|  |  |
| --- | --- |
| **Consejo 2022 Ginebra, 21-31 de marzo de 2022** |  |
|  | |
|  |  |
| **Punto del orden del día: PL 1.4** | **Documento C22/18-S** |
|  | **18 de febrero de 2022** |
|  | **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 2021 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) *(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), [C20/18](https://www.itu.int/md/S20-CL-C-0018/es) *y* [*C21/18*](https://www.itu.int/md/S21-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 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 dos reuniones en abril y agosto/septiembre de 2021, en las que la CE 17 estableció 22 [nuevos temas de trabajo de normalización](https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17) y dos sesiones plenarias electrónicas en los meses de enero de 2021 y de 2022. La CE 17 aprobó más de 30 Recomendaciones nuevas o revisadas sobre seguridad de las TIC, a saber: X.1011, X.1046, X. 1047, X.1054 (revisada), X.1060, X.1061, X.1080.2, X.1217, X.1233, X.1234, X.1235, X.1252, X.1333, X.1369, X.1376, X.1405, X.1406, X.1407, X.1408, X.1453, X.1470, X.1643, X.1712, X.1752, X.1770, X.1811 y X.Suppl.36.

3.3 La CE 17 también alcanzó un acuerdo en relación con el Informe Técnico "Marco para la normalización de la seguridad de los servicios virtualizados".

3.4 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.1102, "Mecanismos de compensación al consumidor y de protección del consumidor relacionados con los OTT”](https://www.itu.int/rec/T-REC-D.1102).

3.5 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-USSD "Encriptado de bajo consumo de recursos y resistencia cuántica de los mensajes USSD para su utilización en los servicios financieros" y Q.Suppl.75, relativo a la lucha contra dispositivos la falsificación y el robo de dispositivos de telecomunicaciones/TIC.

3.6 La CE 9 del UIT-T aprobó las Recomendaciones [UIT-T J.1026](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14868), [J.1027](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14869), [J.1028](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14870) y [J.1204](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14357) revisadas. La CE 9 aprobó también la J.1205 y continuó la actualización de la Guía del Implementador de la UIT-T [J.1012](https://www.itu.int/ITU-T/recommendations/rec.aspx?id=13573) y dos Suplementos a las siguientes Recomendaciones 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) y [J.Sup8](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14287).

3.7 La CE 13 del UIT-T aprobó las siguientes Recomendaciones: UIT-T 3056 eY.3057 sobre los marcos de confianza para la gestión de datos personales y UIT-T 3805 e Y.3806, sobre las redes de distribución de claves cuánticas.

3.8 La CE 15 del UIT-T aprobó el Suplemento UIT-T G.Suppl.OTNsec, "Optical transport network security" (Seguridad de las redes ópticas de transporte).

3.9 La CE 16 del UIT-T aprobó la Recomendación UIT-T F.747.10 "Requisitos de los sistemas de libro mayor distribuido para la prestación de servicios con factor humano protegido" (en publicación), que establece los requisitos generales y las capacidades funcionales de los sistemas de libro mayor distribuido (DLS) que permiten garantizar la seguridad de los servicios personales.

3.10 La CE 20 del UIT-T preparó las siguientes Recomendaciones sobre seguridad: [Y.4808](https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14381), Y.4810 e Y.4811.

3.11 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 relativo a federaciones de bancos de pruebas para las IMT-2020 y sistemas posteriores (FG-TBFxG)*](https://www.itu.int/en/ITU-T/focusgroups/tbfxg/Pages/default.aspx); 2) [Grupo Temático del UIT-T relativo a "inteligencia artificial (IA) e Internet de las Cosas (IoT) para la agricultura digital" (GT-AI4A)](https://www.itu.int/en/ITU-T/focusgroups/ai4a/Pages/default.aspx); 3) [*Grupo Temático del UIT-T sobre Inteligencia artificial para la gestión de catástrofes naturales (FG AI4NDM)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ndm/Pages/default.aspx); 4) [*Grupo Temático del UIT-T sobre Redes Autónomas (FG-AN)*](https://www.itu.int/en/ITU-T/focusgroups/an/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 eficiencia energética para la inteligencia artificial y otras tecnologías emergentes (FG-AI4EE)*](https://www.itu.int/en/ITU-T/focusgroups/ai4ee/Pages/default.aspx)*; 7) ;* [*Grupo Temático del UIT-T sobre Inteligencia artificial para la salud (FG AI4H)*](https://www.itu.int/en/ITU-T/focusgroups/ai4h)*;* y 8)[*Grupo Temático sobre multimedios en vehículos (FG-VM)*](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx).

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). 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 En 2021, la UIT realizó evaluaciones técnicas para valorar la preparación a efectos del establecimiento de Equipos de intervención en caso de incidente informático (EIII) en más de 80 países y está adoptando las medidas de seguimiento necesarias para prestar asistencia a los Estados Miembros en su implantación. Antes de 2021 se realizó la participación directa en el establecimiento y/o la mejora de 17 EIII nacionales, tres (3) proyectos se completaron en 2021, se efectuó una evaluación de los EIII para Guinea Bissau, Bahamas, Mongolia y Guyana, se revisó el diseño de los EIII para Eswatini, y actualmente hay cuatro proyectos de implantación de EIII en curso. La UIT también ha ayudado a Malí y a Malawi a diseñar los marcos nacionales de la infraestructura de clave pública (PKI) para cada uno de los países.

4.2 La UIT ha realizado, hasta la fecha, 34 [cibersimulacros](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) en más de 120 países. Entre septiembre y diciembre de 2021, la UIT ha organizado y ejecutado un ITU 2021 [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 de dos Cibersimulacros subregionales para los países de la CEDEAO y la SADC y un Cibersimulacro nacional para la India. Asimismo, en 2021 se elaboraron dos publicaciones: "Operational framework and guidelines for the planning and execution of ITU regional CyberDrills" y "ITU cybersecurity programme: CIRT framework".

# 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 La UIT facilitó el proceso de actualización de la [Guía para la elaboración de una estrategia nacional de ciberseguridad](https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018) (NCS). Más de [20 organizaciones](https://ncsguide.org/partners/) contribuyeron a la [segunda edición de la Guía](https://ncsguide.org/the-guide/), que se presentó en noviembre de 2021 mediante un seminario web mundial en el que se examinó el desarrollo del ciclo de vida y la implementación de una NCS, se destacaron los retos y las oportunidades y se pidió una mayor cooperación. Se han emprendido actividades de asistencia técnica sobre las NCS con Bahamas, Rwanda, Marruecos y la región de la SADEC, y hay conversaciones en curso con otros Estados Miembros que necesitan asistencia. La UIT también concluyó y publicó en línea el curso de formación "[Ciclo de vida, principios y buenas prácticas en la elaboración e implementación de la Estrategia Nacional de Ciberseguridad](https://academy.itu.int/training-courses/full-catalogue/lifecycle-principles-and-good-practices-national-cybersecurity-strategy-development-and)" en la plataforma de la Academia de la UIT en tres idiomas (inglés, francés y español). La versión rusa del curso estará disponible en marzo de 2021. La UIT se está asociando con el Grupo del Banco Mundial para organizar seminarios web regionales con el fin de proporcionar información operativa sobre cómo desarrollar un plan de acción de NCS. La UIT está desarrollando una herramienta de evaluación comparativa de las NCS para apoyar a los Estados Miembros y a los profesionales de la ciberseguridad en sus esfuerzos de implantar una NCS. La prueba piloto de la herramienta finalizó en enero y el trabajo de actualización continuará en 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 [El 29 de junio de 2021 se presentó](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI/GCIv4-Report-Launch.aspx) la cuarta edición del informe sobre el [Índice de Ciberseguridad Global](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (ICG).  Esta edición del índice abarca 193 Estados Miembros y el Estado de Palestina, y ha contado con la contribución de 169 países que han aportado datos.  Ya se ha empezado a trabajar en un cuestionario actualizado para el ICG. En octubre de 2021 se presentó virtualmente el nuevo conjunto de documentos a la Comisión de Estudio 2 del UIT-T en el marco de la Cuestión 3, y la Comisión de Estudio creó un Grupo por Correspondencia virtual para aportar contribuciones sobre el cuestionario revisado. Se prevé publicar una nueva edición del cuestionario del ICG a principios de 2022.

5.6 Para promover la participación de los jóvenes en el campo de la ciberseguridad y para concienciar sobre la escasez de mano de obra en todo el mundo, la UIT está organizando actividades y colaboraciones, por y para los jóvenes, en el marco de la iniciativa Generation Connect.

5.7 La UIT ha completado con éxito la primera edición del 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. En abril de 2022 se iniciará una nueva cohorte, cuyos grupos objetivo residen en las regiones de África, los países árabes y Asia-Pacífico.

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

6.2 El Consejo, en su reunión de 2019, encargó al Secretario General que presentara al Consejo las directrices apropiadas elaboradas para la utilización de la Agenda sobre Ciberseguridad Global (ACG), para su examen y aprobación. En consecuencia, el Secretario General preparó y presentó a la Consulta Virtual de Consejeros de 2021 (C21/VCC1) el [Documento C21/71](https://www.itu.int/md/S21-CL-C-0071/es). Tras los debates celebrados en la C21/VCC-1, los Estados Miembros del Consejo encargaron a la secretaría que "*celebre nuevas consultas con los Estados Miembros del Consejo, habida cuenta de las contribuciones recibidas y los comentarios realizados en la reunión en curso. La secretaría debe volver a presentar la revisión del Documento 71 para su examen y aprobación en la próxima reunión del Consejo*". Actualmente se están celebrando consultas con los Estados Miembros del Consejo y se presentará un documento revisado al Consejo de 2022 para su examen y aprobación.

6.3 En su calidad de facilitador principal de la Línea de Acción C5 de la CMSI, la UIT organizó una sección dedicada a la ciberseguridad que constaba de varias sesiones en el [Foro de la CMSI](https://www.itu.int/net4/wsis/forum/2020/es) 2021, en particular una sesión de facilitadores de la Línea de Acción C5 sobre sobre "Ciberseguridad: medidas multidimensionales de ciberseguridad – Oportunidades y retos actuales en el uso de índices para comprender la ciberseguridad", la Segunda Consulta Abierta sobre el proyecto de Directrices para la utilización de la ACG, y un diálogo de alto nivel sobre la "Comprobación de la preparación de la IA: Impacto político, oportunidades y retos".

# 7 Protección de la Infancia en Línea (COP)

7.1 Se incorporó la protección de la infancia en línea como uno de los elementos clave del cuarto pilar en el proyecto conjunto de la UIT y UNICEF Giga.

7.2 La UIT también ha firmado un acuerdo de colaboración con la Fundación SCORT sobre la PIeL. La UIT ha contribuido a muchos debates, como el Día de la Seguridad en Internet 2021 y la 15ª Conferencia Europea de Fútbol para el Desarrollo, así como a una mesa redonda con clubes de fútbol europeos.

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 comenzó en 2021 con la firma de un documento de proyecto interno de la UIT. La UIT ha comenzado a ejecutar el proyecto centrándose en la capacitación mediante el desarrollo de formaciones en línea autogestionadas para todas las partes interesadas pertinentes y otras soluciones interactivas para que los niños y los jóvenes se conviertan en ciudadanos digitales responsables.

7.4 Todas las regiones de la UIT empezaron a poner en práctica las actividades del proyecto mundial "Creación de un ciberentorno seguro y habilitador para la infancia". El primer país que emprendió esta iniciativa fue Albania, seguido de Malawi y Marruecos.

7.5 Para celebrar el Día de la Seguridad en Internet 2021, la UIT publicó varios comunicados, entre ellos una entrada en el [blog](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. Además, la mascota de la COP moderó diferentes eventos virtuales, como por ejemplo el segmento dedicado a la seguridad en línea de la serie de [eventos conmemorativos del Día de las Niñas](https://www.itu.int/women-and-girls/girls-in-ict/girlsinict-online-safety-moment/) en las TIC y la [Sesión 4: Inclusión Digital Segura – Protección Infantil en Línea](https://www.itu.int/es/ITU-D/Conferences/GSR/2021/Pages/global.aspx) en el GSR 2021.

7.6 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. El [curso sobre seguridad en línea con Sango](https://www.itu-cop-guidelines.com/children), dividido en cinco episodios, ofrece consejos prácticos a los niños de hasta 9 años sobre los riesgos a los que pueden exponerse en línea.

7.7 A través de la Academia de la UIT, la UIT impartió una sesión de formación para los reguladores de la Región Árabe sobre la protección de los niños en línea.

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