|  |  |
| --- | --- |
| **Consejo 2021****Consulta virtual de los consejeros, 8-18 de junio de 2021** |  |
|  |
|  |  |
| **Punto del orden del día: PL 1.4** | **Documento C21/71-S** |
|  | **22 de abril de 2021** |
|  | **Original: inglés** |
| Informe del Secretario General |
| directrices para la utilización de la Agenda sobre Ciberseguridad Global |

|  |
| --- |
| ResumenEn 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 explique cómo utiliza actualmente la UIT 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)).De conformidad con estas instrucciones, se ha elaborado el proyecto de Directrices con el apoyo del Alto Magistrado (retirado) Stein Schjolberg (Expresidente del GEAN), la Prof. Solagne Ghernaouti y el Sr. Noburo Nakatani, y con la participación de los Estados Miembros y otros interesados, para su examen y aprobación por el Consejo. Es importante señalar que este esfuerzo no está destinado a abordar ni abordará cuestiones relacionadas con la revisión de la ACG.Con arreglo al proceso de elaboración del proyecto de directrices, definido en la [Carta Circular (CL-20/55)](https://www.itu.int/md/S20-SG-CIR-0055/es),se organizaron dos consultas abiertas para todas las partes interesadas de la CMSI los días 23 de abril de 2020 y 1 de marzo de 2021 para formular comentarios sobre el proyecto de directrices. Se preparó, para su presentación a la reunión del Consejo de 2020, una versión anterior de este documento, signatura [C20/65](https://www.itu.int/md/S20-CL-C-0065/es), que no se examinó.Acción solicitadaEste documento se presenta al consejo para su **consideración** y **aprobación**, según proceda. \_\_\_\_\_\_\_\_\_\_\_\_Referencia*[Resolución](https://www.itu.int/en/council/Documents/basic-texts/RES-130-E.pdf)**[130 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios](https://www.itu.int/en/council/Documents/basic-texts/RES-130-E.pdf),*[*Agenda de Ciberseguridad Global (ACG)*](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)*,* [*Documento C21/36*](https://www.itu.int/md/S21-CL-C-0036/es) |

**Índice**

 Página

[**Sección 1 − Introducción 3**](#_Toc41378325)

[Antecedentes 4](#_Toc41378326)

[Contexto 5](#_Toc41378327)

[Continuidad de la pertinencia y aplicabilidad de la ACG como marco mundial para la acción 8](#_Toc41378328)

[**Sección 2 − Pilar 1: Medidas jurídicas 8**](#_Toc41378329)

[Introducción 8](#_Toc41378330)

[Evolución del panorama legal desde 2008 9](#_Toc41378331)

[Directrices para utilizar el Pilar 1 − Medidas jurídicas 12](#_Toc41378334)

[**Sección 3 − Pilar 2: Medidas técnicas y de procedimiento 13**](#_Toc41378335)

[Introducción 13](#_Toc41378336)

[Evolución del panorama de las medidas técnicas y de procedimiento desde 2008 14](#_Toc41378337)

[Directrices para utilizar el Pilar 2 − Medidas técnicas y de procedimiento 15](#_Toc41378339)

[**Sección 4 − Pilar 3: Estructura orgánica 16**](#_Toc41378340)

[Introducción 16](#_Toc41378341)

[Evolución del panorama de las estructuras organizativas desde 2008 16](#_Toc41378342)

[Directrices para utilizar el Pilar 3 – Estructuras organizativas 18](#_Toc41378343)

[**Sección 5 − Pilar 4: Capacitación 19**](#_Toc41378344)

[Introducción 19](#_Toc41378345)

[Evolución del panorama de la capacitación desde 2008 19](#_Toc41378346)

[Directrices para utilizar el Pilar 4 – Capacitación 20](#_Toc41378347)

[**Sección 6 − Pilar 5: Cooperación internacional 22**](#_Toc41378348)

[Introducción 22](#_Toc41378349)

[Evolución del panorama de la cooperación internacional desde 2008 22](#_Toc41378350)

[Directrices para utilizar el Pilar 5 – Cooperación internacional 24](#_Toc41378354)

[**Sección 7 − Directrices generales para el Marco de la ACG 26**](#_Toc41378355)

# Sección 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/council/Documents/basic-texts/RES-130-S.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 *se utilice el marco de la Agenda sobre Ciberseguridad Global (ACG) para seguir encauzando la labor de la Unión*, *que 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](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx), 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 conformidad con estas instrucciones, se ha formulado el citado proyecto de directrices para la utilización de la ACG por la UIT, con el apoyo del Alto Magistrado (retirado) Stein Schjolberg (Expresidente del GEAN) y con la participación de los Estados Miembros, para su examen y aprobación por el Consejo[[4]](#footnote-4). El Secretario General también agradece la orientación y contribución de la Prof. Solange Ghernaouti (*Swiss Cybersecurity Advisory & Research Group*, Universidad de Lausana) a las secciones relacionadas con los Pilares 2 y 4 de la ACG, y la del Sr. Noboru Nakatani (Exdirector Ejecutivo del *Global Complex for Innovation* de INTERPOL) a la sección relativa al Pilar 3 de la ACG. Es importante señalar que este esfuerzo no está destinado a abordar ni abordará cuestiones relacionadas con la revisión de la ACG.

**1.5** De conformidad con el proceso de elaboración del proyecto de directrices, expuesto en la Carta Circular [(CL-20/55)](https://www.itu.int/md/S20-SG-CIR-0055/es), el 23 de abril de 2020 y el 1 de marzo de 2021 se celebraron dos consultas a todas las partes interesadas de la CMSI para que formularan observaciones sobre el proyecto de directrices (consulta abierta). Más de 160 participantes asistieron a la reunión y proporcionaron información sección por sección sobre el proyecto de directrices. Se han publicado también en el [sitio web](https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx) de la ACG todas las observaciones recibidas por escrito de los participantes antes o después de las consultas abiertas.

## Antecedentes

**1.6** 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).

**1.7** 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 en 2005, "Creación de confianza y seguridad en la utilización de las TIC"[[5]](#footnote-5), en respuesta a lo cual la UIT lanzó en 2007 la ACG como marco para la cooperación internacional en esta materia.

**1.8** La ACG incluye cinco Pilares o áreas de trabajo: medidas legales; medidas técnicas y de procedimiento; estructuras organizativas; capacitación, y cooperación internacional. Se ha concebido para mejorar la cooperación y la eficiencia de las múltiples partes interesadas, fomentar la colaboración con y entre todos los asociados pertinentes y aprovechar las iniciativas existentes para evitar la duplicación de esfuerzos.

**1.9** 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. Lo presidió el Alto Magistrado (retirado) Stein Schjolberg.

**1.10** 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)[[6]](#footnote-6). En el informe, el Presidente del GEAN destacó que:

 *Los costes asociados a los ciberataques son significativos en cuanto a pérdida de ingresos, pérdida de datos confidenciales, daños a los equipos, ataques de denegación de servicio y apagones de red. El futuro crecimiento y el potencial de la sociedad de la información en línea están en peligro debido al creciente número de ciberamenazas. Además, el ciberespacio no tiene fronteras: los ciberataques pueden causar daños inconmensurables en diferentes países en cuestión de minutos. Las ciberamenazas son un problema mundial que requiere una solución mundial en la que participen todas las partes interesadas.*

**1.11** En 2008, el trabajo en relación con los cinco Pilares del 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.

## Contexto

**1.12** El marco que ofrecen los cinco Pilares del ACG ha sido ampliamente apreciado por los miembros de la UIT y, en general, ha resistido la prueba del tiempo. Sigue constituyendo un marco amplio para la cooperación internacional en materia de ciberseguridad, en el que se inscriben los documentos finales de la CMSI, en particular los principios indicados en la Línea de Acción C5. Las recomendaciones conexas incluidas en el Informe del GEAN de 2008 siguen siendo pertinentes hoy[[7]](#footnote-7) , salvo algunos aspectos específicos que podrían considerarse anticuados o que han sido sustituidos por otros nuevos.

**1.13** Por supuesto, el panorama de las TIC ha cambiado drásticamente desde 2008, ya que ahora las TIC subyacen en todos los sectores de la sociedad y en el conjunto de las infraestructuras fundamentales[[8]](#footnote-8). El mundo está asistiendo a la rápida aparición y adopción de nuevas tecnologías, como, por ejemplo:

• la mayor adopción de la Internet de las cosas, que interconectará decenas, si no centenares, de miles de millones de nuevos dispositivos, que abre la puerta a un número considerable de nuevas vulnerabilidades potenciales;

• el crecimiento de la inteligencia artificial como herramienta para aprovechar los datos, especialmente los macrodatos, que permite a las personas tomar decisiones con mayor conocimiento de causa, y a las máquinas tomar decisiones autónomas y supuestamente inteligentes sin intervención humana, con los consecuentes problemas de seguridad y confianza de los usuarios, así de salvaguardia de los derechos humanos;

• nuevas tecnologías y normas de comunicación como la 5G que permiten la comunicación a una velocidad exponencialmente superior a la que actualmente es viable;

• la computación cuántica que ofrece velocidades de computación muy superiores a las actuales, generando grandes oportunidades, pero también poniendo en peligro, entre otras cosas, los algoritmos criptográficos actuales; y

• nuevas tecnologías de seguridad, como las tecnologías de libro mayor distribuido (siendo las cadenas de bloques una de sus materializaciones más populares), que ofrecen mecanismos considerablemente más eficaces para salvaguardar los sistemas y los datos conexos. Cada vez más países de todo el mundo avanzan hacia la adopción de sistemas de identidad digital.

**1.14** Por otra parte, el ecosistema mundial de las TIC también se ha reconfigurado de manera importante desde 2008, con la adopción mundial a gran escala de las redes sociales. Algunas redes sociales tienen más usuarios que la población de muchos países juntos – por ejemplo, en 2020 Facebook tenía casi 2 800 millones de usuarios activos mensuales[[9]](#footnote-9). Los medios sociales han desempeñado un papel fundamental en la conexión de personas de todo el mundo, difuminando las fronteras geográficas y proporcionando un acceso fácil a información y oportunidades a una escala y una velocidad que antes no existían. También ha suscitado importantes preocupaciones en materia de confianza, en relación con la privacidad y la seguridad de los usuarios y los datos que éstos generan, la autenticidad y la fiabilidad de la información disponible en las redes sociales, la difusión de contenidos que incitan al odio, etc.[[10]](#footnote-10)

**1.15** Además, otros factores, como la aparición de la web oscura, han seguido suscitando en todo el mundo una creciente preocupación por las actividades delictivas en el ciberespacio, en particular en aspectos como el acceso a instrumentos, servicios y contenidos malignos.

**1.16** Habida cuenta de estos acontecimientos, todos los interesados, incluidos los gobiernos, reconocen cada vez más la diversidad de medidas urgentes que es necesario adoptar para promover la ciberseguridad, que van desde la protección de la infraestructura crítica hasta la salvaguardia de la privacidad de los usuarios. Como problema que podría plantear una amenaza a la seguridad nacional de todos los países, la ciberseguridad ha llegado a los programas de más alto nivel político de los gobiernos, que invierten cada vez más en medidas de gobernanza y administrativas para impulsar una respuesta del gobierno en su conjunto con el fin de fortalecer su capacidad de ciberresiliencia.

**1.17** La pandemia del COVID-19 no ha hecho más que poner de relieve la importancia de las TIC para la salud y la seguridad, y para que nuestra economía y nuestra sociedad sigan avanzando. Desde el teletrabajo y el comercio electrónico hasta la telemedicina y el aprendizaje a distancia, los servicios y la infraestructura de TIC proporcionan un acceso continuo a las necesidades esenciales. La crisis de COVID-19 también ha acentuado la necesidad de hacer frente a la rápida evolución y el carácter crítico de los retos de ciberseguridad que plantea el alto grado de dependencia de la sociedad respecto de las TIC.

**1.18** En el marco de la ACG, cada uno de los cinco Pilares ha evolucionado a su manera a lo largo del último decenio.

**1.19** En 2020, más de 125 países habían firmado y/o ratificado diferentes convenios, declaraciones, directrices o acuerdos sobre ciberseguridad y ciberdelincuencia, como el [Convenio del Consejo de Europa sobre la Ciberdelincuencia de 2001](http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185) (Convenio de Budapest), el Acuerdo entre Gobiernos de los Estados Miembros de la Organización de Cooperación de Shanghái sobre la cooperación para garantizar la seguridad de la información a nivel internacional (2009) y el [Convenio de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales (2014)](https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection).

**1.20** De conformidad con las Resoluciones de la AGNU, un Grupo de Expertos Gubernamentales (GEG)[[11]](#footnote-11) y un Grupo de Trabajo de Composición Abierta (GTCA)[[12]](#footnote-12) han estudiado varios asuntos relacionados con la utilización de las TIC en el contexto de la seguridad internacional, entre otros, hacer que los Estados tengan un comportamiento más responsable en el ciberespacio, la aplicabilidad del Derecho internacional al ciberespacio, la capacitación y la necesidad de definir e implementar medidas que aumenten la confianza en el ciberespacio.

**1.21** Las tecnologías innovadoras de TIC, como la computación en nube, las redes definidas por software (SDN), la virtualización de funciones de red (NFV), 5G, los macrodatos, IA, etc., desdibujan las fronteras geográficas y del mercado, haciendo que el ecosistema de la ciberseguridad sea cada vez más dinámico y complejo. Las nuevas tecnologías y los agentes comerciales pueden provocar la exposición a nuevas vulnerabilidades y amenazas, en particular porque al centrarse el sector privado en el rendimiento, la cuota de mercado y los costos, las inversiones en estos ámbitos suelen tener prioridad sobre las inversiones en seguridad en la etapa de diseño. Hay una serie de cuestiones que plantean importantes retos al abordar esas tecnologías, como encontrar la manera de reducir y controlar el número de vulnerabilidades al tiempo que se garantiza la seguridad mediante el diseño (ya que los productos siguen siendo vulnerables ya desde la fase de diseño), aumentar la confianza en los productos y servicios a lo largo de su ciclo de vida mediante planes, protocolos y normas de acreditación, y el uso legítimo de los datos generados por los usuarios, protegiendo al mismo tiempo la intimidad de éstos. Los procesos de normalización y de certificación/acreditación periódica podrían ayudar a reducir el número y los efectos de las vulnerabilidades contribuyendo a desarrollar una cultura de seguridad mediante el diseño, lo que a su vez fomentaría la confianza en esas tecnologías. Sin embargo, la normalización de la seguridad, es decir, el desarrollo de medidas técnicas y de procedimiento para la seguridad, sigue siendo un objetivo que cambia continuamente, porque para ello se necesita una industria avanzada, unos reguladores expertos en tecnología y unos órganos de ejecución capaces, en su caso.

**1.22** Se han creado varias organizaciones nacionales, regionales e internacionales para abordar la cuestión de la ciberseguridad. Entre los ejemplos de iniciativas nacionales y regionales figuran AFRIPOL, AMERIPOL, GCCPOL, el Centro de Ciberseguridad de Oceanía (OCSC), el Centro de Ciberseguridad de Australia (ACSC), el Centro Europeo de Lucha contra el Ciberdelito (EC3), el Centro Nacional de Coordinación sobre Incidentes Informáticos de Rusia y el Centro de Coordinación sobre el Ciberdelito de la India (I4C). En lo que respecta a las entidades internacionales, entre las iniciativas recientes cabe mencionar el *Global Cyber Security Capacity Centre* (GCSCC), el *Global Forum on Cyber Expertise* (GFCE), el Global Complex for Innovation de la INTERPOL (IGCI) y el Global Centre for Cybersecurity del WEF, el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA), la Comunidad Económica de los Estados de África Occidental (CEDEAO), la Comunidad de Desarrollo del África Meridional (SADC), entre otros.

**1.23** Además, la falta de conocimientos y de experiencia en las dimensiones técnicas, jurídicas, organizativas y humanas de la ciberseguridad también puede afectar negativamente a las infraestructuras nacionales vitales. Es probable que muchos usuarios finales de las TIC no comprendan plenamente los problemas de ciberseguridad o no tengan las aptitudes o herramientas necesarias para proteger mejor sus datos, privacidad y activos, y que los usuarios más vulnerables, entre ellos las mujeres y los niños, corran un riesgo especial. La creación de aptitudes, competencias y medidas que contribuyan a lograr una cultura de ciberseguridad eficaz sigue siendo un reto crucial.

## Continuidad de la pertinencia y aplicabilidad de la ACG como marco mundial para la acción

**1.24** Las actividades llevadas a cabo aplicando el marco de la ACG han ido evolucionando a tenor de los cambios producidos en el panorama de las TIC, incluidas las emprendidas por la UIT en el marco de su mandato y de su función como facilitadora de la Línea de Acción C5 de la CMSI.

**1.25** La ACG ha sido muy útil en los esfuerzos de la UIT para fomentar la confianza y la seguridad en la utilización de las TIC. Como marco, es aplicable en los planos mundial, regional y nacional, y debería seguir aplicándose como tal. En el marco de su mandato, guiándose por el marco de la ACG, la UIT ha procurado reunir a diferentes partes interesadas para que colaboren en una serie de iniciativas, incluida la asistencia a los países para definir su estrategia nacional de ciberseguridad, fortalecer su infraestructura mediante la elaboración y aplicación de normas internacionales de seguridad, crear sus equipos de intervención en caso de incidente informático, desplegar iniciativas de protección de la infancia en línea y crear la capacidad y los conocimientos humanos necesarios. En el marco de la ACG se han puesto en marcha diversas iniciativas multipartitas, como la relativa a la protección de la infancia en línea[[13]](#footnote-13).

**1.26** En las secciones siguientes se ofrece más orientación destinada a apoyar los esfuerzos encaminados a utilizar la ACG. Al elaborar estas orientaciones se han tenido en cuenta las recomendaciones del Informe del GEAN de 2008, las actividades desplegadas desde entonces por la UIT, las novedades en esta materia desde 2008 y las [aportaciones recibidas de los Estados Miembros y otros interesados](https://www.itu.int/md/S20-GCA-C/es) (de conformidad con las Cartas Circulares ([CL-20/18](https://www.itu.int/md/S20-SG-CIR-0018/es) y [CL-20/55](https://www.itu.int/md/S20-SG-CIR-0055/es))).

**1.27** Si bien se reconoce la mutua interdependencia de los cinco Pilares, en cada sección se aborda un pilar específico de la ACG y se proponen directrices concretas para su utilización. La sección 2 se centra en las medidas legales. La sección 3 trata de las medidas técnicas y de procedimiento. La sección 4 trata de la capacitación. La sección 5 trata de las estructuras organizativas y la sección 6 se refiere a la cooperación internacional. La Sección 7 contiene algunas directrices transversales generales para el uso del marco de la ACG.

# Sección 2 Pilar 1: Medidas jurídicas

## Introducción

**2.1** La dimensión jurídica de la ciberseguridad es uno de los factores fundamentales para facilitar la confianza en la utilización de las TIC.

**2.2** En el Informe del GEAN de 2008 se indicaba que el Pilar 1 de la ACG tenía por objeto promover la cooperación y proporcionar asesoramiento estratégico al Secretario General de la UIT respecto de las respuestas legislativas para abordar las cuestiones jurídicas en materia de ciberseguridad, en particular la forma en que podían abordarse las actividades delictivas cometidas en relación con las TIC mediante la legislación de una manera que sea compatible a nivel internacional. En los debates se indicó que la UIT podría elaborar estrategias para la formulación de una legislación modelo sobre el ciberdelito en forma de directrices. En el Informe se recomendaban también como referencia iniciativas regionales pertinentes.

## Evolución del panorama legal desde 2008

**2.3** Las organizaciones regionales han elaborado numerosas convenciones, declaraciones, acuerdos y directrices en materia de ciberseguridad a partir de 2008. Como se ha mencionado anteriormente, muchos países han firmado y/o ratificado diferentes convenios, declaraciones, directrices o acuerdos sobre ciberseguridad y ciberdelincuencia, lo que ha dado lugar a la fragmentación y diversidad a nivel internacional.

**2.4** Dentro del sistema de las Naciones Unidas, como ya se indica en la sección 1 anterior, la Asamblea General de las Naciones Unidas ha puesto en marcha dos procesos para tratar el tema de la seguridad en la utilización de las TIC: el Grupo de Expertos Gubernamentales (GEG) y el Grupo de Trabajo de Composición Abierta (GTCA). Desde 2004, la Asamblea General de las Naciones Unidas ha creado seis GEG para estudiar las amenazas que plantea la utilización de las TIC en el contexto de la seguridad internacional y cómo hacer frente a dichas amenazas, siendo el último de ellos el [Grupo de Expertos Gubernamentales para la promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional](https://www.un.org/disarmament/group-of-governmental-experts/), 2019/2021 ([Resolución 73/266](https://dig.watch/instruments/resolution-ares73266-advancing-responsible-state-behaviour-cyberspace-context-international)). En sus conclusiones, el GGE 2014/2015 acordó que existen obligaciones en virtud del derecho internacional aplicables a la utilización que hacen los Estados de las TIC y que los Estados deben cumplir con su obligación de respetar y proteger los Derechos Humanos y las libertades fundamentales. En 2018, [el GTCA sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional](https://www.un.org/disarmament/open-ended-working-group/) (Resolución 73/27), abierto a todos “los Estados interesados”, se creó para estudiar las amenazas actuales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para hacerles frente; seguir elaborando las reglas, normas y principios de comportamiento responsable de los Estados; estudiar la forma en que el derecho internacional se aplica a la utilización de las TIC por los Estados, así como las medidas de fomento de la confianza y la capacitación, además de la posibilidad de establecer un diálogo institucional periódico con amplia participación bajo los auspicios de las Naciones Unidas. El GTCA 2019-2021 adoptó su [primer Informe sustantivo](https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf) en marzo de 2021 y en él reafirma que el derecho internacional, y en particular la Carta de las Naciones Unidas, es de aplicación en el ciberespacio y recomienda, además, a los miembros a propiciar la capacitación en la esfera del derecho internacional, la legislación natural y la política, pues así conseguirán llegar a una interpretación común de cómo el derecho internacional se aplica a la utilización de las TIC por los Estados. El GTCA prevé proseguir su trabajo, pues en la Resolución 75/240 se crea un Grupo de Trabajo de Composición Abierta sobre la seguridad y la utilización de las tecnologías de la información y las comunicaciones para el periodo 2021-2025.

**2.5** En el marco del sistema de las Naciones Unidas se han puesto en marcha diversas iniciativas y procesos para identificar y solucionar los problemas jurídicos que plantea la ciberseguridad en todo el mundo. Por ejemplo, se han adoptado varias Resoluciones de la Asamblea General de las Naciones Unidas al respecto, como la [Resolución de la Asamblea General de las Naciones Unidas de 27 de diciembre de 2019, *Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos* (Resolución 74/247)](https://undocs.org/pdf?symbol=en/A/RES/74/247), en la que se decide establecer un comité intergubernamental especial de expertos de composición abierta, representativo de todas las regiones a fin de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.

**2.6** Habida cuenta de lo anterior, los Estados están debatiendo estos temas en diversos foros y es necesario que intensifiquen la cooperación entre ellos y con otros interesados a fin de definir las bases de un entendimiento, interpretación y defensa comunes del derecho internacional en el ciberespacio, facilitando, en particular, un mayor intercambio de información y prácticas idóneas.

Medidas jurídicas y nuevas tecnologías

**2.7** Algunos expertos han sugerido que las nuevas tecnologías y los modelos de conducta en el ciberespacio con fines delictivos deberían quedar abarcados por el derecho penal[[14]](#footnote-14). Muchos países han adoptado o se están preparando para promulgar nuevas leyes que abarquen algunas de esas conductas. Es importante que toda medida jurídica procedente definida a este respecto se diseñe en el respeto de las obligaciones para con los derechos humanos. A continuación, se presentan algunos ejemplos de tecnologías y tendencias recientes e incipientes que podrían repercutir en las medidas jurídicas:

**a)** **Ciberataques mundiales**

Los ciberataques mundiales contra infraestructuras de comunicaciones e información críticas se han convertido en una amenaza para la seguridad nacional e internacional. Los gobiernos, las organizaciones internacionales y las instituciones privadas que han sido objeto de tales ciberataques necesitan definir marcos jurídicos nacionales robustos para hacer frente a este problema.

**b)** **Conductas criminales en redes sociales**

Se piden medidas para contrarrestar las conductas ilegales, como la incitación al odio, en las redes sociales. Han surgido nuevas iniciativas para abordar esas cuestiones, como la asociación del [Foro Mundial de Internet para la Lucha contra el Terrorismo](https://www.gifct.org/about/) entre las Naciones Unidas y las empresas de tecnología Facebook, Microsoft, Twitter y YouTube.

**c)** **Internet de las cosas (IoT)**

La tecnología inteligente está cambiando la forma en que la población mundial vive, interactúa y trabaja[[15]](#footnote-15). En los últimos tiempos ha habido numerosos ataques a la infraestructura web de todo el mundo mediante redes robot de dispositivos conectados, desde cámaras web hasta encaminadores. Con la aparición de nuevas tecnologías como la 5G y la existencia de dispositivos interconectados ubicuos es probable que aumenten los riesgos.

**d)** **Inteligencia artificial (IA)**

La transparencia algorítmica, incluida la trazabilidad de las medidas adoptadas, es un factor muy importante para establecer la rendición de cuentas y la responsabilidad por las decisiones adoptadas por sistemas parcial o totalmente automatizados, y garantizar así la confianza en las aplicaciones y servicios de TIC. Los expertos han observado que, en el caso de varios tipos de técnicas de inteligencia artificial como el aprendizaje profundo, es difícil aclarar cómo se alcanzan los resultados. A medida que los procesos de adopción de decisiones automatizados se generalicen en las aplicaciones y servicios para consumidores y empresas, se pondrá de relieve la necesidad de una mayor claridad en los aspectos jurídicos relativos a la rendición de cuentas y la responsabilidad por los análisis y decisiones que esos procesos aportan[[16]](#footnote-16).

**e)** **Explotación y abuso sexuales de niños en línea**

La [Convención sobre los Derechos del Niño (CDN)](https://www.ohchr.org/SP/ProfessionalInterest/Pages/CRC.aspx) de las Naciones Unidas fue adoptada en 1989. El Artículo 34 de la Convención obliga a los Estados Parte a adoptar medidas apropiadas para proteger a los niños frente a todas las formas de explotación y abuso sexuales. En 2002, entró en vigor un [Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía](https://www.ohchr.org/SP/Pages/Home.aspx) (Nueva York, 2000). El abuso sexual de niños en línea se ha extendido con el crecimiento de Internet y los medios de comunicación social. Los expertos han pedido que se adopte un enfoque integral para la prevención de esos abusos[[17]](#footnote-17). Esto incluye medidas para prevenir la creación de y el acceso a sitios web con contenido relacionado con el abuso sexual de niños, incluido el bloqueo, el filtrado o cualquier otra tecnología similar. En marzo de 2021 el Comité sobre los Derechos del Niño adoptó su [Observción General nº 25 sobre los derechos de los niños en relación con el entorno digital](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=es), en la que se explica cómo los Estados partes deben aplicar la CDN en relación con el entorno digital y ofrece orientaciones sobre medidas legislativas, políticas y de otro tipo pertinentes.

**2.8 Leyes procesales − Principios generales**

Se ha considerado que la adopción de las leyes procesales necesarias para definir las facultades y procedimientos para el enjuiciamiento de conductas delictivas en el ciberespacio es una medida jurídica esencial para la prevención, la investigación y el enjuiciamiento de ciberdelitos y la garantía de la ciberseguridad. Sin embargo, algunos expertos han señalado que esas facultades y procedimientos también podrían ser necesarios para el enjuiciamiento de otros delitos penales cometidos por medio de un sistema informático, y que podrían aplicarse reglamentos a la recopilación de pruebas en forma electrónica de todos los delitos penales[[18]](#footnote-18). Todas las leyes procesales deben ser compatibles con las obligaciones y normas establecidas en virtud de las normas internacionales en materia de derechos humanos. En este sentido, habida cuenta de que el principio de soberanía del Estado se aplica en el ciberespacio, también se ha pedido un debate acerca de los mecanismos que podrían facilitar el acceso legal al contenido de las comunicaciones cuando éstas están encriptadas de extremo a extremo, garantizando al mismo tiempo la protección de los derechos fundamentales y la seguridad de los ciudadanos[[19]](#footnote-19). Algunos interesados sostienen que un mecanismo de este tipo debilitaría la seguridad de internet y pondría en serio riesgo de peligro la economía mundial, los servicios esenciales de lo que depende mucha gente y la vida de las personas.

**2.9** A la luz de lo anterior, es evidente que los países deben seguir adoptando medidas jurídicas apropiadas para proteger sus infraestructuras críticas de comunicación e información (y cualquier activo, sistema o parte de ellas) que sean esenciales para el mantenimiento de funciones sociales vitales tales como la sanidad, la seguridad y el bienestar económico o social de las personas, y a que eviten toda perturbación o destrucción que pueda tener una repercusión importante en esas infraestructuras críticas o que haga que falle el funcionamiento de las mismas.

## Directrices para utilizar el Pilar 1 − Medidas jurídicas

**2.10** Como se ha reconocido anteriormente, los cinco pilares de la ACG son interdependientes entre sí, y el de las medidas legales es transversal para todos ellos.

**2.11** Desde el lanzamiento de la ACG, la UIT se ha centrado en ámbitos de la ciberseguridad que se corresponden con su mandato fundamental y su ámbito de competencia, y más concretamente en las esferas técnica y del desarrollo, y no en las áreas relacionadas con la aplicación de principios legales o políticos por parte de los Estados Miembros en relación con la defensa nacional, la seguridad nacional, los contenidos y el ciberdelito, que corresponden a sus derechos soberanos. Por consiguiente, con respecto a las actividades correspondientes al Pilar 1, la UIT se ha centrado principalmente en facilitar la colaboración, mediante mecanismos como los memorandos de entendimiento, con otras organizaciones internacionales y partes interesadas pertinentes (como la INTERPOL y la ONUDD) que pueden tener un mandato rector de prestación de asistencia a los países en esta esfera. Esto ha incluido ayudar a los Estados Miembros a comprender los aspectos jurídicos de la ciberseguridad, mediante recursos como los [Recursos de Legislación sobre Ciberdelincuencia de la UIT](http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html) y el [Repositorio sobre Ciberdelincuencia de la ONUDD](https://sherloc.unodc.org/cld/v3/sherloc/index.jspx?tmpl=cybrepo). También se trabajó para ayudar a los Estados Miembros del Caribe, el África subsahariana y las islas del Pacífico a armonizar las reglamentaciones y legislaciones sobre las TIC, incluidos los marcos jurídicos sobre el ciberdelito.

|  |
| --- |
| **2.12** Habida cuenta de los rápidos avances de la tecnología, es necesario que las medidas adoptadas por las organizaciones y los países evolucionen al ritmo de dichos cambios. Esto aporta nuevas complejidades al reto de la ciberseguridad, que requieren un examen detenido desde diversas perspectivas. En este contexto, se exponen a continuación las directrices propuestas para la utilización del Pilar 1:**a)** La UIT debe seguir esforzándose por facilitar los debates y la colaboración entre las múltiples partes interesadas sobre los retos ligados al tratamiento de la cuestión de la ciberseguridad y, en particular, fortalecer su relación con los asociados y otras partes interesadas para prestar asistencia a los Estados Miembros en esta materia.**b)** La UIT debe seguir colaborando, dentro de su ámbito de competencia, con los asociados para desarrollar y mantener recursos, como los Recursos de Legislación sobre Ciberdelincuencia, para ayudar a los Estados Miembros a entender los aspectos jurídicos de la ciberseguridad, apoyando al mismo tiempo el intercambio de experiencias y conocimientos entre los Estados Miembros para apoyar sus esfuerzos en la elaboración de marcos en esta materia, incluida la legislación.**c)** La UIT, en colaboración con socios apropiados, debería promover una mejor comprensión de los retos y riesgos relacionados con la ciberseguridad que plantean las nuevas tecnologías para las medidas jurídicas existentes, y facilitar el intercambio de estudios de casos y buenas prácticas a nivel nacional, regional e internacional.**d)** También es necesario que todas las partes interesadas adopten medidas jurídicas apropiadas para aplicar programas eficaces que impidan o prohíban la difusión de material en línea relacionado con la explotación y el abuso sexuales de los niños, incluida la adopción de medidas preventivas para detectar, obstaculizar y desmantelar las redes, organizaciones o estructuras utilizadas para la producción y/o distribución de **material** en línea relacionado con el abuso sexual y de otro tipo de los niños, y para establecer mecanismos que permitan detectar y enjuiciar a los delincuentes al tiempo que se identifica y protege a las víctimas. A este respecto, la UIT debería seguir fortaleciendo el programa de protección de la infancia en línea como plataforma para trabajar con los asociados y las partes interesadas a fin de promover el intercambio de conocimientos, información, actividades y resultados en todos los aspectos, incluidas las medidas jurídicas que puedan facilitar y dar soporte a las medidas de los países en este ámbito fundamental.  |

# Sección 3 Pilar 2: Medidas técnicas y de procedimiento

## Introducción

**3.1** La ACG ha guiado el desarrollo y la aplicación de diversas iniciativas, contribuyendo a la madurez del debate sobre la ciberseguridad a nivel internacional, regional y nacional. La necesidad de medidas de ciberseguridad eficaces y eficientes, ya sea a nivel estratégico u operacional, tiene que satisfacerse con un enfoque coherente, lo cual sigue constituyendo un gran desafío.

**3.2** Hoy en día, puede parecer que las dimensiones identificadas por los Pilares 1, 3, 4 y 5 de la ACG están adquiriendo cada vez más importancia en el ámbito de la ciberdiplomacia y el diálogo internacional, y a menudo prevalecen sobre el Pilar 2. Sin embargo, las cuestiones técnicas pueden estar a menudo en la base de todos los demás Pilares. La gestión del ciberriesgo mediante medidas tecnológicas y de procedimiento (por ejemplo, administrativas, operativas o de gestión) sigue siendo de primordial importancia, especialmente en el contexto de las infraestructuras críticas. Habida cuenta de la función desempeñada tradicionalmente por la UIT, en su calidad de organismo especializado de las Naciones Unidas y de organización mundial de normalización, está bien situada para avanzar en la esfera de las normas y medidas técnicas relacionadas con la seguridad.

## Evolución del panorama de las medidas técnicas y de procedimiento desde 2008

**3.3** Las tecnologías (actuales y emergentes) y las prácticas digitales que de ellas se derivan están en constante evolución. Esta dimensión dinámica de la técnica es hasta cierto punto independiente de los demás Pilares de la ACG, y evoluciona en gran medida por sí misma, teniendo en cuenta hasta cierto punto las necesidades e implicaciones en esta materia para los otros cuatro Pilares.

**3.4** Para que toda la infraestructura, las aplicaciones y los servicios funcionen es fundamental crear y aplicar normas. Además, es importante que en el proceso de definición de esas normas se tengan también en cuenta las obligaciones para con los derechos humanos.

**3.5** La UIT, por su composición multipartita, ofrece una plataforma global única para la elaboración de normas de TIC mundiales de adopción voluntaria por los Estados Miembros de la UIT. Dentro de la UIT, la CE 17 del UIT-T es la Comisión de Estudio rectora para las normas de seguridad, y ha publicado más de 200 normas centradas en la seguridad. Actualmente está trabajando en varios ámbitos tecnológicos emergentes, entre ellos los de la seguridad de la tecnología financiera, la seguridad de la IoT (incluida la seguridad industrial de Internet), la seguridad de los sistemas de transporte inteligente, la tecnología de libro mayor distribuido, la distribución de claves cuánticas, el aprendizaje automático para combatir el correo basura, la seguridad de 5G, la computación periférica, la protección de la información de identificación personal, la computación multipartita y las directrices para la creación, el funcionamiento y la automatización de los centros de ciberdefensa, entre otras. Al aplicar las recomendaciones del Informe del GEAN de 2008 sobre "colaboración" (por ejemplo, 2.1, 2.6, 2.7, 2.10, 2.12 y 2.16), la CE 17 reúne y mantiene una base de datos de normas de seguridad de las TIC[[20]](#footnote-20) de acceso público, que incluye 2 600 normas de seguridad de las TIC existentes y en fase de elaboración de 13 organizaciones de normalización clave, entre ellas el 3GPP, ATIS, ETSI, IEEE, IETF, ISO/CEI JTC 1, UIT, OASIS, OneM2M, etc.

**3.6** Si bien la CE 17 del UIT-T sigue siendo la principal Comisión de Estudio sobre normas de seguridad, la mayoría de las demás Comisiones de Estudio, si no todas, también se ocupan de aspectos relacionados con la seguridad dentro de sus respectivos ámbitos de estudio, por ejemplo, la CE 20 sobre la IoT y sus aplicaciones (incluidas las ciudades y comunidades inteligentes), la CE 13 sobre redes de próxima generación, o la CE 16 sobre codificación, sistemas y aplicaciones multimedios, entre otras. Los diversos Grupos Temáticos sobre tecnologías emergentes, como la IA y la salud, el aprendizaje automático y la 5G, las tecnologías de libro mayor digitales, la tecnología informática cuántica para redes y otras, también se ocupan de los problemas relacionados con la seguridad. Es importante que se desarrolle una estrecha cooperación entre los diversos grupos, aportando la CE 17 una función de coordinación/liderazgo, a fin de que se mantenga el mayor grado posible de seguridad de extremo a extremo a lo largo del proceso de normalización del ciclo de desarrollo de los productos/servicios de TIC.

Proliferación de iniciativas de normalización y necesidad de mayor cooperación

**3.7** La normalización internacional de la ciberseguridad es difícil debido a la variedad de tecnologías y a la aparición de diversos actores en todos los sectores, y especialmente difícil para los países en desarrollo, que pueden carecer de capacidad operativa y de conocimientos técnicos en materia de ciberseguridad.

**3.8** A este respecto, la recomendación 2.1 del Informe del Grupo de expertos de alto nivel de 2008 mantiene hoy más que nunca su validez: *En lo que respecta a las oportunidades de mejorar la colaboración con la labor de ciberseguridad existente que se desarrolla fuera de la UIT, la UIT debe colaborar con los centros de conocimientos especializados externos existentes para identificar, promover y fomentar la adopción de procedimientos y medidas técnicas de seguridad mejorados*[[21]](#footnote-21).

**3.9** Además, como se especifica en la recomendación 2.2 del Informe del GEAN de 2008, la UIT se considera como *el centro de excelencia mundial*[[22]](#footnote-22) que se ocupa del proceso de normalización internacional y de las normas relacionadas con las medidas técnicas y de procedimiento. Para lograrlo, se debe incentivar a los países más avanzados tecnológicamente y a sus sectores privados a que participen en las actividades de la UIT y colaboren en la elaboración de normas técnicas y de procedimiento, incluidas las relacionadas con la seguridad.

**3.10** Es importante seguir reforzando la coordinación y la colaboración con las demás SDO, sobre la base de la reciprocidad, de modo que se garantice la seguridad de extremo a extremo, la seguridad por diseño, la evaluación de riesgos y la interoperabilidad durante todo el ciclo de vida del producto.

**3.11** En el Informe del GEAN de 2008 se hace hincapié en la importancia de *las medidas esenciales para abordar las insuficiencias de los productos de soporte lógico, entre otras cosas, mediante planes de acreditación, protocolos y normas*[[23]](#footnote-23).A este respecto, la UIT debería seguir adaptando su labor en función de las nuevas tecnologías y necesidades. Para cada una de estas tecnologías/dominios, deberían tenerse en cuenta los siguientes requisitos:

• necesidad de seguridad por diseño/seguridad por defecto en cada elemento e interfaz en un ecosistema de TIC heterogéneo en la etapa de diseño;

• necesidad de un sistema de medición apropiado para determinar el nivel de seguridad en la etapa de implementación; y

• necesidad de procesos de evaluación y certificación periódicos para homologar el nivel de seguridad de un conjunto de datos/producto/sistema/servicio a lo largo de su ciclo de vida después de su despliegue.

## Directrices para utilizar el Pilar 2 − Medidas técnicas y de procedimiento

|  |
| --- |
| **3.12** Las Recomendaciones relacionadas con el Pilar 2 del Informe del GEAN de 2008 siguen siendo válidas. A la luz de lo anterior, se proponen las siguientes directrices para el Pilar 2: **a)** Las Comisiones de Estudio de la UIT deberían centrarse en tecnologías emergentes a fin de estudiar y formular directrices de seguridad para la utilización de las tecnologías conexas, y recomendar a los Estados Miembros que las apliquen voluntaria y oportunamente a fin de contrarrestar las ciberamenazas cambiantes y en aumento.**b)** Debería crearse un mecanismo para establecer una estrecha cooperación entre las diversas Comisiones de Estudio del UIT-T en lo que respecta al estudio de las cuestiones relacionadas con la seguridad, en el que la CE 17 desempeñe una función coordinadora y rectora, de modo que se mantenga el mayor grado posible de seguridad de extremo a extremo a lo largo del proceso de normalización de todos los componentes e interfaces de los productos de las TIC.**c)** Se debe alentar una estrecha coordinación y colaboración, de la UIT con otras SDO sobre la base de la reciprocidad, para garantizar que se mantiene la seguridad de extremo a extremo de los productos de las diversas aplicaciones y servicios a lo largo de todo el ciclo del producto.**d)** La UIT debería seguir divulgando normas de seguridad de las TIC a nivel mundial. Se alienta a otras organizaciones de normalización y grupos industriales a que presenten sus normas sobre medidas técnicas y de procedimiento al UIT-T para su adopción como Recomendaciones del UIT-T.**e)** La UIT debe proseguir sus esfuerzos por convertirse en "el centro de excelencia mundial" para la elaboración de recomendaciones sobre medidas técnicas y de procedimiento en materia de ciberseguridad en los ámbitos abarcados por su mandato (como se indica en el Informe del GEAN de 2008), entre otras cosas, incentivando a sus Miembros a intensificar su participación en las actividades de normalización de la UIT y creando asociaciones estratégicas. **f)** La UIT debe seguir alentando a sus Miembros a concluir/participar en acuerdos de certificación mutua con miras a la creación de un marco internacional de certificación de la ciberseguridad global basado en normas armonizadas. |

# Sección 4 Pilar 3: Estructura orgánica

## Introducción

**4.1** Las estructuras organizativas a nivel de coordinación nacional, regional e internacional pueden analizarse en función de si el propósito de su cooperación es estratégico u operativo. En una estructura estratégica, las organizaciones hacen más hincapié en el establecimiento de una relación de colaboración que en la realización de operaciones conjuntas en caso de un incidente cibernético. Por otra parte, en una estructura operacional, las organizaciones crean sistemas para compartir la información que permitan intercambiar rápidamente la información a fin de reaccionar con rapidez a los ciberincidentes. Esta distinción puede ser útil a la hora de comparar las diferentes estructuras organizativas en todo el mundo.

**4.2** Se necesitan mecanismos y estructuras institucionales eficaces a nivel nacional para prepararse y hacer frente de manera fiable a las amenazas e incidentes cibernéticos. La ausencia de esas instituciones y la falta de capacidad nacional plantean problemas para responder de manera adecuada y eficaz a los ciberataques. Los equipos nacionales de intervención en caso de incidentes informáticos (EIII) desempeñan un papel fundamental en la mejora de la preparación y la resiliencia a nivel nacional.

## Evolución del panorama de las estructuras organizativas desde 2008

**4.3** En lo que atañe Pilar 3, se han observado importantes avances en el último decenio. Se han creado numerosas organizaciones nacionales, regionales e internacionales para abordar la cuestión de la ciberseguridad.

**4.4** Cabe citar como ejemplos de iniciativas regionales AFRIPOL, AMERIPOL, GCCPOL,el Centro de Ciberseguridad de Oceanía (OCSC), el Centro de Ciberseguridad de Australia (ACSC), el Centro Europeo de Ciberdelincuencia (EC3), el Centro de Coordinación de Ciberdelincuencia de la India (I4C) y el Portal de Denuncias de Ciberdelitos, el Centro Nacional de Preparación para Incidentes y Estrategia para la Ciberseguridad y el Centro de Control del Ciberdelito (JC3) de Japón, la Agencia Nacional de Ciberseguridad de Malasia (NACSA), la Agencia Nacional de Ciberseguridad de Francia (ANSSI), el Centro Nacional de Ciberseguridad de Lituania (NCSC), el Centro Nacional de Ciberseguridad de Suiza, el Centro Nacional de Ciberseguridad del Reino Unido (NCSC), la Célula de Coordinación Internacional de Ciberdelitos de los Estados Unidos (IC4), el Centro Nacional de Coordinación de Incidentes Informáticos de Rusia, así como el Centro de Coordinación Consultiva de la Organización del Tratado de Seguridad Colectiva para la Respuesta a Incidentes Informáticos (CCC CSTO), el Comité Interamericano contra el Terrorismo (CICTE) y el Programa de Ciberseguridad de la OEA, la Autoridad Nacional de Ciberseguridad (NCA) de Arabia Saudita y la Autoridad Nacional de Ciberseguridad de Rwanda.

**4.5** A pesar de las crecientes inversiones de los Estados Miembros en los EIII y del alcance regional e internacional independiente de los EIII nacionales, todavía hay 85 países que no cuentan con un EIII nacional, situación que es muy preocupante dado el carácter mundial de las ciberamenazas[[24]](#footnote-24).

**4.6** La UIT, a través de su Oficina de Desarrollo, está trabajando con los Estados Miembros, los asociados y las organizaciones regionales e internacionales para crear capacidades a nivel nacional y regional, desplegar capacidades y ayudar a crear y mejorar los EIII nacionales. Hasta la fecha, la UIT ha procedido a más de 80 evaluaciones de la preparación de los EIII para ayudar a los países a estimar su preparación nacional en materia de ciberseguridad y su capacidad de respuesta a los incidentes[[25]](#footnote-25). La UIT ha prestado apoyo a efectos de la creación/mejora de 22 proyectos de EIII nacionales para los respectivos Estados Miembros de la UIT[[26]](#footnote-26). Para llevar a cabo estas evaluaciones de los países, la UIT colabora con asociados como el Foro sobre los equipos de seguridad y respuesta ante incidentes (FIRST), el Centro Mundial de Capacidad en Ciberseguridad y otros.

**4.7** En cuanto a las organizaciones internacionales, ha habido varias iniciativas, algunos ejemplos de las cuales se enumeran a continuación:

• El [Centro de Mundial de Capacidad en Ciberseguridad](https://www.oxfordmartin.ox.ac.uk/cyber-security/) (GCSCC) es un centro internacional de investigación sobre la creación eficiente y eficaz de capacidad en materia de ciberseguridad, y colaboró con la UIT en la elaboración de la [Guía para la formulación de una estrategia nacional de ciberseguridad (NCS)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx), que se utiliza actualmente para realizar ejercicios prácticos sobre las NCS, así como para impartir a los países capacitación sobre buenas prácticas en la elaboración de un marco nacional de estrategia de ciberseguridad efectivo.

• El [Global Forum on Cyber Expertise](https://thegfce.org/) (GFCE), creado en 2015, tiene por objeto intercambiar buenas prácticas y proporcionar conocimientos especializados sobre la creación de cibercapacidad a los países, las organizaciones internacionales y el sector privado. El GFCE y la UIT han puesto en marcha conjuntamente la [iniciativa CSIRT Maturity](https://cybilportal.org/projects/csirt-maturity-initiative-3/) y han colaborado en otras actividades en el campo de la ciberseguridad como la creación de la colección de herramientas "[Combatting Cybercrime](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cybercrime-toolkit.pdf)".

• El [INTERPOL Global Complex for Innovation](https://www.interpol.int/en/News-and-Events/News/2014/INTERPOL-Global-Complex-for-Innovation-opens-its-doors) (IGCI), inaugurado en 2015 en Singapur, proporciona a los organismos nacionales encargados de velar por el cumplimiento de la ley un apoyo práctico especializado y capacitación para adaptarse a la evolución de la delincuencia. En 2018, la UIT y la INTERPOL firmaron un acuerdo de cooperación encaminado a establecer un marco oficial para que la INTERPOL y la UIT cooperen en beneficio mutuo y en el ámbito de sus respectivos mandatos y recursos, en el fomento de la confianza y la seguridad en la utilización de las TIC.

• El WEF presentó el [Global Centre for Cybersecurity](https://www.weforum.org/centre-for-cybersecurity/) en 2018 con el objetivo de crear una plataforma mundial para que gobiernos, empresas, expertos y organismos encargados de hacer cumplir la ley colaboren en los desafíos de la ciberseguridad. Ese mismo año, la UIT y el WEF acordaron cooperar en la promoción de proyectos e iniciativas de ciberseguridad destinados a mitigar las ciberamenazas, y también explorar nuevas oportunidades de cooperación en la promoción de la ciberseguridad.

## Directrices para utilizar el Pilar 3 – Estructuras organizativas

|  |
| --- |
| **4.8** Aunque se reconoce que las recomendaciones del Informe del GEAN de 2008 han servido para orientar los esfuerzos de la UIT en relación con el Pilar 3 y siguen siendo pertinentes, las siguientes directrices propuestas, especialmente pertinentes para la labor de la Oficina de Desarrollo de la UIT (BDT), podrían contribuir a fortalecer los esfuerzos a este respecto: **a)** La UIT debe seguir prestando asistencia a los países en desarrollo en la implementación de los EIII nacionales y otras unidades/organizaciones técnicas conexas. **b)** La UIT debe dar prioridad a los países en los que aún no se han implantado las estructuras organizativas de ciberseguridad adecuadas.**c)** La UIT debería promover una colaboración más abierta e inclusiva, así como la coordinación entre las diversas organizaciones nacionales, regionales o internacionales que participan en el esfuerzo por establecer estructuras organizativas nacionales sostenibles, a fin de garantizar un apoyo eficaz y evitar la duplicación de esfuerzos. **d)** La UIT debería aumentar sus esfuerzos para medir los compromisos institucionales de los Estados Miembros, aprovechando instrumentos como el Índice Mundial de Ciberseguridad, para promover la ciberseguridad como factor transversal de sus esfuerzos en la transformación digital. **e)** En lo que respecta en particular a las estructuras nacionales, la UIT debería ayudar a los Estados Miembros facilitando estrategias para elaborar un marco de coordinación a escala de todo el gobierno, a fin de mejorar la aplicación coherente y transversal de los esfuerzos nacionales de ciberseguridad.**f)** La UIT debería seguir fomentando una mayor colaboración entre las estructuras organizativas de la ciberseguridad a nivel regional y mundial mediante actividades como los simulacros cibernéticos, entre otras. |

# Sección 5 Pilar 4: Capacitación

## Introducción

**5.1** El desarrollo y despliegue de las calificaciones adecuadas, de una cultura de ciberseguridad y de buenas prácticas entre todos los interesados es una cuestión crucial.

**5.2** Todos los países y todas las organizaciones se enfrentan a la necesidad de contar con los recursos humanos y las cualificaciones suficientes y necesarios para:

• implementar medidas estratégicas y operativas de ciberseguridad;

• realizar evaluaciones nacionales de riesgos de ciberseguridad;

• gestionar crisis relacionadas con los incidentes de ciberseguridad que ocurran;

• fortalecer la robustez y resiliencia de las infraestructuras y servicios digitales; y

• desarrollar procesos, competencias y prácticas coherentes.

**5.3** Es importante señalar también que, habida cuenta de los rápidos avances de las TIC y de los problemas ya existentes de acceso y conectividad, los usuarios finales –y en particular segmentos de población como las mujeres, los niños, las personas de edad, las personas con discapacidad y con necesidades específicas– pueden ser a menudo más vulnerables a las amenazas y los incidentes de ciberseguridad. Por consiguiente, los programas educativos relacionados con la ciberseguridad, además de sensibilizar respecto de las amenazas a la ciberseguridad que afectan a los usuarios finales vulnerables, podrían ser fundamentales para reducir los riesgos de ciberseguridad para la sociedad en su conjunto.

## Evolución del panorama de la capacitación desde 2008

**5.4** Dado que la ciberseguridad tiene una dimensión mundial y se ocupa de una amplia gama de cuestiones –como los usos debidos o indebidos de las TIC, las medidas técnicas y las cuestiones económicas, jurídicas y políticas–, es importante desarrollar una cultura mundial de la ciberseguridad para mejorar el nivel de comprensión de cada uno de los actores de la cadena de la ciberseguridad. Al desarrollar una cultura de la ciberseguridad, uno de los principales retos es identificar correctamente cuáles son los problemas mundiales e internacionales y cuáles son las necesidades locales específicas, pues las culturas dependen principalmente de factores locales y temporales. Las normas técnicas internacionales pueden contribuir a identificar los problemas clave de alcance mundial y genérico relacionados con la dimensión técnica y procesal de la cultura de ciberseguridad.

**5.5** Es importante una respuesta colectiva para proteger las infraestructuras digitales. Esto es cada vez más urgente, ya que el cambio tecnológico está llevando a una interconectividad mayor y permanente a través de las TIC[[27]](#footnote-27). Todo lo que puede ser conectado podría estar en peligro. Por otra parte, la miniaturización de los componentes gracias a las nanotecnologías, incluyendo varios tipos de chips inteligentes y autónomos, ha llevado a que estos chips se integren en tecnologías que afectan a todas nuestras actividades.

**5.6** La ACG ha servido como un marco interdisciplinario innovador y eficiente para los esfuerzos de capacitación en el que los actores pertinentes pueden seguir elaborando respuestas globales, programables y específicas para colaborar eficazmente. El marco de la ACG se ha creado para hacer frente al desafío de construir una sociedad de la información inclusiva y segura.

**5.7** Las recomendaciones formuladas a este respecto por el Informe del GEAN de 2008 siguen siendo pertinentes hoy en día. Teniendo en cuenta la labor realizada por la UIT, en particular desde la primera publicación de la "[The Cybersecurity Guide for Developing Countries](https://www.itu.int/pub/D-STR-SECU-2006)" (Guía sobre ciberseguridad para los países en desarrollo) en 2006, y sobre la base del marco de la ACG y del Informe del GEAN de 2008, se ha llevado a cabo una amplia labor en materia de capacitación en todos los Estados Miembros, incluidas actividades de formación, sensibilización y educación a nivel nacional, regional e internacional.

**5.8** Utilizando el marco de la ACG, la UIT sigue prestando asistencia a los países, en particular en lo que respecta a la creación de la capacidad y las calificaciones humanas necesarias, la definición de sus estrategias nacionales en materia de ciberseguridad, la ayuda al desarrollo de calificaciones para la gestión de equipos de intervención en caso de incidente informático (EIII) y la elaboración de recursos para la protección de la infancia en línea.

**5.9** Por ejemplo, en lo que respecta a la sensibilización, es importante reconocer la contribución del [Índice Mundial de Ciberseguridad (GCI)](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx). Desde que se publicara por primera vez en 2015, el GCI –que mide el compromiso de los Estados Miembros con la ciberseguridad– se ha publicado con éxito en otras tres ocasiones como resultado de la fuerte demanda de los Estados Miembros, el sector privado, el mundo académico y otros. Gracias a orientación hacia la sensibilización, el GCI sigue prestando apoyo a los Estados Miembros para que mejoren su posición en materia de ciberseguridad mediante el intercambio de buenas prácticas para la aplicación efectiva de la ciberseguridad. El GCI ha demostrado ser una herramienta de valor incalculable para la sensibilización y la capacitación que debe seguirse aprovechando y fortaleciendo.

## Directrices para utilizar el Pilar 4 – Capacitación

**5.10** Deberían adoptarse medidas concretas a nivel nacional para crear o mejorar la capacidad en materia de ciberseguridad de las diversas partes interesadas de manera que puedan resolver los problemas de ciberseguridad nacionales e internacionales. Dado que las actividades de capacitación se realizan principalmente a nivel nacional, deberían asignarse recursos adecuados a los agentes nacionales[[28]](#footnote-28).

**5.11** Además, desde una perspectiva mundial, el empoderamiento de los recursos humanos requiere un marco educativo general, modular y flexible en materia de ciberseguridad para responder a las necesidades de una mayor sensibilización del público y ofrecer un plan de estudios adaptado a profesionales concretos. Se debe prestar especial atención a la brecha de género en esta área. Hay mucho capital humano desaprovechado que puede utilizarse para contribuir al campo de la ciberseguridad, incluidas las mujeres, que todavía representan sólo el 20% de la fuerza de trabajo de la ciberseguridad[[29]](#footnote-29).

**5.12** La calidad de la educación formal a nivel escolar o universitario y la sensibilización del público en general dependen en cierta medida de la calidad, madurez y pertinencia de la investigación.

**5.13** Además, es importante que se preste atención al fomento de la capacidad de las microempresas y las pequeñas y medianas empresas (MIPYMES) que son ahora uno de los agentes clave de la creciente economía digital, permitiéndoles identificar y gestionar ciberriesgos y utilizar los activos de TIC (incluidas la banda ancha e Internet) de manera segura y sostenible.

|  |
| --- |
| **5.14** Habida cuenta de lo anterior, la ACG y las recomendaciones con arreglo a este Pilar del Informe del GEAN de 2008 siguen proporcionando un marco sólido que mejora y promueve un enfoque interdisciplinario de la creación de capacidad. Teniendo esto en cuenta, se propone que la UIT, a través de su Oficina de Desarrollo de las Telecomunicaciones (BDT): **a)** Siga promoviendo una colaboración más abierta e inclusiva, así como la coordinación, entre las diversas organizaciones nacionales, regionales o internacionales dedicadas a la capacitación en materia de ciberseguridad, a fin de garantizar la eficacia y de evitar la duplicación de esfuerzos.**b)** Siga prestando apoyo a los países en desarrollo para las actividades de capacitación en materia de ciberseguridad, con el apoyo de las comunidades de creación de capacidad en materia de ciberseguridad nacionales e internacionales.**c)** Siga prestando asistencia a los países en desarrollo, en colaboración con los asociados interesados y otras comunidades de desarrollo de la capacidad, en la elaboración de estrategias, planes y políticas nacionales de ciberseguridad y en la creación de capacidad de respuesta en caso de incidente.**d)** Siga impartiendo capacitación para cerrar la brecha de normalización, incluso mediante la prestación de asistencia técnica a los países que la soliciten.**e)** Mejore la promoción y facilite el intercambio de buenas prácticas de los Estados Miembros a fin de ayudar a los países rezagados en materia de ciberseguridad a mejorar su situación en dicho ámbito y a reducir el déficit de capacidad.**f)** Siga desarrollando sus actividades de capacitación, teniendo en cuenta la necesidad de nuevas calificaciones para adaptarse a las necesidades de seguridad de las tecnologías emergentes. A este respecto, debería fomentarse una mayor colaboración con las instituciones académicas, el sector privado y los Estados Miembros.**g)** Siga prestando especial atención en sus actividades de capacitación a las necesidades de los grupos más vulnerables como las mujeres, los niños, las personas con discapacidad y las personas con necesidades específicas, así como las personas de edad. **h)** Siga desarrollando y fortaleciendo el GCI como herramienta para la capacitación y la sensibilización.**i)** Elabore una "Guía para la definición y aplicación del programa de educación en materia de ciberseguridad" con el fin de prestar apoyo a los Estados Miembros en la elaboración y adopción de cursos de ciberseguridad para jóvenes en los sistemas de enseñanza primaria, secundaria, y para adultos en la enseñanza universitaria y profesional, a fin de contribuir a la formación de más profesionales de la ciberseguridad a nivel mundial e incluir el elemento de ciberseguridad en todas las disciplinas y sensibilizar a todos los futuros profesionales.**j)** Siga facilitando la identificación de actividades de investigación relacionadas con la ciberseguridad o los diálogos entre las distintas partes interesadas, especialmente en las nuevas esferas tecnológicas, aprovechando los miembros académicos y del sector privado de la UIT, como se ha hecho, por ejemplo, en la Cumbre Mundial "AI for Good", que celebra anualmente la UIT.**k)** Difunda herramientas, recursos y buenas prácticas a los Estados Miembros, la industria y otras partes interesadas con el fin de apoyar sus esfuerzos en la creación de capacidad de las MIPYMES para hacer frente a los desafíos de seguridad, y crear confianza en el uso de las TIC.**l)** Siga fomentando una cultura de ciberseguridad. |

# Sección 6 Pilar 5: Cooperación internacional

## Introducción

**6.1** En el último decenio ha quedado claro que ninguna entidad u organización por sí sola puede hacer frente a toda la gama de problemas de ciberseguridad actuales y emergentes. Esos problemas pueden abordarse mediante asociaciones que entrañen una estrecha colaboración y coordinación entre todos los interesados a fin de contribuir a la creación de un ecosistema de TIC universalmente disponible, abierto, seguro y fiable.

**6.2** Por lo tanto, el Pilar 5 sobre la cooperación internacional es un pilar transversal de la ACG, que constituye la base de todos los aspectos relacionados con la creación de confianza y seguridad en el uso de las TIC. En el Informe del GEAN de 2008, este pilar trataba de elaborar una estrategia de cooperación, diálogo y coordinación internacionales para hacer frente a las ciberamenazas.

## Evolución del panorama de la cooperación internacional desde 2008

Diálogos mundiales de alto nivel

**6.3** Los debates sobre diversos aspectos de la ciberseguridad −incluidos los aspectos técnicos, el ciberdelito, la privacidad, la protección de los datos y otros− se llevan a cabo en muchos foros y procesos. Algunos de ellos han sido acogidos por diversos organismos de las Naciones Unidas, incluida la UIT u otras organizaciones internacionales, y otros han sido iniciados por otras partes interesadas, así como otros foros internacionales y regionales.

**6.4** Si bien todos los foros y procesos están realizando una buena labor de sensibilización y mejora de la comprensión, es importante identificar las sinergias entre estos diversos esfuerzos para que la comunidad internacional pueda reunirse y encontrar soluciones.

**6.5** La plataforma de las Naciones Unidas, con su importante capacidad de convocatoria, está bien situada para fomentar la cooperación, los diálogos y la coordinación a nivel internacional entre las partes interesadas de todas las naciones para hacer frente a los desafíos relacionados con el ciberespacio. Como se destaca en el Informe del GEAN de 2008, la UIT, habida cuenta de su posición como organismo especializado en las TIC en el sistema de las Naciones Unidas, puede seguir desempeñando una función clave, en el marco de su mandato, en los ámbitos de desarrollo conexos.

**6.6** Si bien en la recomendación 1.15 del Informe del GEAN de 2008 se sugería la celebración de una "conferencia mundial"[[30]](#footnote-30), también podrían aprovecharse mejor las conferencias, foros y procesos actuales que surgieron del proceso de la Cumbre Mundial sobre la Sociedad de la Información y se consolidaron posteriormente −el [Foro de la CMSI](https://www.itu.int/net4/wsis/forum/2020/es) para las cuestiones de desarrollo y el [Foro de Gobernanza de Internet (IGF)](https://www.intgovforum.org/multilingual/es/) para las cuestiones de gobernanza− para ello. El Foro de la CMSI, la mayor reunión anual de la comunidad de las TIC para el desarrollo, ofrece varios mecanismos para reunir a la comunidad mundial con el fin de examinar y definir soluciones concretas para los problemas de desarrollo relativos al fomento de la confianza y la seguridad en la utilización de las TIC (Línea de Acción C5), entre ellos, la vía del facilitador de la Línea de Acción, los diálogos de alto nivel y las reuniones de partes interesadas con fines específicos.

**6.7**Un acontecimiento importante del último decenio ha sido el reconocimiento de la importancia decisiva de la ciberseguridad al más alto nivel político de los gobiernos nacionales. Ello se refleja en la adopción, por muchos países, de una estrategia para la transformación digital que asume un enfoque a escala de todo el gobierno y crea mecanismos centrales de coordinación intersectorial que suelen informar directamente a los Jefes de Estado o de Gobierno.

**6.8** Otra novedad conexa ha sido el importante número de conversaciones bilaterales que se están celebrando entre países y regiones tecnológicamente avanzados.

Asociaciones internacionales de múltiples partes interesadas

**6.9** La UIT ha tenido varios éxitos en el fomento de la cooperación internacional gracias a su papel como única facilitadora de la Línea de Acción C5 de la CMSI.

**6.10** La UIT ha forjado toda una gama de asociaciones de múltiples partes interesadas, ya sea mediante:

• mecanismos formales tales como los memorandos de entendimiento o acuerdos similares (por ejemplo con FIRST, Interpol, ONUDD, WEF, y otros);

• iniciativas como la protección de la infancia en línea, en asociación[[31]](#footnote-31) con más de 80 entidades de todos los grupos de partes interesadas; o

• Mecanismos como los grupos temáticos, por ejemplo, los grupos temáticos sobre tecnologías de libro mayor digitales, tecnologías cuánticas, IA y salud, etc., que ofrecen una plataforma para que todas las partes interesadas traten de los problemas de fiabilidad y confianza en las tecnologías emergentes.

**6.11** Al haber ampliado considerablemente el número de sus miembros de las múltiples partes interesadas en el último decenio, especialmente en la gama de empresas del sector privado e instituciones académicas, la UIT cuenta con 193 Estados Miembros y casi 900 empresas del sector privado, universidades y organizaciones internacionales y regionales, lo que refleja la naturaleza rápidamente cambiante de la sociedad digital actual.

Mejora de la coordinación dentro del sistema de las Naciones Unidas

**6.12** Como ya se ha indicado en los puntos 2.4 y 2.5 anteriores, la Asamblea General de las Naciones Unidas ha puesto en marcha una serie de procesos para hacer frente al reto que supone garantizar la seguridad internacional en el ciberespacio. Entre esos procesos se cuenta el trabajo de los GEG y los GTCA. En su [primer Informe sustantivo](https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf), el GTCA 2019-2021 concluye, entre otras cosas, que el futuro diálogo institucional periódico no debe duplicar los mandatos, esfuerzos y actividades de las Naciones Unidas ya existentes dedicados a la dimensión digital de otros asuntos, y que todo futuro mecanismo de diálogo institucional periódico bajo los auspicios de las Naciones Unidas debe ser un proceso orientado a la acción con objetivos específicos, que se base en los resultados ya cosechados y sea inclusivo, transparente, rigiéndose por el consenso y los resultados. Teniendo esto en cuenta, es importante que el trabajo de la UIT complemente los trabajos que ya se están realizando en el sistema de las Naciones Unidas sobre este tema, en particular los de los procesos de la AGNU mencionados.

**6.13** La compleja articulación del mandato del sistema de las Naciones Unidas puede a veces impedir un enfoque armonizado pragmático y eficaz. Por lo tanto, para ser más eficaz es imperativo que el sistema de las Naciones Unidas siga trabajando en la armonización de sus esfuerzos, incluida la racionalización de los programas y actividades en materia de ciberseguridad.

**6.14** Es, por tanto, importante promover dentro de las Naciones Unidas la construcción de una manera compartida de entender las necesidades y los requisitos para crear programas e iniciativas apropiados que apoyen efectivamente los esfuerzos emprendidos por los gobiernos, la industria y todas las demás partes interesadas pertinentes.

**6.15** En 2010 se dio un primer paso importante para mejorar la coordinación interna entre los organismos de las Naciones Unidas en la asistencia que prestan a los Estados Miembros en materia de ciberseguridad. La UIT y la ONUDD, en colaboración con otros 33 organismos de las Naciones Unidas, encabezaron un esfuerzo de dos años para elaborar un marco de las Naciones Unidas sobre ciberseguridad y ciberdelitos, que fue adoptado por la Junta de Jefes Ejecutivos (JJE) del Sistema de las Naciones Unidas en noviembre de 2013.

**6.16** Aunque fue un paso fundamental, se requieren más cambios a escala de todo el sistema para asegurar una coordinación eficaz. El hecho de que el Secretario General de las Naciones Unidas haya dado prioridad a la cooperación digital[[32]](#footnote-32) ofrece la oportunidad de abordar la necesidad de que el sistema de las Naciones Unidas en su conjunto siga mejorando la coordinación y la cooperación internas mediante la utilización de diversos mecanismos interinstitucionales, entre ellos la JJE.

## Directrices para utilizar el Pilar 5 – Cooperación internacional

|  |
| --- |
| **6.17** Dado el carácter intersectorial de este pilar, y teniendo en cuenta la gama de colaboraciones y asociaciones en los diferentes sectores de la UIT, es importante que todos los sectores de la UIT trabajen en estrecha colaboración y coordinen sus esfuerzos, tanto a nivel interno como externo, utilizando mecanismos eficaces de coordinación intersectorial y coordinadores designados. Las recomendaciones del Informe del GEAN de 2008 a este respecto siguen siendo pertinentes y, sobre la base de la información proporcionada en la sección anterior, se proponen además las siguientes directrices para la utilización del Pilar 5: **a)** Las Naciones Unidas desempeñan un papel singular en el fomento de la cooperación, el diálogo y la coordinación en cuestiones de ciberseguridad a escala mundial entre todas las naciones, así como con el sector privado y otras partes interesadas. Habida cuenta de su posición dentro del sistema de las Naciones Unidas como organismo especializado en las TIC y única facilitadora de la Línea de Acción C5 (Fomento de la confianza y la seguridad en la utilización de las TIC), la UIT debe seguir desempeñando un papel destacado, en ámbitos correspondientes a su mandato, en los acontecimientos conexos.**b)** Sobre la base del proceso de la CMSI y teniendo en cuenta los esfuerzos del Grupo de Alto Nivel sobre Cooperación Digital del Secretario General de las Naciones Unidas, especialmente la recomendación 4 (Compromiso Mundial sobre Confianza y Seguridad), la UIT debería contribuir a fortalecer los esfuerzos de facilitación para reunir a los diferentes actores. Esto podría hacerse a través de los mecanismos ofrecidos en el marco de los procesos relacionados con la Línea de Acción C5 a través del Foro de la CMSI, así como los ofrecidos por el IGF, entre otros.**c)** Al tiempo que deben seguir alentándose los debates bilaterales y multilaterales entre los principales actores, dado el carácter mundial de las ciberamenazas, también es importante que se faciliten debates de mayor alcance entre grupos más amplios, incluidos el sector privado y otras partes interesadas. La UIT podría, dentro de su ámbito de competencia, desempeñar una función de facilitación a este respecto, colaborando con los asociados para ayudar a reunir a todos los interesados en el contexto global más amplio de las Naciones Unidas.**d)** La UIT debería seguir explorando mecanismos innovadores, flexibles y ágiles para crear asociaciones, teniendo en cuenta la rápida evolución del sector tecnológico y la gama de nuevas entidades que están surgiendo, especialmente las empresas de nueva creación y las MIPYME.**e)** La UIT debe seguir colaborando activamente con otros organismos clave del sistema de las Naciones Unidas las actividades encaminadas a armonizar los esfuerzos internos de la Secretaría de las Naciones Unidas y a racionalizar sus programas y actividades en materia de ciberseguridad, a fin de prestar un servicio más eficaz a la comunidad mundial. |

# Sección 7 Directrices generales para el marco de la ACG

|  |
| --- |
| **7.1** En el proceso de elaboración de directrices para la utilización de la ACG surgieron algunas directrices transversales amplias que son aplicables y pertinentes para toda la labor de la UIT y los cinco Pilares de la ACG.Al reconocer las fuertes interrelaciones entre los Pilares, así como la necesidad de que la UIT y sus miembros trabajen en pro de una visión global y exhaustiva de la acción en materia de ciberseguridad, se proponen las siguientes directrices generales:**a)** Habida cuenta de la proliferación de partes interesadas, organizaciones, asociaciones y lugares que trabajan en el ámbito de la ciberseguridad y que impulsan diferentes aspectos de los avances, la UIT debe seguir fortaleciendo y ampliando sus colaboraciones e implicaciones en beneficio colectivo de todas esas partes interesadas, a fin de mejorar el intercambio de conocimientos, de información y de experiencias, evitando al mismo tiempo la duplicación de esfuerzos.**b**)La UIT debe servir de depósito de información para las diversas actividades, iniciativas y proyectos mundiales que están llevando a cabo en las diferentes facetas de la ciberseguridad otras partes interesadas y organizaciones activas en esta esfera, y que pueden tener el mandato, la función y/o las responsabilidades principales en esas facetas específicas, a fin de que la comunidad internacional pueda tener un punto de acceso fácil a todos esos recursos.**c**) Toda labor que lleve a cabo la UIT de conformidad con la ACG debe basarse en una evaluación clara de las necesidades y los objetivos de sus miembros utilizando herramientas como el GCI, los productos necesarios para satisfacerlos y responder a los sistemas de medición y las medidas apropiadas que se han diseñado específicamente con este fin.**d)** La UIT debería seguir realizando el seguimiento del desarrollo y la utilización de las TIC nuevas y emergentes, a fin de orientar a los Estados Miembros y las partes interesadas acerca de los aspectos de seguridad de esas tecnologías, dentro de su ámbito de competencia, y, cuando proceda, la posible aplicación de las mismas para contrarrestar las ciberamenazas.**e)** Habida cuenta de las repercusiones intrínsecamente transnacionales e intersectoriales de la ciberseguridad, la UIT debe promover actividades, iniciativas y proyectos que puedan ayudar a los Estados Miembros a propiciar un mismo enfoque a escala de todo el gobierno para abordar la cuestión. |

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

1. Actas de la decimoséptima Sesión Plenaria de la Conferencia de Plenipotenciarios, Dubái, 15 de noviembre de 2018, disponible en <https://www.itu.int/md/S18-PP-C-0174/es>. [↑](#footnote-ref-1)
2. Transmisión del Informe del Expresidente del Grupo de Expertos de Alto Nivel de la Agenda sobre Ciberseguridad Global (C19/58), UIT, 8 de mayo de 2019, disponible en <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, disponible en <https://www.itu.int/md/S19-CL-C-0117/es>. [↑](#footnote-ref-3)
4. Para más información sobre el proceso, y para las contribuciones recibidas de los Estados Miembrosy otros interesados, sírvase visitar:
<https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx>. [↑](#footnote-ref-4)
5. Documentos de resultados de la CMSI, 2005, disponible en <https://www.itu.int/net/wsis/outcome/booklet.pdf>. [↑](#footnote-ref-5)
6. Véase Magistrado Stein Schjolberg, Informe del Presidente del GEAN:
<https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>. [↑](#footnote-ref-6)
7. Las recomendaciones del Informe del GEAN de 2008 se presentan con un resumen anotado de las opiniones y los debates celebrados durante la reunión en relación con cada una de ellas. Aunque los miembros del GEAN no lograron un consenso pleno respecto de cada recomendación, la mayoría de los expertos del Grupo de expertos de alto nivel estuvieron de acuerdo en general con muchas de las recomendaciones. [↑](#footnote-ref-7)
8. La [Directiva del Parlamento Europeo y del Consejo de la Unión Europea del 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco (2005) del Consejo](https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32013L0040) cuenta con una definición de infraestructura crítica en los siguientes términos: un elemento*, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población, y cuya perturbación o destrucción tendría un impacto significativo en un Estado miembro al no poder mantener esas funciones*. [↑](#footnote-ref-8)
9. Número de usuarios activos mensuales de Facebook en todo el mundo, al 4º trimestre de 2020, disponible en: <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>. [↑](#footnote-ref-9)
10. Mark Zuckerberg: *The Internet needs new rules.* *Let’s start in these four areas,* Washington Post, 30 de marzo de 2019, disponible en: <https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html>. [↑](#footnote-ref-10)
11. Grupo de Expertos Gubernamentales, disponible en <https://www.un.org/disarmament/group-of-governmental-experts/> [↑](#footnote-ref-11)
12. Grupo de Trabajo de Composición Abierta, disponible en <https://www.un.org/disarmament/open-ended-working-group/> [↑](#footnote-ref-12)
13. Para más información, véase:

– Informe anual de actividades de la UIT al Consejo de la UIT sobre la creación de confianza y seguridad en el uso de las TIC, disponible en <https://www.itu.int/es/council/2021/Pages/default.aspx>.

– Informe al Consejo de 2021 sobre la utilización de la ACG por la UIT, disponible en <https://www.itu.int/md/S21-CL-C-0036/es>. [↑](#footnote-ref-13)
14. Stein Schjolberg, *The History of Cybercrime* (3ª edición, febrero de 2020). [↑](#footnote-ref-14)
15. La Comisión de la Unión Europea puso en marcha un programa denominado [Horizonte 2020](https://ec.europa.eu/programmes/horizon2020/en) para desarrollar el potencial de la Internet de las cosas, y el programa de trabajo de 2016-2017 para apoyar la experimentación y la innovación. Se invitaba a presentar propuestas sobre diversos temas, entre ellos la seguridad y privacidad de la IoT. Se presentaban conceptos para la seguridad de extremo a extremo en entornos de IoT altamente distribuidos, heterogéneos y dinámicos. Los enfoques deben ser holísticos e incluir la identificación y la autenticación, la protección de datos y la prevención de los ciberataques a nivel de dispositivos y sistemas. Deben abordar los elementos de seguridad y privacidad pertinentes, como son la confidencialidad, el conocimiento y el control de los datos de los usuarios, la integridad, la resiliencia y la autorización (véase la Decisión C (2015) 6776 de la Comisión Europea, de 13 de octubre de 2015). [↑](#footnote-ref-15)
16. T. Ballell, *Legal challenges of artificial intelligence: modelling the disruptive features of emerging technologies and assessing their possible legal impact*, Uniform Law Review, volumen 24, número 2, junio de 2019, páginas 302–314, disponible en <https://doi.org/10.1093/ulr/unz018>. [↑](#footnote-ref-16)
17. Un modelo de marco jurídico puede ser la [Directiva 2011/92/EU del Parlamento y el Consejo Europeos del 13 de diciembre de 2011](https://ec.europa.eu/anti-trafficking/legislation-and-case-law-eu-legislation-criminal-law/directive-201192eu_en), sobre lucha contra el abuso sexual y la explotación sexual de niños y la pornografía infantil. [↑](#footnote-ref-17)
18. Judge Stein Schjolberg, 2018 & Judge Stein Schjolberg, 2019, disponible en <https://www.cybercrimelaw.net/Cybercrimelaw.html>. [↑](#footnote-ref-18)
19. Por ejemplo, <https://www.justice.gov/olp/lawful-access> [↑](#footnote-ref-19)
20. *ITU Standards Landscape*, disponible en <https://www.itu.int/net4/ITU-T/landscape#?topic=0.1&workgroup=1.3935&searchValue=&page=1&sort=Revelance>. [↑](#footnote-ref-20)
21. Informe del GEAN 2008, párrafo 2.1, pág. 9, *id* en 6. [↑](#footnote-ref-21)
22. Informe del GEAN 2008, párrafo 2.2, pág. 9, *id* en 6. [↑](#footnote-ref-22)
23. Informe del GEAN 2008, párrafo 2, pág.9, *id* en 6. [↑](#footnote-ref-23)
24. EIII nacionales, UIT, disponible en <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx>. [↑](#footnote-ref-24)
25. *Ibid*. [↑](#footnote-ref-25)
26. *Ibid*. [↑](#footnote-ref-26)
27. Tim Berners-Lee, *30 years on, what’s next #ForTheWeb?*, 12 de marzo de 2019(disponible en <https://webfoundation.org/2019/03/web-birthday-30/>) con ocasión del 30º aniversario de la web, en una carta abierta, declaró que *mientras que la web ha creado oportunidades, ha dado voz a los grupos marginados, y ha hecho nuestra vida diaria más fácil, también ha creado oportunidades para los estafadores, ha dado voz a los que propagan el odio, y ha hecho que todo tipo de crímenes sean más fáciles de cometer.* [↑](#footnote-ref-27)
28. S. Ghernaouti, *Cyberpower, Crime, Conflict and Security in Cyberspace,* EPFL Press 2013. [↑](#footnote-ref-28)
29. Laurence Bradford, *Cybersecurity needs women: Here’s why*, 18 October 2018, available at
<https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurity-needs-women-heres-why/#5a7a3cc447e8> [↑](#footnote-ref-29)
30. Informe del GEAN de 2008, párrafo 1.15, página 9, *id* en 6. [↑](#footnote-ref-30)
31. Puede encontrarse más información al respecto en <https://www.itu.int/en/cop/Pages/partners.aspx> [↑](#footnote-ref-31)
32. Para más información, visite <https://www.un.org/en/digital-cooperation-panel/>. [↑](#footnote-ref-32)