|  |  |
| --- | --- |
| **Consejo 2020 Ginebra, 9-19 de junio de 2020** |  |
|  | |
|  |  |
| **Punto del orden del día: PL 1.4** | **Documento C20/36-S** |
|  | **5 de mayo de 2020** |
|  | **Original: inglés** |
| Informe del Secretario General | |
| informe en el que se explica cómo utiliza actualmente la UIT  la [Agenda sobre Ciberseguridad Global](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) (ACG) | |

|  |
| --- |
| Resumen  En su reunión de 2019, el Consejo encargó al Secretario General que, en paralelo, presentara a la próxima reunión del Consejo: 1) un informe en el que se explicara cómo utilizaba actualmente la UIT el marco de la [Agenda sobre Ciberseguridad Global](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) (ACG), y 2) con la participación de los Estados Miembros, unas directrices apropiadas para la utilización de la ACG por la UIT para su examen y aprobación por el Consejo ([C19/117](https://www.itu.int/md/S19-CL-C-0117/es), [C19/58](https://www.itu.int/md/S19-CL-C-0058/es)).  Acción solicitada  Se invita al Consejo a **tomar nota** del Informe.  \_\_\_\_\_\_\_\_\_\_\_\_  Referencias  [*Agenda sobre Ciberseguridad Global (ACG)*](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)*;* [*Documento C20/65 del Consejo*](https://www.itu.int/md/S20-CL-C-0065/es) |

# 1 Introducción

**1.1** La Conferencia de Plenipotenciarios de la UIT de 2018, celebrada en Dubái, adoptó la [Resolución 130](https://www.itu.int/en/action/cybersecurity/PublishingImages/Lists/resolutions/AllItems/Res%20130.pdf): *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*. La Resolución resuelve, entre otras cosas, que *se utilice el marco de la* [*Agenda sobre Ciberseguridad Global (ACG)*](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx) *para seguir encauzando la labor de la Unión* *en sus esfuerzos por crear confianza y seguridad en la utilización de las tecnologías de la información y la comunicación (TIC).*

**1.2** Durante las discusiones plenarias justo antes de la adopción de la Resolución 130, el Secretario General de la UIT *observó con satisfacción que en las deliberaciones sobre el proyecto de Resolución se había reconocido ampliamente el valor de la ACG*. *Instó a la Plenaria a que aceptara conservar el* resuelve *12.1, que permitirá a la UIT utilizar la ACG para orientar su labor relativa a la creación de confianza y seguridad en las TIC*. *A ese respecto, solicitaría el asesoramiento del Consejo y del expresidente del Grupo de Expertos de Alto Nivel que se ocupa de la ACG, el Magistrado Stein Schjolberg*.[[1]](#footnote-1)

**1.3** Se presentó a la reunión de 2019 del Consejo un informe del expresidente del Grupo de Expertos de Alto Nivel (GEAN) de la ACG, en el que se aconsejaba que se elaboraran directrices apropiadas para una mejor utilización de la AGC[[2]](#footnote-2). El Consejo encargó al Secretario General que, en paralelo, presentara a la próxima reunión del Consejo: 1) un informe en el que se explicara cómo utilizaba actualmente la UIT el marco de la Agenda sobre Ciberseguridad Global (ACG), y 2) con la participación de los Estados Miembros, unas directrices apropiadas para la utilización de la ACG por la UIT para su examen y aprobación por el Consejo.[[3]](#footnote-3)

**1.4** De acuerdo con las citadas instrucciones, se ha elaborado el proyecto de directrices para la utilización de la ACG por la UIT, con la ayuda del Alto Magistrado (retirado) Stein Schjolberg (expresidente del GEAN) y con la implicación de los Estados Miembros, para su examen y aprobación por el Consejo[[4]](#footnote-4). En paralelo, el Secretario General ha preparado el presente Informe para explicar de qué manera está utilizando la UIT en la actualidad la ACG, para su consideración por el Consejo.

# 2 Antecedentes

**2.1** Una función fundamental de la UIT, sobre la base de las orientaciones de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) y la Conferencia de Plenipotenciarios de la UIT, es fomentar la confianza y la seguridad en la utilización de las tecnologías de la información y las comunicaciones (TIC).

**2.2** Durante la CMSI, los Jefes de Estado y los dirigentes mundiales encargaron a la UIT que actuara como facilitadora de la Línea de Acción C5, "Creación de confianza y seguridad en la utilización de las TIC", en respuesta a lo cual la UIT lanzó en 2007 la ACG como marco para la cooperación internacional en esta materia.

**2.3** La ACG se presentó en 2007 – concebida para la cooperación y la eficiencia, alentar la colaboración con y entre las partes interesadas. Incluye cinco pilares o áreas de trabajo: medidas legales; medidas técnicas y de procedimiento; estructuras organizativas; capacitación, y cooperación internacional.

**2.4** Posteriormente, en octubre de 2007 se creó el GEAN de la ACG para ayudar al Secretario General de la UIT a elaborar propuestas estratégicas destinadas a los Estados Miembros sobre la promoción de la ciberseguridad, presidido por el Alto Magistrado (retirado) Stein Schjolberg.

**2.5** El GEAN está integrado por un grupo independiente de casi 100 expertos mundiales de múltiples partes interesadas de todo el mundo. El Grupo entregó sus recomendaciones al Secretario General respecto de los cinco pilares, en un informe del Presidente presentado en agosto de 2008 (Informe del GEAN 2008).[[5]](#footnote-5)

**2.6** En 2008, el trabajo en relación con los cinco pilares de la ACG representaba una importante innovación en el enfoque mundial de las cuestiones de ciberseguridad. Ya han transcurrido más de diez años desde que se presentara el Informe del GEAN de 2008. En general, se ha producido un reconocimiento mundial de las TIC como herramienta indispensable para lograr los Objetivos de Desarrollo Sostenible de las Naciones Unidas (ODS), y del hecho de que, para que las TIC puedan desempeñar este papel, es importante que todos, en todos lados, crean y confíen en la utilización de las TIC. Así pues, el objetivo de la "Creación de confianza y seguridad en la utilización de las TIC" es, más que nunca, un objetivo esencial para lograr los ODS.

**2.7** El marco que ofrecen los cinco pilares de la ACG ha merecido una amplia aprobación por parte de los miembros de la UIT y, en general, ha resistido la prueba del tiempo y sigue ofreciendo un amplio marco para la cooperación internacional en materia de ciberseguridad, en el marco de los documentos finales de la CMSI, especialmente los principios descritos en la Línea de Acción C5. Todas las actividades de la UIT en esta esfera siguen estructurándose en torno a los cinco pilares de la ACG.

**2.8** Desde la presentación de la ACG, la UIT ha informado coherentemente al Consejo acerca de sus actividades para crear confianza y seguridad en la utilización de las TIC a través de un informe anual organizado en torno a los cinco pilares, en el que se muestra el carácter complementario de los actuales programas de trabajo de la UIT y se facilita la realización de las actividades de la BDT, la TSB y la BR al respecto.

**2.9** Se dispone de información detallada sobre estas actividades en los Documentos [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), [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/es). En las siguientes secciones se facilitan algunos ejemplos de las actividades de la UIT en el marco de la ACG.

# 3 Algunos ejemplos de las actividades de la UIT

**3.1** En su calidad de facilitadora de la Línea de Acción C5, la UIT aprovecha el marco de la ACG para reunir a los diferentes interesados a fin de ayudar a los países a hacer frente a los riesgos asociados a las TIC, y en todos sus sectores y actividades trabaja en estrecha colaboración con otras organizaciones para fomentar la confianza en la utilización de las TIC.

**3.2** Si bien se reconoce la mutua interdependencia de los cinco pilares, en las secciones que figuran a continuación se destacan ejemplos de las actividades de la UIT en relación con cada uno de ellos. Con ello se pretende ofrecer instantáneas de algunas de las actividades, disponiéndose de informaciones más detalladas en los distintos informes anuales presentados al Consejo desde 2008 (véase el párrafo 2.9 *supra*).

**3.3** Se ha incluido una sección separada sobre la [iniciativa de Protección de la Infancia en Línea](https://www.itu.int/en/cop/Pages/default.aspx) como ejemplo de una iniciativa transversal que abarca los cinco pilares de la ACG.

## 3.4 Pilar 1 de la ACG: Medidas legales

a) Un componente que forma parte de cualquier estrategia nacional de ciberseguridad es la adopción de una legislación apropiada contra el uso indebido de las TIC con fines delictivos y que esté armonizada con las políticas y prácticas regionales e internacionales.

b) En lo que atañe a las medidas jurídicas, la UIT colabora estrechamente con la ONUDD y otros expertos en la materia. La UIT sigue 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), que tiene como finalidad contribuir a la armonización de sus marcos jurídicos.

## 3.5 Pilar 2 de la ACG: Medidas técnicas y de procedimiento

a) Las [Comisiones de Estudio de la UIT](https://www.itu.int/es/mediacentre/backgrounders/Pages/itu-study-groups.aspx) ofrecen una plataforma neutral y mundial para que los miembros de la UIT se reunieran y colaboraran en trabajos de normalización relacionados con la seguridad sobre diversos tema: arquitecturas y marcos de seguridad; seguridad de las aplicaciones de y los servicios para tecnologías actuales y emergentes tales como las tecnologías de libro mayor distribuido (una aplicación de las cuales es la cadena de bloques), la computación en la nube, los macrodatos, la inteligencia artificial y el aprendizaje automático, las redes definidas por *software*, 5G, Internet de las cosas, sistemas de transporte inteligente y redes inteligentes; fundamentos de seguridad como la infraestructura de clave pública (PKI), la gestión y autentificación de la identidad; y la ciberseguridad (incluido el intercambio de información sobre ciberamenazas).

b) La [Comisión de Estudio 17 del UIT-T](https://www.itu.int/es/ITU-T/studygroups/2013-2016/17/Pages/default.aspx) es la encargada de crear confianza y seguridad en la utilización de las TIC. Ello incluye el estudio de diversas tecnologías respecto de la ciberseguridad. Es la Comisión de Estudio Rectora para la seguridad y gestión de la identidad (IdM), y sigue contribuyendo al estudio y la normalización de la ciberseguridad, la lucha contra el correo basura, la IdM, la infraestructura de clave pública (certificados UIT-T X.509), 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. Hasta la fecha, el Grupo ha desarrollado más de 200 normas. Entre otras cosas, el Grupo de Estudio está trabajando ahora en la seguridad basada en la cuántica y ha desarrollado las especificaciones de la Recomendación X.1701 de "Arquitectura de un generador de números aleatorio de ruido cuántico".

c) Otras Comisiones de Estudio como la CE 9, CE 13, CE 15 y CE 20 (IoT) también están trabajando en normas relacionadas con la seguridad.

d) Las cuestiones de confianza y seguridad también han formado parte de los debates en muchos de los [Grupos Temáticos del UIT-T](https://www.itu.int/en/ITU-T/focusgroups/Pages/default.aspx), entre ellos: 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) el [*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) el [*Grupo Temático del UIT-T sobre inteligencia artificial para la salud (FG AI4H)*](https://www.itu.int/en/ITU-T/focusgroups/ai4h) 4) el [*Grupo Temático del UIT-T sobre multimedios en vehículos (FG VM*](https://www.itu.int/en/ITU-T/focusgroups/vm/Pages/default.aspx)*)* 5) el [*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) y 6) el [*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).

e) El UIT-R prosigue sus trabajos en el campo de la 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).

## 3.6 Pilar 3 de la ACG: Estructuras organizativas

a)Se necesitan mecanismos y estructuras institucionales eficaces a nivel nacional para hacer frente de manera fiable a las amenazas e incidentes cibernéticos. La ausencia de esas instituciones y la falta de capacidades nacionales plantean un verdadero problema a la hora de responder de manera adecuada y eficaz a los ataques cibernéticos. equipos de intervención en caso de incidentes informáticos (EIII) nacionales, desempeñan un papel importante en la solución.

b)La UIT colabora con los Estados Miembros para desarrollar la capacidad a nivel nacional y regional, desplegar capacidades y ayudar a crear y mejorar los EIII nacionales. La UIT ha llevado a cabo evaluaciones técnicas para valorar el grado de preparación con miras a la [creación de EIII](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx) en 76 países y participa en 20 proyectos de creación de EIII, 14 de los cuales concluyeron con éxito con esa capacidad nacional plenamente operativa. Hay más en curso o previstos.

c) La UIT ha venido realizando periódicamente [simulacros de ciberseguridad](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx) regionales y nacionales a fin de mejorar la capacidad de los países para responder a las amenazas, fortaleciendo así la cooperación nacional e internacional entre los Estados Miembros de la UIT frente a las ciberamenazas y los ciberataques. Hasta la fecha, la UIT ha realizado 28 simulacros de ciberseguridad en los que han participado más de 100 países.

## 3.7 Pilar 4 de la ACG: Capacitación

a) 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.

b) La UIT ayuda a los Estados Miembros a elaborar y mejorar estrategias nacionales de ciberseguridad eficaces. La [Guía para la elaboración de una estrategia nacional de ciberseguridad](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf), elaborada mediante un proceso de colaboración entre múltiples partes interesadas, constituye una guía de buenas prácticas y un conjunto de herramientas prácticas que han utilizado países de todas las regiones para elaborar y mejorar sus estrategias de ciberseguridad. Desde su lanzamiento en septiembre de 2018, se han organizado cursos prácticos nacionales y regionales en más de 20 países, y tres países han recibido asistencia directa para elaborar y revisar las estrategias nacionales de ciberseguridad utilizando la Guía citada.

c) La UIT ha puesto en marcha el [Índice Mundial de Ciberseguridad](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx) (GCI) que es una referencia fiable que mide el compromiso de los países con la ciberseguridad a escala mundial – para sensibilizar acerca de la importancia y las diferentes dimensiones de la cuestión. El nivel de desarrollo o compromiso de cada país se evalúa en relación con los cinco pilares de la ACG, que proporcionan la base y el marco general de la iniciativa. Sobre la base de un enfoque y una iniciativa multipartitos, el GCI aprovecha los conocimientos técnicos especializados de distintas organizaciones con el objetivo de mejorar la calidad de la encuesta, fomentando la cooperación internacional y promoviendo el intercambio de conocimientos en esta materia. Ya se han iniciado los trabajos con miras a la cuarta versión del Índice Mundial de Ciberseguridad.

## 3.8 Pilar 4 de la ACG: Cooperación internacional

a) La ACG se basa en la cooperación internacional y trata de que todos los interesados participen en un esfuerzo concertado por crear confianza y seguridad en la utilización de las TIC.

b) La UIT sigue forjando relaciones y asociaciones con diversas organizaciones e iniciativas regionales/internacionales, tales como el Foro Económico Mundial (WEF), 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.Estas asociaciones facilitan la colaboración de múltiples partes interesadas en actividades que abarcan todos los pilares de la ACG.

c) En su calidad de facilitadora de la Línea de Acción C5 de la CMSI, la UIT aprovecha el proceso de la CMSI, incluido el Foro anual de la CMSI, para ayudar a facilitar el diálogo entre las múltiples partes interesadas. La UIT organiza cada año diálogos de alto nivel, reuniones de facilitadores de la Línea de Acción C5 y talleres específicos sobre el tema de la ciberseguridad en el marco del [Foro de la CMSI](https://www.itu.int/net4/wsis/forum/2019/es/).

d) Reconociendo la importancia de trabajar para crear en el seno de las Naciones Unidas una manera común de entender las necesidades y los requisitos para la debida creación de programas e iniciativas que apoyen eficazmente los esfuerzos realizados por todas las partes interesadas, en 2010 se dio un primer paso importante hacia una mayor coordinación interna entre los organismos de las Naciones Unidas en su asistencia a los Estados Miembros en materia de ciberseguridad. A petición de la Junta de Jefes Ejecutivos del sistema de las Naciones Unidas para la coordinación, la UIT y la ONUDD, en colaboración con otros 33 organismos de las Naciones Unidas, encabezaron una iniciativa de dos años de duración para elaborar un marco sobre ciberseguridad y ciberdelito para todo el sistema de las Naciones Unidas, que fue aprobado por la Junta de Jefes Ejecutivos del sistema de las Naciones Unidas para la coordinación en noviembre de 2013. Desde entonces, la UIT ha seguido contribuyendo a diversas iniciativas conexas encaminadas a mejorar la coordinación y la cooperación internas dentro del sistema de las Naciones Unidas.

## 3.9 Iniciativa de Protección de la Infancia en Línea

a) La UIT lanzó la iniciativa de [Protección de la Infancia en Línea (PIeL)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx) en noviembre de 2008 como esfuerzo de múltiples partes interesadas en el marco de la ACG. La iniciativa congrega a asociados de todos los sectores de la comunidad mundial para elaborar estrategias de ciberseguridad y promover entornos en línea seguros para los niños en todo el mundo.

b) Los principales objetivos de la PIeL son a) detectar los riesgos y vulnerabilidades para los niños en el ciberespacio; b) sensibilizar; c) desarrollar herramientas prácticas para contribuir a minimizar los riesgos, y d) compartir conocimientos y experiencias.

c) La PIeL adopta un enfoque global para promover la seguridad de la infancia en línea, elaborando estrategias que abarcan los cinco pilares de la ACG:

**• Medidas legales**: un marco jurídico integral es un instrumento esencial para promover un entorno de apoyo y más seguro en línea para los niños y los jóvenes. La PIeL hace un seguimiento de los enfoques adoptados en diferentes países con distintos sistemas jurídicos y elabora directrices destinadas a ayudar a los Estados Miembros a alcanzar sus objetivos.

**• Medidas técnicas y de procedimiento**: la PIeL elabora recomendaciones y normas clave para contribuir a la protección de la infancia en línea por parte de todos los actores clave implicados.

**• Estructuras organizativas**: la PIeL promueve un marco modelo nacional para ayudar al desarrollo de un entorno en línea positivo para los niños y los jóvenes. La PIeL fomenta la creación de unidades de la PIeL a escala nacional y está desarrollando una serie de indicadores para ayudar a medir los progresos en la aplicación de las iniciativas de protección de la infancia en línea a nivel mundial, regional y nacional.

**• Capacitación**: la PIeL presta apoya a los países en la aplicación de marcos nacionales de PIeL y organiza eventos estratégicos a nivel regional y mundial para apoyar estos procesos.

**• Cooperación internacional**: la PIeL promueve una cultura mundial de ciudadanía digital y alienta la creación de acuerdos de cooperación para compartir información a fin de eliminar o mitigar los riesgos para los niños y los jóvenes en línea.

d) Se han emprendido diversas actividades en el marco de los distintos pilares de la ACG, cuyos detalles se pueden consultar en el [sitio web de la PIeL](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx), así como en los informes anuales presentados al Consejo desde la puesta en marcha de la iniciativa. Entre ellas se incluye el desarrollo de herramientas y recursos tales como directrices destinadas a los niños, padres y educadores, la industria y los responsables políticos. Un grupo de trabajo multipartito de expertos, formado por más de 50 organizaciones y expertos individuales, está revisando actualmente 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.

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

1. Actas de la decimosexta Sesión Plenaria de la Conferencia de Plenipotenciarios, Dubái, jueves 15 de noviembre de 2018. [↑](#footnote-ref-1)
2. Transmisión del Informe del expresidente del Grupo de Expertos de Alto Nivel de la ACG (C19/58), UIT, 8 de mayo de 2019, <https://www.itu.int/md/S19-CL-C-0058/es>. [↑](#footnote-ref-2)
3. Resumen de los debates de la sexta Sesión Plenaria (C19/117), UIT, 20 de junio de 2019, <https://www.itu.int/md/S19-CL-C-0117/es>. [↑](#footnote-ref-3)
4. Publicado en línea para consulta abierta con las partes interesadas de la CMSI. Disponible en <https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx>. [↑](#footnote-ref-4)
5. Véase Magistrado Stein Schjolberg, Informe del Presidente del GEAN:  
   <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>. [↑](#footnote-ref-5)