdefensa (CDC),

reconociendo

*a)* los resultados muy satisfactorios obtenidos a través del enfoque regional en el marco de la Resolución 54 (Rev. Hammamet, 2016) de la Asamblea Mundial de Normalización de las Telecomunicaciones;

*b)* que el UIT-T lleva a cabo una labor sumamente prioritaria en el marco de la Resolución 50 (Rev. Nueva Delhi, 2024), de conformidad con sus competencias y conocimientos técnicos, en particular mediante la promoción del 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;

*c)* el auge de la transformación digital y la dependencia de las TIC en los países en desarrollo;

*d)* el rápido aumento del volumen, la gravedad y la sofisticación de las ciberamenazas y los ciberataques contra la infraestructura de telecomunicaciones/TIC, y la complejidad que reviste la gestión de la infraestructura de ciberdefensa, las herramientas, las personas y los servicios de seguridad;

*e)* que las ciberamenazas y los ciberataques evolucionan al ritmo de los servicios y las tecnologías de la infraestructura de telecomunicaciones/TIC, y que las ciberamenazas no sólo pueden propagarse a través de ordenadores, sino también de dispositivos móviles, servidores, redes e incluso tecnología operativa, mientras que los ciberataques se centran cada vez más en infraestructuras de telecomunicaciones/TIC críticas y datos importantes;

*f)* la labor realizada por el Sector de Desarrollo de las Telecomunicaciones (UIT-D) en el marco de la antigua Cuestión 22/1 de la Comisión de Estudio 1 del UIT-D y de la actual Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D sobre este particular,

observando

*a)* que muchos países, especialmente los países en desarrollo, aún cuentan con un escaso nivel de preparación para casos de emergencia relacionados con la ciberseguridad;

*b)* que el alto grado de interconectividad de las redes de TIC podría verse afectado por el lanzamiento de ataques desde redes de países y regiones menos preparados;

*c)* la importancia de disponer de un nivel apropiado de preparación para casos de emergencia relacionados con la ciberseguridad;

*d)* la necesidad de crear equipos de intervención en caso de incidente informático (EIII), también conocidos como equipos de intervención en caso de incidente de ciberseguridad/ciberincidente, sobre una base nacional, y así como la importancia de la coordinación con los EIII existentes dentro de los países y regiones y entre los mismos;

*e)* que existen varios sinónimos del término "EIII", entre ellos, "EIEI" (equipo de intervención en caso de emergencia informática), "EIISI" (equipo de intervención en caso de incidente de seguridad informática), "CRII" (centro de respuesta a incidentes informáticos) y "CDC";

*f)* los trabajos de la Comisión de Estudio 17 del Sector de Normalización de las Telecomunicaciones de la UIT (UIT‑T) con respecto a los EIII, en particular para los países en desarrollo, y la cooperación entre ellos, contenidos en productos de la Comisión de Estudio tales como la Recomendación UIT-T X.1060, relativa al marco para la creación y operación de un centro de ciberdefensa, que ofrece directrices encaminadas a garantizar que las organizaciones cuenten con las capacidades de ciberdefensa necesarias, así como con unos servicios de seguridad eficaces, para protegerse de los ciberataques y las amenazas a la seguridad,

teniendo presente

que el buen funcionamiento de los EIII en los países en desarrollo servirá para mejorar el nivel de participación de dichos países en las actividades mundiales de respuesta ante emergencias de ciberseguridad y contribuirá a un funcionamiento adecuado y seguro de la infraestructura mundial de TIC,

resuelve

1 apoyar la creación de EIII nacionales en aquellos Estados Miembros de la UIT donde aún no existan y se necesiten, y promover el correspondiente marco operativo en los Estados Miembros que ya dispongan de un EIII, si procede;

2 apoyar al Director de la BDT en la promoción de las mejores prácticas nacionales, regionales e internacionales en materia de creación de EIII, a través de Recomendaciones y Suplementos técnicos,

encarga a la Comisión de Estudio 17

1 que siga elaborando Recomendaciones y Suplementos que faciliten la creación de EIII y la promoción del marco operativo conexo;

2 que promueva estudios relativos al marco de los centros de ciberdefensa que tratan de minimizar los ciberriesgos y reducir la incidencia de las violaciones a la seguridad aplicando procesos y procedimientos eficaces de detección y respuesta, tecnologías y parámetros de evaluación de los servicios de seguridad de la infraestructura mundial de telecomunicaciones/TIC;

3 que preste apoyo al Director de la Oficina de Normalización de las Telecomunicaciones en las iniciativas destinadas a reducir la brecha de normalización entre los países desarrollados y en desarrollo en favor de los CDC, que deberían incluir puntos de trabajo sobre la labor de normalización de los CDC en el ámbito de la seguridad, y comparta información con los grupos pertinentes del UIT-D en calidad de Comisión de Estudio rectora sobre seguridad;

4 que promueva actividades conjuntas de coordinación relacionadas con los CDC entre todas las Comisiones de Estudio y todos los Grupos Temáticos pertinentes de la UIT, así como entre otros organismos de normalización;

5 que siga definiendo un conjunto de capacidades de CDC, incluidas infraestructuras y organizaciones, e incorpore la seguridad en el diseño de los CDC (lo que significa que las capacidades y funcionalidades de seguridad deben estar disponibles desde la fase de diseño) para la infraestructura de telecomunicaciones/TIC,

encarga al Director de la Oficina de Normalización de las Telecomunicaciones que, en colaboración con el Director de la Oficina de Desarrollo de las Telecomunicaciones

1 defina las mejores prácticas en materia de creación de EIII y promoción del marco operativo correspondiente de acuerdo con la colección de herramientas de la UIT;

2 identifique dónde se necesitan EIII nacionales, en especial en los países en desarrollo, y aliente su creación;

3 colabore con expertos y entidades internacionales para llevar a cabo el establecimiento de EIII nacionales;

4 proporcione el apoyo que corresponda dentro de los recursos presupuestarios existentes;

5 facilite la cooperación entre los EIII nacionales, por ejemplo en materia de creación de capacidades y de intercambio de información, en un marco apropiado;

6 adopte las medidas necesarias para avanzar en la aplicación de esta Resolución,

invita a los Estados Miembros

1 a considerar la posibilidad de crear un EIII nacional con carácter de alta prioridad;

2 a colaborar con otros Estados Miembros y Miembros de Sector,

invita a los Estados Miembros y a los Miembros de Sector

a colaborar estrechamente con el UIT-T y el UIT-D a este respecto.

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

1. 1 Este término comprende 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)