|  |  |
| --- | --- |
| **Consejo 2022Ginebra, 21-31 de marzo de 2022** |  |
|  |
|  |  |
| **Punto del orden del día: PL 1.4** | **Revisión 1 alDocumento C22/32-S** |
|  | **15 de marzo de 2022** |
|  | **Original: inglés** |
| Informe del Secretario General |
| PROYECTO DE DIRECTRICES PARA LA UTILIZACIÓN DE LA AGENDASOBRE CIBERSEGURIDAD GLOBAL POR LA UIT |

|  |
| --- |
| 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 (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, C19/58).De conformidad con estas instrucciones, se elaboró 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, que fue presentado, junto con el informe de la Secretaría (C21/36) a la Consulta Virtual de los Consejeros de 2021 (C21/CVC-1) para su examen y aprobación (C21/71).Tras la consulta (C21-CVC-1)**,** los Estados Miembros del Consejo tomaron nota del informe de la Secretaría y adoptaron por correspondencia la decisión relativa al proyecto de Directrices en la que se encarga a la Secretaría que celebre nuevas consultas con los Estados Miembros del Consejo, teniendo en cuenta las contribuciones recibidas y los comentarios formulados durante esa reunión. La Secretaría debería presentar un documento revisado para su examen y aprobación en la próxima reunión del Consejo.Por consiguiente, se llevaron a cabo nuevas consultas con los Estados Miembros del Consejo y, teniendo en cuenta las contribuciones recibidas, se elaboró el siguiente proyecto revisado de Directrices junto con un documento de información complementaria ([C22/INF/8](https://www.itu.int/md/S22-CL-INF-0008/es)). Es importante señalar que el propósito de esta labor no es abordar cuestiones relacionadas con la revisión de la ACG.Acción solicitadaEste documento se presenta al Consejo para su **consideración** y **aprobación**, según proceda.***Nota: Este proyecto de Directrices se ha actualizado teniendo en cuenta los debates mantenidos por los Estados Miembros del Consejo el día 14 de marzo sobre los apartados pendientes indicados entre corchetes del Documento 32. En esta versión del documento, quedan dos párrafos entre corchetes.***\_\_\_\_\_\_\_\_\_\_\_\_Referencias[*Resolución 130 (Rev. Dubái, 2018)* de la Conferencia de Plenipotenciarios](https://www.itu.int/en/council/Documents/basic-texts/RES-130-S.pdf),[*Agenda de Ciberseguridad Global (ACG)*](https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)*,* [Documentos del Consejo *C21/36*](https://www.itu.int/md/S21-CL-C-0036/es)*,* [*C21/71*](https://www.itu.int/md/S21-CL-C-0071/es)*,* [*C19/117*](https://www.itu.int/md/S19-CL-C-0117/es)*,* [*C19/58*](https://www.itu.int/md/S19-CL-C-0058/es)*,* [*C22/INF/8*](https://www.itu.int/md/S22-CL-INF-0008/es) |

# 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). En esa reunión, 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 definió el proceso para la elaboración del proyecto de Directrices en la Carta Circular ([CL-20/55](https://www.itu.int/md/S20-SG-CIR-0055/es)) y se celebraron dos consultas abiertas para todas las partes interesadas de la CMSI el 23 de abril de 2020 y el 1 de marzo de 2021, con el fin de que formularan observaciones sobre el proyecto de Directrices (consulta abierta) Más de 160 participantes asistieron a esas reuniones y formularon observaciones sección por sección sobre el proyecto de Directrices. Se han publicado 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.

**1.5** Sobre la base de las contribuciones recibidas, la Secretaría elaboró el informe en que se explica la manera en que la UIT utiliza actualmente el marco de la ACG ([Informe de la Secretaría](https://www.itu.int/md/S21-CL-C-0036/es)) y preparó el proyecto de Directrices para la utilización de la ACG ([proyecto de Directrices](https://www.itu.int/md/S21-CL-C-0071/es)), 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. 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 el propósito de esta labor no es abordar cuestiones relacionadas con la revisión de la ACG.

**1.6** Debido a la pandemia de COVID-19, la presentación de estos documentos se pospuso a la CVC de 2021, que tuvo lugar del 8 al 18 de junio de 2021. Tras la CVC de 2021, los Estados Miembros del Consejo tomaron nota del informe de la Secretaría y adoptaron por correspondencia la decisión sobre el proyecto de Directrices en la que se "*encarga a la Secretaría que celebre nuevas consultas con los Estados Miembros del Consejo, teniendo en cuenta de las contribuciones recibidas y los comentarios formulados durante esa reunión. La Secretaría debería presentar el* [*Documento 71*](https://www.itu.int/md/S21-CL-C-0071/es) *revisado para su examen y aprobación en la próxima reunión del Consejo"*.

**1.7** En consecuencia, se llevaron a cabo nuevas consultas con los Estados Miembros del Consejo y, teniendo en cuenta las contribuciones recibidas, se elaboraron dos documentos:

a) un documento de información ([C22/INF/8](https://www.itu.int/md/S22-CL-INF-0008/es)) en el que se exponen los antecedentes, la evolución del entorno y el contexto para la elaboración de este proyecto de Directrices; y

b) este proyecto de Directrices que se expone a continuación y que se ha elaborado para su examen y aprobación por el Consejo en su reunión de 2022.

Para la elaboración de estos documentos 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)).

**1.8** 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 jurídicas. 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

**2** En vista 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 añade complejidad al reto de la ciberseguridad, que requiere un examen detenido desde diversas perspectivas. En este contexto, se exponen a continuación las directrices propuestas para la utilización del Pilar 1 por la UIT en el marco de su mandato:

**a)** La UIT debe seguir esforzándose por facilitar los debates y la colaboración entre las múltiples partes interesadas para hacer frente a los retos relacionados con la ciberseguridad y, en particular, fortalecer su relación con todas las partes interesadas para prestar asistencia a los Estados Miembros en esta materia.

**b)** La UIT debe seguir colaborando con los asociados pertinentes para fomentar la creación y el mantenimiento de recursos relativos a la legislación sobre ciberseguridad y ciberdelincuencia, a fin de ayudar a los Estados Miembros a entender los aspectos jurídicos de la ciberseguridad, [incluidos los marcos internacionales pertinentes [en vigor]], facilitando al mismo tiempo el intercambio de experiencias y conocimientos entre los Estados Miembros y respaldando sus esfuerzos en la elaboración de marcos en esta materia.

**c)** La UIT, en colaboración con todas las partes interesadas pertinentes, debería promover una mejor comprensión de los retos y riesgos jurídicos relacionados con la ciberseguridad que plantean las nuevas tecnologías, y facilitar el intercambio de estudios de casos y buenas prácticas a nivel nacional, regional e internacional.

**d)** La UIT debería seguir fortaleciendo el programa de protección de la infancia en línea, que es una plataforma que permite trabajar con los asociados y las partes interesadas a fin de promover el intercambio de conocimientos, información y actividades (incluidas las relacionadas con las medidas jurídicas) que puedan facilitar y servir de apoyo a las medidas adoptadas por los países en este ámbito fundamental.

# Sección 3. Pilar 2 – Medidas técnicas y de procedimiento

**3** Las Recomendaciones relacionadas con el Pilar 2 del Informe del GEAN de 2008 siguen siendo válidas. Por consiguiente, se proponen las siguientes directrices para el Pilar 2:

**a)** Las Comisiones de Estudio de la UIT deberían centrarse en tecnologías emergentes relacionadas con las telecomunicaciones/TIC a fin de estudiar y proponer directrices de en materia de ciberseguridad y Recomendaciones para general confianza y seguridad en la utilización de esas tecnologías, y recomendar a los Estados Miembros que las apliquen voluntaria y oportunamente.

**b)** Debería crearse un mecanismo que posibilite la cooperación estrecha entre las diversas Comisiones de Estudio del UIT-T en lo que respecta al estudio de cuestiones relacionadas con la ciberseguridad, 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 organizaciones de normalización sobre una base de reciprocidad, para garantizar que se mantenga 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 y colaborar con otras organizaciones de normalización y grupos industriales, alentándolos a que presenten sus normas sobre medidas técnicas y de procedimiento al UIT-T y al UIT-R para su aprobación como Recomendaciones del UIT-T y del UIT-R.

**e)** La UIT debe proseguir sus esfuerzos para la elaboración de recomendaciones sobre medidas técnicas y de procedimiento en materia de ciberseguridad en los ámbitos abarcados por su mandato, incentivando a sus Miembros a intensificar su participación en las actividades de normalización de la UIT y creando asociaciones estratégicas, y las consultas con las universidades y las organizaciones de normalización.

**f)** La UIT debe seguir alentando a sus Miembros a establecer/participar en acuerdos de certificación mutua con miras a la creación de normas de ciberseguridad armonizadas.

# Sección 4. Directrices para la utilización del Pilar 3 – Estructuras organizativas

**4** 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, los países menos adelantados y los pequeños Estados insulares en desarrollo (PEID) en la concepción e implementación de los EIII nacionales y otras unidades/organizaciones técnicas conexas.

**b)** Para evitar la duplicación de esfuerzos, la UIT debe seguir promoviendo una colaboración abierta e inclusiva, así como la coordinación, en el marco de su mandato, entre las diversas organizaciones nacionales, regionales o internacionales que participan en el esfuerzo por establecer estructuras organizativas nacionales sostenibles.

**c)** 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.

**d)** En lo que respecta en particular a las estructuras nacionales y a petición de los Estados Miembros, la UIT debería prestarles ayuda en la elaboración de estrategias de coordinación a escala de todo el gobierno, destinadas a mejorar la aplicación coherente y transversal de los esfuerzos nacionales de ciberseguridad.

**e)** 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. Directrices para la utilización del Pilar 4 – Capacitación

**5** 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, y 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, a los países menos adelantados y a los PEID 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, a los países menos adelantados y a los PEID, en colaboración con los asociados interesados y las comunidades de creación de capacidad, en la elaboración de estrategias, planes y políticas nacionales de ciberseguridad y la capacidad de respuesta en caso de incidente.

 Siga impartiendo capacitación para cerrar la brecha de normalización, incluso mediante la prestación de asistencia técnica a los países que la soliciten.

**d)** Mejore y facilite el intercambio de buenas prácticas de los Estados Miembros a fin de ayudar a los países rezagados en materia de conocimientos sobre la ciberseguridad a mejorar su situación en dicho ámbito y a reducir el déficit de capacidad.

**e)** Siga desarrollando sus actividades de capacitación, teniendo en cuenta la necesidad de nuevas calificaciones para adaptarse a las oportunidades y retos que plantean las tecnologías emergentes en el ámbito de la ciberseguridad. A este respecto, debería fomentarse una mayor colaboración con las instituciones académicas, el sector privado y los Estados Miembros.

**f)** 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 con discapacidad relacionada con la edad.

**g)** Siga desarrollando y fortaleciendo el Índice Mundial de Ciberseguridad (GCI) como herramienta para la capacitación y la sensibilización.

**h)** Siga prestando asistencia a los Estados Miembros con programas de capacitación 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 y de sensibilizar en la materia.

**i)** Siga facilitando la identificación de actividades de investigación relacionadas con la ciberseguridad entre las partes interesadas, especialmente en las nuevas esferas tecnológicas, aprovechando los miembros académicos y del sector privado de la UIT.

**j)** 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 crear confianza en el uso de las TIC y seguir fomentando una cultura de ciberseguridad.

# Sección 6. Directrices para la utilización del Pilar 5 – Cooperación internacional

**6** 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. 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 por la UIT en las esferas comprendidas en su mandato:

**a)** 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 los acontecimientos conexos.

**b)** Sobre la base del proceso de la CMSI, incluidos los procesos relativos a la Línea de Acción C5, y teniendo en cuenta la labor del Panel de Alto Nivel sobre la Cooperación Digital del Secretario General de las Naciones Unidas, la UIT debería apoyar los esfuerzos para reunir a los diferentes actores, por ejemplo, en el Foro de la CMSI y 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 la ciberseguridad, también es necesario que se faciliten debates de mayor alcance entre grupos más amplios, incluidos el sector privado, los organismos de las Naciones Unidas, las instituciones académicas, la sociedad civil y otras partes interesadas, con miras a lograr un entendimiento común [mundial] de la ciberseguridad para mitigar las dificultades conexas. La UIT debería 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 con otros organismos clave del sistema de las Naciones Unidas con objeto de respaldar la labor que realiza la Secretaría de las Naciones Unidas para armonizar y racionalizar sus programas y actividades en materia de ciberseguridad, a fin de prestar servicios más eficaces a la comunidad internacional.

# Sección 7. Directrices generales para el marco de la ACG

**7** 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, disponibles 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)