|  |  |
| --- | --- |
| **Consejo 2019 Ginebra, 10-20 de junio de 2019** | **logo_S_** |
|  | |
|  |  |
| **Punto del orden del día:** **PL 1.5** | **Documento C19/18-S** |
|  | **1 de abril de 2019** |
|  | **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 | |

|  |
| --- |
| Resumen  En el presente Informe se resumen las actividades de la UIT desde la reunión de 2018 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 solicitada  Se invita al Consejo a **tomar nota** del Informe.  \_\_\_\_\_\_\_\_\_\_\_\_  Referencia  *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),* [*181*](https://www.itu.int/en/council/Documents/basic-texts/RES-181-S.pdf) *(Guadalajara, 2010),* [*Reglamento de las Telecomunicaciones Internacionales*](http://www.itu.int/pub/S-CONF-WCIT-2012/en) *(Rev. Dubái, 2012),* [*Resolución 1306 del Consejo*](https://www.itu.int/md/S15-CL-C-0109/en)*, Resoluciones* [*45*](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/45revDubai.pdf) *(Rev. Dubái, 2014),* [*2, 67, 69*](https://www.itu.int/md/D14-WTDC17-C-0115/en) *(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/en)*), Resoluciones* [*50*](https://www.itu.int/pub/T-RES-T.50-2016)*,* [*52*](https://www.itu.int/pub/T-RES-T.52-2016)*,* [*75*](https://www.itu.int/pub/T-RES-T.75-2016) *(Rev. Hammamet, 2016),* [*58*](https://www.itu.int/pub/T-RES-T.58-2016) *(Rev. Dubái, 2012) de la AMNT, Documentos del Consejo* [*C05/32*](http://www.itu.int/md/S05-CL-C-0032/en)*,* [*C05/INF/10*](https://www.itu.int/md/S05-CL-INF-0010/en)*,* [*C06/4*](http://www.itu.int/md/S06-CL-C-0004/en)*,* [*C07/21*](http://www.itu.int/md/S07-CL-C-0021/en)*,* [*C08/33*](http://www.itu.int/md/S08-CL-C-0033/en)*,* [*C09/50*](http://www.itu.int/md/S09-CL-C-0050/en), [*C10/12*](http://www.itu.int/md/S10-CL-C-0012/en)*,* [*C11/54*](http://www.itu.int/md/S11-CL-C-0054/en)*,* [*C12/29*](http://www.itu.int/md/S12-CL-C-0029/en)*,* [*C13/23*](http://www.itu.int/md/S13-CL-C-0023/en), [*C14/23*](http://www.itu.int/md/S14-CL-C-0023/en), [*C15/18*](http://www.itu.int/md/S15-CL-C-0018/en)*,* [*C16/18*](https://www.itu.int/md/S16-CL-C-0018/en)*,* [*C17/18*](https://www.itu.int/md/S17-CL-C-0018/en) y [*C18/18*](https://www.itu.int/md/S18-CL-C-0018/en). |

# 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.

1.2 La Conferencia de Plenipotenciarios de la UIT de 2018, celebrada del 29 de octubre al 16 de noviembre de 2018 en Dubái, EAU, revisó sus Resoluciones 130 y 179.

# 2 Medidas jurídicas

2.1 En el marco del Objetivo 2.2 del Plan de Acción de Buenos Aires, 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 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 [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 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 tres reuniones, en marzo de 2018, agosto-septiembre de 2018 y enero de 2019. La CE 17 ha definido [55 nuevos temas de trabajo](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17). La CE 17 ha aprobado 17 Recomendaciones UIT-T nuevas o revisadas sobre seguridad de las TIC, a saber: [Aplicaciones genéricas de la sintaxis de mensaje criptográfico ASN.1](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12848); [arco de seguridad para el funcionamiento de redes de voz por evolución a largo plazo (VoLTE)](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13603); [Servicios de seguridad con interconexión de redes definidas por software](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13803); [Marco y requisitos de seguridad para el encadenamiento de funciones de servicio basada en la interconexión de redes definidas por software](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13872); [Control de acceso telebiométrico con tarjetas de identificación inteligentes](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13725); [autentificación telebiométrica por bioseñales](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13873); [Marco y requisitos de seguridad para la analítica de macrodatos en los servicios de Internet móvil](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13726); [Técnicas de evaluación de seguridad en redes de telecomunicaciones/TIC](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13404); [Casos de Uso de la Expresión de información sobre amenazas estructurada (STIX)](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13849); [Marco técnico para la lucha contra la publicidad basura en aplicaciones móviles](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13605); [Protocolo y metadatos de actualización de autentificación versión 1.0](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13606); [Marco de autentificación universal (MAU)](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13727); [Protocolo cliente a autentificador/marco universal de 2 factores](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13728); [Directrices de seguridad para dispositivos de red de área residencial (HAN) en sistemas de red eléctrica inteligente](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13405); [marco de seguridad para la Internet de las cosas basada en el modelo de pasarela](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13607); [Directrices sobre autentificación híbrida y mecanismos de gestión de claves en el modelo cliente-servidor](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13729). También ha acordado la [Recomendación sobre Requisitos de seguridad de los datos para el servicio de supervisión de la computación en la nube](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13406).

3.3 La CE 17 ha acordado la revisión del [Suplemento a la Recomendación UIT-T X.1051: Guía del usuario de controles de seguridad de la información en organizaciones de telecomunicaciones](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13730&lang=en), así como cinco nuevos Suplementos a la serie X de Recomendaciones UIT-T: [Suplemento a UIT-T X.805: Directrices de seguridad para operadores de red móvil virtual (MVNO)](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13410&lang=en); [Suplemento a UIT-T X.660: Directrices sobre utilización de identificadores de objeto para Internet de las Cosas](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13411&lang=en); [Suplemento a UIT-T X.1058: Código de práctica para la protección de información de identificación personal basada en UIT-T X.1058 para organizaciones de telecomunicaciones](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13593&lang=en); [Suplemento a UIT-T X.1231: Marco técnico para la lucha contra estafas en el servicio telefónico](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13731&lang=en), y [Suplemento a UIT-T X.1051 | ISO/CEI 27011 (2016): Tecnología de la información – Técnicas de seguridad – Código de práctica para controles de seguridad de la información basados en ISO/CEI 27002 para organizaciones de telecomunicaciones](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13869&lang=en).

3.4 El [Grupo Regional de la CE 17 para la Región Árabe](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/sg17rgarb/Pages/default.aspx) celebró su segunda reunión en Kuwait (octubre de 2018). El Grupo Regional de la CE 17 para África y el Grupo Regional para la Región Árabe se reunirán en Túnez, Túnez (abril de 2019).

3.5 La CE 17 organizó un [taller de la UIT sobre seguridad 5G (marzo de 2018)](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180319/Pages/default.aspx), [un taller de la UIT sobre ataques de seguridad avanzados y ransomware (agosto de 2018)](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180828/Pages/default.aspx), [un taller de la UIT sobre inteligencia artificial/aprendizaje automático y seguridad (enero de 2019)](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190121/Pages/default.aspx) y [un taller sobre comunicaciones cuánticas seguras (enero de 2019)](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/Secure%20quantum%20communication.aspx), destinados a identificar cómo la CE 17 puede abordar de la mejor manera la normalización de estos temas en el futuro, incluidos posibles nuevos temas de estudio.

3.6 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 (SC&C)".

3.7 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 Interfax común integrada para soluciones CA/DRM intercambiables.

3.8 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.

3.9 La CE 15 del UIT-T aprobó la Recomendación UIT-T G.9978, Admisión segura en redes G.hn, revisada.

3.10 La CE 20 del UIT-T aprobó la Recomendación UIT-T Y.4205, Requisitos y modelo de referencia de los sistemas de colaboración abierta relacionados con al IoT.

3.11 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 ha llevado a cabo 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 75 países y está realizando las actividades de seguimiento necesarias. Se ha finalizado la participación directa en 14 de esas actividades y hay más en curso o planificadas para 2019.

4.2 La UIT estableció una asociación con el Centro de Mundial de Capacidad en Ciberseguridad (Centro Académico Oxford Martin) para la realización conjunta de exámenes de capacidad de ciberseguridad en Tailandia, Sierra Leona y Madagascar. Gracias a la financiación del Gobierno australiano (DOCA), la UIT llevará a cabo evaluaciones de EIII en Samoa, Tonga, Vanuatu, y Papua New Guinea, seguidas de revisiones de capacidad de ciberseguridad. Además, la UIT realizó evaluaciones EIII en Albania, Bosnia y Herzegovina, Malawi, Mauritania y la República Democrática del Congo.

4.3 La UIT ha realizado 24 [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 [Grand Bassam, Côte d’Ivoire](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/IvoryCoastcyberdrill2018.aspx) (región de África, octubre de 2018); [Ciudad de La Plata, Argentina](https://www.itu.int/es/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2018/20577.aspx) (región de las Américas, junio de 2018); [Kuwait City, Kuwait](https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Pages/Events/2018/Cyber/Cyber.aspx) (región Árabe, octubre de 2018); [Limassol, Chipre](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/CYBDRILL/ITU-ALERT-Cyber-drill.aspx) (región de Europa, noviembre de 2018) y [Baku, Azerbaiyán](https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Pages/EVENTS/2018/09_Baku/09_Baku.aspx) (región CEI, septiembre de 2018). Se está organizando un Cibersimulacro 2019 para Europa en [Rumania (mayo de 2019)](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2019/CyberDrill/ITU-Cyber-Drill-for-Europe-Region-.aspx).

4.4 En el marco de un proceso de colaboración multipartita facilitado por la UIT, en el que han participado 15 organizaciones intergubernamentales, miembros del sector privado, instituciones académicas y representantes de la sociedad civil, se publicó en septiembre de 2018 la [Guía de elaboración de estrategias nacionales de ciberseguridad (ENC)](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf). La iniciativa ENC ofrece una herramienta funcional de ayuda a los gobiernos a la hora de elaborar y mejorar sus estrategias de ciberseguridad. La UIT está organizando talleres nacionales y regionales sobre estrategias de ciberseguridad para ayudar a sus Estados Miembros a elaborar sus ENC. En 2018 se celebró un taller nacional en Polonia y en junio de 2019 se celebrará el taller para la región de Europa. Están en curso las negociaciones para organizar talleres similares para los países de la SADC, Malta, Benín y Guinea. La UIT prestó su asistencia a Mauritania para la elaboración de su ENC y celebró un taller de validación (Nuakchott, diciembre de 2018) para presentar el informe intermedio de la ENC 2019-2022 en Mauritania. La UIT prestó asimismo su asistencia a Kiribati y Bhután para la definición de su ENC (noviembre de 2018).

# 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.

5.2Después de la CMDT-2017, 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=1&sp=2014&rgq=D14-SG02-RGQ03.2&stg=2)) proseguirá su labor en el periodo de estudios 2018-2021.

5.3 La UIT, la ICANN y la WATRA organizaron un taller de capacitación sobre ciberseguridad, EIEI y el ecosistema ICANN (Uagadugú, Burkina Faso – octubre de 2018) por invitación de la Autoridad de Reglamentación de Correos y Comunicaciones Electrónicas (ARCEP).

5.4 La UIT y el Centro de Ciberseguridad de la UIT para la Región Árabe organizaron la [Semana regional de la ciberseguridad](https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Pages/Events/2018/Cyber/Cyber.aspx) (Kuwait – octubre de 2018), plataforma para intensificar la cooperación y la comunicación entre los EIII árabes.

5.5 La UIT, el Centro de Formación Avanzada en Telecomunicaciones y la Facultad de Ciencias aplicadas de correos y telecomunicaciones (Facultad TIC, República Islámica de 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).

5.6 En marzo de 2019, en paralelo a la reunión de las Comisiones de Estudio del UIT-D, se publicó la tercera versión del [Índice Mundial de Ciberseguridad](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCIv3), en el que han participado 155 Estados Miembros. GCIv3 contiene más detalles sobre la ciberseguridad al haber ampliado la asociación hasta convertirla en una plataforma de colaboración multipartita. La UIT ha iniciado la fase preparatoria del proceso GCIv4, que dará comienzo en abril de 2019.

5.7 La UIT organizó el [Taller regional de la UIT para Europa y la CEI sobre ciberseguidad y protección de la infancia en línea](https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Pages/EVENTS/2018/04_Odessa/04_Odessa.aspx) (Odessa, Ucrania – abril de 2018).

# 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 EIISI/EIEI regionales, como el EIEI AP, el EIEI ÁFRICA y el EIEI OIC.

A finales de 2016 cesaron todas las actividades emprendidas en el marco de la asociación de la UIT con IMPACT al haberse completado la ejecución de los proyectos pendientes. IMPACT comunicó su disolución oficial a principios de 2018. Tal disolución implica la expiración con efecto inmediato del MoU y el acuerdo de cooperación concluidos entre UIT e IMPACT.

6.2 La UIT, principal organismo facilitador de la Línea de Acción C5 de la CMSI, organizó en el [Foro de la CMSI 2018](https://www.itu.int/net4/wsis/forum/2018/) varias reuniones dedicadas al 10º aniversario de la GCA y la iniciativa Protección de la Infancia en Línea. Durante el [Foro de la CMSI 2019](https://www.itu.int/net4/wsis/forum/2019/) también se celebraron sesiones de alto nivel, entre otras cosas sobre inteligencia artificial y seguridad.

6.3 En julio de 2018 la UIT organizó un [Diálogo Mundial sobre IA, IoT, Política de Ciberseguridad y Oportunidades y Retos Reglamentarios](https://www.itu.int/net4/ITU-D/CDS/GSR/2018/default.asp), que reunió a organismos reguladores de distintos Estados Miembros y otras organizaciones.

6.4 La UIT se asoció con instituciones académicas de la región Árabe (Red de Investigación y Educación de los Estados Árabes y Universidad Árabe Naïf de Ciencias de Seguridad) para intensificar su participación en el fomento de una cultura de la ciberseguridad y una activa participación en el trabajo de la UIT. En el marco de esas asociaciones se organizaron actividades en la región Árabe.

6.5 En el marco de la Iniciativa Regional de la UIT para Europa, la UIT ha coorganizado una serie de eventos de ciberseguridad entre los que se cuentan los siguientes: [6ª Plataforma de diálogo público-privado sobre ciberseguridad en la Europa central](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/CYBR/Cyber-Security-in-Romania.aspx) (Sibiu, Rumania – septiembre de 2018); Foro Internacional sobre ["Nuevos retos mundiales de ciberseguridad"](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/CERT-ROForum/default.aspx) (Bucarest, Rumania – octubre de 2018); Pl[ataforma de diálogo público-privado sobre ciberseguridad en la Europa occidental](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/CYBCONGR/Second-Western-European-Cybersecurity-Public-Private-Dialogue-Platform.aspx) (Porrentruy, Suiza – noviembre de 2018); [Semana de la ciberseguidad de Viena – Protección de la infraestructura esencial](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/cybervienna.aspx) (Viena, Austria (coorganizado por la CEI con el apoyo de la OSCE) – marzo de 2019).

# 7 Protección de la Infancia en Línea (PIeL)

7.1 La UIT brindó asistencia a Sudán para la elaboración de su estrategia de PIeL nacional. Además, se organizaron en diversos países árabes varias conferencias y concursos para, en colaboración con las partes interesadas pertinentes, dar a conocer la importancia de la seguridad en Internet a niños, educadores y padres.

7.2 En el marco de la Iniciativa Regional de la UIT para Europa, la UIT prestó asistencia a Georgia para la elaboración de su estrategia de PIeL nacional. Se ha previsto llevar a cabo actividades semejantes en otros países a lo largo del próximo periodo. Además, la UIT ha coorganizado diversos eventos destinados a la capacitación entre los que se cuentan los siguientes: [Evento Naciones sobre Protección de la Infancia en Línea: Concienciación de niños y adolescentes](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/NECOP/default.aspxhttps:/www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/NECOP/default.aspx) (Noto, Italia – mayo de 2019); [Foro Digital de la Juventud](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/DYF/default.aspx) (Varsovia, Polonia – mayo de 2018); Conferencia Internacional sobre ["Mantener la seguridad de los niños y los jóvenes en línea"](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/COP/default.aspx) (Varsovia, Polonia – septiembre de 2018), y [Día de Internet más segura 2019](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2019/SID/Safer-Internet-Day-2019.aspx) (Tirana, Albania – febrero de 2019).

7.3. En noviembre de 2018, la UIT prestó asistencia a Kiribati y Bhután en el marco de las evaluaciones PIeL. La UIT preparó también un artículo sobre la "Mejora de las medidas de protección de la infancia en línea en ASEAN: Asociación con la industria" y un [Entorno de aprendizaje virtual multiusuario 3D](https://www.youtube.com/watch?v=SymYlZq5v1k&feature=youtu.be) para aumentar la visibilidad de los riesgos que corren los niños en línea.

7.4. La UIT celebró el Día de Internet más segura 2019 a través de diversas actividades, incluida la promoción de la protección de la infancia en línea.

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