|  |  |
| --- | --- |
| **Consejo 2017Ginebra, 15-25 de mayo de 2017** | **logo_S_** |
|  |
|  |  |
| **Punto del orden del día: PL 1.5** | **Documento C17/18-S** |
|  | **14 de marzo de 2017** |
|  | **Original: inglés** |
| Informe del Secretario General |
| ACTIVIDADES DE LA UIT SOBRE EL FORTALECIMIENTO DE SU PAPEL EN LA CREACIÓN DE CONFIANZA Y SEGURIDAD EN LA UTILIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN |

|  |
| --- |
| ResumenEn el presente Informe se resumen las actividades de la UIT desde la reunión de 2016 del Consejo en relación con la Resolución 130 (Rev. Busán, 2014), la función de la UIT como único organismo facilitador de la Línea de Acción C5 de la CMSI, y otras decisiones adoptadas por los miembros 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).Acción solicitadaSe invita al Consejo a **tomar nota** del Informe.\_\_\_\_\_\_\_\_\_\_\_\_Referencias*Resoluciones* [*71*](http://www.itu.int/en/council/planning/Documents/PP-14_Res71.pdf)*,* [*130*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20130.pdf)*,* [*140*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20140.pdf)*,* [*174*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20174.pdf)*,* [*179*](http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20179.pdf) *(Rev. Busán, 2014),* [*181*](http://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_181.pdf) *(Guadalajara, 2010) de la Conferencia de Plenipotenciarios,* [*Reglamento de las Telecomunicaciones Internacionales*](http://www.itu.int/pub/S-CONF-WCIT-2012/es) *(Rev. Dubái, 2012),* [*Resolución 1306*](https://www.itu.int/md/S15-CL-C-0109/es) *del Consejo, Resoluciones* [*2*](https://www.itu.int/en/ITU-D/TIES_Protected/WTDC14/WTDC14-FinalReport-E.pdf)*,* [*45*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/45revDubai.pdf)*,* [*67*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/67revDubai.pdf)*,* [*69*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/69revDubai.pdf) *(Rev. Dubái, 2014) de la CMDT,* [*Objetivo 3*](https://www.itu.int/en/ITU-D/TIES_Protected/WTDC14/WTDC14-FinalReport-E.pdf) *del PADu/CMDT-14, Resoluciones* [*50*](https://www.itu.int/pub/T-RES-T.50-2016/es)*,* [*52*](https://www.itu.int/pub/T-RES-T.52-2016/es)*,* [*75*](https://www.itu.int/pub/T-RES-T.75-2016/es) *(Rev. Hammamet, 2016),* [*58*](https://www.itu.int/pub/T-RES-T.58-2016/es) *(Rev. Dubái, 2012) de la AMNT, Documentos del Consejo* [*C05/32*](https://www.itu.int/md/S05-CL-C-0032/es)*,* [*C05/INF/10*](https://www.itu.int/md/S05-CL-INF-0010/es)*,* [*C06/4*](https://www.itu.int/md/S06-CL-C-0004/es)*,* [*C07/21*](https://www.itu.int/md/S07-CL-C-0021/es)*,* [*C08/33*](https://www.itu.int/md/S08-CL-C-0033/es)*,* [*C09/50*](https://www.itu.int/md/S09-CL-C-0050/es)*,* [*C10/12*](https://www.itu.int/md/S10-CL-C-0012/es)*,* [*C11/54*](https://www.itu.int/md/S11-CL-C-0054/es)*,* [*C12/29*](https://www.itu.int/md/S12-CL-C-0029/es)*,* [*C13/23*](https://www.itu.int/md/S13-CL-C-0023/es)*,* [*C14/23*](https://www.itu.int/md/S14-CL-C-0023/es)*,* [*C15/18*](https://www.itu.int/md/S15-CL-C-0018/es) *y* [*C16/18*](https://www.itu.int/md/S16-CL-C-0018/es) |

# 1 Actividades en materia de ciberseguridad y lucha contra el spam

1.1 El desarrollo de las TIC, sobre una base de seguridad y confianza, ha sido reconocido como un factor esencial para el desarrollo sostenible. El presente Informe, organizado en torno a los cinco pilares de la [Agenda sobre Ciberseguridad Global (ACG)](http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx), muestra el carácter complementario de los actuales programas de trabajo de la UIT y facilita la realización de las actividades de la BDT, la TSB y la BR al respecto.

# 2 Medidas jurídicas

2.1 En el contexto del Objetivo 3 del Plan de Acción de Dubái, y teniendo en cuenta la Cuestión 3/2 (antigua Cuestión 22/1) del UIT-D, la UIT está ayudando a los Estados Miembros a comprender los aspectos jurídicos de la ciberseguridad poniendo a disposición de los mismos sus [Recursos de la UIT sobre la legislación del ciberdelito](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx), con el fin de contribuir a la armonización de sus marcos jurídicos.

2.2 En lo que atañe a las medidas jurídicas, la UIT colabora estrechamente con la ONUDD y otros asociados con conocimientos especializados en la materia.

# 3 Medidas técnicas y de procedimiento

3.1 La [Comisión de Estudio 17 (CE 17) del UIT-T](http://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx), Comisión de Estudio Rectora sobre seguridad y gestión de identidad (IdM), sigue contribuyendo al estudio y la normalización en ámbitos tales como la ciberseguridad, la lucha contra el correo basura, la IdM, los certificados X.509, la gestión de la seguridad de la información, las redes de sensores ubicuos, la telebiometría, la seguridad de la TVIP, la seguridad de la virtualización con miras a la seguridad de la computación en la nube, la arquitectura de la seguridad y la seguridad de las aplicaciones, a menudo en cooperación con organizaciones y consorcios de normalización externos.

3.2 Desde la reunión de 2016 del Consejo de la UIT, la CE 17 ha aprobado las nuevas Recomendaciones sobre ciberseguridad UIT-T X.1038 "Requisitos de seguridad y arquitectura de referencia para las redes definidas por software", UIT-T X.1039 "Medidas técnicas de seguridad para la implementación de las dimensiones de seguridad de la Recomendación UIT-T X.805", X.1085 "Tecnología de la información – Técnicas de seguridad – Marco de autentificación telebiométrica mediante un módulo de seguridad de hardware biométrico", X.1087 "Contramedidas técnicas y operativas para las aplicaciones telebiométricas en dispositivos móviles", X.1258 "Autentificación de entidades mejorada basada en la agregación de atributos", X.1542 "Formato de intercambio de mensajes de información de sesión", X.1641 "Directrices para la seguridad de los datos de cliente en el servicio en la nube", y efectuó una importante revisión de las Recomendaciones de la serie X.500 sobre "Tecnología de la información – Interconexión de sistemas abiertos – El directorio".

3.3 Está previsto que se aprueben en marzo de 2017 y por el procedimiento TAP siete proyectos de Recomendación sobre ciberseguridad, protección de la información de identificación personal, control de acceso, encriptación para la IoT, percepción por el usuario extremo de los indicadores de fiabilidad y capacidad de actualización de software segura para sistemas de transporte inteligentes, y se prevé finalizar otros ocho proyectos de Recomendación sobre técnicas estructuradas de intercambio de información de ciberseguridad, lucha contra las redes robot de teléfonos inteligentes, lucha contra el spam en mensajería instantánea (SPIM), peska por SMS, medidas contra el robo de teléfonos móviles y seguridad de las capacidades abiertas de los servicios de telecomunicaciones para poner en marcha el proceso de aprobación AAP. Se han empezado a preparar proyectos de Recomendación sobre la lucha contra el fraude por servicios telefónicos, medición inteligente de la seguridad del servicio en las redes eléctricas inteligentes, procesamiento de desidentificación, autentificación híbrida y mecanismos clave de gestión en el modelo cliente-servidor, analítica de macrodatos en servicios de Internet móvil, seguridad de los macrodatos como servicio, la comunicación como servicio y la red como servicio, autentificación telebiométrica mediante bioseñales, detección telebiométrica antisuplantación y perfil de sintaxis de mensaje criptográfico (CMS).

3.4 El [Grupo Regional de la CE 17 para África](http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/sg17rgafr/Pages/default.aspx) celebró su segunda reunión los días 27 y 28 de julio de 2016 en Jartum (República del Sudán).

3.5 La CE 17 prosiguió la coordinación con la CE 20 del UIT-T "IoT y sus aplicaciones, incluidas las ciudades y comunidades inteligentes (SC&C)" en el ámbito de la seguridad de la IoT.

3.6 El UIT-R prosigue sus trabajos sobre normalización de las radiocomunicaciones, adaptándose a la constante evolución de las redes de telecomunicación modernas. Ese Sector ha establecido principios de seguridad claros para las redes IMT (3G, 4G y 5G) (Recomendaciones UIT-R M.1078, M.1223, M.1457, M.1645, M.2012 y M.2083). Ha publicado también Recomendaciones sobre cuestiones de seguridad en la arquitectura de la gestión de red para sistemas digitales de satélite (Recomendación UIT-R S.1250) y mejoras en el comportamiento del protocolo de control de transmisión por redes de satélites (Recomendación UIT-R S.1711).

# 4 Estructuras institucionales

4.1 La UIT sigue contribuyendo a la creación de capacidades a escala regional e internacional. Ha iniciado comprobaciones técnicas a fin de evaluar el grado de preparación para el [establecimiento de equipos de intervención en caso de incidentes informáticos (EIII)](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx) en 68 países, y prosigue sus actividades con miras a la adopción de las medidas de seguimiento necesarias. Se están creando y mejorando los EIII nacionales de Burundi, Gambia, Chipre y Kenya tras haber finalizado satisfactoriamente las actividades en esta materia en 12 países.

4.2 La UIT se asoció con el Global Cyber Security Capacity Centre en la Oxford Martin School y juntos efectuaron exámenes de capacidad de ciberseguridad en Tailandia, Sierra Leona y Madagascar.

4.3 La UIT sigue organizando [ciberejercicios de simulación](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx) para sus países asociados con el propósito de mejorar las capacidades de los equipos participantes en materia de comunicación y de intervención en caso de incidente, y de aumentar la cooperación nacional e internacional contra las ciberamenazas. Por el momento, la UIT ha realizado 16 ciberejercicios de simulación para más de 100 países. En el periodo abarcado por el presente Informe, se han organizado ciberejercicios de simulación internacionales en Quito (Ecuador), en la [Región de las Américas](http://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2016/15551.aspx) (27 de junio – 1 de julio de 2016), en Túnez (Túnez), en la [Región Árabe](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Tunisia_cyberdrill_2016.aspx) (23-27 de mayo de 2016) y en Mauricio en la [Región de África](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Mauritius_cyberdrill_2016.aspx) (4-8 de abril de 2016).

4.4 Se encuentra en fase de desarrollo una colección de herramientas de [estrategia nacional de ciberseguridad](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx), como esfuerzo de múltiples partes interesadas facilitado por la UIT. Para avanzar en los trabajos, se celebraron tres talleres de los asociados los días 18 y 19 de febrero de 2016 en la Sede de la UIT en Ginebra (Suiza), los días 6 y 7 de junio de 2016 en la Saïd Business School de la Universidad de Oxford (Reino Unido), y los días 13 y 14 de octubre de 2016 en Washington DC (Estados Unidos), siendo la anfitriona de este último la Organización de Estados Americanos (OEA). El producto se está finalizando y estará a disposición del público antes de finales de 2017.

4.5 La UIT prestó asistencia a Nepal para la preparación de su Política Nacional de Ciberseguridad, incluida la Protección de la Infancia en Línea (4-8 de julio de 2016), aumentando la sensibilización y formado a 100 participantes del gobierno, del regulador y del sector privado, mostrando también una exitosa simulación de ciberseguridad y mejorando la cooperación con la Autoridad de Telecomunicaciones de Nepal (NTA).

4.6 Se realizó una encuesta de preparación en materia de ciberseguridad en países de la región Asia-Pacífico (2015-2016) sobre la base de los cinco pilares de la AGC.

# 5 Creación de capacidades

5.1 La UIT sigue organizando [foros regionales de ciberseguridad](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Events.aspx) para todas las regiones, y los utiliza como vehículo de creación de capacidades para diversos programas y actividades del UIT-D, y como plataforma operacional de cooperación a escala regional e internacional.

5.2 La Comisión de Estudio 2 del UIT-D sigue su labor en el periodo de estudios 2014-2018 sobre la Cuestión 3/2: [Seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad](http://www.itu.int/net4/ITU-D/CDS/sg/rgqlist.asp?lg=3&sp=2014&rgq=D14-SG02-RGQ03.2&stg=2).

5.3 La UIT y la ATU, con el apoyo de la TSB y la BDT, celebraron del 24 al 26 de julio de 2016, el taller "[Estrategia de ciberseguridad en los países africanos](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/cybersecurity/Pages/default.aspx)" en la sede de la National Telecommunication Corporation (NTC) en Jartum (República del Sudán).

5.4 Por primera vez, la UIT se asoció formalmente con la European Network and Security Agency (ENISA) para organizar el [Foro Regional sobre Ciberseguridad UIT-ENISA](http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2016/RCYBF/Regional-Cybersecurity-Forum.aspx), que se celebró los días 29 y 30 de noviembre de 2016 en Sofía (Bulgaria).

5.5 La 4ª edición de la "[Plataforma de diálogo público-privado sobre ciberseguridad en la Europa central](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2016/CYBR/Cyber-Security-in-Romania.aspx)" se celebró del 14 al 16 de septiembre de 2016 en Sibio (Rumania).

5.6 Tras la presentación de los primeros resultados del [Índice Mundial de Ciberseguridad (IMC)](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx) en 2014, se encuentra en fase de elaboración una [nueva versión del IMC](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2016.aspx), que contará con un índice mejorado y con una serie de asociados. Hasta la fecha, 136 países han contestado al cuestionario. El análisis de las respuestas está en curso.

5.7 La UIT contribuyó a formar recursos técnicos para la respuesta a incidentes en Myanmar, Viet Nam, R.D.P. Lao y Camboya en 2016.

# 6 Cooperación internacional

6.1 La UIT sigue forjando relaciones y [asociaciones](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/partnership.aspx) con diversas organizaciones e iniciativas regionales e internacionales, tales como la Iniciativa contra la ciberdelincuencia de la Commonwealth, ENISA, INTERPOL, CEDEAO, el Banco Mundial, FIRST y las asociaciones de EIISI/EIEI regionales, como el EIEI AP, el EIEI ÁFRICA y el EIEI OIC.

6.2 La UIT, principal organismo facilitador de la Línea de Acción C5 de la CMSI, organizó varias actividades en el [Foro de la CMSI 2016](http://www.itu.int/net4/wsis/forum/2015/) que facilitaron el intercambio de experiencias entre todos los grupos de interesados en la labor encaminada a promover la confianza y seguridad en la utilización de las TIC.

6.3 En el marco del Foro Telecom 2016, la UIT organizó, en colaboración con el EastWest Institute (EWI) una mesa redonda sobre "[ICT trust, innovation and trade](http://www.itu.int/net4/Telecom/webs/TelecomWorld/session/description/C-00001734)".

6.4 La UIT participó en la [Conferencia Internacional Multipartita "Cyberspace, Energy & Development-Protecting Critical Energy Infrastructure"](https://www.energypact.org/energypact-foundation_conferences/), organizada por el Gobierno austriaco, la EnergyPact Foundation y el Instituto Austriaco de Tecnología, con el apoyo de la CEI, la ONUDD y la UIT, que se celebró el 16 de febrero de 2017 en Viena (Austria).

6.4 Están disponibles para el público [195 perfiles de país](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx) en el sitio web de la UIT. Esos perfiles son representaciones objetivas, no analíticas, de la situación en materia de ciberseguridad de cada país, sobre la base de los [cinco pilares de la GCA](http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx). Los perfiles son documentos activos que se ponen al día a medida que se ponen a disposición del público nuevos datos relativos a los países.

# 7 Protección de la Infancia en Línea (PIeL)

7.1 Desde el periodo cubierto por su último informe, el [Grupo de Trabajo del Consejo sobre Protección de la Infancia en Línea (GTC-PIeL)](http://www.itu.int/en/council/cwg-cop/Pages/default.aspx) se reunió en dos ocasiones y ha organizado una consulta abierta en línea con los jóvenes sobre diversos temas. Puede encontrarse más información en el Documento [C17/15](https://www.itu.int/md/S16-CL-C-0015/es).

7.2 La UIT y sus asociados siguen colaborando estrechamente con miras a la consecución de los Objetivos de Desarrollo Sostenible y, en particular, del ODS 16.2, "Poner fin al maltrato, la explotación, la trata, la tortura y todas las formas de violencia contra los niños".

7.3 En las dos últimas reuniones del GTC-PIeL, la Child Helpline International (CHI) presentó los resultados de la campaña conjunta "[Juntos para proteger a los niños y los jóvenes](http://www.itu.int/en/cop/Pages/consultation-may2016.aspx)" de la UIT-CHI. La campaña se puso en marcha en mayo de 2016 y sus resultados definitivos se presentaron el 15 de noviembre de 2016 en el marco de ITU Telecom World 2016 junto con nuevas maneras de desarrollar los servicios de líneas de ayuda a menores. Se insistió en la colaboración entre los Miembros de la UIT y las líneas de ayuda. Los miembros del GTC-PIeL se felicitaron de la campaña y el Presidente animó a la Secretaría a proseguir en esta línea para avanzar en la consecución del ODS 16.

7.4 Las Oficinas Regionales de la UIT siguen prestando asistencia a los Estados Miembros en el análisis de la protección de la infancia en línea en los respectivos países a fin de elaborar y proponer un marco sostenible que pueda aplicarse a largo plazo.

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