|  |  |
| --- | --- |
| **Consejo 2021 Consulta virtual a los consejeros, 8-18 de junio de 2021** |  |
|  | |
|  |  |
| **Punto del orden del día: PL 1.4** | **Documento C21/18-S** |
|  | **22 de febrero de 2021** |
|  | **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 realizadas por la UIT en 2020 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).  La versión de 2020 de este informe (C20/18), preparada para la reunión del Consejo de 2020, no ha sido examinada.  Acción solicitada  Se invita al Consejo a **tomar nota** del Informe, así como del Documento C20/18.  \_\_\_\_\_\_\_\_\_\_\_\_  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) *(Rev. Dubái, 2018) y* [*181*](https://www.itu.int/en/council/Documents/basic-texts/RES-181-S.pdf) *(Guadalajara, 2010) de la Conferencia de Plenipotenciarios,* [*RTI*](https://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 [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)*,* [*C19/18*](https://www.itu.int/md/S19-CL-C-0018/es) *y* *[C20/18](https://www.itu.int/md/S20-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), 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 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 ONUDC y otras organizaciones pertinentes que prestan asistencia a los Estados Miembros.

# 3 Medidas técnicas y de procedimiento

3.1 La [Comisión de Estudio 17 del UIT-T (CE 17)](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 2020, en la que la CE 17 estableció [15 nuevos temas de trabajo de normalización](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17). Y una sesión Plenaria electrónica, el 7 de enero de 2021. La CE 17 aprobó más 40 Recomendaciones nuevas o revisadas en materia de seguridad de las TIC, a saber: [X.510 | ISO/IEC 9594-11](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14320); [serie X.680‑690](https://www.itu.int/rec/T-REC-x/en); [X.1046](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1046); [X.1052 (revisada)](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14044) y [X.1054 (revisada, en fase de aprobación)](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1054); [X.1148](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14249); [X.1149](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14250); [X.1216](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14259), [X.1217](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1217)y [X.1218](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14444); [X.1254 (revisada)](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14260), [X.1279](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14261), [D.1140/X.1261](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1261), [X.1451](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14252) y [X.1452](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14451); [X.1363](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14087), [X.1364](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14088), [X.1365](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14089), [X.1366](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14262), [X.1367](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14263), y [X.1368](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1368);[X.1371](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14090), [X.1374](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14446), [X.1375](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14447) y [X.1376](https://www.itu.int/rec/T-REC-x/recommendation.asp?lang=en&parent=T-REC-X.1376); [X.1400](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14449), [X.1401](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14092), [X.1402](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14251), [X.1403](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14264) y [X.1404](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14450); [X.1606](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14265); [X.1710](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14452) y [X.1714](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14453); [X.1750](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14266) y [X.1751](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14267), yX.1811 (en fase de aprobación)**.**

3.3 La CE 17 también adoptó los siguientes informes técnicos: "Marco de seguridad para la distribución de claves cuánticas en las redes de telecomunicaciones", "Problemas, requisitos y posibles soluciones para la resolución de OID", "Seguridad en las telecomunicaciones y en la tecnología de la información (7ª edición)", "Utilización satisfactoria de las normas de seguridad (2ª edición)", "Descripción del mecanismo de incubación y formas de mejorarlo", "Enfoques estratégicos para la transformación de los estudios de seguridad", y "Modelo de seguridad unificado (USM): Sistema integrado neutral para la ciberseguridad".

3.4 En el marco de los preparativos para la AMNT-20, la CE 17 convino en reestructurar sus actuales 14 Cuestiones para dejarlas en 12 Cuestiones. Al haberse aplazado la AMNT-20, este nuevo conjunto de 12 Cuestiones fue aprobado por el GANT en su reunión de enero de 2021 y entró en vigor el 18 de enero de 2021 para el resto del periodo de estudio.

3.5 La CE 3 del UIT-T sigue estudiando los aspectos económicos y políticos de los macrodatos y la identidad digital en relación con los servicios de telecomunicaciones internacionales en el marco de su Cuestión 11/3. La CE 3 aprobó recientemente la [Recomendación UIT-T D.267/X.1261](https://www.itu.int/rec/T-REC-D.1140-202008-I).

3.6 La CE 11 del UIT-T sigue mejorando los protocolos de señalización para hacerlos más seguros, lo que incluye el desarrollo de requisitos adicionales para el intercambio de mensajes de señalización y protocolos particulares. La CE 11 del UIT-T aprobó el [Informe técnico QSTR-SS7-DFS](https://www.itu.int/pub/publications.aspx?lang=en&parent=T-TUT-PROTO-2019), la pila de protocolos SS7 revisada (Q.731.3-Q.731.6) y la Recomendación UIT-T [Q.3057](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.3057). Asimismo, la CE 11 del UIT-T sigue elaborando normas UIT-T [Q.5050](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5050), [Q.5051](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5051), [Q.5052](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5052) y [Q.5053](https://www.itu.int/rec/T-REC-q/recommendation.asp?lang=en&parent=T-REC-Q.5053) relativas a la lucha contra dispositivos la falsificación y el robo de dispositivos de telecomunicaciones/TIC.

3.7 La CE 9 del UIT-T aprobó las siguientes Recomendaciones sobre seguridad: UIT-T [J.1012](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13573), [J.1013](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13574), [J.1014](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13575), [J.1015](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13576), y [J.1015.1](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13837); UIT-T [J.1204](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14357); y [J.1031](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14280), [J.1032](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14355), y [J.1033](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14356). La CE 9 también aprobó tres Suplementos a las Recomendación de la serie J (UIT‑T J.1012-J.1015.1), a saber ([J.Sup7](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14286), [J.Sup8](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14287) y [J.Sup9](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14288)).

3.8 La CE 13 del UIT-T aprobó las siguientes Recomendaciones: UIT-T [Y.3055](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14393) sobre marcos de confianza para la gestión de datos personales y UIT-T [Y.3801](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14258), [Y.3802](https://www.itu.int/rec/T-REC-y/recommendation.asp?lang=en&parent=T-REC-Y.3802), [Y.3803](https://www.itu.int/rec/T-REC-y/recommendation.asp?lang=en&parent=T-REC-Y.3803) y [Y.3804](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14409) sobre redes de distribución de claves cuánticas.

3.9 La CE 20 del UIT-T preparó las siguientes Recomendaciones sobre seguridad: [Y.4560](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14379), [Y.4561](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14380), [Y.4808](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14381), y [Y.4907](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14382).

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) [*Grupo Temático del UIT-T sobre Inteligencia artificial para la salud (FG AI4H)*](https://www.itu.int/en/ITU-T/focusgroups/ai4h); 2) [*Grupo Temático del UIT-T sobre multimedios en vehículos (FG VM)*](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx);3) [*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); 4) [*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)*;* 5) [*Grupo Temático del UIT-T sobre la IA para la gestión de catástrofes naturales (FG-AI4NDM)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ndm/Pages/default.aspx)*;*y 6)[*Grupo Temático del UIT-T sobre redes autónomas (FG-AN)*](https://www.itu.int/en/ITU-T/focusgroups/an/Pages/default.aspx)

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). La información sobre las [tecnologías móviles futuristas, las “IMT para 2020 y en adelante”](https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx), figura en el sitio web.

# 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 (CIRT) en más de 80 países y está adoptando las medidas de seguimiento necesarias para prestar asistencia a los Estados Miembros en su implementación. En 2020, la UIT evaluó los CIRT de Guyana y Bermudas, y finalizó el informe de evaluación de Liberia. Se ha realizado la participación directa en el establecimiento y/o mejora de 14 CIRT nacionales, y de los 7 proyectos que están actualmente en curso, 3 finalizarán durante el primer trimestre de 2021. La UIT y el Gobierno de las Bahamas también han firmado un acuerdo de cooperación para, entre otras cosas, la creación de un CIRT nacional.

4.2 La UIT ha realizado, hasta la fecha, 29 [cibersimulacros](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) en más de 100 países. Entre septiembre y diciembre de 2020, la UIT ha organizado y ejecutado un ITU 2020 [Cibersimulacro mundial](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx) en diversos eventos en línea que consistieron en diálogos regionales, seminarios técnicos y de política por la web y formación sobre utilización de herramientas y desarrollo de aptitudes, además del [Cibersimulacro para las Islas del Pacífico](https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2020/Pacific%20Cyberdrill/Pacific-Cyberdrill21.aspx), de ámbito regional.

# 5 Capacitación

5.1 Con ocasión del [Cibersimulacro Mundial de la UIT](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx), la BDT organizó foros regionales de ciberseguridad para todas las regiones de la UIT para la capacitación humana y organizativa.

5.2 De conformidad con la CMDT-17, 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)) prosiguió sus trabajos durante en el periodo de estudios 2018-2021.

5.3 Ya ha comenzado el proceso para actualizar la [Guía para la elaboración de una estrategia nacional de ciberseguridad](https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018) (NCS) y cabe esperar en octubre de 2021. Actualmente hay más de 20 organizaciones que contribuyen a la actualización. La UIT también realizó el seminario web: “[Estrategias Nacionales de Ciberseguridad – implementación y supervisión](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/2020-NCS-IM-webinar.aspx)” el 19 de octubre de 2020, para examinar el ciclo de desarrollo e implementación de una NCS. Las actividades de asistencia técnica en materia de NCS han comenzado con Fiyi, Liberia y Chad, y hay conversaciones en curso con otros Estados Miembros que necesitan asistencia. El 20 de febrero de 2020 se celebró en Melbourne (Australia) un taller regional para la región de Asia-Pacífico sobre “[Ciclo de vida y desarrollo de estrategias nacionales de ciberseguridad](https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/ITU-regional-workshop-national-cybersecurity-strategies.aspx)”. La UIT también está finalizando el material didáctico en línea para el desarrollo de las NCS que se impartirán a través de la Academia de la UIT en el segundo trimestre de 2021.

5.4 A través de la [Academia de la UIT](https://academy.itu.int/training-courses/full-catalogue?search_api_fulltext=&field_taxon_registration=All&field_course_fee=All&field_taxon_region=All&field_taxon_type=All&field_taxon_topics=109&field_taxon_languages=All&date_start=&date_end=&items_per_page=10), la UIT y CoE siguen impartiendo actividades y talleres de formación en diversos ámbitos del dominio de ciberseguridad.

5.5 Para hacer frente a los problemas de ciberseguridad durante la pandemia COVID-19 y [suministrar a la infraestructura sanitaria de los Estados Miembros información oportuna sobre las ciberamenazas](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Covid-19-CNI-Solution.aspx), los BitSight, un Miembro de Sector de la UIT, proporcionó acceso a su plataforma de valoración de seguridad a los Estados Miembros de la UIT.

5.6 La cuarta versión de la encuesta del [Índice de Ciberseguridad Mundial](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (ICM) de la UIT, con un cuestionario y una metodología mejorados, se ha puesto en marcha y está actualmente en curso. La encuesta GCI ha concluido el 30 de septiembre de 2020. Además de los expertos del mundo académico y del sector privado, se invitó a todos los Estados Miembros a designar expertos para participar y contribuir a la reunión del [Grupo de Expertos en la ponderación del ICM](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx), celebrada el 15 de octubre de 2020.

5.7 Para promover la participación de los jóvenes en el campo de la ciberseguridad y para hacer frente a la escasez de mano de obra en todo el mundo, la UIT lanzará la iniciativa Youth4Cyber.

5.8 La UIT también está ultimando el plan para poner en marcha el programa de tutorías sobre ciberseguridad para mujeres, destinado a capacitar a las jóvenes profesionales que deseen entrar o prosperar en el campo de la ciberseguridad.

# 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 CIRT/CERT regionales, como el CERT AP, el CERT ÁFRICA y el CERT OIC.

6.2 Siguiendo las instrucciones de la reunión del Consejo de 2019, el Secretario General presentará a la próxima reunión del Consejo: 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. De conformidad con el proceso establecido por el Consejo de 2019 para la elaboración del proyecto de Directrices, y tras la primera consulta abierta en línea celebrada el 23 de abril de 2020 para que todas las partes interesadas de la CMSI formulen comentarios sobre el proyecto de Directrices, se celebrará una segunda consulta abierta en línea para todas las partes interesadas de la CMSI el 1 de marzo de 2021.

6.3 En su calidad de facilitador principal de la Línea de Acción C5 de la CMSI, la UIT organizó varias sesiones en el [Foro de la CMSI 2020](https://www.itu.int/net4/wsis/forum/2020/en), en particular una relativa a "La ciberseguridad en la era de la tecnología de la información cuántica (TIQ): retos y consideraciones para las redes de TIC" y un diálogo de alto nivel sobre "Garantizar una atención sanitaria digna de confianza en un mundo de la inteligencia artificial”.

# 7 Protección de la Infancia en Línea (COP)

7.1 Un grupo de trabajo multipartito de expertos, integrado por más de 50 organizaciones y expertos de distintos sectores, ha examinado cuatro series de [Directrices sobre la protección de la infancia en línea para responsables políticos, industria, padres y educadores, y niños](https://www.itu.int/en/cop/Pages/guidelines.aspx). Tras el [lanzamiento mundial de las nuevas Directrices](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/2020-COP-Guidelines-launch-webinar.aspx) se organizaron varios [eventos regionales de promoción](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/2020/Regional-Launches-COP-2020-Guidelines.aspx) destinados a examinar las oportunidades de implementación a escala regional y nacional.

7.2 En África, antes del lanzamiento de las Directrices en la región, se impartió la primera formación sobre COP, en inglés y francés, destinada a los responsables políticos. En la región de la CEI, la Oficina Regional de la UIT para la CEI elaboró un [Curso de seguridad en línea](https://onlinesafety.info/#/home) en colaboración con la Academia Nacional de Telecomunicaciones A.S. Popov de Odessa. En la región de Asia-Pacífico, se prestó asistencia para el desarrollo de estrategias nacionales de COP y marcos conexos a seis pequeños países insulares en desarrollo, basadas en las Directrices de CP, en coordinación con otros asociados, a través de un proyecto conjunto con el Departamento de Comunicaciones y Artes (DoCA) de Australia. En las Américas, se han iniciado conversaciones con Colombia, Costa Rica, Brasil y Paraguay sobre la elaboración y aplicación de marcos estratégicos nacionales. El despliegue de las Directrices de COP avanzó significativamente en Europa, donde se llevaron a cabo numerosas actividades, en el contexto de la iniciativa regional sobre la mejora de la fiabilidad y confianza en la utilización de las TIC.

7.3 El Reino de Arabia Saudí y la UIT firmaron un acuerdo para poner en marcha un programa mundial de tres años de duración sobre la "Creación de un ciberentorno seguro y habilitador para los niños", que consiste en la asistencia política a los gobiernos y en el desarrollo de las competencias y la alfabetización digitales para los usuarios finales. La ejecución del programa comenzará en el primer trimestre de 2021.

7.4 Se publicó un informe sobre la “[situación de los ecosistemas nacionales de protección de la infancia en línea en el sureste de Europa](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/FINAL%20REPORT.pdf)”, complementado por numerosos eventos y foros (co)organizados sobre el tema de la protección de la infancia en línea en Europa.

7.5 Para celebrar el Día de la Seguridad en Internet 2021, la UIT publicó varios comunicados, entre ellos una entrada en la [bitácora](https://www.itu.int/en/myitu/News/2021/02/08/18/38/Sango-Internet-safety-drawing-child-online-protection-COP) sobre la aplicación de la mascota de la COP en un concurso nacional de dibujo en Hungría. La mascota de la COP anunció además un [proyecto de colaboración con Eni y Deloitte Italia](https://www.bing.com/videos/search?q=sango+announcing+eni+youtube&docid=13903411089711&mid=271E2ABE304F85C97D50271E2ABE304F85C97D50&view=detail&FORM=VIRE) para sensibilizar y capacitar a niños y educadores sobre la seguridad en línea.

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