



# MARCO PARA EL DESARROLLO DE UNA POLÍTICA DE CIBERSEGURIDAD QUE RESPONDA A LAS CUESTIONES DE GÉNERO

NORMATIVAS, REGLAS Y DIRECTRICES

**Marco para el desarrollo de una política de ciberseguridad que responda a las cuestiones de género:**

Normativas, reglas y directrices

Esta publicación fue desarrollada y producida por APC. La autora es la investigadora externa Paz Peña.

Coordinación y edición: Verónica Ferrari y Paula Martins (APC)

Apoyo editorial: Gaurav Jain (APC)

Corrección y revisión: Lori Nordstrom (APC)

Traducción: Clio E. Bugel

Diseño y compaginación: Cathy Chen (APC)

Publicado en 2023 por APC

Reconocimiento 4.0 Internacional (CC BY 4.0)

[https://creativecommons.org/licenses/by/4.0/deed.es\\_ES](https://creativecommons.org/licenses/by/4.0/deed.es_ES)

978-92-95113-62-6

APC-202306-GAPS-R-ES-DIGITAL-352



Esta publicación ha sido desarrollada con el apoyo del gobierno de Reino Unido.



**LA CONVENCIÓN SOBRE LA ELIMINACIÓN  
DE TODAS LAS FORMAS DE  
DISCRIMINACIÓN CONTRA LA MUJER  
(CEDAW)**



**AGENDA MUJERES, PAZ Y SEGURIDAD  
(MPS), TAL COMO SE ESTABLECIÓ EN  
LA RESOLUCIÓN 1325 DEL CONSEJO DE  
SEGURIDAD DE ONU Y LOS PLANES DE  
ACCIÓN NACIONAL DE MPS**



**LA AGENDA 2030 PARA EL  
DESARROLLO SOSTENIBLE  
Y LOS OBJETIVOS DE  
DESARROLLO SOSTENIBLE**



**INICIATIVAS DE LA UNIÓN  
INTERNACIONAL DE  
TELECOMUNICACIONES  
(UIT)**



**LA DECLARACIÓN DE BEIJING Y  
LA PLATAFORMA DE ACCIÓN**



**DOCUMENTOS FINALES DE LA  
CUMBRE MUNDIAL SOBRE LA  
SOCIEDAD DE LA INFORMACIÓN  
(CMSI)**



**INFORMES Y RESOLUCIONES DEL  
CONSEJO DE DERECHOS HUMANOS  
DE NACIONES UNIDAS**



**PROCESOS DE CIBERSEGURIDAD  
DEL SISTEMA DE NACIONES UNIDAS**

# INTRODUCCIÓN

Si bien es notable el enorme progreso que ha habido en cuanto al reconocimiento de que las amenazas y los abusos por cuestiones de género en contextos digitales se pueden abordar desde una perspectiva de derechos humanos, el impacto que tienen la desigualdad de género y las operaciones e incidentes cibernéticos a nivel internacional sobre las mujeres y las niñas sigue siendo una parte poco explorada del discurso en los foros y procesos dedicados a la ciberseguridad.

En este sentido, existen herramientas, agendas y abordajes relevantes a los que pueden recurrir las personas responsables de formular políticas de ciberseguridad cuando se trata de promover la perspectiva de género dentro de la ciberseguridad local, o multilateral. Según Brown y Pytlak, esos instrumentos se pueden utilizar como fuente de información, o para establecer una coherencia política con los compromisos ya asumidos de los Estados con la igualdad de género.<sup>1</sup>

Este trabajo, que forma parte de un marco elaborado por la Asociación para el Progreso de las Comunicaciones (APC) para promover una política de ciberseguridad que incluya las cuestiones de género, presenta una visión general de los instrumentos más relevantes.

1. Brown, D., & Pytlak, A. (2020). *Why Gender Matters in International Cyber Security*. Liga Internacional de las Mujeres por la Paz y la Libertad y Asociación para el Progreso de las Comunicaciones. <https://www.apc.org/en/node/36261>



## LA CONVENCIÓN SOBRE LA ELIMINACIÓN DE TODAS LAS FORMAS DE DISCRIMINACIÓN CONTRA LA MUJER (CEDAW)

La Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW, por su sigla en inglés), adoptada por la Asamblea General de Naciones Unidas en 1971<sup>2</sup>, comienza reconociendo que la discriminación general contra las mujeres viola los principios de igualdad de derechos y respeto de la dignidad humana. Así, se trata del primer instrumento internacional que extiende la responsabilidad del Estado a las acciones cometidas por personas privadas, empresas, instituciones no estatales y organizaciones no gubernamentales. El Artículo 2(e) establece que los Estados tienen la obligación de “Tomar todas las medidas apropiadas para eliminar la discriminación contra la mujer practicada por cualesquiera personas, organizaciones o empresas”.<sup>3</sup>

El Comité para la Eliminación de la Discriminación contra las Mujeres supervisa el cumplimiento de las obligaciones por parte de los Estados miembro de la Convención, que en 2020 ascendían a 189. Los Estados miembro deben presentar un informe cada cuatro años, que luego se analiza en una sesión anual. El Comité puede también dar recomendaciones generales que funcionan como interpretaciones autorizadas de los artículos de la Convención. Brown y Pytlak enumeran diversas formas de incorporar las tecnologías de la información y la comunicación (TIC) en las recomendaciones adoptadas por el Comité en los últimos años.<sup>4</sup> Por ejemplo:

- La recomendación general num. 35 sobre “sobre la violencia por razón de género contra la mujer, por la que se actualiza la recomendación general num.19” incluye, en su interpretación actualizada sobre la violencia de género contra las mujeres “la redefinición de lo público y lo privado a través de entornos tecnológicos, como las formas contemporáneas de violencia que se producen en línea y en otros entornos digitales”.<sup>5</sup>
- La recomendación general num. 36 “sobre el derecho de las niñas y las mujeres a la educación” reconoce que las niñas y las mujeres tienen poca representación “en el uso de conocimientos sobre tecnologías de la información y las comunicaciones (TIC)” y llama a las escuelas a eliminar los obstáculos que impiden el acceso a la información y reducen las oportunidades de empleo en las industrias relevantes.<sup>6</sup>
- A lo anterior, hay que agregarle la más reciente Recomendación general núm. 38 (2020), relativa a “la trata de mujeres y niñas en el contexto de la migración mundial”. La sección E, sobre el “Uso de la tecnología digital en la trata”, destaca que, si bien las tecnologías tienen un impacto positivo en la sociedad, también plantean “nuevos problemas de seguridad a nivel individual y estatal”. “El uso de monedas electrónicas ofrece instrumentos para ocultar información personal, como la identidad de las partes involucradas en la transacción y su ubicación, y permite hacer pagos anónimos, sin siquiera revelar el propósito de la transacción, todo lo cual facilita la trata. Los canales de demanda, a través de los medios sociales, la web oscura y las plataformas de mensajería, proporcionan acceso fácil a las posibles víctimas, lo cual aumenta su vulnerabilidad”.<sup>7</sup>

2. <https://www.un.org/womenwatch/daw/cedaw/text/econvention.htm>

3. Ibid.

4. Brown, D., & Pytlak, A. (2020). Op. cit.

5. CEDAW/C/GC/35. [https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1\\_Global/CEDAW\\_C\\_GC\\_35\\_8267\\_E.pdf](https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf)

6. CEDAW/C/GC/36. [https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1\\_Global/CEDAW\\_C\\_GC\\_36\\_8422\\_E.pdf](https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_36_8422_E.pdf)

7. CEDAW/C/GC/38. <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-recommendation-no38-2020-trafficking-women>

## CEDAW y la Agenda de Mujeres, paz y seguridad (MPS)

Según Myrttinen, la sinergia entre CEDAW y la Resolución 1325 que inaugura la Agenda MPS (que se analiza con mayor profundidad más adelante en este trabajo) se subraya en la recomendación 30 de CEDAW “sobre las mujeres en la prevención de conflictos y en situaciones de conflicto y posteriores a conflictos”, en la que el Comité de CEDAW vincula la implementación de la Resolución a los mecanismos de notificación de CEDAW.<sup>8</sup>



8. Myrttinen, H. (2020). *Herramienta 1: Gobernanza del sector de la seguridad, reforma del sector de seguridad y género*. DCAF, OSCE/ODIHR y ONU Mujeres. <https://www.dcaf.ch/tool-1-security-sector-governance-security-sector-reform-and-gender>



## LA DECLARACIÓN DE BEIJING Y LA PLATAFORMA DE ACCIÓN

La Declaración y la Plataforma de Acción de Beijing<sup>9</sup> fueron adoptadas por los Estados participantes de la Cuarta Conferencia Mundial sobre la Mujer en 1995. Se negoció con bastantes insumos de la sociedad civil y, según la propia ONU Mujeres, se considera “el plan más progresista que jamás ha existido para promover los derechos de la mujer”.<sup>10</sup> La Plataforma de acción está organizada en 12 áreas de particular interés, varias de ellas vinculadas al género y la ciberseguridad aunque no se mencionen directamente.

### Sección E: Las mujeres y los conflictos armados

Esta sección critica el gasto militar excesivo y llama a adoptar una perspectiva de género para dichos gastos. Establece, por ejemplo, que:

- Párrafo 138: “Las personas más afectadas por los conflictos y los gastos militares excesivos son las que viven en la pobreza, que se ven privadas de servicios básicos debido a la falta de inversión en dichos servicios”.
- Párrafo 141: “Al encarar los conflictos armados o de otra índole, debería fomentarse un criterio activo y visible de incorporar en todas las políticas y programas una perspectiva de género, de manera que antes de adoptar una decisión se analicen los efectos sobre la mujer y el hombre respectivamente”.

El objetivo estratégico E.2 delinea varias acciones para reducir los gastos militares excesivos y controlar la disponibilidad de armamento.

### Sección J: La mujer y los medios de comunicación

Esta sección se refiere al papel que tienen los medios de comunicación y difusión en el bienestar de las mujeres, e incluye explícitamente las nuevas tecnologías de información y comunicación. Así, por ejemplo, se reconoce que:

- Párrafo 234: “En el último decenio, los avances en la tecnología de la información han facilitado el desarrollo de una red mundial de comunicaciones que trasciende las fronteras nacionales y que influye en las políticas estatales, las actitudes privadas y el comportamiento, en especial de los niños y adultos jóvenes. Existe en todas partes la posibilidad de que los medios de comunicación contribuyan en mucha mayor medida al adelanto de la mujer”.
- Párrafo 236: Hay que suprimir la proyección constante de imágenes negativas y degradantes de la mujer en los medios de comunicación, sean electrónicos, impresos, visuales o sonoros. Los medios impresos y electrónicos de la mayoría de los países no ofrecen una imagen equilibrada de los diversos estilos de vida de las mujeres y de su aportación a la sociedad en un mundo en evolución”.
- Párrafo 237: “Así pues, es necesario que las mujeres intervengan en la adopción de las decisiones que afectan al desarrollo de las nuevas tecnologías, a fin de participar plenamente en su expansión y en el control de su influencia”.

9. <https://www.un.org/womenwatch/daw/beijing/pdf/BDPfA%20E.pdf>

10. <https://www.unwomen.org/en/digital-library/publications/2015/01/beijing-declaration>

Uno de los objetivos estratégicos de la Sección J trata en particular sobre el vínculo entre género y tecnologías digitales. Se trata del Objetivo estratégico J.1, que llama a incrementar “el acceso de la mujer y su participación en la expresión de sus ideas y la adopción de decisiones en los medios de difusión y por conducto de ellos, así como en las nuevas tecnologías de comunicación”. Las medidas sugeridas a los gobiernos para alcanzar este objetivo que son de interés para la agenda de ciberseguridad son las siguientes:

- Estimular y reconocer las redes de comunicación de mujeres, entre ellas las redes electrónicas y otras nuevas tecnologías aplicadas a la comunicación, como medio para la difusión de información y el intercambio de ideas, incluso en el plano internacional, y brindar apoyo a los grupos de mujeres que participan en todos los ámbitos de los medios de difusión y de los sistemas de comunicación a ese efecto.
- Fomentar la organización de programas de educación y capacitación de las mujeres a fin de que se prepare información destinada a los medios de difusión, incluida la financiación de actividades experimentales y la utilización de nuevas tecnologías aplicadas a la comunicación, la cibernética y la comunicación espacial y por satélite, ya sea en la esfera pública o privada.
- Alentar la utilización de los sistemas de comunicación, incluidas las nuevas tecnologías, como medio de fortalecer la participación de la mujer en los procesos democráticos.

### La Declaración de Beijing y los Objetivos de Desarrollo Sostenible

En 2020, ONU Mujeres publicó un análisis sobre los derechos de las mujeres 25 años después de la Declaración de Beijing y estableció vínculos entre las 12 áreas claves de la Plataforma de Acción de Beijing y los 17 Objetivos de desarrollo sostenible, destacando cuatro catalizadores universales de cambio, entre los cuales destaca el de “Dominar la tecnología para la igualdad de género”. El estudio reconoce el enorme potencial que tienen las nuevas tecnologías para el empoderamiento de las mujeres y las niñas, pero advierte sobre la necesidad de cerrar primero la brecha digital de género, además de eliminar nuevos riesgos tales como la ciberviolencia, las amenazas contra el derecho a la privacidad y los algoritmos que perpetúan prejuicios inconscientes.<sup>11</sup>



11. ONU Mujeres. (2020, 9 de marzo). Declaración de apertura de la Secretaria General Adjunta de Naciones Unidas y Directora Ejecutiva de ONU Mujeres, Phumzile Mlambo-Ngcuka, durante la 64a sesión de la Comisión sobre el estatuto de las mujeres. <https://www.unwomen.org/en/news/stories/2020/3/speech-ed-phumzile-csw64>



## AGENDA MUJERES, PAZ Y SEGURIDAD (MPS), TAL COMO SE ESTABLECIÓ EN LA RESOLUCIÓN 1325 DEL CONSEJO DE SEGURIDAD DE ONU Y LOS PLANES DE ACCIÓN NACIONAL DE MPS

En octubre de 2000, la Resolución 1325 del Consejo de Seguridad de Naciones Unidas creó la Agenda MPS, que se aplica a todos los miembros de ONU. La resolución ya no ve a las mujeres como meras víctimas y afirma que tienen un papel clave en la prevención y resolución de conflictos, el mantenimiento de la paz, la construcción de la paz, la respuesta humanitaria y la reconstrucción nacional posterior a los conflictos, y urge a los Estados a incrementar la participación de las mujeres en todo el trabajo de ONU por la paz y la seguridad, incluyendo la toma de decisiones relativas a la seguridad. La Agenda MPS se basa por ende en el principio de que la integración de la perspectiva de género y los derechos de las mujeres puede tener un impacto importante y positivo en la vida de las mujeres, los hombres, las niñas y los niños.

Dado que la resolución incorpora los principios esenciales de igualdad y no discriminación, refuerza la normativa de derechos humanos establecida por instrumentos internacionales que incluyen, en particular, la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer.

A aquella resolución inicial de 2000, le siguieron otras nueve resoluciones de MPS, y todas juntas forman la base de su agenda. Sin embargo, ninguna de las resoluciones contiene referencias a lo “cibernético”, “en línea”, “tecnología”, “digital”, o “internet”, ni al ciberespacio o la ciberseguridad; y cuando hay alguna referencia indirecta, tiende a enfocarse en dos aspectos: el uso de TIC para fomentar los derechos de las mujeres y la participación política, y el uso de TIC para abusar o perpetrar actos de violencia contra las mujeres.<sup>12</sup>

La Agenda MPS tiene cuatro pilares: participación, protección, prevención (estos tres primeros se conocen como “las tres P”), y alivio y recuperación. Para implementar la Agenda MPS, existen Planes de Acción Nacional y Planes de Acción Regional. Sólo dos Planes nacionales mencionan la ciberamenaza: el Plan de Acción Nacional 2019 de Irlanda, y el de Namibia.<sup>13</sup>

12. Sharland, L., et al. (2021). *System Update: Towards a Women, Peace and Cybersecurity Agenda*. UNIDIR. <https://doi.org/10.37559/GEN/2021/03>

13. Ibid.

## Oportunidades para la Agenda MPS y la ciberseguridad

Según Brown y Pytlak, aún no se ha estudiado bien cómo integrar o impulsar la Agenda MPS, o los Planes de acción nacional, en el debate internacional sobre políticas de ciberseguridad.<sup>14</sup> Sin embargo, debido a la naturaleza jurídicamente vinculante de las resoluciones del Consejo de Seguridad de ONU para todos los Estados miembro, podría servir para informar los esfuerzos a fin de cerrar la brecha digital y ofrecer una mejor protección en línea.

Más específicamente, Sharland et al. proponen que, a fin de cerrar la brecha entre la Agenda MPS y la ciberseguridad, y con el objetivo de actualizar la seguridad internacional al siglo XXI, esta Agenda debe ocuparse de seis desafíos:

### 1. La participación de las mujeres en las negociaciones de ciberseguridad

La Agenda MPS se propone lograr una participación eficiente y significativa de las mujeres en todo el espectro de la seguridad internacional, incluso las negociaciones y la toma de decisiones a nivel internacional sobre asuntos cibernéticos. En este aspecto, uno de los desafíos más identificables consiste en incrementar la participación de las mujeres en la toma de decisiones sobre ciberseguridad a nivel internacional. Más aún, resulta prioritario incorporar activamente la perspectiva de género a las políticas y programas que complementan estos esfuerzos.

### 2. Ciberviolencia contra las mujeres y las niñas

La protección de las mujeres y las niñas contra la ciberviolencia forma parte de la Agenda MPS y debe incluirse en los Planes de acción nacional y Planes de acción regional para implementar la Resolución 1325. Esto implicará que los Estados ajusten su manera de resolver los asuntos que tradicionalmente se enmarcaban como problemas domésticos (por ejemplo, los daños humanos de la ciberviolencia), para incluirlos entre los Planes de acción nacional sobre mujeres, paz y seguridad, en lugar de enfocarse solamente en los peligros de la seguridad exterior.

### 3. Participación de las mujeres en los procesos políticos

La participación de las mujeres en política y en las instituciones del gobierno es clave para fortalecer su representación y amplificar sus voces, con el fin de promover la agenda de las mujeres y las niñas. Sin embargo, el obstáculo para su participación en los procesos políticos es que, mediante el uso de TIC, resulta más fácil intimidarlas y acosarlas.

### 4. Género y radicalización en línea

El uso de internet para difundir ideología y radicalizar a los individuos ha llevado a un aumento exponencial del número de organizaciones extremistas. Sin embargo, en la literatura y los debates estatales casi no se ha explorado la influencia y el impacto que tiene la retórica en línea de la extrema derecha sobre las mujeres y las niñas. Es fundamental entender la atracción que ejercen esas plataformas y conseguir que las mujeres participen en ellas para poder enfrentar algunos de los riesgos que implican para la paz y la seguridad, a fin de prevenir y responder a la radicalización de los individuos a través de esas plataformas.

14. Brown, D., & Pytlak, A. (2020). Op. cit.

## 5. Impactos de género de los ciberincidentes

Se necesita más investigación sobre el impacto, diferenciado según los géneros, de los instrumentos políticos de ciberseguridad (por ejemplo, los apagones de internet), la violación de datos y los ataques contra infraestructura clave. Los Estados también deberían tratar de incorporar una perspectiva de género al desarrollar sus políticas sobre protección de infraestructura clave y ello incluye enmarcar y definir qué es "infraestructura clave" e "infraestructura informática clave", así como la prioridad que se le asigna a los diversos tipos de incidentes.

## 6. Prejuicios de género en las tecnologías digitales

Las investigaciones muestran que el modelo de amenazas, la notificación al/a usuario/a y los procedimientos de control, así como la publicidad sobre tecnologías de ciberseguridad, hacen que sea más probable que se minimice o se omita la importancia de las amenazas a la ciberseguridad de las mujeres. Entre las tantas maneras posibles de enfrentar este problema, se puede garantizar la diversidad en la fuerza de trabajo y los procesos del área de la cibernética y la inteligencia artificial, además de incorporar una perspectiva de género a todas las iniciativas, materiales y programas de capacitación relacionados con la cibernética y la inteligencia artificial.<sup>15</sup>



15. Sharland, L., et al. (2021). Op. cit.



## DOCUMENTOS FINALES DE LA CUMBRE MUNDIAL SOBRE LA SOCIEDAD DE LA INFORMACIÓN (CMSI)

El proceso de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) consistió en dos conferencias, patrocinadas por Naciones Unidas, sobre la información, las comunicaciones y la sociedad de la información. La cumbre se organizó en dos etapas: Ginebra, en 2003, y Túnez en 2005. Uno de los principales objetivos era ayudar a cerrar la brecha digital entre los países industrializados y los países en desarrollo incrementando el acceso a servicios modernos de TIC.

Los párrafos siguientes de la Declaración de Principios de Ginebra (documento final de la primera etapa),<sup>16</sup> que contó con el apoyo de los Estados miembro de ONU y todas las partes interesadas, son de especial interés:

- 12. Afirmamos que el desarrollo de las TIC brinda ingentes oportunidades a las mujeres, las cuales deben ser parte integrante y participantes clave de la Sociedad de la Información. Nos comprometemos a garantizar que la Sociedad de la Información fomente la potenciación de las mujeres y su plena participación, en pie de igualdad, en todas las esferas de la sociedad y en todos los procesos de adopción de decisiones. A dicho efecto, debemos integrar una perspectiva de igualdad de género y utilizar las TIC como un instrumento para conseguir este objetivo.
- 13. Al construir la Sociedad de la Información, prestaremos especial atención a las necesidades especiales de los grupos marginados y vulnerables de la sociedad, en particular los migrantes, las personas internamente desplazadas y los refugiados, los desempleados y las personas desfavorecidas, las minorías y las poblaciones nómadas. Reconoceremos, por otra parte, las necesidades especiales de personas de edad y las personas con discapacidades.

El Compromiso de Túnez (adoptado durante la segunda fase)<sup>17</sup> reconoce la existencia de la brecha de género y reafirma el compromiso de todas las partes interesadas con la promoción de la participación de las mujeres en los procesos de toma de decisiones. Los párrafos que siguen son particularmente relevantes:

- 13. Reconocemos también que la revolución de las TIC puede tener enormes consecuencias positivas como instrumento del desarrollo sostenible. Además, un entorno habilitador apropiado, que exista a escala nacional e internacional, podría impedir el aumento de las divisiones sociales y económicas y de las disparidades entre los países, las regiones y los individuos ricos, y los países, regiones e individuos pobres – incluidas las existentes entre hombres y mujeres.
- 23. Reconocemos la existencia en la sociedad de una brecha entre los géneros que forma parte de la brecha digital, y reafirmamos nuestro compromiso con la promoción de la mujer y con una perspectiva de igualdad de género, a fin de que podamos superar esta brecha. Reconocemos además que la plena participación de las mujeres en la Sociedad de la Información es necesaria para garantizar la integración y el respeto de los derechos humanos dentro de la misma. Animamos a todas las partes interesadas a respaldar la participación de la mujer en los procesos de adopción de decisiones y a contribuir a la conformación de todas las esferas de la Sociedad de la Información a nivel internacional, regional y nacional.

16. WSIS-03/GENEVA/DOC/4-E. <https://www.itu.int/net/wsis/docs/geneva/official/dop.html>

17. WSIS-05/TUNIS/DOC/7-E. <https://www.itu.int/net/wsis/docs2/tunis/off/7.html>

El texto también reconoce que la comunidad internacional debería prestar especial atención a las necesidades particulares de los grupos marginados y vulnerables de la sociedad.

### **Resolución 70/125: Documento final de la reunión de alto nivel de la Asamblea General sobre la revisión general de la implementación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información**

En 2015, cuando se hizo un análisis de la Cumbre Mundial sobre la Sociedad de la Información 10 años después, la Asamblea General de Naciones Unidas adoptó la Resolución 70/125<sup>18</sup> en la que se expresa inquietud por la persistencia de la brecha digital entre hombres y mujeres y se declara: “Alentamos a todas las partes interesadas a que aseguren la plena participación de las mujeres en la sociedad de la información y que tengan acceso a las nuevas tecnologías, especialmente las tecnologías de la información y las comunicaciones para el desarrollo”.

Además, se señala que en el contexto de los singulares desafíos emergentes que presentan las tecnologías en todos los países, se debe prestar “especial atención también a resolver las dificultades específicas que presentan las tecnologías de la información y las comunicaciones para los niños, los jóvenes, las personas con discapacidad, las personas de edad, los pueblos indígenas, los refugiados y los desplazados internos, los migrantes y las comunidades remotas y rurales”.

Específicamente, la resolución exige que se adopten “medidas inmediatas para lograr la igualdad entre los géneros entre los usuarios de Internet para 2020, especialmente mediante la mejora sustancial de la educación de las mujeres y las niñas y su participación en las tecnologías de la información y las comunicaciones, como usuarias, creadoras de contenido, empleadas, empresarias, innovadoras y dirigentes. Reafirmamos nuestro compromiso de asegurar la plena participación de las mujeres en el proceso de adopción de decisiones referentes a las tecnologías de la información y las comunicaciones”.



18. A/RES/70/125. [https://unctad.org/system/files/official-document/ares70d125\\_en.pdf](https://unctad.org/system/files/official-document/ares70d125_en.pdf)



## LA AGENDA 2030 PARA EL DESARROLLO SOSTENIBLE Y LOS OBJETIVOS DE DESARROLLO SOSTENIBLE

La Agenda 2030 para el desarrollo sostenible constituye un marco global e interdependiente sobre desarrollo socioeconómico sostenible, basado en procesos y acuerdos multilaterales previos. Los 17 Objetivos de desarrollo sostenible (ODS) son los principales mecanismos de la Agenda 2030, adoptada el 25 de septiembre de 2015 por la Asamblea General de ONU en la resolución A/RES/70/1: “Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible”.<sup>19</sup>

Interesa en particular el ODS 5, “Lograr la igualdad de género y empoderar a todas las mujeres y las niñas”. Al igual que todos los Objetivos, el ODS 5 contiene un conjunto de metas específicas e indicadores correspondientes, algunos de los cuales son particularmente relevantes para el campo de la ciberseguridad:

- 5.1 5.1 Poner fin a todas las formas de discriminación contra todas las mujeres y las niñas en todo el mundo
- 5.2 Eliminar todas las formas de violencia contra todas las mujeres y las niñas en los ámbitos público y privado, incluidas la trata y la explotación sexual y otros tipos de explotación
- 5.5 Asegurar la participación plena y efectiva de las mujeres y la igualdad de oportunidades de liderazgo a todos los niveles decisorios en la vida política, económica y pública.
- 5.b Mejorar el uso de la tecnología instrumental, en particular la tecnología de la información y las comunicaciones, para promover el empoderamiento de las mujeres.

La Resolución 70/25 (adoptada por la Asamblea General de Naciones Unidas durante el análisis a 10 años de la CMSI, el 16 de diciembre de 2015)<sup>20</sup> establece también que:

Reconocemos que la eliminación de la brecha digital entre los géneros y la consecución del quinto Objetivo de Desarrollo Sostenible sobre la igualdad entre los géneros son actividades que se refuerzan mutuamente, y nos comprometemos a incorporar la perspectiva de género en el proceso de la Cumbre Mundial sobre la Sociedad de la Información, entre otras cosas mediante un énfasis renovado en las cuestiones de género en la aplicación y el seguimiento de las líneas de acción, con el apoyo de las entidades pertinentes de las Naciones Unidas, entre ellas la Entidad de las Naciones Unidas para la Igualdad de Género y el Empoderamiento de las Mujeres (ONU-Mujeres).

Según un informe publicado por New America, aunque la literatura sobre el tema aún está en su etapa inicial, la ciberseguridad tiene un papel fundamental para este objetivo, ya que las desigualdades en esta área exacerban las desigualdades sociales existentes, tales como las que se basan en el género.<sup>21</sup> Además, los recursos en línea para denunciar discriminación y violencia contra las mujeres requieren estrictos controles de privacidad, de lo contrario, se corre el riesgo de aumentar el peligro que corren.

19. A/RES/70/1. [https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A\\_RES\\_70\\_1\\_E.pdf](https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_70_1_E.pdf)

20. A/RES/70/125. [https://unctad.org/system/files/official-document/ares70d125\\_en.pdf](https://unctad.org/system/files/official-document/ares70d125_en.pdf)

21. Morgus, R. (2018). *Securing Digital Dividends. Mainstreaming Cybersecurity in International Development*. New America. <https://www.newamerica.org/cybersecurity-initiative/reports/securing-digital-dividends>

## La interpretación de la Unión Internacional de Telecomunicaciones sobre el quinto ODS

La Unión Internacional de Telecomunicaciones (UIT) ha dedicado un esfuerzo considerable a cerrar las múltiples brechas que experimentan las mujeres en el área de las tecnologías.<sup>22</sup> Sus esfuerzos se centraron en fomentar la participación de las mujeres y las niñas en las carreras de ciencias, tecnología, ingeniería y matemática, y también en integrarse a EQUALS, una innovadora red global que tiene por objetivo generar un cuerpo de evidencia y mejorar el acceso de las mujeres a la tecnología, construir capacidades digitales y otras, y promover el liderazgo de las mujeres en el sector de las tecnologías (APC también forma parte de EQUALS). Por ejemplo, en 2021, UIT organizó la primera edición del Programa de mujeres en cibermentorías, que apunta a construir la capacidad de mujeres jóvenes profesionales que desean entrar, o progresar en el campo de la ciberseguridad.<sup>23</sup>



22. <https://www.itu.int/en/mediacentre/backgrounders/Pages/icts-to-achieve-the-united-nations-sustainable-development-goals.aspx>

23. ITU. (2021). *ITU Contribution to the Implementation of the WSIS Outcomes: 2021*. Draft as of 25/10/2021. [https://www.itu.int/en/itu-wsis/Documents/ITUContribution/2021\\_ITU\\_Contribution\\_to\\_WSIS-Implementation-20211025.pdf](https://www.itu.int/en/itu-wsis/Documents/ITUContribution/2021_ITU_Contribution_to_WSIS-Implementation-20211025.pdf)



## INFORMES Y RESOLUCIONES DEL CONSEJO DE DERECHOS HUMANOS DE NACIONES UNIDAS

### **A/HRC/38/47: Informe de la Relatora Especial sobre violencia contra las mujeres, sus causas y consecuencias sobre la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos**

En 2018, la Relatora Especial de Naciones Unidas sobre violencia contra las mujeres, sus causas y consecuencias, publicó un informe especial sobre la violencia de género en línea<sup>24</sup> que significó un gran avance en cuanto a la definición y el análisis de este fenómeno. El documento formula también una serie de recomendaciones, entre las cuales hay varias relativas a la ciberseguridad, tales como:

- 100. Los Estados deben velar por que se adopten medidas efectivas para impedir la publicación de material nocivo que comprenda la violencia de género contra la mujer, y para que este se suprima con carácter urgente. Los Estados deben aprobar, o adaptar (según proceda) sus causas penales y civiles para que los autores rindan cuentas de sus actos. Estas medidas legislativas deben aplicarse también a las amenazas de publicación en línea de información o contenidos nocivos.
- 105. Los Estados deben proporcionar capacitación a los magistrados, abogados, agentes de policía y otros funcionarios encargados de hacer cumplir la ley y los trabajadores de primera línea a fin de asegurar su capacidad para investigar y enjuiciar a los responsables, y fomentar la confianza del público en la obtención de justicia para los casos de violencia en línea y facilitada por las TIC.
- 107. Los Estados deben ofrecer medidas de protección y servicios para las víctimas de la violencia de género en línea, que incluyan líneas telefónicas de asistencia especializada para prestar apoyo a las personas que han sido objeto de ataques en línea, centros de acogida y órdenes de protección.
- 110. Los Estados deben proporcionar educación, divulgación y capacitación con perspectiva de género a los usuarios de Internet sobre la violencia en línea y facilitada por las TIC contra las mujeres y las niñas en las escuelas y comunidades, como una manera de prevenirla.
- 112. Los Estados deben garantizar el cumplimiento de normas firmes de protección de datos y asegurar la rendición de cuentas de los titulares de los datos en caso de infracciones.
- 113. Los Estados deben proteger y fomentar el desarrollo de la tecnología, en particular de las herramientas de cifrado y anonimato que protegen los derechos y la seguridad de las mujeres en línea.

Las recomendaciones a los intermediarios de internet en relación a la ciberseguridad incluyen los siguientes puntos:

- 118. Los intermediarios deben garantizar la seguridad y la privacidad de los datos, y velar por que la utilización de los datos respete el derecho internacional de los derechos humanos y cuente con el consentimiento plenamente informado de los proveedores de datos.

24. A/HRC/38/47. <https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and>

- 119. Las plataformas de Internet deben comprometerse a erradicar la violencia de género en línea. En tal sentido, deben asignar recursos a las campañas de información y educación sobre la prevención de la violencia facilitada por las TIC contra las mujeres y las niñas, y sobre la promoción de los derechos humanos y la seguridad digital.

### **A/HRC/RES/38/5: Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevenir la violencia contra las mujeres y las niñas en los contextos digitales y responder a ese fenómeno**

En 2018, el Consejo de derechos humanos de Naciones Unidas adoptó una resolución liderada por Canadá que obtuvo el consenso de más de 50 copatrocinadores de todas las regiones. Dicha resolución establece que la violencia de género en línea constituye una violación de derechos humanos "que impide una participación plena, equitativa y efectiva en los asuntos económicos, sociales, culturales y políticos, y es un impedimento para lograr la igualdad de género y el empoderamiento de todas las mujeres y las niñas."<sup>25</sup>

Las acciones recomendadas a los Estados incluyen:

- b) Den prioridad a la integración de las perspectivas de género y aseguren la pronta, plena y eficaz participación de las mujeres y las niñas en la elaboración y aplicación de políticas, leyes, programas, proyectos, estrategias e instrumentos reglamentarios y técnicos nacionales en la esfera de las tecnologías digitales; creen mecanismos de vigilancia y rendición de cuentas para garantizar la aplicación de políticas y reglamentos que tengan en cuenta las cuestiones de género, y analicen las repercusiones de género de esas políticas en consulta y colaboración con mujeres especialistas en tecnología digital, las organizaciones de la sociedad civil y los defensores de la igualdad de género.

La resolución exhorta a los Estados a exigir a los actores privados del área de las tecnologías digitales que adopten una serie de acciones con el fin de acabar con este tipo de violencia, incluyendo la incorporación de una perspectiva de género en el diseño, el desarrollo y la aplicación de las tecnologías.



25. A/HRC/RES/38/5. [https://ap.ohchr.org/documents/dpage\\_e.aspx?si=A/HRC/RES/38/5](https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/38/5)



## INICIATIVAS DE LA UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT)

### **Resolución 70: Incorporación de una perspectiva de género en la UIT y promoción de la igualdad de género y el empoderamiento de la mujer por medio de las telecomunicaciones/ tecnologías de la información y la comunicación**

En la Reunión plenipotenciaria de 2018, los Estados miembro de la UIT adoptaron la Resolución 70, titulada: "Incorporación de una perspectiva de género en la UIT y promoción de la igualdad de género y el empoderamiento de la mujer por medio de las telecomunicaciones/ tecnologías de la información y la comunicación".<sup>26</sup>

Entre otras cosas, la Resolución reconoce que:

- El acceso equitativo a las TIC y la participación en pie de igualdad en todas las áreas, especialmente en política y en la toma de decisiones, benefician a la sociedad en su conjunto.
- Para cerrar la brecha digital de género hay que promover el conocimiento y las capacidades digitales, la educación y la tutoría de mujeres y niñas a fin de promover su participación y liderazgo en la creación, el desarrollo y el despliegue de las telecomunicaciones/TIC.
- Hay que fomentar más la participación de las mujeres y las niñas en el campo de las telecomunicaciones/tecnologías de información y comunicación desde una temprana edad y brindar información para el desarrollo de nuevas políticas.

La resolución incluye una serie de compromisos sobre la adopción de medidas para incorporar una perspectiva de género y promover la igualdad de género dentro de la propia UIT, y compromete a los Estados miembro de la UIT a llevar a cabo una serie de acciones en torno de:

- Empleo, formación y promoción
- Facilitar la capacitación
- Examinar políticas y estrategias
- Atraer a más mujeres adultas y jóvenes a las carreras de ciencias, tecnología, ingeniería y matemática, y reconocer el éxito de las que ya operan en ese campo.

### **El proyecto de directrices para la utilización de la Agenda sobre Ciberseguridad Global por la UIT**

La Agenda sobre Ciberseguridad Global (GCA, por su sigla en inglés)<sup>27</sup>, lanzada en 2007, es un marco de cooperación internacional cuyo objetivo es mejorar la confianza y la seguridad en la sociedad de la información. La GCA fue diseñada con fines de cooperación y eficiencia, y para aumentar la colaboración con todos los socios relevantes, así como entre ellos, de forma de aprovechar las iniciativas existentes para evitar la duplicación de esfuerzos. Se basa en cinco pilares estratégicos: medidas jurídicas, medidas técnicas y procedimentales, estructuras institucionales, capacitación y cooperación internacional. La GCA es la base utilizada por la UIT

26. Resolución 70 (Rev. Dubai, 2018). [https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/Resolutions/RESOLUTION%2070%20\(REV.%20DUBAI,%202018\).pdf](https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/Resolutions/RESOLUTION%2070%20(REV.%20DUBAI,%202018).pdf)

27. <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>

para publicar su Índice de ciberseguridad global (ICG)<sup>28</sup> a fin de arrojar más luz sobre los compromisos de ciberseguridad de los países. Se analiza el nivel de desarrollo, o de compromiso de cada país en base a los cinco pilares de la GCA.

En 2021, UIT publicó las últimas directrices de cómo utiliza el GCA la organización<sup>29</sup> y en marzo de 2022, los Estados miembro del Consejo de UIT aprobaron los documentos para su transmisión a la Conferencia Plenipotenciaria 2022 de UIT. Entre esos documentos se encuentra el "Proyecto de documento de información sobre los lineamientos para la utilización de la Agenda sobre Ciberseguridad Global"<sup>30</sup> en el que se reconoce que muchos/as usuarios/as finales de TIC no comprenden del todo los problemas de ciberseguridad, o no tienen la capacidad o las herramientas necesarias para proteger sus datos, su privacidad y sus bienes. Los/as usuarios/as más vulnerables son las mujeres y los niños y las niñas, que se encuentran particularmente expuestos/as a los riesgos. Por ende, el desafío principal sigue siendo construir la capacidad y las competencias, además de tomar las medidas necesarias para generar una verdadera cultura de ciberseguridad.

Dentro del marco de este análisis, se presentan algunas sugerencias relativas al género dentro de la categoría de la capacitación:

- 5.3 Es importante notar también que, dada la velocidad de los avances en el área de TIC y los problemas de acceso y conectividad ya existentes, los/as usuarios/as finales – y en particular poblaciones tales como las mujeres, los niños y niñas, las personas de edad, las personas con discapacidades y necesidades especiales – pueden ser a menudo más vulnerables a los peligros e incidentes de ciberseguridad. Por lo tanto, los programas de educación en torno a la ciberseguridad son esenciales para reducir los riesgos de ciberseguridad de la sociedad en su conjunto, junto con las acciones de sensibilización sobre las amenazas a la ciberseguridad relevantes para los/as usuarios/as finales vulnerables.
- 5.11 Además, desde una perspectiva global, empoderar a los recursos humanos implica contar con un marco general de educación en ciberseguridad, modular y flexible, a fin de responder a las necesidades de una mayor conciencia pública y brindar programas educativos adaptados para profesionales específicos/as. Se debe prestar especial atención a la brecha de género en esta área. Existe una gran cantidad de capital humano desaprovechado que se puede traer para contribuir al campo de la ciberseguridad, incluso mujeres, que aún representan apenas 20% de la fuerza de trabajo en ciberseguridad.

En el área de la capacitación, en particular, UIT se compromete a prestar especial atención a las necesidades de los grupos más vulnerables tales como las mujeres, los niños y las niñas, las personas de edad, y las personas con discapacidades y necesidades especiales.

## **Guía para la elaboración de una Estrategia nacional de ciberseguridad**

Para poder cosechar los beneficios de la digitalización y asimismo gestionar los desafíos que conlleva, cada país debe enmarcar su transformación digital, así como la proliferación de infraestructura y servicios de TIC, en una Estrategia nacional de ciberseguridad.

Así fue que, para ayudar a los gobiernos en este sentido, un consorcio de organizaciones de los sectores público y privado, la sociedad civil y el mundo académico, facilitado por UIT, desarrollaron y publicaron en forma conjunta una guía para la elaboración de una estrategia nacional de ciberseguridad en 2018.<sup>31</sup> La edición 2021 de la guía<sup>32</sup> actualiza, refina, aclara y amplía la versión original.

28. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>

29. <https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx>

30. <https://www.itu.int/md/S22-CL-INF-0008/en>

31. [https://www.itu.int/pub/D-STR-CYB\\_GUIDE.01](https://www.itu.int/pub/D-STR-CYB_GUIDE.01)

32. <https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf>

Dado que la ciberseguridad afecta a numerosas áreas del desarrollo socioeconómico y se ve influida por diversos factores dentro del contexto nacional, la sección 5 de la edición 2021 de la guía "Buenas prácticas en estrategias nacionales de ciberseguridad" presenta un conjunto de elementos de buena práctica que pueden hacer que la estrategia sea más abarcadora y eficiente, permitiendo a la vez que se realicen adaptaciones para cada contexto nacional.

Si bien se hace referencia a la cuestión de género, vuelve a hacerse dentro del marco de la "capacidad, capacitación y sensibilización". Por ejemplo, en la guía se recomienda:

- La estrategia también debe fomentar iniciativas destinadas a desarrollar trayectorias profesionales dedicadas a la ciberseguridad, en particular para el sector público, e incentivos para aumentar la oferta de profesionales cualificados en materia de ciberseguridad. Estas iniciativas deben crearse en colaboración con el mundo académico, el sector privado y la sociedad civil. Para eliminar la actual brecha de género de especialistas en ciberseguridad, debe considerarse la posibilidad de adoptar un equilibrio de género que motive, aliente y facilite una mayor participación de las mujeres en todas las actividades encaminadas al desarrollo de competencias y formación, garantizando así la inclusión en el futuro.
- La Estrategia debe identificar a los grupos de la sociedad que requieren particular atención en lo que se refiere a capacidad, capacitación y sensibilización en cuanto a ciberseguridad. Entre dichos grupos se incluye a aquéllos que han sido identificados como grupos de riesgo especial, o a los que hay que empoderar para que se protejan, tales como la pequeña y mediana empresa, las organizaciones comunitarias, las comunidades sin servicio y/o los grupos de bajos ingresos





## PROCESOS DE CIBERSEGURIDAD DEL SISTEMA DE NACIONES UNIDAS

En el Primer Comité de la Asamblea General de ONU había dos procesos dedicados a analizar la misma cuestión: el comportamiento responsable de los Estados en el ciberespacio. Tales procesos eran el Grupo de expertos gubernamentales (GEG) y el Grupo de trabajo de composición abierta (OEWG, por su sigla en inglés).

### Grupo de Expertos Gubernamentales (GEG)

La resolución 73/266 de la Asamblea General, “Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional”, adoptada en diciembre de 2018, exhorta a recrear el Grupo de Expertos Gubernamentales (GEG) a fin de seguir estudiando la forma de aplicar el derecho internacional a las acciones del Estado en el ciberespacio, entre otros objetivos.<sup>33</sup> Del mismo modo, entre 2019 y 2021, el GEG siguió trabajando en la promoción de una concepción compartida y la efectiva implementación de posibles medidas de cooperación para enfrentar peligros existentes y potenciales en la esfera de la seguridad informática. Su informe de 2021<sup>34</sup> contiene los hallazgos del Grupo sobre las amenazas existentes y emergentes; las normas, reglas y principios para una conducta responsable por parte de los Estados; el derecho internacional; medidas para generar confianza; y cooperación y asistencia internacional para la seguridad y la capacitación en el área de TIC.

En la sección “Normas, reglas y principios de comportamiento responsable de los Estados”, el GEG establece en la Norma 13 (e) que:

Para garantizar la utilización segura de las TIC, los Estados deben acatar las resoluciones 20/8 y 26/13 del Consejo de Derechos Humanos sobre la promoción, la protección y el disfrute de los derechos humanos en Internet, así como las resoluciones 68/167 y 69/166 de la Asamblea General sobre el derecho a la privacidad en la era digital, a fin de garantizar el pleno respeto de los derechos humanos, incluido el derecho a la libertad de expresión.

La explicación de la norma se refiere específicamente al género como manera de contribuir a la no discriminación:

- 36. Esta norma recuerda a los Estados que deben respetar y proteger los derechos humanos y las libertades fundamentales, tanto en línea como fuera de ella, de acuerdo con sus respectivas obligaciones. A este respecto, requieren especial atención el derecho a la libertad de expresión, incluido el derecho a buscar, recibir y difundir información sin limitación de fronteras y por cualquier medio de expresión, y otras disposiciones pertinentes previstas en el Pacto Internacional de Derechos Civiles y Políticos y el Pacto Internacional de Derechos Económicos, Sociales y Culturales, y contempladas en la Declaración Universal de Derechos Humanos. El cumplimiento de esta norma también puede contribuir a promover la no discriminación y a reducir la brecha digital, en particular en los que respecta al género.

33. Brown, D. (2019, 10 de enero). UN General Assembly adopts record number of resolutions on internet governance and policy: Mixed outcomes for human rights online. APC. <https://www.apc.org/en/node/35253>

34. [https://front.un-arm.org/wp-content/uploads/2021/08/A\\_76\\_135-2104030E-1.pdf](https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf)

- 40. Aunque se reconoce la importancia de la innovación tecnológica para todos los Estados, las tecnologías nuevas y emergentes también pueden tener importantes consecuencias para los derechos humanos y la seguridad de las TIC. Para abordar esta cuestión, los Estados pueden considerar la posibilidad de promover e invertir en medidas técnicas y jurídicas a fin de orientar el desarrollo y el uso de las TIC de una manera más inclusiva y accesible y que no afecte negativamente a los miembros de comunidades o grupos individuales.
- 41. El Grupo observa que en el seno de las Naciones Unidas hay varios foros que se dedican específicamente a cuestiones de derechos humanos. Además, reconoce que diversas partes interesadas contribuyen de distintas maneras a la protección y promoción de los derechos humanos y las libertades fundamentales en línea y fuera de ella. La participación de estas voces en los procesos de elaboración de políticas relacionadas con la seguridad de las TIC puede servir de apoyo a los esfuerzos de promoción, protección y disfrute de los derechos humanos en línea y contribuir a aclarar y minimizar los posibles efectos negativos de las políticas en las personas, incluidas las que se encuentran en situaciones vulnerables.

### **Grupo de trabajo de composición abierta (OEWG, por su sigla en inglés)**

A raíz de la Resolución 73/27 de la Asamblea General de Naciones Unidas, se creó un Grupo de Trabajo de Composición Abierta (OEWG) sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional del que todos los Estados miembro de ONU fueron invitados a participar. El Grupo se reunió por primera vez en 2019 y publicó su informe final en 2021.<sup>35</sup>

En ese informe, el OEWG apreció el alto grado de participación de delegadas mujeres en sus sesiones y la importancia de las perspectivas de género en sus intercambios. Más aún, su introducción destaca la importancia de reducir la “brecha digital de género” y promover una participación y un liderazgo significativos por parte de las mujeres en los procesos de toma de decisiones relativos al uso de TIC en el contexto de la seguridad internacional. Sin embargo, a pesar de ello, las conclusiones y recomendaciones son muy limitadas en lo que se refiere a las consideraciones de género:

- 21. Los Estados concluyeron que cada Estado experimenta las amenazas de manera diferente según su grado de digitalización, sus capacidades, la seguridad y la resiliencia de TIC, la infraestructura y el desarrollo. Las amenazas también tienen un impacto diferente en diferentes grupos y entidades, por ejemplo, las personas jóvenes, las personas de edad, las mujeres y los hombres, las personas vulnerables, algunas profesiones específicas, la pequeña y mediana empresa, y otros/as.
- 56. La capacitación debe respetar los derechos humanos y las libertades fundamentales, ser inclusivas y sensibles a las cuestiones de género, además de universales y no discriminatorias.

35. <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP2.pdf>

## Crítica al documento final del primer OEWG

Aunque el informe final del primer OEWG, en 2021, destaca la participación de las mujeres en los espacios de elaboración de políticas para el ciberespacio y reconoce la importancia de superar la brecha digital de género, “el debate sobre estos asuntos y lo que pueden hacer los Estados en este sentido está casi ausente de las diversas secciones del informe”<sup>36</sup>. Creemos que se podría haber ido más lejos considerando al género como una de las cuestiones claves en los intercambios sobre los peligros del ciberespacio. Junto con otras organizaciones de la sociedad civil, APC sigue involucrada en este proceso y vuelve a llamar la atención en este sentido.



36. Ferrari, V. (2021). Why should gender matter (more) for the OEWG? *Cyber Peace & Security Monitor*, 1(10). <https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.10.pdf>



**APC**

ASOCIACIÓN PARA  
EL PROGRESO DE  
LAS COMUNICACIONES