|  |  |
| --- | --- |
| **Consejo 2020Ginebra, 9-19 de junio de 2020** |  |
|  |
|  |  |
| **Punto del orden del día: PL 1.4** | **Documento C20/18-S** |
|  | **30 de marzo de 2020** |
|  | **Original: inglés** |
| Informe del Secretario General |
| ACTIVIDADES DE LA UIT SOBRE EL FORTALECIMIENTO DE SU PAPELEN LA CREACIÓN DE CONFIANZA Y SEGURIDAD EN LA UTILIZACIÓNDE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN |

|  |
| --- |
| ResumenEn el presente Informe se resumen las actividades de la UIT desde la reunión de 2019 del Consejo en relación con la Resolución 130 (Rev. Dubái, 2018), 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*](https://www.itu.int/en/council/Documents/basic-texts/RES-071-S.pdf)*,* [*130*](https://www.itu.int/en/council/Documents/basic-texts/RES-130-S.pdf)*,* [*140*](https://www.itu.int/en/council/Documents/basic-texts/RES-140-S.pdf)*,* [*174*](https://www.itu.int/en/council/Documents/basic-texts/RES-174-S.pdf)*,* [*179*](https://www.itu.int/en/council/Documents/basic-texts/RES-179-S.pdf) *de la Conferencia de Plenipotenciarios (Rev. Dubái, 2018) y* [*181*](https://www.itu.int/en/council/Documents/basic-texts/RES-181-S.pdf) *(Guadalajara, 2010),* [*RTI*](https://www.itu.int/pub/S-CONF-WCIT-2012/es) *(Rev. Dubái, 2012),* [*Resolución 1306 del Consejo*](https://www.itu.int/md/S15-CL-C-0109/es)*, Resoluciones* [*45*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/45revDubai.pdf) *(Rev. Dubái, 2014),* [*2, 67 y 69*](https://www.itu.int/md/D14-WTDC17-C-0115/es) *(Rev. Buenos Aires, 2017) de la CDMT, Objetivo 2/Resultado 2.2 del UIT-D (*[*Plan de acción de Buenos Aires*](https://www.itu.int/md/D14-WTDC17-C-0115/es)*), 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) y* [*58*](https://www.itu.int/pub/T-RES-T.58-2016/es) *(Rev. Dubái, 2012) de la AMNT, Documentos recientes del Consejo* [*C15/18*](http://www.itu.int/md/S15-CL-C-0018/es)*,* [*C16/18*](https://www.itu.int/md/S16-CL-C-0018/es)*,* [*C17/18*](https://www.itu.int/md/S17-CL-C-0018/es)*,* [*C18/18*](https://www.itu.int/md/S18-CL-C-0018/es) *y* [*C19/18*](https://www.itu.int/md/S19-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), 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 marco del Objetivo 2/Resultado 2.2 del Plan de Acción de Buenos Aires, y teniendo en cuenta la Cuestión 3/2 (antigua Cuestión 22/1) de la CE 2 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 los [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. En lo que atañe a las medidas jurídicas, la UIT colabora estrechamente con la ONUDD y otros expertos en la materia.

# 3 Medidas técnicas y de procedimiento

3.1 La [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 de la ciberseguridad, la lucha contra el correo basura, la IdM, los certificados X.509 del UIT-T, la gestión de la seguridad de la información, las redes de sensores ubicuos, la telebiometría, la seguridad móvil, la seguridad de la virtualización con miras a la seguridad de la computación en la nube, y la arquitectura para la protección y seguridad de información de identificación personal, en cooperación con otros organismos de normalización externos.

3.2 Desde su último informe presentado al Consejo, la CE 17 ha celebrado una reunión en septiembre de 2019, en la que la CE 17 estableció [25 nuevos temas de trabajo de normalización](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17). La CE 17 aprobó más de 30 Recomendaciones UIT-T nuevas o revisadas en materia de seguridad de las TIC, a saber: 9ª edición de las normas básicas para la ciberseguridad de las Recomendaciones de la serie X.500 sobre infraestructura pública, X.1044 "Requisitos de seguridad de la virtualización de la red", X.1045 " Arquitectura de la cadena de servicios de seguridad para redes y aplicaciones", X.1059 "Guía de aplicación para las organizaciones de telecomunicaciones sobre la gestión de riesgos de sus activos accesibles a nivel mundial en redes basadas en el IP", X.1702 "Arquitectura de un generador de números aleatorio de ruido cuántico", X.1232 "Marco técnico para contrarrestar el spam publicitario en la información generada por el usuario", X.677 "Mecanismo de identificación de vehículos aéreos no tripulados mediante identificadores de objetos", X.1402 "Seguridad de tecnología de libro mayor distribuido", X.1197 Enmienda 1 "Revised guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection", X.694 Cor.1 y X.893 Cor.1 sobre ASN.1, serie Z.100 revisada sobre SDL y serie Z.160 revisadas sobre la versión 3 de la Notación de pruebas y de control de pruebas (TTCN-3). La CE 17 también aprobó un nuevo Suplemento sobre casos de utilización del Marco de garantía de autentificación de entidad (EAA) y revisó la guía del implementador de la serie Z.

3.3 La CE 17 organizó un [Taller de la UIT sobre seguridad de la tecnología financiera](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190826/Pages/default.aspx) de un día de duración el 26 de agosto de 2019, que finalizó con sugerencias para las actividades de seguimiento de la CE 17 en colaboración con otras organizaciones de normalización de la seguridad de las tecnologías financieras identificadas, por ejemplo FG-DLT, FG-DFC, ISO TC 307, W3C sobre DLT. La CE 17 también organizó un [minitaller sobre retos de ciberseguridad en la conducción automática](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/mini-workshop_ITS.aspx) el día 26 de agosto de 2019, en cooperación con la Colaboración sobre los STI de la UIT (CITS) y el WP29 de la CEPE de las Naciones Unidas.

3.4 Debido al brote mundial del Coronavirus, la reunión de la CE 17 del 17 al 26 de marzo de 2020 se convirtió en la primera reunión totalmente virtual de una Comisión de Estudio del UIT‑T. Además, la CE 17 tuvo que aplazar su [Taller conjunto de la CE 17 del UIT-T y el TC 307 de la ISO sobre "Seguridad de la DLT, gestión de la identidad y privacidad"](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20200316/Pages/default.aspx) prevista inicialmente para el 16 de marzo de 2020.

3.5 La CE 17 de la UIT prosiguió su labor sobre seguridad de la IoT, así como la coordinación con la CE 20 del UIT-T "IoT y sus aplicaciones, incluidas las ciudades y comunidades inteligentes (C+CI)".

3.6 La CE 9 del UIT-T determinó cinco proyectos de Recomendación UIT-T, J.1012, J.1013, J.1014, J.1015 y J.1015.1, sobre la Interfaz común integrada para soluciones CA/DRM intercambiables.

3.7 La CE 13 del UIT-T aprobó la Enmienda 1 de la Recomendación UIT-T Y.3053 (2018), "Marco de creación fiable de redes con dominios de red centrados en la confianza: Enmienda 1 – Arquitectura y procedimiento fiables de despliegue de redes", la Recomendación Y.3514 Cor. 1 "Computación en la nube – Marco y requisitos de computación fiable entre nubes" y la Recomendación Y.3517 "Computación en la nube – Visión general de la gestión de la confianza entre nubes".

3.8 La CE 15 del UIT-T está trabajando en el Suplemento (G.Sup.otnsec) que describe el lenguaje y una infraestructura de datos común en las capas de protocolo de la Red de Transporte Óptico (OTN) existentes que se necesita para utilizar los protocolos criptográficos propuestos de forma independiente a fin de crear soluciones de transporte seguro en determinadas capas de la OTN.

3.9 La CE 20 del UIT-T aprobó la Recomendación UIT-T Y.4807 "Agility by design for Telecommunications/ICT Systems Security used in the Internet of Things".

3.10 Varios Grupos Temáticos del UIT-T están estudiando los aspectos de confianza de varias tecnologías emergentes como parte de su trabajo. Estos incluyen 1) el [*Grupo Temático del UIT-T sobre aprendizaje automático para redes futuras, incluidas las 5G (FG-ML5G)*](https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx) 2) [*Grupo Temático del UIT-T sobre Tecnologías para la Red 2030 (FG NET-2030)*](https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx) 3) [*Grupo Temático del UIT-T sobre Inteligencia artificial para la salud (FG AI4H)*](https://www.itu.int/en/ITU-T/focusgroups/ai4h) 4) [*Grupo Temático del UIT-T sobre multimedios en vehículos (FG VM*](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx)*)* 5) [*Grupo Temático del UIT-T sobre IA para la conducción autónoma y asistida* *(FG-AI4AD)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ad/Pages/default.aspx) 6) [*Grupo Temático del UIT-T sobre tecnología de la información cuántica para redes (FG-QIT4N)*](https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx)*.*

3.11 La UIT, en colaboración con la Fundación Bill y Melinda Gates, el Grupo del Banco Mundial y el Banco de Pagos Internacionales, organizó un [Taller sobre la seguridad, la infraestructura y la confianza en los servicios financieros digitales](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201912/Pages/default.aspx), que se celebró los días 4 y 5 de diciembre de 2019 en la sede de la UIT en Ginebra (Suiza).

3.12 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 realizó evaluaciones técnicas para valorar la preparación a efectos del establecimiento de Equipos de intervención en caso de incidente informático (EIII) en 76 países y está adoptando las medidas de seguimiento necesarias. Se ha completado la participación directa en 14 de esas actividades. Mediante la ejecución del proyecto de servicios y capacidades conexas de los EIII, se prestó asistencia al Estado de Palestina en la creación y el despliegue de las capacidades técnicas y la capacitación conexa para las operaciones del EIII. Kiribati y las Islas Salomón recibieron asistencia para elaborar sus estrategias nacionales de seguridad cibernética. Se proporcionó capacitación al EIII de Papua Nueva Guinea y Vanuatu mediante el [proyecto del Departamento de Comunicaciones y Artes de la UIT, Australia (DoCA)](https://www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=9RAS18061). Se celebraron en Chad y Liberia cursos prácticos de evaluación de la preparación para el EIII. Las partes interesadas nacionales del EIII de Gambia recibieron capacitación sobre las operaciones del EIII. Se iniciaron cuatro proyectos de EIII y su ejecución sigue en curso en Botswana, Burundi, Gambia y Malawi. En Kenya, está en curso la mejora del EIII existente (que se completará en 2020).

4.2 La UIT ha realizado 28 [ciberejercicios de simulación](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) en más de 100 países. Se han llevado a cabo ciberejercicios de simulación en [Uganda](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Africa-Cyberdrill-2019.aspx) (Región de África, noviembre de 2019); [Omán](https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Pages/Events/2018/Cyber/Cyber.aspx)(Región Árabe, octubre de 2019); [Malasia](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/ASP-CIS-Cyberdrill-2019.aspx) (Región de Asia y el Pacífico, septiembre de 2019) y Rumania (Región de Europa y la CEI, mayo de 2019). Está previsto realizar 5 ciberjercicios de simulación en 2020.

# 5 Creación de capacidad

5.1 La UIT ha organizado [foros regionales de ciberseguridad](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Events.aspx) para todas sus regiones a fin de aumentar las capacidades en el marco de varios programas y actividades de la BDT y para ofrecer una plataforma operacional de cooperación regional e internacional.

5.2 Después de la CMDT-17, la Cuestión 3/2 de la CE 2 del UIT-D ([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)) proseguirá su labor en el periodo de estudios 2018-2021.

5.3 La Guía de la UIT sobre formulación de una estrategia nacional de ciberseguridad es una guía de prácticas idóneas que utilizan países de todas las regiones. Se organizaron los siguientes talleres en 2019: a) El Ministerio de Informática y la Agencia de Ciberseguridad de Indonesia acogieron un taller regional en Yakarta dedicado a las estrategias de ciberseguridad (los debates trataron de la reglamentación general de protección de datos); b) en Macedonia se dedicó un taller regional a la mejora de las estrategias nacionales en cinco países de los Balcanes; c) Túnez acogió un taller regional dedicado a la mejora de las estrategias nacionales de los países de las Regiones de África y los Estados Árabes. Participaron activamente 20 países. Tres países recibieron asistencia directa para la formulación y revisión de sus estrategias nacionales de ciberseguridad utilizando la Guía.

5.4 Se impartió capacitación y se prestó asistencia técnica a Sudán a fin de mejorar su estrategia de protección de las infraestructuras de información esenciales.

5.5 Durante la Semana Regional de la Ciberseguridad en la región de los Estados Árabes, el Centro de Ciberseguridad de la Región Árabe de la UIT (CCRA-UIT) promovió la compartición de información y la capacitación en ciberseguridad. Esta Semana ofreció a expertos en TIC y ciberseguridad del sector público de la región la oportunidad de reunirse con las partes interesadas pertinentes y debatir acerca de las amenazas, la evolución, las oportunidades y retos de la ciberseguridad.

5.6 Se celebró en Chisinau, Moldova, la Semana de la Ciberseguridad de Moldova con el apoyo de la UIT. Esta conferencia ofreció oportunidades de creación de redes de contactos y una plataforma para el intercambio de ideas, el debate y la colaboración para la definición de estrategias y soluciones globales de ciberseguridad a través de la innovación.

5.7 Se celebró el Cyber Shield 2019 en Ankara, Turquía, con el apoyo de la UIT. Los principales objetivos fueron aumentar la capacidad de respuesta frente a incidentes y los niveles de preparación, aumentar la comprensión mutua de los ciberriesgos y los efectos asociados, y garantizar un esfuerzo de colaboración constante entre las partes interesadas en la seguridad cibernética internacional, especialmente los equipos nacionales de intervención en caso de incidente informático (EIII), a fin de mitigar las ciberamenazas. La UIT también organizó una sesión de formación para Kirguistán acerca de la manera de crear un centro de operaciones de ciberseguridad.

5.8 La UIT, el Centro de Formación Avanzada en Telecomunicaciones y la Facultad de ciencias aplicadas de correos y telecomunicaciones (Facultad TIC, República Islámica del Irán) organizaron una [formación de ciberseguridad en el CoE ASP de la UIT (Teherán, Irán, diciembre de 2018)](https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2018/CybersecurityASPCOE/cybersecurity.aspx).

5.9 La tercera versión del [Índice Mundial de Ciberseguridad](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCI) muestra una considerable mejora en el compromiso con la ciberseguridad en todo el mundo. Se ha puesto en marcha la cuarta versión de la encuesta del Índice Mundial de Ciberseguridad, con un cuestionario y una metodología mejorados. En asociación con Deloitte, se realizó un examen del panorama de la ciberseguridad en Côte d'Ivoire, en el que se incluyeron las conclusiones del Índice Mundial de Ciberseguridad. El examen ayudó al país a determinar las iniciativas prioritarias en materia de ciberseguridad para mejorar su situación al respecto.

# 6 Cooperación internacional

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

6.2 La UIT está prestando apoyo a la Presidencia del G20 (Arabia Saudita), a petición de ésta, como asociado en materia de conocimientos en diversos ámbitos, incluida la prioridad de la seguridad en la economía digital, como parte del esfuerzo de múltiples partes interesadas emprendido por la Secretaría del G20 para implicar a las organizaciones internacionales pertinentes.

6.3 La UIT, como principal organismo facilitador de la Línea de Acción C5 de la CMSI, organizó en el [Foro de la CMSI 2019](https://www.itu.int/net4/wsis/forum/2019/es) una sesión de alto nivel sobre inteligencia artificial y confianza, así como una sesión sobre la importancia de la medición de la ciberseguridad.

6.4 Siguiendo las instrucciones de la reunión del Consejo de 2019, el Secretario General ha presentado a la reunión del Consejo de 2020: 1) un informe en el que se explica la forma en que la UIT utiliza actualmente el marco de la ACG y; 2) con la participación de los Estados Miembros, directrices apropiadas elaboradas para la utilización de la ACG por la UIT, para su examen y aprobación por el Consejo.

# 7 Protección de la Infancia en Línea (PIeL)

7.1 Un grupo de trabajo multipartito de expertos, formado por más de 50 organizaciones y expertos, ha empezado a revisar las [Directrices para la Protección de la Infancia en Línea](https://www.itu.int/en/cop/Pages/guidelines.aspx), publicadas por primera vez en 2009.

7.2 En África se empezó a hablar de la implementación de marcos estratégicos nacionales en Chad, Kenya, Malawi y Rwanda. Concretamente, el Foro Regional de la PIeL, celebrado en Ghana, reunió a una amplia gama de expertos para analizar las eventuales soluciones y medidas que se pueden adoptar. En la Región Asia-Pacífico se prestó asistencia al desarrollo del Marco regional de la ASEAN para la Protección de la Infancia en Línea, aprovechando las Directrices para la PIeL, en coordinación con otros socios, como TELSOM/TELMIN. Se llevaron a cabo otras actividades en Europa, como parte de la iniciativa regional para aumentar la confianza y seguridad en la utilización de las TIC.

7.3 La UIT se ocupa también de la Secretaría de la Comisión de la Banda Ancha para el Desarrollo Sostenible. El Grupo de Trabajo sobre seguridad de la infancia en línea, dirigido por la *World Childhood Foundation* y Zain, publicó su [informe](https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Declaration.pdf) completo en Nueva York en octubre de 2019. Las Directrices para la PIeL sirvieron de referencia y se toman como base para la implementación de las recomendaciones del informe.

7.4 Se elaboró un estudio regional sobre los enfoques nacionales para mantener la seguridad de los jóvenes y los niños en línea, que se sometió a examen y consultas con los países. También se prestó asistencia a Georgia y Ucrania en la formulación de una estrategia nacional de protección de la infancia en línea.

7.5 La UIT celebró el Día de Internet más segura 2020 a través de diversas actividades, incluida la promoción de la protección de la infancia en línea. En el Día de Internet más segura 2020 se presentó la nueva mascota de la PIeL. Unos niños se encargaron de concebir y crear el [relato y antecedentes](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx) a comienzos de enero de 2020.

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