OEA | CICTE

UNIDIR

Un enfoque novedoso para las 11 normas de la ONU sobre el comportamiento responsable de los Estados en el ciberespacio:

Directrices para una implementación con perspectiva de género

DR. KATHARINE MILLAR • VERÓNICA FERRARI

Un enfoque novedoso para las 11 normas de la ONU sobre el comportamiento responsable de los Estados en el ciberespacio:

Directrices para una implementación con perspectiva de género

Dr. Katharine Millar, Profesora Adjunta de Relaciones Internacionales,
London School of Economics and Political Science

Verónica Ferrari, Coordinadora de Incidencia Política Global,
Asociación para el Progreso de las Comunicaciones (APC)

Contenido

Lista de abreviaturas **09**

Resumen ejecutivo **10**

Introducción **11**

1.

Género, ciberseguridad y las 11 normas de la ONU **13**

1.1 Género, ciberseguridad y normas: definiciones clave 14
1.2 Género y ciberseguridad 17
1.3 Enfoque de género en la gobernanza de la ciberseguridad 19
1.4 Enfoque de género en la gobernanza de la ciberseguridad a nivel regional y nacional 20
1.5 Ciberseguridad y la Agenda de Mujeres, Paz y Seguridad (Agenda MPS) 21

2.

Directrices para la implementación con perspectiva de género de las 11 normas de la ONU para el comportamiento responsable de los Estados en el ciberespacio **22**

Norma a: Cooperación entre Estados 24
Norma b: Toda la información pertinente 25
Norma c: Prevención del uso malicioso de las TIC 26
Norma d: Cooperación para evitar la delincuencia y el terrorismo 28
Norma e: Derechos humanos y privacidad 29
Norma f: Daños a la infraestructura pública 32
Norma g: Protección de infraestructura crítica 33
Norma h: Respuesta a las solicitudes de asistencia 35
Norma i: Seguridad de la cadena de suministro 36
Norma j: Divulgación de las vulnerabilidades relacionadas con las TIC 37
Norma k: Daños a los equipos de respuesta a emergencias 39

3.

Ciberseguridad con perspectiva de género en la práctica: aprendizajes de Canadá, Chile y Costa Rica 43

3.1 Canadá: Integración de la ciberseguridad y la Agenda MPS 44
3.2 Chile: Un enfoque con perspectiva de género en las estrategias nacionales de ciberseguridad 46
3.3 Costa Rica: Adopción de enfoques con perspectiva de género en ciberseguridad tras incidentes cibernéticos de gran alcance 51

4.

Ideas para la acción 53

4.1 Acciones a nivel internacional y regional 54
4.2 Acciones a nivel nacional 55

Referencias 58

Agradecimientos

Esta investigación es una colaboración entre la Sección de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA) y el Programa de Género y Desarme del Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR).

Este proyecto ha recibido el apoyo financiero del Gobierno de Canadá bajo la iniciativa de la OEA/CICTE denominada "Cynder – Cerrando la Brecha de Género en la Agenda de Ciberseguridad de las Américas y el Caribe."

El Programa de Género y Desarme cuenta con el apoyo de los gobiernos de Alemania, Canadá, Irlanda, Malta y Noruega.

Las autoras desean expresar su agradecimiento a las siguientes personas por su retroalimentación y experticia aportados a este informe.

- Kerry-Ann Barrett, CICTE, Organización de los Estados Americanos
- Andrea Gronke, UNIDIR
- Alexis Henshaw, Troy University
- Renata Hessmann Dalaqua, UNIDIR
- Paula Martins, Asociación para el Progreso de las Comunicaciones (APC)
- Dominique Steinbrecher, UNIDIR
- Katya Vera, CICTE, Organización de los Estados Americanos

Las autoras desean expresar su agradecimiento a los equipos del UNIDIR y del CICTE/OEA por su colaboración y apoyo a lo largo de este proyecto de investigación.

Diseño y maquetación:

- María Paula Lozano, CICTE, Organización de los Estados Americanos

Notas

Las designaciones empleadas y la presentación del material en esta publicación no implican la expresión de ninguna opinión de ningún tipo por parte de la Secretaría de las Naciones Unidas o de la Organización de los Estados Americanos con respecto a la condición jurídica de ningún país, territorio, ciudad o área, o con respecto a sus autoridades o en relación con la delimitación de sus fronteras o límites. Los puntos de vista expresados en esta publicación son responsabilidad exclusiva de sus autoras. No reflejan necesariamente los puntos de vista ni las opiniones de las Naciones Unidas, la Organización de los Estados Americanos, el UNIDIR, los miembros de su personal o sus patrocinadores.

Para citar esta obra

Millar, Katharine, y Ferrari, Verónica. (2025). *Un enfoque novedoso de las 11 normas de la ONU para el comportamiento responsable de los Estados en el ciberespacio: directrices para una implementación con perspectiva de género*. Washington, D.C.: Organización de los Estados Americanos; Ginebra: Instituto de las Naciones Unidas de Investigación sobre el Desarme.

Acerca de la Sección de Ciberseguridad de la OEA/CICTE

Con más de 20 años de experiencia, la Sección de Ciberseguridad del CICTE es el líder regional en apoyar a los Estados miembros de la OEA en el fortalecimiento de sus capacidades técnicas y de nivel político en materia de ciberseguridad. Sus iniciativas y actividades tienen por objetivo garantizar un ciberespacio abierto, seguro y resiliente en todo el hemisferio occidental.

En 2022, con el apoyo del Gobierno de Canadá, la Sección de Ciberseguridad lanzó la iniciativa trienal "Cerrando la Brecha de Género en la Agenda de Ciberseguridad de las Américas y el Caribe", también conocida como "Cynder", que promueve investigaciones innovadoras sobre la relación entre ciberseguridad y género, además de otros objetivos clave.

Acerca del Programa de Género y Desarme (UNIDIR)

El Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) es un órgano autónomo dentro de las Naciones Unidas, financiado a través de contribuciones voluntarias. Es uno de los pocos institutos de investigación y análisis de políticas en el mundo que se enfoca en el desarme, genera conocimiento y promueve el diálogo y la acción en materia de desarme y seguridad. Con sede en Ginebra, el UNIDIR ayuda a la comunidad internacional a desarrollar ideas prácticas e innovadoras necesarias para encontrar soluciones a problemas críticos de seguridad.

El Programa de Género y Desarme contribuye a las metas estratégicas de lograr la igualdad de género en los foros sobre desarme y aplicar de manera eficaz las perspectivas de género en los procesos de desarme. Abarca investigaciones originales, actividades de divulgación y herramientas para apoyar a las partes interesadas en el desarme a convertir la concienciación sobre las cuestiones de género en acciones prácticas. El Programa de Género y Desarme cuenta con el apoyo de los gobiernos de Alemania, Canadá, Irlanda, Malta y Noruega.

Acerca de las autoras

Katharine Millar

Katharine M. Millar es Profesora Adjunta de Género y Relaciones Internacionales en el Departamento de Relaciones Internacionales de la *London School of Economics and Political Science* (LSE). Sus investigaciones abarcan la relación entre género, política y violencia. Ha publicado trabajos sobre mujeres combatientes, género y muertes violentas, masculinidad militar y civil, así como militarismo. Actualmente, sus proyectos examinan el género y la ciberseguridad y la historia política del desarme. Participa activamente en procesos de política relacionados con el género y las fuerzas armadas, la formación militar profesional, y el género y la ciberseguridad.

Verónica Ferrari

Verónica Ferrari es la coordinadora de incidencia política global en la Asociación para el Progreso de las Comunicaciones (APC, por sus siglas en inglés – *Association for Progressive Communications*). En este cargo, coordina la participación de la organización y sus miembros en foros de políticas globales, incluyendo el Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre las Tecnologías de la Información y las Comunicaciones, y el Examen Periódico Universal del Consejo de Derechos Humanos de las Naciones Unidas. Verónica también se desempeña como representante de la APC y copresidenta de la Red Asesora de la *Freedom Online Coalition*. Antes de unirse a la APC, Verónica trabajó como asesora principal de políticas en la Secretaría de Modernización del Gobierno de Argentina, contribuyó con su trabajo al Berkman Klein Center de la Universidad de Harvard y al Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE). Además, ha trabajado como consultora, colaborando con diversas organizaciones de derechos digitales en América Latina. Su enfoque profesional se centra en políticas digitales, ciberseguridad y género, e inclusión digital.

Lista de abreviaturas

CBM	Medida de Fomento de la Confianza
CDH	Consejo de Derechos Humanos de las Naciones Unidas
CEDAW	Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer
CERT	Equipo de Respuesta ante Emergencias Informáticas
CICTE	Comité Interamericano contra el Terrorismo
CIRT	Equipo de Respuesta a Incidentes Cibernéticos
CSIRT	Equipo de Respuesta a Incidentes de Seguridad Informática
MPS	Mujeres, Paz y Seguridad (Agenda MPS)
OEA	Organización de los Estados Americanos
OEWG	Grupo de Trabajo de Composición Abierta
PAN	Plan de Acción Nacional (de Canadá) sobre las Mujeres, la Paz y la Seguridad 2023–2029
PNC	Política Nacional de Ciberseguridad
TIC	Tecnologías de la Información y las Comunicaciones
UN	Organización de las Naciones Unidas
UN GGE	Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional
UNIDIR	Instituto de las Naciones Unidas de Investigación sobre el Desarme
VGFT	Violencia de género facilitada por la tecnología

Resumen ejecutivo

La ciberseguridad tiene implicaciones importantes para la igualdad de género. Los incidentes de ciberseguridad afectan de manera diferenciada a personas de distintos géneros. Por ejemplo, las filtraciones de datos, las campañas de desinformación, los discursos de odio y las interrupciones del acceso a Internet repercuten de manera desproporcionada en las mujeres, así como en las personas con orientaciones sexuales, identidades y expresiones de género diversas.

Además, la falta de atención a las cuestiones de género reduce la eficacia de la ciberseguridad. Introduce vulnerabilidades no detectadas en los sistemas técnicos y en las respuestas políticas ante las amenazas cibernéticas. La subrepresentación de las mujeres y de las personas con orientaciones sexuales, identidades y expresiones de género diversas en los roles técnicos y de formulación de políticas en materia de ciberseguridad impide que el sector se beneficie de la innovación, la creatividad y la riqueza que aportan los equipos diversos.

Las 11 normas de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio tienen por objetivo regular la conducta de los Estados en cuestiones relacionadas con el ciberespacio en sus interacciones con otros Estados. Estas normas no abordan explícitamente las cuestiones de género. No obstante, la implementación de dichas normas es un proceso continuo y dinámico que evoluciona en paralelo con el desarrollo de las capacidades cibernéticas de los Estados.

Basándose en la Agenda de Mujeres, Paz y Seguridad (Agenda MPS), este informe sirve de orientación a responsables de la formulación de políticas y a profesionales del sector sobre cómo integrar la perspectiva de género en las políticas y prácticas de ciberseguridad, a través de un enfoque novedoso y centrado en las personas para la interpretación e implementación de las 11 normas de las Naciones Unidas. El enfoque consta de dos componentes:

- Una interpretación de las normas teniendo en cuenta la perspectiva de género, que identifique de qué manera pueden estar relacionadas con desigualdades entre personas de distintos géneros, y que ofrezca sugerencias para su mitigación.
- Recomendaciones para que la implementación de las normas responda a cuestiones de género, a través de acciones específicas orientadas a promover la igualdad de género.

Las recomendaciones están dirigidas a las entidades que trabajan a nivel internacional, regional y nacional en todos los ámbitos cubiertos por las normas de las Naciones Unidas. Los estudios de caso de Canadá, Chile y Costa Rica ilustran buenas prácticas en materia de ciberseguridad que responden a cuestiones de género y destacan lecciones que pueden aplicarse a nivel mundial.

El informe hace hincapié en la necesidad de:

- Cerrar la brecha digital de género en lo que respecta al acceso, la alfabetización digital y el desarrollo de competencias.
- Incorporar de manera transversal la perspectiva de género en las estrategias nacionales de ciberseguridad, en la cooperación internacional y en las iniciativas de desarrollo de capacidades en ciberseguridad.
- Integrar las políticas nacionales sobre Mujeres, Paz y Seguridad en las estrategias nacionales de ciberseguridad.
- Recopilar datos desglosados por género y otras dimensiones de desigualdad sobre la experiencia de las personas en el ciberespacio.
- Incluir a aquellas partes interesadas que se centran en cuestiones de género en la gobernanza de la ciberseguridad y promover la importancia de realizar consultas con múltiples partes interesadas, en particular, las organizaciones de la sociedad civil.
- Elaborar planes de emergencia y de respuesta a incidentes cibernéticos que respondan a cuestiones de género.

El marco que se propone contribuirá a que los Estados y otras entidades del sector de la ciberseguridad refuercen la seguridad y la estabilidad del ciberespacio internacional, al tiempo que promueven la igualdad de género.

Introducción

La ciberseguridad tiene implicaciones importantes para la igualdad de género. Los incidentes de ciberseguridad afectan de manera diferenciada a personas de distintos géneros.[1] las filtraciones de datos, las campañas de desinformación, los discursos de odio y las interrupciones del acceso a Internet, entre otros incidentes, afectan de manera desproporcionada a las mujeres y a personas con orientaciones sexuales, identidades y expresiones de género diversas.[2] Las nociones tradicionales de seguridad no tienen en cuenta las necesidades, capacidades y vulnerabilidades en material de seguridad de las mujeres, las personas con orientaciones sexuales, identidades y expresiones de género diversas, ni de los miembros de grupos marginados, y no abordan los impactos específicos por razón de género que generan las fallas en ciberseguridad.

La falta de atención a las cuestiones de género reduce la eficacia de la ciberseguridad. Introduce vulnerabilidades no detectadas en los sistemas técnicos y en las respuestas políticas ante las amenazas cibernéticas. La subrepresentación de las mujeres y de las personas con orientaciones sexuales, identidades y expresiones de género diversas en los roles técnicos y de formulación de políticas en materia de ciberseguridad impide que las organizaciones del sector se beneficien plenamente del talento, las capacidades y los conocimientos de una parte importante de la población, así como de la innovación, la creatividad y la riqueza que aportan los equipos diversos.

Los Estados han reconocido esta realidad. Ambos procesos multilaterales, bajo los auspicios de la Primera Comisión de la Asamblea General de las Naciones Unidas que se centran en la ciberseguridad internacional y en el comportamiento responsable de los Estados en el ciberespacio, han abordado cuestiones de género. En su informe de 2019–2021, el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional (UN GGE, por sus siglas en inglés) destacó la importancia de las 11 normas de las Naciones Unidas sobre el comportamiento responsable en el ciberespacio en relación con los derechos humanos, con un énfasis especial en cerrar la brecha digital de género.[3]
En su informe sustantivo final, el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional 2019–2021 (OEWG 2019-2021) acogió con beneplácito la incorporación de perspectivas de género en sus deliberaciones, subrayó la importancia de reducir la brecha digital de género y destacó la necesidad de promover la participación y el liderazgo efectivos y significativos de las mujeres en los procesos de toma de decisiones relacionados con el uso de las tecnologías de la información y las comunicaciones (TIC) en el contexto de la seguridad internacional[4]. En el mismo informe, el OEWG 2019-2021 también adoptó principios de desarrollo de capacidades que establecen que este fortalecimiento de las capacidades cibernéticas sea sensible al género, inclusivo y no discriminatorio.

El Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso 2021–2025 (OEWG 2021–2025), en sus informes anuales de progreso, continuó visibilizando las dimensiones de género en la seguridad vinculada al uso de las TIC[5] y subrayó la necesidad de incorporar una perspectiva de género para abordar las amenazas relacionadas con estas tecnologías. Asimismo, instó a promover un desarrollo de capacidades que responda a cuestiones de género. Durante las deliberaciones del Grupo, varias delegaciones también promovieron la integración de una perspectiva de género en las políticas nacionales sobre las TIC y en el desarrollo de capacidades, así como la elaboración de listas de verificación o cuestionarios para identificar las necesidades y brechas pertinentes.[6]

El género también ha ganado protagonismo en la cooperación en materia de ciberseguridad en los ámbitos regional y nacional. Por ejemplo, la Organización de los Estados Americanos (OEA), a través de su Sección de Ciberseguridad, ha priorizado las cuestiones de género en la gobernanza de la ciberseguridad,[7] y los Estados miembros de la OEA han acordado una medida de fomento de la confianza específica sobre cuestiones de género como parte de la cooperación regional en

el ciberespacio.[8] En algunos países de América Latina como Argentina, Chile, Costa Rica y Ecuador, las consideraciones de igualdad de género han sido incluidas en las estrategias nacionales de ciberseguridad.[9]

A pesar de estos avances y del interés manifestado por los Estados en incorporar consideraciones de género en la práctica y la gobernanza de la ciberseguridad, no existe una orientación práctica sobre cómo interpretar e implementar las 11 normas de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio que respalde la igualdad de género. El presente informe aborda esta carencia proporcionando un enfoque novedoso y centrado en las personas que integra la perspectiva de género en la aplicación de las 11 normas de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio.

El enfoque propuesto consta de dos componentes. En primer lugar, ofrece una interpretación con perspectiva de género de las 11 normas de las Naciones Unidas. Identifica formas de interpretar dichas normas con el fin de reducir las desigualdades entre hombres, mujeres y personas con orientaciones sexuales, identidades y expresiones de género diversas. En segundo lugar, busca dotar a quienes se encargan de la formulación de políticas y a quienes implementan acciones en el ámbito de la ciberseguridad de herramientas que les permitan aplicar las normas de manera que respondan a cuestiones de género y contribuyan a promover la igualdad de género.

Desde el punto de vista metodológico, el informe se basa en una combinación de investigación documental, entrevistas a personas expertas[10] y aportes de un grupo focal de múltiples partes interesadas. La interpretación con perspectiva de género de las 11 normas de las Naciones Unidas se fundamenta en un examen bibliográfico exhaustivo de las políticas e investigaciones académicas existentes sobre la relación entre la igualdad de género, la seguridad y el ciberespacio. Desde un enfoque empírico, la interpretación con perspectiva de género de las normas se ilustra mediante ejemplos y prácticas de política extraídas de las Américas. Este análisis se nutre de entrevistas con personas expertas en cuestiones de género, diplomáticas y diplomáticos especializados en ciberseguridad, representantes de entidades nacionales de ciberseguridad y especialistas en ciberseguridad de organizaciones internacionales y de la sociedad civil.

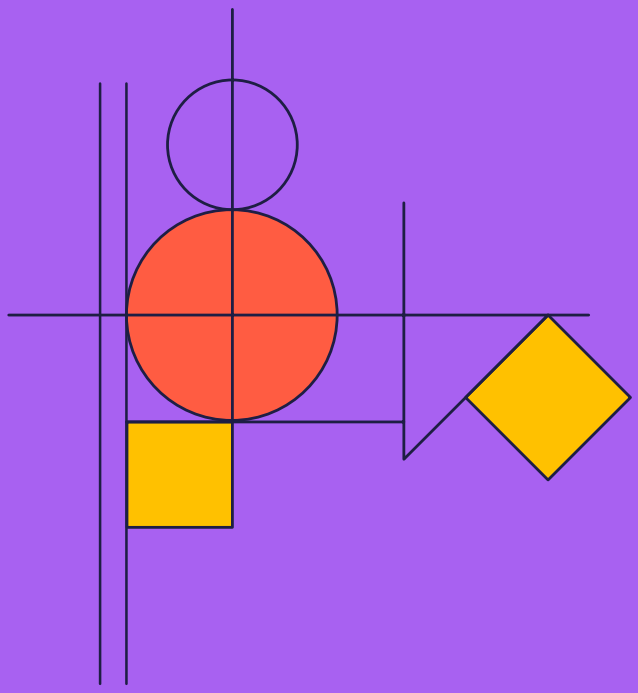
El informe comienza por definir los conceptos clave. A continuación, explica la relevancia del género en la ciberseguridad, con especial atención al marco de la Agenda de Mujeres, la Paz y la Seguridad (MPS). Posteriormente, presenta un análisis de las 11 normas de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio. Seguidamente, destaca buenas prácticas para una implementación que responda a cuestiones de género, a través de estudios de caso procedentes de las Américas — Canadá, Chile y Costa Rica —, extrayendo enseñanzas que pueden aplicarse ampliamente, más allá de la región. El informe concluye con propuestas de acción a nivel internacional, regional y nacional.

Una interpretación de las normas de las Naciones Unidas con perspectiva de género fortalece su implementación y, en consecuencia, la seguridad y la estabilidad del ciberespacio internacional. Garantiza que tanto las y los responsables políticos como profesionales de la ciberseguridad puedan abordar una amplia gama de posibles amenazas, daños y vulnerabilidades en el ciberespacio, y que se protejan los derechos humanos, las necesidades y el bienestar de las personas y las comunidades, tanto en línea como fuera de línea.

1. Género, ciberseguridad y las 11 normas de la ONU

Esta sección introduce los conceptos clave utilizados en el análisis de la relación entre género, ciberseguridad y las 11 normas de las Naciones Unidas. A continuación, expone cómo se ha abordado la cuestión de género en los debates sobre la gobernanza de la ciberseguridad y examina la Agenda MPS como marco de referencia para analizar estas interrelaciones.

1.1 Género, ciberseguridad y normas: Definiciones clave

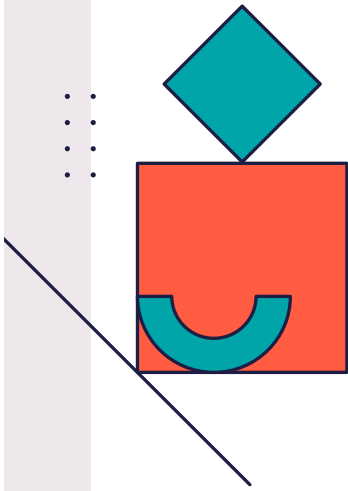


Las **11 normas de Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio,** acordadas por el Grupo de Expertos Gubernamentales de la ONU y respaldadas por la Asamblea General en 2015,[11] y posteriormente desarrolladas en los procesos multilaterales sobre el uso estatal de las TIC, establecen un consenso internacional sobre el comportamiento apropiado de los Estados en el ciberespacio. Las once normas representan un componente central de la cooperación estatal para promover y mantener la estabilidad y seguridad en el ciberespacio. Estas "proporcionan una base común para que un Estado diseñe una orientación estratégica, desarrolle capacidades y ejecute acciones de manera responsable".[12]

La ciberseguridad se entiende habitualmente desde dos perspectivas principales: (a) la técnica —cuando se refiere a garantizar la confidencialidad, integridad y disponibilidad de las redes, sistemas, datos y dispositivos de TIC—; o (b) de seguridad nacional —cuando abarca los ámbitos de defensa nacional, inteligencia y protección de la infraestructura crítica.[13]

Los enfoques centrados en las personas amplían las definiciones habituales de la ciberseguridad para situar al individuo y a las comunidades en el centro de las preocupaciones en materia de ciberseguridad. La ciberseguridad centrada en las personas considera no sólo aspectos técnicos relacionados con el diseño y la respuesta a incidentes, sino también el contexto social, económico y jurídico en el que se inserta su aplicación. Incluye aspectos relacionados con los derechos humanos, tanto en línea como fuera de línea (como la privacidad y la libertad de expresión),[14] así como la seguridad y el bienestar individual (incluidas las protecciones frente al odio y el acoso en línea).[15]

El enfoque de género aplicado a las 11 normas de las Naciones Unidas que se desarrolla en el presente informe abarca las tres concepciones de la ciberseguridad y se basa directamente en el enfoque centrado en las personas. Su objetivo es fomentar que los proyectos, las medidas y las políticas reconozcan las cuestiones de género y de exclusión, y, por tanto, promuevan la igualdad de género. La ciberseguridad eficaz, la igualdad de género y los derechos humanos se refuerzan mutuamente.



Género[16] se refiere a "los roles, comportamientos y atributos que cada sociedad y cultura considera apropiados para los hombres y las mujeres, construidos social y culturalmente, en un tiempo y lugar determinados. Las Normas de género son cambiantes a lo largo del tiempo; configuran las identidades individuales, las relaciones sociales y la distribución de los recursos y el poder en la sociedad. Aunque a menudo el género se entiende socialmente como expectativas acerca del comportamiento considerado apropiado para hombres y mujeres, el género no es binario y es diverso. Se refiere a personas de todas las identidades y expresiones de género".[17]

La orientación sexual se entiende como "los sentimientos o atracción romántica, emocional o física de una persona hacia personas del mismo, distinto o más de un sexo".[18] La atracción heterosexual hacia personas de un género diferente es a menudo una expectativa social fundamental de los roles de género asignados a hombres y mujeres. En consecuencia, las personas lesbianas, gays, bisexuales, pansexuales y queer —de todas las identidades y expresiones de género— pueden experimentar discriminación, estigmatización y violencia tanto por su orientación sexual como por su identidad de género.[19] Si bien el género y la orientación sexual son conceptos distintos, es fundamental tener en cuenta la sexualidad cuando se aborda la igualdad de género.

LGBTQI+: "Es una sigla que significa personas lesbianas, gays, bisexuales, transgénero, intersexuales, queer y otras personas con orientaciones sexuales, identidades y expresiones de género y características sexuales que no se ajustan a las normas sociales tradicionales."[20]

La igualdad de género hace referencia al principio según el cual "las mujeres y los hombres, las niñas y los niños [y las personas con orientaciones sexuales, identidades y expresiones de género diversas] deben tener las mismas condiciones, el mismo trato y las mismas oportunidades para desarrollar plenamente su potencial, sus derechos humanos y su dignidad, así como para contribuir al desarrollo económico, social, cultural y político (y beneficiarse de él)".[21]

La desigualdad de género es cada vez más reconocida como **interseccional**, es decir, vinculada a otras dinámicas de posible marginación y opresión,[22] tales como la raza, la etnia, la clase social, la casta, la edad, la discapacidad, el nivel educativo, el entorno rural o urbano, la nacionalidad y la condición de pertenencia a pueblos indígenas.[23]

La igualdad de género está consagrada en la Carta de las Naciones Unidas y en la Declaración Universal de Derechos Humanos, y ha sido reafirmada en la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW 1979); la Declaración y Plataforma de Acción de Beijing (1995); la Agenda de Mujeres, Paz y Seguridad (Agenda MPS); los Objetivos de Desarrollo Sostenible de la Agenda 2030; así como en instrumentos regionales como la Carta de la Organización de los Estados Americanos (1948), la Declaración Americana de los Derechos y Deberes del Hombre (1948), la Convención Americana sobre Derechos Humanos (1969) y la Convención de Belém do Pará (1994).[24]

La formulación de políticas teniendo en cuenta la perspectiva de género evalúa las políticas en función de sus posibles impactos diferenciados en mujeres, hombres, niñas, niños y personas con orientaciones sexuales, identidades y expresiones de género diversas. Su objetivo es identificar y mitigar cualquier consecuencia negativa relacionada con el género y la desigualdad de género.[25]

La formulación de políticas que respondan a cuestiones de género va más allá de meramente abordar desigualdades en políticas específicas; implica diseñar políticas que contribuyan activamente al avance de la igualdad de género. Este enfoque se considera cada vez más una buena práctica internacional.[26] Dado que la desigualdad de género es interseccional y no un asunto aislado, este informe aborda el género junto con otros patrones históricos o contextuales de marginación interseccional, cuando corresponda, incluyendo sus posibles implicaciones para comunidades minoritarias.

La transversalización de la perspectiva de género es "el proceso de evaluar las implicaciones para las mujeres y los hombres [y para las personas con orientaciones sexuales, identidades y expresiones de género diversas] de cualquier acción planificada, incluyendo la legislación, las políticas o los programas, en todas las áreas y en todos los niveles. Es una estrategia para lograr que las preocupaciones y experiencias tanto de las mujeres como de los hombres [y de las personas con orientaciones sexuales, identidades y expresiones de género diversas] constituyan una dimensión integral en el diseño, la implementación, el seguimiento y la evaluación de las políticas y los programas en todas las esferas políticas, económicas y sociales[27] [...] de modo que las mujeres y los hombres [y las personas con orientaciones sexuales, identidades y expresiones de género diversas] se beneficien en igualdad de condiciones y no se perpetúen las desigualdades".[28]

1.2 Género y ciberseguridad

El género influye en la interpretación y la implementación de las 11 normas de las Naciones Unidas, ya que contribuye a mejorar la seguridad de todas las partes interesadas: organizaciones intergubernamentales, sector privado, Estados, comunidades e individuos. Las **concepciones de ciberseguridad sin perspectiva de género**, que presuponen que las personas de todos los géneros experimentan las amenazas cibernéticas de la misma manera, pueden, de forma involuntaria, socavar la eficacia de la ciberseguridad. Las prácticas de ciberseguridad que no incorporan la perspectiva de género introducen sesgos en los procesos técnicos, generan vulnerabilidades tanto sociales como técnicas,[29] y no reconocen los impactos diferenciados por razones de género que generan las amenazas y los fallos de ciberseguridad.[30] Para que todas las personas puedan ejercer plenamente sus derechos humanos, es indispensable que tengan acceso a un entorno digital seguro, accesible, asequible y libre de violencia.[31] Para ello, es esencial garantizar la protección frente a los daños relacionados con el ciberespacio para personas con orientaciones sexuales, identidades y expresiones de género diversas.

Al igual que ocurre en el ámbito de la seguridad convencional, las mujeres, las niñas, los hombres, los niños y las personas con orientaciones sexuales, identidades y expresiones de género diversas tienen capacidades, necesidades, experiencias y vulnerabilidades diferenciadas en relación con el ciberespacio.[32] El género se relaciona con la ciberseguridad de tres maneras complementarias:

Suposiciones y valores de género en la política y la práctica de la ciberseguridad:
La forma común de entender la ciberseguridad y de tomar decisiones al respecto incorpora creencias, supuestos y valores vinculados al género. Estas suposiciones se encuentran en todos los ámbitos de la práctica de la ciberseguridad, desde los sesgos en el diseño tecnológico hasta en las culturas laborales. No obstante, el supuesto más relevante —y compartido con la seguridad convencional— es que los y las responsables políticos/as y las personas que trabajan en seguridad tienden a priorizar las actividades e instituciones asociadas a los hombres y la masculinidad, como la defensa nacional, el Estado, el comercio y las empresas.

Las concepciones de seguridad que ignoran la perspectiva de género tienden a asumir que las actividades e instituciones vinculadas a hombres y a la masculinidad se experimentan de manera similar o universal por todas las personas.[33] Esto dificulta identificar y priorizar las actividades, instituciones e ideas de seguridad que son más relevantes para mujeres, niñas, hombres, niños y personas con orientaciones sexuales, identidades y expresiones de género diversas.[34] Las definiciones convencionales de ciberseguridad —centradas en sistemas, dispositivos y redes, o en la capacidad cibernética estatal— no contemplan las necesidades, vulnerabilidades, daños y derechos humanos de individuos y comunidades, en especial los de las mujeres y los miembros de grupos marginados y minoritarios.[35]

Efectos diferenciados por razón de género de las amenazas y fallos de ciberseguridad:
Las mujeres, las niñas, los hombres, los niños y las personas con orientaciones sexuales, identidades y expresiones de género diversas experimentan las amenazas cibernéticas de maneras distintas y, en ocasiones, desproporcionadas. Este impacto se agrava significativamente cuando también pertenecen a otros grupos marginados. Se identifican dos categorías de ciberdaños diferenciados por género.[36]

- **Amenazas directamente relacionadas con el género:** Son amenazas cibernéticas dirigidas específicamente en función de la orientación sexual y/o la identidad y expresión de género. Estas amenazas incluyen, de manera destacada, la violencia de género facilitada por la tecnología, como la difusión no consensuada de imágenes íntimas, el acoso y el discurso de odio en línea, y el uso de las TIC para perpetrar violencia doméstica y violencia en relaciones de pareja.[37] Si bien estos daños pueden ser experimentados por personas de todos los géneros, diversas investigaciones han demostrado que las mujeres y las personas con orientaciones sexuales, identidades y expresiones de género diversas que enfrentan múltiples formas de

marginación interseccional sufren niveles más elevados de acoso y discurso de odio en línea.[38] Por otro lado, un estudio reciente sugiere que los hombres y las personas con orientaciones sexuales, identidades y expresiones de género diversas pueden enfrentar con mayor frecuencia casos de chantaje sexual relacionado con imágenes (anteriormente denominado "sextorsión"), a menudo en relación con el estigma social asociado a la homosexualidad.[39]

• **Amenazas indirectamente relacionadas con el género:** Las amenazas cibernéticas dirigidas a un objetivo amplio (como Estados, empresas o comunidades en su conjunto) pueden tener efectos diferenciados por género. Por ejemplo, las filtraciones de bases de datos médicas afectan a personas de todos los géneros, pero pueden generar estigma, discriminación o violencia especialmente hacia las mujeres, las personas con orientaciones sexuales, identidades y expresiones de género diversas, y quienes pueden quedar embarazadas si se filtraran datos sobre su estado reproductivo o historial médico.[40] Los cortes de Internet, que suelen ser utilizados por los gobiernos como herramienta de control sobre las poblaciones bajo su jurisdicción, y también como táctica en situaciones de conflicto contra otras poblaciones, han demostrado producir efectos desproporcionados en función del género y otras interseccionalidades de las personas afectadas. Ejemplos de estos efectos incluyen impactos en la seguridad personal de las mujeres, en su desarrollo profesional y económico, en su bienestar emocional, en su educación y en su conectividad.[41]

■ **Participación con perspectiva de género en la práctica y gobernanza de la ciberseguridad:** La gobernanza y la práctica de la ciberseguridad se caracterizan por una brecha de género. A nivel mundial, el 65 % de las mujeres frente al 70 % de los hombres tienen acceso a Internet, lo que equivale a 244 millones menos de mujeres conectadas que de hombres.[42] Esta desigualdad se conoce como la "brecha digital de género".[43]

Las competencias digitales necesarias para utilizar Internet de manera significativa y segura[44] presentan una brecha de género aún mayor: a nivel mundial, hay solo 65 mujeres jóvenes con competencias digitales por cada 100 hombres jóvenes.[45] Además, las mujeres están subrepresentadas tanto en funciones técnicas como en los espacios de formulación de políticas en materia de ciberseguridad. Las mujeres constituyen aproximadamente el 25 % de la fuerza laboral mundial en ciberseguridad y cerca del 30 % del cuerpo diplomático que participa en la formulación de políticas internacionales sobre ciberseguridad[46] —aunque se están logrando avances importantes hacia la paridad de género. Por ejemplo, la participación significativa de las mujeres en el OEWG 2021-2025 aumentó de aproximadamente un 37 % en 2021 a más del 50 % en 2025; este es el porcentaje más alto de participación femenina registrado en un proceso multilateral centrado en la seguridad internacional.[47]

Figura 1: Género y ciberseguridad

1.3 Enfoque de género en la gobernanza de la ciberseguridad

Desde una perspectiva política, una interpretación con perspectiva de género de las 11 normas de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio se fundamenta en importantes avances en la ciberdiplomacia que sitúan el género en el centro de la gobernanza y la práctica de la ciberseguridad. Como se señala en el informe final del Grupo de Expertos Gubernamentales (GGE) 2019--2021, dichas normas son relevantes para los derechos humanos, con especial énfasis en promover la no discriminación y cerrar la brecha digital de género.[48]

Tanto el GGE como el OEWG 2019-2021 en su informe sustantivo final, subrayaron la importancia del equilibrio de género y la necesidad de fomentar la participación eficaz y significativa de mujeres en los procesos de toma de decisiones sobre el uso de las TIC en el contexto de la seguridad internacional. El informe del OEWG 2019-2021 también destacó la prominencia de una perspectiva de género en sus discusiones y la urgencia de reducir la brecha digital de género. Reconoció además que las amenazas cibernéticas pueden tener impactos diferenciados [49]

El OEWG 2021--2025 continúa enfatizando la necesidad de una perspectiva de género a la hora de abordar las amenazas relacionadas con las TIC, e insta a promover los esfuerzos de creación de capacidad en ciberseguridad que respondan a las cuestiones de género, mediante la integración de una perspectiva de género en las políticas nacionales de TIC y de creación de capacidad, así como mediante la elaboración de listas de comprobación o cuestionarios para determinar las necesidades y lagunas en ese ámbito.[50]

Durante ambos OEWG, diversas delegaciones solicitaron la aplicación de una perspectiva de género a la ciberseguridad.[51] Entre las propuestas específicas presentadas se incluyen:[52]

- Transversalización de la perspectiva de género en la implementación de las 11 normas de las Naciones Unidas
- Creación de capacidades en materia de ciberseguridad que responda a cuestiones de género[53]
- Cierre de la brecha digital de género
- Investigación sobre las experiencias diferenciadas por razones de género en relación con incidentes cibernéticos de gran magnitud y amenazas cibernéticas
- Colaboración inclusiva con las partes interesadas para comprender el contexto más amplio de un incidente relacionado con las TIC, incluyendo su impacto en los derechos de las mujeres

Varios de estos aspectos también fueron destacados por algunos Estados y partes interesadas durante las negociaciones sobre un futuro mecanismo permanente de las Naciones Unidas en materia de ciberseguridad.[54]

1.4 Enfoque de género en la gobernanza de la ciberseguridad a nivel regional y nacional

Las organizaciones regionales pueden desempeñar un papel único y fundamental al apoyar a sus Estados miembros en la implementación de las normas para fortalecer la estabilidad y la seguridad regionales.[55] La OEA ha realizado importantes aportes a mecanismos eficaces de cooperación regional para reforzar la capacidad de la región frente a los incidentes cibernéticos. La Sección de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) ha priorizado la perspectiva de género en la gobernanza de la ciberseguridad a través del proyecto "Cerrando la brecha de género en la agenda de ciberseguridad de las Américas y el Caribe".[56] El Grupo de Trabajo de la OEA sobre Cooperación y Medidas de Fomento de la Confianza en el Ciberespacio[57] se ha centrado en el desarrollo de medidas de fomento de la confianza (CBMs, por sus siglas en inglés) para fortalecer la seguridad y mejorar la capacidad de respuesta frente a incidentes cibernéticos. Este esfuerzo llevó a que, en 2022, los Estados miembros de la OEA adoptaran nuevas medidas regionales de fomento a la confianza Agenda MPS.[58]

En este contexto de creciente conciencia, tanto a nivel multilateral como regional, sobre la importancia de integrar la perspectiva de género en la ciberseguridad, muchas estrategias nacionales de ciberseguridad (documentos clave de política pública que desempeñan un papel central en la implementación de las 11 normas de las Naciones Unidas a nivel nacional[59]) han comenzado, de manera progresiva, a incluir consideraciones de género. Sin embargo, a 2023, de los 114 Estados que contaban con una estrategia nacional de ciberseguridad, solo 14 hacían referencia a las mujeres o al género, y generalmente lo hacían en el contexto de la participación de las mujeres en el sector tecnológico.[60]

1.5 Ciberseguridad y la Agenda de Mujeres, Paz y Seguridad (Agenda MPS)

La Agenda de Mujeres, Paz y Seguridad refleja un consenso internacional que reconoce que el conflicto y la seguridad no son neutrales al género, sino que afectan de forma distinta y desproporcionada a las mujeres y niñas. La Resolución 1325 del Consejo de Seguridad de las Naciones Unidas (S/RES/1325, 2000),[61] que inició la Agenda MPS en octubre de 2000, genera obligaciones para los Estados de apoyar los derechos de participación de las mujeres y las niñas en la resolución de conflictos y la gobernanza de la seguridad; prevenir conflictos y violaciones de sus derechos humanos; y proteger los derechos, la dignidad y el bienestar de las mujeres y niñas, incluyendo frente a la violencia por razón de género y particularmente la violación y otras formas de abusos sexuales.

La Agenda MPS reafirma que la igualdad de género es esencial para abordar el conflicto y garantizar la seguridad. Las resoluciones posteriores del Consejo de Seguridad vinculadas a la Agenda MPS y el marco Normaativo internacional asociado han establecido la importancia y la eficacia de integrar la perspectiva de género en todos los aspectos del conflicto y de la gobernanza de la seguridad. La integración de la Agenda MPS en la gobernanza y las políticas de ciberseguridad, aunque relativamente reciente, se está expandiendo rápidamente.[62] Algunas delegaciones estatales ante el OEWG han subrayado la necesidad de fortalecer los esfuerzos estatales existentes para promover la igualdad de género en el marco de la diplomacia y la gobernanza cibernéticas mediante una conexión más estrecha con la Agenda MPS.[63]

Desde 2021, ONU Mujeres Asia y el Pacífico lleva a cabo un proyecto regional titulado "Mujeres, Paz y Ciberseguridad: Promoviendo la participación de las mujeres en la ciberseguridad", que proporciona un marco accesible que vincula la ciberseguridad con el marco Normaativo y los objetivos políticos existentes de la Agenda MPS.[64] Este proyecto de ONU Mujeres incluye formación y capacitación sensible al género en varias áreas de la ciberseguridad y derechos digitales; apoyo a la alfabetización y el acceso digitales; investigación que responde a cuestiones de género y consultas con múltiples partes interesadas sobre derechos digitales y seguridad; y la armonización de Normaativas regionales y nacionales sobre conflicto, igualdad de género, seguridad nacional y ciberseguridad. Asimismo, el Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) ha elaborado informes de alto nivel que describen cómo fortalecer la igualdad de género en ciberseguridad mediante su integración con la Agenda MPS.[65]

La extensión de la Agenda MPS hacia la ciberseguridad y los derechos digitales cuenta también con el respaldo de la sociedad civil y el mundo académico.[66] Por ejemplo, ICT4Peace, una organización de la sociedad civil que utiliza las TIC para abordar el conflicto y promover la paz, ha realizado un mapeo exhaustivo sobre la relación actual entre ciberseguridad y la Agenda MPS, proporcionando un marco integral para entender el vínculo entre género y amenazas cibernéticas en escenarios afectados por la guerra.[67]

Integrar los aportes de la Agenda MPS en la gobernanza de la ciberseguridad proporciona herramientas útiles para aplicar una perspectiva de género a las 11 normas de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio. Las amenazas cibernéticas y las prácticas de ciberseguridad afectan de manera distinta a las personas según su género, y todas, sin importar identidad de género, expresión u orientación sexual, tienen derecho a participar no solo como usuarias online sino también como profesionales y referentes en el ámbito de la ciberseguridad y la formulación de políticas. Dada la relevancia de estas normas en la gobernanza internacional de la ciberseguridad, adoptar una perspectiva de género en su implementación no solo es esencial para abordar los daños de género asociados, sino que también representa una poderosa oportunidad para promover la igualdad de género y fortalecer la ciberseguridad internacional.

2.

Directrices para la implementación con perspectiva de género de las 11 normas de la ONU para el comportamiento responsable de los Estados en el ciberespacio

Esta sección se basa en el análisis sobre igualdad de género, seguridad y ciberespacio presentado en la Sección 1, con el fin de ofrecer una interpretación con enfoque de género de las 11 normas de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio, así como orientaciones para una implementación que responda a cuestiones de género.[68]

Por tanto, esta sección aborda dos preguntas interrelacionadas:

- ¿Cuáles son las implicaciones de las normas de las Naciones Unidas sobre el comportamiento responsable de los Estados en el ciberespacio para la igualdad de género?

- ¿Cómo pueden interpretarse e implementarse dichas normas empleando un enfoque de género?

Las 11 normas fueron concebidas inicialmente para regular el comportamiento de los Estados en relación con otros Estados y no abordan explícitamente las cuestiones de género. Sin embargo, su implementación constituye un proceso dinámico y en constante evolución que avanza en paralelo con el desarrollo de las capacidades cibernéticas de los Estados. Por ejemplo, los análisis feministas de la jurisprudencia internacional han destacado que los marcos normativos existentes y el derecho internacional, como el derecho internacional humanitario, aun cuando no incorporaron de manera explícita el enfoque de género en su formulación original, pueden interpretarse desde una perspectiva sensible al género para promover la igualdad de género y los derechos humanos.[69] El informe de 2021 del Grupo de Expertos Gubernamentales de las Naciones Unidas apoya este planteamiento, indicando que el cumplimiento de la Norma e —que exige el respeto de los derechos humanos— puede contribuir a promover la no discriminación y a cerrar la brecha digital de género.[70]

Este informe se basa en los principios de interpretación dinámica y evolutiva para ofrecer orientación sobre una interpretación con perspectiva de género de las 11 normas. La interpretación con perspectiva de género, en este contexto, implica evaluar el impacto de las normas sobre personas de distintos géneros e identificar formas de mitigar efectos diferenciales. El informe propone ideas que responden a cuestiones de género y preguntas orientadoras para su aplicación. La implementación con enfoque de género de las normas hace referencia, aquí, a acciones y políticas que contribuyen positivamente a la igualdad de género.

Para facilitar la lectura, las normas se presentan de manera secuencial. Esta estructura está alineada con la lista de comprobación establecida por el presidente del OEWG de 2024 para la implementación voluntaria, práctica y ejecutable de las normas,[71] de modo que las propuestas de acción de este informe puedan integrarse fácilmente con enfoques y recursos ya existentes.[72]

Norma a: Cooperación entre Estados

Norma a: *"Los Estados, en consonancia con los propósitos de las Naciones Unidas, incluido el mantenimiento de la paz y la seguridad internacionales, deberían colaborar en la elaboración y aplicación de medidas para incrementar la estabilidad y la seguridad en el uso de las TIC, y evitar las prácticas en la esfera de las TIC que se considera que son perjudiciales o que pueden poner en peligro la paz y la seguridad internacionales.."*

Las interpretaciones existentes de la *Norma a* se han centrado principalmente en la cooperación entre Estados para promover la paz y la seguridad internacionales.[73] No obstante, al implementar las 11 normas, el concepto de paz y seguridad internacional puede ampliarse para incorporar un enfoque de género sensible y centrado en las personas, alineado con los principios de la Agenda MPS. Esta ampliación permitiría que las normas de las Naciones Unidas se apliquen más allá de los contextos tradicionales de defensa y seguridad nacional, atendiendo también las distintas necesidades, capacidades y vulnerabilidades de las mujeres, las niñas, los hombres, los niños y las personas con orientaciones sexuales, identidades y expresiones de género diversas en materia de ciberseguridad. Esta interpretación sensible al género de la seguridad podría incluir también la evaluación de prácticas estatales destinadas a prevenir el uso nocivo de las TIC desde una perspectiva de género. Sin este enfoque, las medidas diseñadas para reforzar la seguridad estatal —como restricciones al cifrado o cortes de Internet [74] — podrían sin pretenderlo limitar la libertad de expresión, la defensa de los derechos humanos, y el acceso de poblaciones marginadas a información relacionada con la seguridad y al apoyo social en línea, generando experiencias de inseguridad diferenciadas según el género.

La implementación con enfoque de género de esta norma podría incluir, con el objetivo de aumentar la estabilidad y la seguridad en el uso de las TIC, la transversalización de la perspectiva de género en la práctica y la gobernanza de la ciberseguridad a nivel internacional, regional y nacional. Este proceso podría contar con el apoyo de consultas incluyentes de múltiples partes interesadas, con especial énfasis en organizaciones de mujeres, personas LGBTQI+, y organizaciones defensoras de los derechos humanos y digitales.

Las buenas prácticas actuales en materia de transversalización de género siguen un enfoque de doble vía: por un lado, la igualdad de género se define como un objetivo específico de gobernanza o práctica; por otro, el enfoque de género se incorpora transversalmente en todos los documentos e instrumentos normativos relevantes.[75] A nivel internacional, los Estados podrían considerar la inclusión de la ciberseguridad y las TIC en los debates de la Agenda MPS en el Consejo de Seguridad de las Naciones Unidas. Del mismo modo, las negociaciones diplomáticas internacionales sobre ciberseguridad y TIC podrían integrar referencias a dicha Agenda. Asimismo, los Estados también pueden promover un enfoque de género en la implementación de las 11 normas mediante la defensa activa y el respaldo a la inclusión de la perspectiva de género en los procesos diplomáticos internacionales de ciberseguridad, tanto en foros multilaterales como en foros regionales y técnicos de múltiples partes interesadas. Además, los Estados podrían fomentar la paridad de género en todos los niveles jerárquicos dentro de sus equipos de diplomacia cibernética y de formulación de políticas nacionales en materia de ciberseguridad.

A nivel nacional, los Estados podrían incorporar una perspectiva de género en los documentos estratégicos y de política de ciberseguridad de más alto nivel.[76] Esta incorporación podría complementarse mediante la inclusión paralela de consideraciones sobre ciberseguridad y las TIC en los planes de acción nacionales existentes relativos a la Agenda MPS.

Algunas de las propuestas de acción recogidas en el presente informe también podrían integrarse en la lista de comprobación para la implementación de las normas voluntarias y no vinculantes del comportamiento responsable de los Estados en el uso de las TIC.

La transversalización de género en las políticas y estrategias nacionales de ciberseguridad debería

revisarse periódicamente para evaluar su eficacia. Para ello, las consultas multisectoriales, con la participación de la sociedad civil y el ámbito académico, podrían contribuir al seguimiento y evaluación de estas políticas. La transversalización de género en las políticas nacionales de ciberseguridad también podría fortalecerse mediante la formación en materia de género dirigida a personas diplomáticas y responsables de políticas cibernéticas, así como mediante la capacitación técnica y el desarrollo de capacidades en materia de ciberseguridad orientados a especialistas y responsables de la implementación de la Agenda MPS.

Preguntas orientadoras

- ¿Qué definiciones de seguridad internacional se utilizan comúnmente y cómo pueden tener en cuenta las diversas necesidades, capacidades y vulnerabilidades en materia de seguridad de personas de distintos géneros?

- ¿Hasta qué punto se prioriza la igualdad de género en los procesos y foros internacionales de diplomacia cibernética?

- ¿Cómo se manifiestan los esfuerzos hacia la paridad de género en los equipos de diplomacia cibernética y de defensa de la ciberseguridad?

Norma b: Toda la información pertinente

Norma b: *"En el caso de incidentes relacionados con las TIC, los Estados deberían tener en cuenta toda la información pertinente, incluido el contexto más amplio en el que se haya producido el hecho, los problemas que plantea la atribución en el entorno de estas tecnologías, así como la naturaleza y el alcance de las consecuencias."*

Una interpretación con perspectiva de género de la *Norma b* podría implicar ampliar las definiciones de: **i)** "toda la información pertinente" relacionada con un incidente de TIC; **ii)** el "contexto más amplio en el que se ha producido el hecho"; y **iii)** la "naturaleza y el alcance de las consecuencias", para incluir datos relativos a las experiencias diferenciadas por género en el ámbito de la ciberseguridad.

Las personas de distintos géneros experimentan los incidentes de TIC de forma diferente. Por ejemplo, se ha documentado que las interrupciones en los servicios de salud y cuidados sociales, así como en la educación, provocadas por incidentes cibernéticos, generan una carga adicional de cuidado y trabajo doméstico en los hogares, generalmente asumida por las mujeres, lo que agrava la desigualdad de género y dificulta su capacidad para ejercer una actividad remunerada.[77] Asimismo, los apagones de Internet, por ejemplo, afectan la capacidad de acceso a teléfonos móviles, una herramienta clave de seguridad personal utilizada por las mujeres en espacios públicos.[78] Investigaciones sobre los efectos de los cortes de energía eléctrica en países con ingresos bajos y medios sugieren que las interrupciones prolongadas pueden obligar a los hospitales a priorizar ciertos cuidados y reducir los partos hospitalarios.[79] Actualmente, sin embargo, muchos procesos de prevención, preparación y respuesta ante incidentes cibernéticos no tienen en cuenta las cuestiones de género, por lo que existen escasos datos sistémicos sobre cómo las personas con orientaciones sexuales, identidades y expresiones de género diversas, y/o los miembros de grupos marginados y minoritarios, viven estos incidentes.

La implementación con enfoque de género de la *Norma b* podría abordar esta laguna de conocimiento en "toda la información pertinente" mediante la recolección de datos desagregados por género e igualdad sobre los efectos de incidentes cibernéticos, yendo más allá de las cuestiones relevantes sobre atribución.[80] Respetando los estándares más rigurosos de privacidad y protección de datos, los Estados podrían colaborar con todos los actores involucrados —incluidas organizaciones civiles de mujeres, LGBTQI+ y de derechos digitales— para recopilar datos y comprender el contexto completo de los incidentes de TIC, así como sus impactos diferenciados por género y otras desigualdades interseccionales. [81]

Para ello, los Estados podrían recurrir a los conocimientos existentes de la academia y la sociedad civil que ofrecen una taxonomía de los ciber-daños[82] y desarrollar una metodología amplia y estandarizada para su seguimiento.[83] Una taxonomía y metodología compartidas que consideren los efectos de los incidentes cibernéticos desde una perspectiva interseccional permitirían compartir los datos recabados a nivel regional e internacional, e impulsar un aprendizaje comparativo más amplio sobre los impactos diferenciados por género de estos incidentes, promoviendo la generación conjunta de buenas prácticas.

Preguntas orientadoras:

- ¿Qué procesos existen para recopilar datos desagregados por género y otras dimensiones de igualdad sobre los efectos de los incidentes cibernéticos? ¿Cómo pueden estos procesos garantizar al mismo tiempo la protección de la privacidad y de los datos personales?

- ¿Cómo se estructura el seguimiento de los datos de género interseccional a lo largo del tiempo, y en qué medida estos datos informan la toma de decisiones frente a incidentes cibernéticos y la planificación de respuestas de emergencia?

Norma c: Prevención del uso malicioso de las TIC

Norma c: *"Los Estados no deberían permitir deliberadamente que su territorio fuera utilizado para la comisión de hechos internacionalmente ilícitos mediante la utilización de las TIC."*

Esta norma refleja la expectativa de que los Estados no deberían permitir, a sabiendas, que su territorio sea utilizado para la comisión de "actos contrarios a los derechos de otros Estados", incluso a través del uso de las TIC.[84] Una interpretación sensible al género de la Norma c constaría de dos componentes.

En primer lugar, esta interpretación puede tener en cuenta los efectos de género de los actos cibernéticos "contrarios a los derechos de los Estados". Por ejemplo,[85] la injerencia coercitiva en procesos electorales —que puede constituir una violación del principio de no intervención— frecuentemente incluye un componente de género.[86] En un informe de 2023, la Relatora Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y expresión concluyó que la desinformación con sesgo de género constituye una amenaza al derecho a la libertad de expresión y participación pública de mujeres y personas con orientaciones sexuales, identidades y expresiones de género diversas.[87]

La interferencia electoral incluye cada vez más el uso de desinformación con sesgo de género, que busca socavar "los derechos humanos, la igualdad de género, el desarrollo sostenible y la democracia".[88] Se ha demostrado que la prevalencia de este tipo de desinformación disuade a las mujeres de postularse a cargos públicos, y que las mujeres racializadas o pertenecientes a grupos marginados por razones contextuales enfrentan mayores niveles de abuso electoral en línea y desinformación por razones de género que otros candidatos.[89]

La desinformación de género —como la difusión de imágenes sexualizadas falsas para desacreditar a mujeres políticas o el uso de estereotipos sexualizados para fomentar la polarización política— se emplea para engañar a la opinión pública, generar división y manipular resultados electorales.[90] Por lo tanto, este tipo de desinformación puede ser parte de una injerencia en los procesos de gobernanza soberana de los Estados, afectando tanto los derechos humanos como los derechos de los Estados. En el ejercicio de la debida diligencia para abordar actos contrarios a los derechos de otros Estados, los Estados podrían, por lo tanto, atender también a los componentes y efectos de género de dichos actos. Dichas medidas podrían incluir, por ejemplo, la incorporación de la perspectiva de género en los marcos (normativos, de política y de cooperación) nacionales destinados a combatir actividades maliciosas mediante las TIC que se desarrollen dentro de su territorio en contra de los derechos de otros Estados.[91] Asimismo, los Estados podrían incluir los efectos de género del uso malicioso de las TIC al momento de notificar a los Estados afectados sobre actos que se originen en su jurisdicción.

El segundo componente de una interpretación con perspectiva de género de la Norma c sería ampliar la definición de "actos contrarios a los derechos de otros Estados" para incluir aquellos actos maliciosos con TIC que tienen impactos significativos en individuos, grupos y comunidades, y que pueden afectar la capacidad de los Estados para proteger a las personas bajo su jurisdicción. En otras palabras, los Estados podrían adoptar un enfoque centrado en las personas respecto al uso potencialmente nocivo de las TIC, en línea con la visión centrada en las personas y con perspectiva de género de la paz y la seguridad internacionales que promueve la Agenda MPS. Como parte del ejercicio de la debida diligencia , los Estados podrían adoptar medidas para prevenir y abordar la violencia de género facilitada por las tecnologías (VGFT) dentro de su territorio, ya que dicho uso transnacional ilícito de las TIC puede afectar el derecho —y la capacidad— de otros Estados para proteger a individuos bajo sus propias jurisdicciones. Ello puede tener el efecto secundario de fortalecer las medidas para abordar la VGFT para proteger asimismo a las personas dentro de la jurisdicción de un Estado.

La implementación con enfoque de género de la *Norma c* podría, por consiguiente, incluir la incorporación de la perspectiva de género en el ejercicio de la debida diligencia por parte de los Estados frente al uso indebido de las TIC en su territorio. Desde una perspectiva práctica, esta norma suele implementarse mediante la investigación y recopilación de datos verificables sobre el uso indebido de las TIC en la jurisdicción de un estado.[92] La implementación con enfoque de género de la Norma c podría incluir la actualización de los marcos jurídicos y de las políticas públicas para abordar el uso indebido transnacional de las TIC centrado en las personas, incluidos los distintos tipos de VGFT, tales como el acoso en línea, la suplantación de identidad, los discursos de odio, la desinformación con sesgo de género, el hackeo, el acecho digital, la recopilación y divulgación pública de información personal o privada de una persona sin su consentimiento[93] Las medidas podrían incluir el fortalecimiento de las capacidades investigativas del sistema de justicia desde un enfoque de género, la recopilación de datos desagregados por género y la colaboración con el sector privado para abordar y prevenir la VGFT.

La implementación con enfoque de género de la *Norma c* también debería asegurar que las medidas adoptadas por los Estados para abordar el uso de su territorio para cometer actos contrarios a los derechos de otros Estados —y al potencial uso malicioso transnacional centrado en las personas de las TIC— sean proporcionales, apropiadas, eficaces y compatibles con el derecho internacional y nacional. Es decir, que respeten los derechos humanos y adopten un enfoque sensible al género. Los Estados deben garantizar que sus marcos jurídicos protejan adecuadamente la libertad de expresión, la privacidad y el derecho a una vida libre de violencia para personas de todos los géneros, evitando una excesiva dependencia en las respuestas penales.

En el contexto de la VGFT, los Estados podrían desarrollar marcos legales y medidas no legales para enfrentar el uso malicioso de las TIC. Esto puede incluir el fortalecimiento de capacidades de investigación que respondan a cuestiones de género para todos los actores del sistema de justicia, la recopilación de datos sobre género y ciberdelitos, y la colaboración con el sector privado para prevenir y mitigar la VGFT. Al abordar este tipo de violencia, los Estados también deberían procurar que la criminalización e investigación de la VGFT. [94]

Preguntas orientadoras:

- ¿Las definiciones existentes de actos ilícitos relacionados con las TIC o de "actos contrarios a los derechos de otros Estados", así como las medidas conexas, incorporan una perspectiva de género?

- ¿Puede ampliarse la debida diligencia actualmente aplicada para abordar actos maliciosos relacionados con las TIC dentro del Estado y contrarios a los derechos de otros Estados, a fin de integrar una comprensión centrada en las personas y sensible al género sobre el uso indebido de las TIC?

- ¿Qué medidas existen para prevenir, investigar y sancionar la violencia de género facilitada por las tecnologías?

- ¿En qué medida el personal pertinente, incluidos los cuerpos de seguridad, el sistema judicial y otros actores clave, recibe formación en materia de género y cuenta con recursos adecuados para una implementación de esta norma que sea inclusiva desde un enfoque interseccional y eficaz?

Norma d: Cooperación para evitar la delincuencia y el terrorismo

Norma d: *"Los Estados deberían estudiar cuál es la mejor manera de cooperar para intercambiar información, prestarse asistencia mutua, entablar acciones penales por el uso de las TIC con fines terroristas o delictivos y aplicar otras medidas de cooperación para hacer frente a tales amenazas. Quizás los Estados deberían considerar si existe la necesidad de elaborar nuevas medidas a este respecto."*

Una interpretación con perspectiva de género de la *Norma d* reconocería que las personas de distintos géneros experimentan de manera diferente tanto el uso ilícito de las TIC como las respuestas estatales a tales actos. Por ejemplo, aunque personas de todos los géneros pueden sufrir la distribución no consentida de imágenes íntimas, la investigación indica que esta práctica afecta de forma desproporcionada a mujeres, niñas y personas con identidades de género diversas,[95] y que quienes las cometen suelen ser hombres.[96] Aunque aún escasean los datos empíricos sobre las imágenes íntimas sintéticas no consentidas o el abuso de imágenes sexualizadas (cada vez más creadas y difundidas con el uso de IA generativa), los estudios iniciales sugieren que sus efectos de género son similares a otras formas de abuso basado en imágenes.[97]

Asimismo, varios estudios empíricos indican que la exposición a contenido extremista en línea puede radicalizar a personas de todos los géneros,[98] siendo los hombres y niños los que particularmente corren mayor riesgo.[99] La interacción con la radicalización en línea hace que las personas sean vulnerables a sufrir daños infligidos directamente por organizaciones extremistas, a cometer actos de violencia contra otras personas o a exponerse a la violencia a través del contacto con las fuerzas del orden estatales.[100] Una interpretación con perspectiva de género de la Norma d debería contemplar tanto los ciber-daños directos con componentes de género como el rol de normas y dinámicas de género en el uso ilícito general de las TIC. También debería enfatizar la importancia de la prevención proactiva del delito –como la alfabetización digital inclusiva y la sensibilización en materia de género– junto con la cooperación en materia de investigación y respuestas a incidentes.

Dado que la cooperación estatal frecuentemente se canaliza a través de sistemas nacionales de justicia y fuerzas de seguridad, la implementación con perspectiva de género de la Norma d podría incorporar una auditoría de género a las leyes, políticas y procedimientos existentes para prevenir, investigar y enjuiciar la ciberdelincuencia y el terrorismo, incluyendo el apoyo a las víctimas. Los Estados podrían entonces modificar estos marcos a fin de que respondan mejor a las necesidades de género, así como formular nuevas políticas y directrices para su implementación de ser necesario. Junto con la sociedad civil y el sector privado, los Estados podrían incorporar la perspectiva de género en los programas de prevención de la delincuencia (especialmente aquellos dirigidos a los hombres jóvenes) y desarrollar alternativas a las respuestas judiciales tradicionales y al encarcelamiento en casos de radicalización basada en la red.

Una implementación con enfoque de género de la Norma d también reconocería que las respuestas estatales a la ciberdelincuencia, al terrorismo y a las solicitudes de cooperación entre estados tienen un impacto sobre la igualdad de género. Por ejemplo, cuando las fuerzas de seguridad solicitan acceso a todos los datos personales de las víctimas de VGFT, existe el riesgo de violar su privacidad, estigmatizar su historial y revictimizarlas durante la investigación del caso.[101] Por ende, los Estados podrían desarrollar capacitación interseccional en materia de género dirigida a todo el personal involucrado (investigadores, abogadas/os, personas encargadas de la cooperación entre Estados y del intercambio de información, etc.) con el fin de evitar daños adicionales a las víctimas de VGFT.

Los Estados también podrían promover y proteger cifrados de alta seguridad y, además, abstenerse de imponer restricciones sobre su uso a través de medidas tales como las prohibiciones, la criminalización o la imposición de normas de cifrado mínimas.[102] La tecnología de cifrado es fundamental para ejercer una amplia gama de derechos humanos relacionados

con la disidencia, la expresión, la asociación y la privacidad.[103] Las restricciones a su uso relacionadas con la seguridad tienen graves consecuencias para las personas con orientaciones sexuales, identidades y expresiones de género diversas, que necesitan comunicaciones cifradas para su privacidad, discreción y seguridad personal, sobre todo en contextos donde su identidad de género u orientación sexual estén estigmatizadas o criminalizadas.[104]

Finalmente, la implementación de prácticas de seguridad estatales y la respuesta a solicitudes de cooperación entre estados teniendo en cuenta la perspectiva de género reducen el riesgo de no solo exacerbar las desigualdades de género interseccionales sino también de facilitar inadvertidamente las violaciones de derechos humanos. Un enfoque sensible al género en el intercambio de información y en respuesta a las solicitudes de información refuerza el respeto al derecho a la privacidad, fortalece la protección interseccional de los derechos humanos y garantiza el debido proceso —especialmente en contextos de disidencia, activismo y denuncias de irregularidades (whistleblowing)— reconociendo a su vez los riesgos que enfrentan las personas con orientaciones sexuales, identidades y expresiones de género diversas en contextos donde sus identidades o la información relacionada con ellas están criminalizadas. Las respuestas de seguridad del Estado y de los cuerpos encargados de hacer cumplir la ley frente a los delitos cibernéticos y el terrorismo también deberían estar sujetas a un análisis de género interseccional, de conformidad con las normas de derechos humanos, y llevarse a cabo respetando el debido proceso.

Preguntas orientadoras:

- ¿Tienen en cuenta las definiciones de ciberdelito y terrorismo las amenazas dirigidas a personas y comunidades? ¿Abordan las necesidades de seguridad y las vulnerabilidades específicas de las mujeres, las niñas, los hombres, los niños y las personas con orientaciones sexuales, identidades y expresiones de género diversas?

- ¿Incluyen las definiciones de ciberdelito la violencia de género facilitada por las tecnologías ?

- ¿Son sensibles al género las políticas y medidas de cooperación dirigidas a combatir el ciberdelito y el terrorismo? ¿Qué impactos no intencionados podrían tener sobre la igualdad de género y los derechos humanos?

- ¿Puede integrarse la prevención del delito con enfoque de género en los esfuerzos por abordar el ciberdelito y el terrorismo?

- ¿Se promueven los derechos a la privacidad y la protección del cifrado junto con las medidas para combatir el ciberdelito y el terrorismo?

Norma e: Derechos humanos y privacidad

Norma e: *"Los Estados, para garantizar la utilización segura de las TIC, han de 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"*

El enfoque explícito de la *Norma e* en los derechos humanos ya es coherente con una interpretación con perspectiva de género. Las dimensiones de género de la ciberseguridad —como el diseño y desarrollo tecnológico con sesgos de género; la paridad de género en los roles técnicos de ciberseguridad y en la diplomacia cibernética; los efectos diferenciados de género de las políticas de ciberseguridad y las amenazas digitales (incluida la violencia de género facilitada por las tecnologías); así como la necesidad de cerrar la brecha digital de género— son cuestiones de igualdad de género. Esta igualdad constituye una parte esencial de los derechos humanos que los Estados deben respetar al garantizar el uso seguro de las TIC.

Los compromisos asumidos por los Estados en virtud de la Declaración Universal de Derechos Humanos y

sus obligaciones en el marco de la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW, por sus siglas en inglés), entre otros instrumentos —como el Pacto Internacional de Derechos Civiles y Políticos, y el Pacto Internacional de Derechos Económicos, Sociales y Culturales—, afirman que la igualdad de género y la no discriminación constituyen componentes fundamentales de los derechos humanos. Además, la CEDAW recomienda que los Estados parte adopten medidas preventivas para abordar todas las formas contemporáneas de violencia de género que se producen en línea y en otros entornos digitales.

El informe final de 2021 del Grupo de Expertos Gubernamentales de las Naciones Unidas sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional establece una conexión explícita entre la Norma e y la dimensión de género, señalando que su cumplimiento también puede contribuir a promover la no discriminación y a reducir la brecha digital, en particular en lo que respecta al género.[105] A nivel mundial, el 62 % de los hombres utiliza Internet, frente al 58 % de las mujeres; además, en los países de ingresos bajos y medianos, las mujeres tienen un 19 % menos de probabilidades de utilizar Internet móvil en comparación con los hombres, lo que representa una diferencia de 310 millones de mujeres menos con acceso.[106] También existe una brecha de género en cuanto a alfabetización digital: las mujeres, a nivel global, tienen menos probabilidades que los hombres de haber realizado tareas básicas relacionadas con el uso del teléfono móvil, como la configuración de códigos PIN. [107] Un estudio de UNICEF realizado en 2023 en 32 países de ingresos bajos y medianos reveló que solo había 65 mujeres jóvenes con competencias digitales por cada 100 hombres jóvenes.[108]

Desde la aprobación de las 11 normas en 2015, el Consejo de Derechos Humanos (CDH) de las Naciones Unidas ha aprobado actualizaciones y ha adoptado nuevas resoluciones directamente relacionadas con los derechos humanos, la igualdad de género y las TIC. Las resoluciones 32/13 (2016)[109] y 38/7 (2018)[110] condenan la VGFT, reafirman la importancia de la privacidad digital, y exhortan a los Estados a cerrar la brecha digital de género. La resolución 38/5 de 2018 reafirma las obligaciones estatales para abordar la VGFT e insta a integrar la perspectiva de género en todas las políticas digitales y su implementación.[111] Las resoluciones 47/23 (2021)[112] y 53/29 (2023) [113] reconocen la relevancia de las tecnologías emergentes para la igualdad de género, así como su potencial para generar discriminación y violencia de género. La resolución de 2021 sobre los derechos humanos en Internet (A/HRC/47/L.22) reconoce específicamente que las brechas digitales impiden el pleno ejercicio de los derechos humanos de las mujeres.

Además, la resolución 73/179 (2018) de la Asamblea General de las Naciones Unidas sobre privacidad en la era digital [114] insta a los Estados a desarrollar políticas con perspectiva de género para proteger el derecho a la privacidad. La resolución 78/213 (2023) de la Asamblea General sobre la protección y promoción de los derechos humanos en el contexto de las tecnologías digitales reclama cerrar la brecha digital de género, incorporar perspectivas de discapacidad, género y raza en las políticas digitales, resalta la importancia del acceso de mujeres y niñas a la tecnología y reconoce la necesidad de combatir la violencia sexual y de género relacionada con la tecnología.[115]

Por tanto, la implementación con enfoque sensible al género de la *Norma e* implicaría aplicar estas resoluciones —y otras vinculadas— para proteger y promover los derechos humanos, incluido el derecho a la privacidad de todas las personas, independientemente de su género. Esto puede requerir la introducción de nuevas medidas legislativas y/o la actualización de los procesos existentes en materia de derechos humanos para poner énfasis en las obligaciones positivas de los Estados de respetar, proteger y garantizar los derechos humanos en la era digital, además del enfoque de seguridad más común que se basa en la mera prevención de daños.

Una implementación que responda a cuestiones de género de la *Norma e* también abarcaría la creación de políticas y normas legales que salvaguarden la privacidad y la libertad de expresión, incluyendo el acceso al cifrado.

Los Estados tienen asimismo la obligación de debida diligencia para proteger a las personas frente a abusos de derechos humanos —incluida la discriminación de

género— cometidos por terceros, incluidas las empresas. Esta obligación se puede ejercer mediante políticas y normativas que incentiven al sector privado a cumplir con sus responsabilidades de derechos humanos,[116] como una debida diligencia sensible al género y mecanismos de reparación cuando se identifiquen impactos adversos provocados o contribuidos por dichas empresas.[117]

La debida diligencia en materia de derechos humanos debería llevarse a cabo de manera sistemática a lo largo de todo el ciclo de vida de las tecnologías, e incluir evaluaciones de impacto regulares y exhaustivas con perspectiva de género. Los Estados también pueden establecer medidas para responsabilizar a los actores terceros, incluidas las empresas, por violaciones de derechos humanos y omisiones en relación con la igualdad de género.[118]

Por ejemplo, los Estados podrían regular la manera en que "los proveedores nacionales y privados gestionan los esfuerzos de recuperación" tras violaciones de datos, "particularmente teniendo en cuenta el daño a la privacidad y la dignidad de las personas derivado de la filtración de información personal sensible".[119] Tras este tipo de incidentes, las víctimas a menudo se encuentran sin apoyo para comprender el alcance y la posible gravedad de la filtración, ni reciben asistencia para protegerse frente al robo de identidad. Los Estados podrían establecer regulaciones que obliguen a los proveedores a notificar a las personas cuando su información haya sido comprometida (especialmente en el caso de datos médicos sensibles), así como ofrecer asistencia y compensación a las víctimas.[120] De forma complementaria, los Estados también podrían incentivar a los actores del sector privado a promover y aplicar prácticas adecuadas de higiene cibernética, tanto en el diseño de productos[121] como mediante la inversión en programas de alfabetización digital que contribuyan a un uso más seguro de sus tecnologías.[122]

Del mismo modo, proteger a las mujeres, niñas y personas con orientaciones sexuales, identidades y expresiones de género diversas frente a amenazas cibernéticas de carácter sexualizado o por razón de género es fundamental; pero también lo es garantizar su capacidad de acceder y beneficiarse de Internet. Ambas dimensiones son esenciales para cerrar la brecha digital de género.[123] La implementación con perspectiva de género de la *Norma e* podría implicar, por tanto, una auditoría de las prácticas, políticas y legislaciones existentes en materia de ciberseguridad (incluidas aquellas que no están directamente relacionadas con el género), con el fin de garantizar que respeten, protejan y cumplan con las obligaciones estatales en materia de derechos humanos e igualdad de género.

Asimismo, esta implementación con enfoque de género de la *Norma e* podría incluir que los Estados, las organizaciones intergubernamentales y el sector privado, en consulta con la sociedad civil, destinen recursos y promuevan la educación orientada a cerrar la brecha digital de género, tanto en términos de acceso como de adquisición de competencias digitales.[124]

Las acciones específicas para cerrar la brecha digital de género podrían incluir la incorporación transversal de una perspectiva de género en las estrategias de conectividad digital (incluidas las decisiones o prioridades regulatorias); el desarrollo de medidas regulatorias para subvencionar el costo de dispositivos inteligentes y datos; la integración de la alfabetización digital en los programas educativos y de desarrollo humano; garantizar que el uso de la inteligencia artificial (IA) y los macrodatos (big data) en la toma de decisiones por parte del sector público y privado no discrimine a las mujeres, a las personas con identidades, expresiones y sexualidades de género diversas y/o a las personas marginadas que no pueden acceder a Internet; así como llevar a cabo investigaciones más detalladas sobre la naturaleza y los factores contextuales que impulsan la brecha digital de género.[125]

Los Estados, las organizaciones intergubernamentales y el sector privado, en consulta con la sociedad civil y la academia, también podrían apoyar y realizar investigaciones sobre los efectos de las tecnologías emergentes —en particular la inteligencia artificial y la computación cuántica— en la igualdad de género.

Preguntas orientadoras:

- ¿Cómo puede actualizarse la comprensión de la igualdad de género, la ciberseguridad y los derechos humanos en el ciberespacio, en consonancia con la orientación de los órganos internacionales y regionales de derechos humanos, como el Consejo de Derechos Humanos de las Naciones Unidas y la Comisión Interamericana de Derechos Humanos?

- ¿Qué procesos existen para realizar de manera periódica una auditoría de género de las políticas de ciberseguridad con el fin de evaluar su cumplimiento con los derechos humanos?

- ¿Qué mecanismos existen para regular y supervisar el respeto de los derechos humanos y la igualdad de género por parte de terceros y empresas del sector privado?

- ¿Cómo se equilibran los derechos a la privacidad y a la libertad de expresión en línea con los esfuerzos por proteger a las mujeres y a las personas con orientaciones sexuales, identidades y expresiones de género diversas frente a la violencia de género facilitada por las tecnologías?

- ¿Cómo se manifiesta la brecha digital de género en distintos entornos políticos, sociales o institucionales, y qué medidas específicas pueden aplicarse para abordarla y cerrarla?

Norma f: Daños a la infraestructura pública

Norma f: *"Un Estado no debería realizar ni apoyar de forma deliberada actividades en la esfera de las TIC contrarias a las obligaciones que le incumben en virtud del derecho internacional que dañaran intencionadamente infraestructuras críticas que prestan servicios al público o dificultaran de otro modo su utilización y funcionamiento."*

Una interpretación con perspectiva de género de la *Norma f* implica ampliar la definición de "infraestructura crítica", a través de consultas con múltiples partes interesadas, a fin de incluir servicios y apoyos que sean especialmente vitales para la vida y el bienestar de las mujeres, las niñas, las personas con orientaciones sexuales, identidades y expresiones de género diversas y/o personas pertenecientes a grupos marginados y/o minoritarios.

Todas las personas dependen de la infraestructura crítica; sin embargo, no todas la experimentan ni acceden a ella de la misma manera, lo que significa que algunos componentes de dicha infraestructura serán más "críticos" para ciertos grupos y comunidades que para otros.[126] Este enfoque para incorporar la perspectiva de género en la definición de "infraestructura crítica" es aplicable a las tres nomas relativas a infraestructura crítica (*Normas f*, *g* and *h*).

La infraestructura crítica se refiere a los sistemas que prestan funciones sociales, de seguridad y económicas esenciales. Aunque la definición de infraestructura crítica no está plenamente consolidada y sigue siendo prerrogativa de cada Estado[127], la definición suele poner énfasis en las funciones y sistemas que son vitales para la seguridad convencional del Estado (y en algunos casos del sector privado), tales como los sectores de la energía, las finanzas, la seguridad nacional, el transporte, la información, así como el sector de la salud.[128] Si bien estos sectores son importantes, restringir la definición de infraestructura crítica únicamente a estos ámbitos implica el riesgo de pasar por alto las experiencias diferenciadas por razón de género ante fallos en otros sectores igualmente vitales.[129] Una encuesta sobre políticas nacionales relativas a la infraestructura crítica reveló que los sectores de agua y alimentación no se mencionaban con frecuencia, siendo el sector educativo el menos mencionado.[130]

Como Costa Rica señaló en el contexto del grave ataque de ransomware (secuestro de archivos a cambio de un rescate) de 2022, las mujeres, las niñas, los miembros de la comunidad LGBTQI+ y otros grupos vulnerables experimentan las fallas en infraestructuras críticas de manera diferenciada.[131] Las mujeres, por ejemplo, pueden experimentar una mayor inseguridad personal en los espacios públicos durante fallos en el suministro eléctrico o en los sistemas de transporte. Quienes dependen en mayor medida de los servicios públicos, como el transporte, suelen ser también quienes enfrentan mayores dificultades para acceder a ellos. Las alteraciones en el transporte público, por ejemplo, pueden afectar de forma desproporcionada a aquellas personas —en particular a las mujeres— que lo utilizan para acceder a sus lugares de trabajo, realizar tareas de cuidados o acceder a otros servicios esenciales.[132] Las personas con orientaciones sexuales, identidades y

expresiones de género diversas suelen depender de la conectividad a Internet para acceder a comunidades, redes de apoyo y recursos para su bienestar, por lo que pueden verse especialmente afectadas por una interrupción del servicio.[133]

La sociedad civil ha aportado pruebas empíricas sobre los impactos humanos y específicos de género de operaciones cibernéticas, como la que se vivió en Costa Rica. [134] En relación con lo anterior, también se han documentado los efectos que tuvo una operación de ransomware en Colombia, que afectó a los servicios de salud, sobre las mujeres cuidadoras, tanto remuneradas como no remuneradas. Las mujeres reportaron una sobrecarga significativa de trabajo al asumir tareas que consumen mucho tiempo, como programar citas médicas y autorizar servicios, lo que tuvo consecuencias físicas, psicológicas y emocionales.[135] Dado que las brechas en todas las formas de infraestructura afectan de manera desproporcionada a las mujeres[136], no incorporar una perspectiva de género interseccional al definir y proteger la infraestructura crítica puede agravar aún más las desigualdades de género.

La implementación con perspectiva de género de la *Norma f* implicaría, por tanto, adoptar una definición amplia e inclusiva de la "infraestructura crítica" que los Estados deben proteger conforme a sus obligaciones internacionales. Dado que la experiencia interseccional de género y la dependencia de las infraestructuras varía según el contexto —e incluso entre regiones dentro de un mismo Estado—, probablemente no sea posible ni deseable establecer una definición universal de infraestructura crítica con enfoque de género. En su lugar, las definiciones pertinentes podrían ser elaboradas por los Estados y las organizaciones intergubernamentales mediante consultas con múltiples partes interesadas, especialmente con organizaciones de la sociedad civil, incluidas aquellas que defienden los derechos de las mujeres, de las personas LGBTQI+ y de las personas con discapacidad.[137] Este proceso consultivo, con la participación significativa de la sociedad civil, podría abordar la exclusión involuntaria o la despriorización de sectores clave —como la educación, el agua y los cuidados sociales— de los planes de protección y respuesta.

Compartir definiciones nacionales, estrategias de consulta y datos interseccionales desagregados por género sobre los impactos de los incidentes cibernéticos, así como buenas prácticas en planes y respuestas de emergencia, puede constituir una medida de fomento de la confianza entre los Estados.

Preguntas orientadoras:

- ¿Hasta qué punto la definición existente de infraestructura crítica prioriza la seguridad de las personas y comunidades, además de la de los Estados y el sector privado?
- ¿Cómo puede adaptarse la definición de infraestructura crítica para que sea inclusiva y con perspectiva de género?
- ¿Tienen las comunidades y organizaciones afectadas la posibilidad de participar de manera significativa en el proceso de identificación de infraestructuras críticas?

Norma g: Protection of critical infrastructure

Norma g: *"Los Estados deberían tomar las medidas apropiadas para proteger sus infraestructuras críticas frente a amenazas relacionadas con las TIC, teniendo en cuenta, la resolución 58/199 de la Asamblea General sobre la creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información críticas y otras resoluciones pertinentes."*

Una interpretación sensible al género de la *Norma g* se alinea con la definición ampliada, con perspectiva de género, e interseccionalmente inclusiva de infraestructura crítica, desarrollada en consulta con organizaciones de la sociedad civil y otras partes interesadas pertinentes, tal como se plantea en la *Norma f.* Por tanto, una implementación que responda a cuestiones de género de la *Norma g* también implicaría procesos de consulta y cooperación con las partes interesadas relevantes, en particular con organizaciones de la sociedad civil, especialmente aquellas que defienden los derechos de las mujeres, de las personas LGBTQI+, de las personas con discapacidad y otros derechos humanos.

La definición ampliada, específica para cada Estado y que responda a cuestiones de género de infraestructura crítica podría integrarse de forma transversal en la planificación, los procedimientos y las respuestas ante incidentes críticos, incluyendo la elaboración de documentos estratégicos clave de política pública. Las políticas y prácticas estándar relacionadas con la infraestructura crítica —como las actualizaciones de software, los sistemas de redundancia, el aislamiento de redes y la formación del personal— podrían incorporar de forma transversal el enfoque de género. Para coordinar la protección de la infraestructura crítica que responda a cuestiones de género , los Estados y las organizaciones intergubernamentales podrían designar asesorías de género y/o puntos focales dentro de las propias instituciones estatales y de los organismos intergubernamentales, encargadas de coordinar el trabajo en materia de género e igualdad entre los diversos organismos y departamentos implicados en la implementación de las normas cibernéticas, garantizando así que las políticas relacionadas sean coherentes y estén articuladas entre sí.

Los planes y escenarios de respuesta ante emergencias también podrían estar fundamentados en modelos de amenazas con enfoque interseccional y perspectiva de género,[138] elaborados por equipos diversos que cooperen entre los sectores estatal, privado y de la sociedad civil.[139] Una preocupación fundamental es la invisibilidad de las comunidades marginadas en los modelos de amenazas, ya que sus experiencias suelen no ser reconocidas en los procesos de diseño.[140] Para abordar esta posible deficiencia, los Estados y las organizaciones intergubernamentales podrían crear un mecanismo transparente de intercambio de información y de reporte de incidentes cibernéticos entre el Estado, el sector empresarial y – de manera fundamental – la sociedad civil. Se podrían formalizar vías específicas para que organizaciones de derechos de las mujeres, personas LGBTQI+, de derechos digitales y otros derechos humanos compartan información con el Estado y aporten retroalimentación sobre la implementación y la gobernanza de la ciberseguridad, dotándolas además de los recursos adecuados para ello.

En este sentido, la "cultura mundial de la seguridad cibernética" puede interpretarse como una expresión de compromiso con la igualdad de género interseccional en la gobernanza y las políticas de ciberseguridad, así como con la promoción de una fuerza laboral diversa y con paridad de género (véanse también las *Normas j* y *k*). La Resolución 58/199 de la Asamblea General de las Naciones Unidas sobre la "creación de una cultura mundial de la seguridad cibernética y la protección de las infraestructuras críticas de información" subraya la necesidad de cerrar la brecha digital y de garantizar el acceso universal a las TIC. Esto, a su vez, puede interpretarse desde una perspectiva sensible al género, prestando especial atención a la brecha digital de género en términos de acceso y desarrollo de competencias (véase la discusión relativa a la *Norma e*). Las personas —con especial atención a las mujeres y a los miembros de grupos marginados— deben tener acceso a información oportuna y fiable sobre seguridad digital, incluyendo detalles sobre los riesgos más comunes a los que podrían enfrentarse.

El desarrollo de una cultura mundial de la ciberseguridad con enfoque de género podría incluir la transversalización de la perspectiva de género en todos los aspectos del desarrollo de capacidades y la cooperación en materia cibernética, junto con el fortalecimiento de habilidades técnicas, sistemas y procesos.[141] El enfoque basado en principios para el desarrollo de capacidades cibernéticas, formulado por el OEWG, establece que dicho desarrollo de capacidades debe "respetar los derechos humanos y las libertades fundamentales, ser sensible al género e inclusivo, universal, así como no discriminatorio".[142] Las medidas de desarrollo de capacidades a nivel internacional, regional, subregional y bilateral podrían ser inclusivas e incorporar a múltiples partes interesadas, incluyendo organizaciones de mujeres, de personas LBTQI+ y otras organizaciones que promueven los derechos humanos y los derechos digitales.[143] Un enfoque de desarrollo de capacidades con perspectiva de género implicaría priorizar tanto la experiencia técnica como la especialización en análisis interseccional de género en ciberseguridad y gobernanza digital. Asimismo, este enfoque podría orientarse a promover la diversidad y la paridad de género entre las personas expertas técnicas en ciberseguridad, así como entre quienes diseñan políticas digitales y de ciberseguridad, en todos los niveles de los procesos de formación, desarrollo de capacidades e intercambio de conocimientos.

Esto podría incluir el desarrollo de campañas de concienciación social y planes de estudio educativos dirigidos, entre otros, a niños, niñas y jóvenes. Los Estados también podrían considerar la implementación de campañas nacionales de sensibilización sobre ciberseguridad que ofrezcan recursos para comprender las amenazas cibernéticas más comunes que afectan a personas y comunidades —incluidos los daños con dimensión de género—, así como orientación para reducir los riesgos. Dado que las investigaciones sobre la brecha de habilidades digitales de género indican que las mujeres mayores que viven en zonas rurales son las menos propensas a tener conocimientos en ciberseguridad[144] y competencias digitales, estas campañas de concienciación podrían complementarse con programas educativos y acciones de divulgación dirigidas a comunidades marginadas. Esto cumpliría una doble función: abordar la brecha digital de género y promover una cultura más amplia de la ciberseguridad.

Preguntas orientadoras:

- ¿Qué tan integral y con enfoque de género es el plan para abordar los incidentes de ciberseguridad que afectan a infraestructuras críticas? ¿En qué medida está adaptado al contexto y se basa en consultas con partes interesadas relevantes y, en particular, con organizaciones de la sociedad civil?

- ¿Qué tan diversos son los equipos que realizan el modelado de amenazas y hasta qué punto el proceso incorpora un análisis de género interseccional?

- ¿La concepción de una cultura de la ciberseguridad integra la igualdad de género interseccional? ¿Se refleja esto en las políticas y programas de sensibilización y educación en ciberseguridad?

- ¿Se ha incorporado transversalmente el enfoque de género en los esfuerzos de desarrollo de capacidades cibernéticas y en la diplomacia cibernética?

Norma h: Respuesta a las solicitudes de asistencia

Norma h: *"Los Estados deberían atender las solicitudes de asistencia apropiadas de otro Estado cuyas infraestructuras críticas fueran objeto de actos malintencionados relacionados con las TIC. Los Estados también deberían atender las solicitudes apropiadas para mitigar toda actividad malintencionada relacionada A/70/174 15-12404 11/20 con las TIC originada en su territorio contra infraestructuras críticas de otro Estado, teniendo debidamente en cuenta la soberanía."*

Una interpretación con perspectiva de género de la *Norma h* se alinea con la definición ampliada e interseccionalmente inclusiva de infraestructura crítica, así como con los procesos de planificación y respuesta a incidentes con perspectiva de género descritos en las *Normas f* y *g*.

En una implementación con enfoque de género de la *Norma h*, las respuestas estatales a las solicitudes de asistencia para abordar actividades malintencionadas relacionadas con las TIC tendrían en cuenta el potencial impacto negativo que dicha cooperación pudiera tener en términos de igualdad de género. Asimismo, las respuestas del Estado respetarían los derechos humanos y se ajustarían al debido proceso (véase también la cooperación en el marco de la *Norma d* y la prevención de actividades maliciosas en el marco de la *Norma c*).

Preguntas orientadoras:

- ¿Los procedimientos para responder a solicitudes de asistencia están alineados con los derechos humanos y el debido proceso?

- ¿En qué medida estos procedimientos incorporan un análisis de género que permita evaluar riesgos potenciales basados en el género, la sexualidad o la identidad y expresión de género?

Norma i: Seguridad de la cadena de suministro

Norma i: *"Los Estados deberían adoptar las medidas pertinentes para garantizar la integridad de la cadena de suministro con miras a que los usuarios finales confiaran en la seguridad de los productos relacionados con las TIC. Los Estados deberían tratar de evitar la proliferación de técnicas e instrumentos malintencionados en la esfera de las TIC, así como el uso de funciones ocultas y dañinas."*

Una interpretación sensible al género de la *Norma i* se basaría en la definición de seguridad amplia, centrada en las personas y con perspectiva de género recogida en la Agenda MPS, para ampliar el énfasis de la norma sobre los riesgos asociados a los "productos relacionados con las TIC" y las "herramientas maliciosas en el ámbito de las TIC" más allá del importante pero limitado enfoque actual en los Estados y las empresas, así como las redes, los dispositivos y los sistemas. Las herramientas maliciosas en el ámbito de las TIC, las funciones ocultas y dañinas, y —aunque no se mencione directamente en esta norma— el uso indebido de tecnologías de doble uso, tienen efectos diferenciados por razón de género.[145]

Algunos Estados, por ejemplo, han cooperado en intentos por frenar la proliferación de software espía (spyware), una forma de malware que se instala en los dispositivos de las personas usuarias sin su conocimiento para transmitir información de manera secreta a un tercero.[146] "El stalkerware, un tipo de malware que también se instala sin el conocimiento de la persona usuaria para transmitir sus datos de forma encubierta, es técnicamente similar al spyware, pero hasta el momento ha sido menos abordado de forma eficaz mediante esfuerzos de no proliferación. El stalkerware se utiliza con frecuencia en contextos de violencia doméstica y/o de pareja íntima como una extensión del control y el abuso.[147]

Las prácticas de diseño relacionadas con el Internet de las Cosas (IoT) —una preocupación clave de seguridad expresada por algunos Estados en relación con sus cadenas de suministro—[148] si no se incorpora explícitamente una perspectiva de género en su desarrollo, pueden generar, de forma inadvertida, riesgos que no tienen en cuenta al género. Por ejemplo, los protocolos administrativos de dispositivos domésticos "inteligentes", como cámaras, timbres o cerraduras, no consideran adecuadamente la posibilidad de situaciones de violencia doméstica, lo que permite a los agresores utilizar dichos dispositivos para vigilar a sus víctimas e impide que las personas sobrevivientes puedan excluir a los perpetradores de los sistemas TIC del hogar.[149] Las etiquetas electrónicas de rastreo presentan riesgos similares: un estudio realizado en Australia en 2024 reveló que una de cada cuatro compras de este tipo de dispositivos durante el año anterior estaba vinculada a antecedentes documentados de violencia doméstica.[150] La adopción de una interpretación sensible al género de los conceptos de "herramientas maliciosas en el ámbito de las TIC" y "funciones ocultas y dañinas" contribuirá, por tanto, a abordar tanto las experiencias de seguridad en la cadena de suministro que afectan directamente a las mujeres y personas de géneros diversos como aquellas que las impactan de forma indirecta.

Desde una perspectiva práctica, la seguridad de la cadena de suministro puede implementarse mediante el desarrollo de normas técnicas de ciberseguridad con perspectiva de género, nuevamente en consulta con organizaciones de mujeres, personas LGBTQI+, organizaciones de derechos humanos y de derechos digitales.[151] En el informe anual de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos sobre los derechos humanos y los procesos de establecimiento de normas técnicas para las tecnologías digitales nuevas y emergentes (A/HRC/53/42),[152] se alienta a los Estados a abstenerse a desarrollar y a prevenir el desarrollo de normas técnicas que puedan facilitar previsiblemente violaciones o abusos de derechos humanos cuando participen en procesos de establecimiento de esas normas.

Para apoyar este proceso, los Estados podrían llevar a cabo consultas inclusivas y significativas con organizaciones de mujeres y de personas LGBTQI+ a fin de comprender mejor los impactos de género de las normas técnicas de ciberseguridad, e incluir a organizaciones pertinentes de la sociedad civil en

sus delegaciones ante los organismos internacionales de establecimiento de normas técnicas. Por su parte, las organizaciones encargadas de establecer normas técnicas podrían adoptar medidas para garantizar que sus propios procesos sean abiertos, transparentes e inclusivos. Esto podría incluir el apoyo a organizaciones representativas de la sociedad civil, así como a grupos y comunidades sociales afectadas, para que desarrollen la capacidad necesaria que les permita participar de manera significativa e independiente en los procesos de establecimiento de normas técnicas en materia de ciberseguridad.

La eficacia de estas normas técnicas podría reforzarse mediante el financiamiento a organizaciones de la sociedad civil y al ámbito académico para que realicen investigaciones sobre los posibles efectos no intencionados y diferenciados por razón de género de las tecnologías emergentes (incluidas la inteligencia artificial generativa y la computación cuántica), sobre funciones técnicas ocultas o maliciosas en productos lícitos, así como auditorías de género de productos y prácticas de ciberseguridad ampliamente utilizados.

Los Estados podrían cooperar a nivel internacional y regional para incorporar la tecnología que facilita la violencia de género en los mecanismos y regímenes existentes de no proliferación (o bien crear nuevos mecanismos). Estos esfuerzos podrían reforzarse mediante la incorporación transversal del enfoque de género —y de la debida diligencia en materia de derechos humanos— en los procesos de gobernanza existentes sobre no proliferación y seguridad de las cadenas de suministro de las TIC, tanto a nivel nacional, regional como intergubernamental (por ejemplo, en los regímenes de control de exportaciones y de armas).

A nivel nacional, los Estados también podrían implementar medidas para regular la disponibilidad y el uso de tecnologías que facilitan la violencia de género. Esto podría incluir disposiciones para responsabilizar a las empresas por una implementación de las normas técnicas que sea conforme a los derechos humanos y con enfoque de género (véase la *Norma e*). La implementación con perspectiva de género de la *Norma i* podría fortalecerse aún más mediante la creación e implementación de marcos de protección de datos que respondan a cuestiones de género, desarrollados a través de procesos de consulta con múltiples partes interesadas, que presten especial atención a las necesidades específicas de privacidad y a las vulnerabilidades particulares de las mujeres y de las personas con identidades, expresiones y orientaciones sexuales diversas.[153]

Preguntas orientadoras:

- ¿La definición actual del uso malicioso de las TIC y de las funciones ocultas incluye un análisis de los posibles efectos adversos sobre personas de diferentes géneros y sexualidades?
- ¿Qué tan activamente se promueve el desarrollo de normas técnicas que respondan a cuestiones de género, incluyendo la participación de la sociedad civil en dicho proceso?
- ¿Se incluyen las tecnologías vinculadas a la violencia de género en los regímenes internacionales de no proliferación? ¿Cómo podría lograrse esta inclusión?

Norma j: Divulgación de las vulnerabilidades relacionadas con las TIC

Norma j: *"Los Estados deberían alentar la divulgación responsable de las vulnerabilidades relacionadas con las TIC y compartir la información conexa sobre los recursos disponibles ante tales vulnerabilidades a fin de limitar, y posiblemente eliminar, las amenazas potenciales para las TIC o infraestructuras dependientes de esas tecnologías."*

Una interpretación con perspectiva de género de la *Norma j* implicaría adoptar una comprensión de las vulnerabilidades que tenga en cuenta el género (véase la *Norma b* sobre la recopilación de datos desagregados por género en incidentes y amenazas cibernéticas), así como una visión amplia e inclusiva de las agencias y actores relevantes en los procesos

de notificación de vulnerabilidades e intercambio de información. Asimismo, esta interpretación de la *Norma j* incorporaría la definición de infraestructura crítica con perspectiva de género e interseccionalidad presentada en las *Normas f*, *g* y *h*.

Las violaciones de bases de datos médicos, por ejemplo, aunque constituyen una grave vulneración de la privacidad para todas las personas, pueden tener consecuencias diferenciadas por razón de género. La filtración de información relacionada con la salud sexual y reproductiva —incluida la relativa a la interrupción del embarazo— para personas con capacidad de gestar puede exponerlas a situaciones de vergüenza, estigmatización, discriminación, riesgo de violencia interpersonal y, en contextos donde el aborto no es legal, a ser objeto de procedimientos judiciales.[154]

La exposición de datos médicos y de aplicaciones de citas de personas con orientaciones sexuales, identidades y expresiones de género diversas conlleva riesgos similares de discriminación, estigmatización, violencia y contacto con el sistema judicial (especialmente en contextos donde la expresión abierta de identidades LGBTQI+ no es legal), además de la vulneración adicional que supone ser forzadamente expuestas.[155] Estos riesgos se agravan aún más cuando las personas, organizaciones y comunidades afectadas no son informadas de la filtración ni reciben apoyo para gestionar sus riesgos digitales y personales una vez que la violación de la base de datos ha ocurrido (véase también la *Norma e*).

Una implementación que responda a cuestiones de género de la *Norma j* podría implicar ampliar los procesos convencionales de ciberseguridad para la notificación de vulnerabilidades y el intercambio de información, yendo más allá de las agencias estatales relevantes y/o las asociaciones público-privadas, para incluir también a la sociedad civil, en particular a las organizaciones de derechos humanos, de mujeres y de personas LGBTIQ+. Hacer que el proceso de gestión de vulnerabilidades en las TIC sea más colaborativo, abierto e inclusivo permitirá identificar y abordar con mayor eficacia las vulnerabilidades y las amenazas cibernéticas con efectos diferenciados por razón de género que enfrentan personas y comunidades.

Una estrategia ambiciosa podría implicar la creación de procesos transnacionales que permitan a socios de múltiples partes interesadas —incluidas organizaciones de la sociedad civil, el ámbito académico y el sector privado— compartir información sobre vulnerabilidades en las TIC y colaborar entre sí, así como con Estados más allá de su país de origen, ubicación o ámbito principal de operaciones, reconociendo el carácter transnacional del uso indebido de las TIC (véase la *Norma c*).

Cualquiera que sea el formato, estos procesos abiertos y participativos de notificación de vulnerabilidades e intercambio de información podrían adoptar la comprensión con perspectiva de género de las vulnerabilidades expuestas anteriormente y, específicamente, informar sobre aquellas que puedan dar lugar a daños diferenciados por razón de género. Esto podría incluir:

- Un requisito normativo para que las empresas notifiquen a las personas consumidoras sobre vulnerabilidades y brechas de seguridad (véase la *Norma e*)

- Campañas de sensibilización sobre vulnerabilidades en las TIC y ciberseguridad dirigidas a grupos específicos (por ejemplo, mujeres mayores en zonas rurales; véase la *Norma g*)

- Intercambio entre Estados de riesgos con dimensión de género observados y de buenas prácticas relacionadas (véase la *Norma b*)

Un intercambio de información eficaz y con perspectiva de género también implicaría fomentar y establecer relaciones de trabajo positivas, basadas en la reciprocidad y la confianza, entre organizaciones intergubernamentales, Estados, empresas y sociedad civil, más allá de centrarse únicamente en la eficiencia o el volumen del intercambio de información.[156] La eficacia del intercambio de información depende del fomento de intercambios respetuosos y entornos de trabajo colaborativos.

Una encuesta mundial sobre la fuerza laboral en seguridad de la información realizada en 2017 reveló que el 87 % de las mujeres en roles de ciberseguridad habían experimentado discriminación indirecta y otro 19 % discriminación directa.[157] No existen datos comparables

para personas con orientaciones sexuales, identidades y expresiones de género diversas, aunque los riesgos relacionados de discriminación también les afectan.[158] Estas dinámicas corren el riesgo de empujar al personal cualificado a abandonar la fuerza laboral, reforzar culturas laborales inequitativas, dificultar el mantenimiento de relaciones profesionales basadas en la confianza y afectar negativamente la diversidad de los equipos encargados de abordar y notificar vulnerabilidades. Una cultura profesional inclusiva y eficaz podría fomentarse mediante la implementación de políticas de recursos humanos que respondan a cuestiones de género, desarrolladas en consulta con trabajadoras y personas LGBTQI+ sobre las políticas que consideran de apoyo (por ejemplo, horarios laborales flexibles, mejores disposiciones de licencias parentales o de cuidados, programas de mentoría).

Los cambios en las políticas de recursos humanos podrían complementarse con formación en género para personas en cargos directivos y de liderazgo técnico o político en materia de ciberseguridad, idealmente como condición para su promoción.[159]

Una implementación que responda a cuestiones de género de la *Norma j*[160] también podría fortalecer la capacidad de las organizaciones de ciberseguridad para notificar y responder de manera oportuna a las vulnerabilidades cibernéticas (véase también la *Norma g* sobre la cultura mundial de la ciberseguridad).

Preguntas orientadoras:

- ¿La comprensión de las vulnerabilidades en las TIC tiene en cuenta los daños diferenciados por razón de género e interseccionalidad?
- ¿Qué tan abierto, accesible e inclusivo es el proceso de notificación y respuesta ante vulnerabilidades en las TIC?
- Una vez identificadas las vulnerabilidades, ¿existe un proceso para informar y asesorar a las comunidades particularmente vulnerables y/o afectadas?
- ¿En qué medida la cultura profesional de trabajo favorece la capacidad de las organizaciones de ciberseguridad para notificar y responder de forma oportuna a las vulnerabilidades, considerando los daños diferenciados por género?
- ¿Cómo experimentan su trabajo e interacción dentro de la organización las mujeres y las personas con orientaciones sexuales, identidades y expresiones de género diversas?

Norma k: Daños a los equipos de respuesta a emergencias

Norma k: *"Los Estados no deberían realizar ni apoyar de forma deliberada actividades que dañaran los sistemas de información de los equipos autorizados de respuesta a emergencias (a veces conocidos como equipos de respuesta ante emergencias informáticas o equipos de respuesta ante incidentes cibernéticos) de otro Estado. Un Estado no debería utilizar equipos autorizados de respuesta a emergencias para participar en una actividad internacional malintencionada.."*

La *Norma k* destaca la importancia de los Equipos de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés) y los Equipos Nacionales de Respuesta ante Incidentes Cibernéticos (CIRT) en la gestión de emergencias derivadas de incidentes cibernéticos. Si bien la versión actual de la *Norma k* se refiere específicamente a la obligación de los Estados de no realizar ni apoyar deliberadamente actividades que dañen los sistemas de información de los CERT o CIRT de otros Estados, ni utilizar sus propios equipos para llevar a cabo operaciones cibernéticas maliciosas a nivel internacional, el presente informe ofrece una interpretación con perspectiva de género de aspectos conexos de la norma. Esta interpretación busca reforzar el propósito fundamental de la *Norma k* mediante el desarrollo de la capacidad y la eficacia de los CERT y CIRT dentro de los Estados, así como en las oficinas de coordinación de las organizaciones intergubernamentales.

Esta interpretación, relacionada con acciones complementarias al núcleo de la *Norma k*, se alinea

con el nivel de entendimiento adicional acordado en el informe del Grupo de Expertos Gubernamentales de 2021 (A/76/135), el cual establece que: "Los CERT, CSIRT u otros órganos de respuesta autorizados tienen responsabilidades y funciones únicas en la gestión y resolución de incidentes relacionados con las TIC, y por lo tanto desempeñan un papel importante en el mantenimiento de la paz y la seguridad internacionales. Son esenciales para detectar y mitigar eficazmente los efectos negativos inmediatos y a largo plazo de los incidentes relacionados con las TIC".[161]

Partiendo de este enfoque sobre la centralidad más amplia de los CERT y CSIRT en la ciberseguridad y la implementación de las normas, una interpretación ampliada y sensible al género de la Norma k pondría atención en la composición de género de los equipos CERT y CSIRT, así como en los beneficios potenciales de contar con una fuerza laboral diversa.

Aunque los datos específicos sobre la composición de género de los equipos CERT y CSIRT son limitados —y representan una línea importante para futuras investigaciones—, como se mencionó anteriormente en este informe, las mujeres están subrepresentadas en los roles técnicos de ciberseguridad. A nivel global, las mujeres constituyen aproximadamente el 25 % de la fuerza laboral técnica en ciberseguridad.[162] Las mujeres también tienden a abandonar los empleos en ciberseguridad y tecnología en tasas más altas que los hombres. Un estudio realizado en Estados Unidos en 2019 reveló que las mujeres tenían un 45 % más de probabilidades de dejar el sector que los hombres, especialmente alrededor de los 35 años, debido a la rigidez en los horarios laborales y las expectativas, el acceso inadecuado a licencias por cuidados o parentales, las desigualdades en las oportunidades de ascenso y culturas laborales no inclusivas.[163]

Los estudios organizacionales sugieren que, bajo las condiciones adecuadas, los equipos más diversos pueden contribuir a mejorar los procesos de toma de decisiones. Los equipos diversos pueden fomentar el pensamiento innovador y la resolución creativa de problemas; ofrecer una comprensión más matizada de los problemas en su contexto social; y aprovechar mejor el talento y el potencial de liderazgo.[164] Aunque el potencial de los equipos diversos depende de una cultura laboral positiva e inclusiva, así como de procesos estructurados de trabajo y comunicación que garanticen que las ideas divergentes se expresen y se tomen en cuenta, existen razones para considerar que los equipos CERT y CIRT diversos e inclusivos en términos de género podrían aportar nuevas perspectivas creativas a una respuesta eficaz ante incidentes cibernéticos. La recopilación de datos sobre la composición de género e identidad de estos equipos, y sobre cómo la diversidad puede influir en sus formas de trabajo, representa una línea importante para futuras investigaciones.

Una implementación que responda a cuestiones de género de la *Norma k* —y, en realidad, de todas las normas— podría orientarse hacia la paridad de género y, en general, hacia una mayor diversificación dentro de los equipos CERT y CIRT, así como en el conjunto de la fuerza laboral técnica en ciberseguridad.[165] Esto podría estar respaldado por iniciativas de desarrollo de capacidades con perspectiva de género orientadas a cerrar la brecha digital y de habilidades (véanse las *Normas e* y *g*).

Preguntas orientadoras:

- ¿Qué tan equitativamente son contratadas y promovidas las mujeres y las personas con identidades, expresiones y orientaciones sexuales diversas en los roles de ciberseguridad?

- ¿Qué aspectos de la cultura laboral actual dentro de los equipos CERT y CIRT favorecen o dificultan la participación de mujeres y personas con identidades, expresiones y orientaciones sexuales diversas?

- ¿Están los CERT y CIRT aprovechando de manera óptima y eficaz la diversidad de sus equipos en la respuesta a incidentes y en la toma de decisiones?

Principios generales / Recomendaciones transversales para un enfoque de género en la interpretación e implementación de las normas:

1) Las definiciones de seguridad, amenazas e infraestructura crítica presentes en las 11 normas para el comportamiento responsable de los Estados podrían alinearse con la definición de paz y seguridad internacional de la Agenda MPS: una visión que responda a cuestiones de género, centrada en las personas e interseccional.

2) En consulta con la sociedad civil, los Estados y las organizaciones intergubernamentales podrían transversalizar el enfoque de género en todas sus políticas de ciberseguridad y gobernanza digital. Esto incluiría el análisis de todos los planes, modelos de amenazas, marcos normativos y prácticas de implementación relacionadas con las 11 normas desde una perspectiva de género interseccional.

3) Los Estados y las organizaciones intergubernamentales podrían trabajar para alcanzar la paridad de género y aumentar la participación de personas con identidades, expresiones y orientaciones sexuales diversas, así como de otros grupos marginados, en todos los aspectos del desarrollo, planificación, respuesta técnica, implementación y evaluación de las normas cibernéticas.

4) Los Estados y la comunidad de múltiples partes interesadas podrían recopilar y generar datos desagregados por género e interseccionalidad, no solo sobre incidentes cibernéticos, sino también sobre medidas de ciberseguridad, participación y otras áreas relevantes. Las partes interesadas podrían promover el intercambio y uso de esta información para fomentar enfoques de gobernanza digital inclusivos y basados en evidencia.

Tabla resumen: Implementación que responde a cuestiones de género de las Normas de la ONU sobre el Comportamiento Responsable de los Estados en el Ciberespacio

Norma	Implementación que responde a cuestiones de género
a: Cooperación entre Estados	■ Transversalizar la perspectiva de género en la lista de comprobación voluntaria para la implementación de normas. ■ Alinear estrategias nacionales de ciberseguridad con planes de acción nacionales de la Agenda MPS. ■ Apuntar a la paridad de género e implementar formación en género para equipos de diplomacia cibernética.
b: Información relevante	■ Recopilar datos desagregados por género sobre los efectos de los incidentes cibernéticos. ■ Consultar con organizaciones de la sociedad civil para comprender los efectos interseccionales más amplios.
c: Prevención del uso indebido de las TIC	■ Analizar el uso indebido convencional de las TIC para identificar efectos con dimensión de género. ■ Adoptar medidas frente al uso de las TIC que afecte los derechos de otros Estados y comunidades, incluyendo la violencia de género facilitada por la tecnología.
d: Cooperación contra la delincuencia y el terrorismo	■ Desarrollar medidas no judiciales para abordar la violencia de género facilitada por la tecnología y otros delitos cibernéticos a través de esquemas de cooperación. ■ Aplicar salvaguardias de derechos humanos para evitar impactos negativos por motivos de género y/o sexualidad.
e: Derechos humanos y privacidad	■ Reconocer la igualdad de género como parte de los derechos humanos en la era digital. ■ Proteger y promover el cifrado. ■ Cerrar la brecha digital de género y de habilidades digitales.
f: Daños a infraestructuras críticas	■ Consultar con la sociedad civil para definir infraestructuras críticas con enfoque de género y en función del contexto. ■ Compartir definiciones con enfoque de género y buenas prácticas para su protección y resiliencia.
g: Protección de infraestructuras críticas	■ Realizar auditorías de género sobre respuestas del pasado a incidentes cibernéticos. ■ Transversalizar la perspectiva de género en la planificación, asignación de recursos y respuesta a incidentes. ■ Fortalecer capacidades tanto técnicas como analíticas en género.
h: Respuesta a solicitudes de asistencia	■ Analizar las solicitudes de asistencia desde una perspectiva de derechos humanos y para evitar efectos adversos por motivos de género.
i: Seguridad de la cadena de suministro	■ Analizar tecnologías emergentes en busca de funciones ocultas dañinas o usos duales maliciosos con efectos diferenciados por género. ■ Incluir tecnologías que facilitan la violencia de género en sistemas de no proliferación. ■ Desarrollar normas técnicas de ciberseguridad con enfoque de género.
j: Divulgación de vulnerabilidades en las TIC	■ Realizar análisis de género sobre vulnerabilidades en las TIC. ■ Incluir organizaciones de la sociedad civil en los procesos de notificación e intercambio de información. ■ Fomentar entornos laborales inclusivos y respetuosos.
k: Daños a equipos de respuesta a emergencias	■ Apuntar a la paridad de género en los equipos CERT y CIRT. ■ Involucrar equipos diversos en la toma de decisiones.

3.

Ciberseguridad con perspectiva de género en la práctica: Aprendizajes de Canadá, Chile y Costa Rica[167]

Esta sección presenta buenas prácticas en acción para la interpretación y la implementación con enfoque de género de las 11 normas de las Naciones Unidas, a través de estudios de caso de Canadá, Chile y Costa Rica. Los casos presentados son ejemplos positivos en cuanto a:

- Repensar los enfoques tradicionales de la ciberseguridad adoptando una visión centrada en las personas y que responda a cuestiones de género
- Integrar el enfoque de género en la diplomacia cibernética con especial atención a la Agenda MPS
- Implementar las normas a nivel nacional a través de estrategias de ciberseguridad

3.1 Canadá: Integración de la ciberseguridad y la Agenda MPS

Este estudio de caso describe cómo Canadá ha utilizado la Agenda MPS y sus planes de acción nacionales para incorporar consideraciones de género en la diplomacia cibernética internacional, incluyendo la cooperación cibernética y el desarrollo de capacidades a nivel global. Este ejemplo busca ilustrar cómo los gobiernos pueden transversalizar el enfoque de género en la diplomacia en materia de ciberseguridad.

¿Qué hace que este caso sea relevante para una ciberseguridad con perspectiva de género?

Canadá ha abordado los impactos diferenciados por razón de género en el ámbito de la ciberseguridad de diversas maneras. Entre ellas, destaca la integración de la Agenda MPS en sus esfuerzos en materia de ciberseguridad, así como la ampliación del enfoque tradicional de dicha agenda para incluir aspectos relacionados con el entorno digital.[167] Además, Canadá ha abogado por la aplicación de la Agenda MPS —y por la igualdad de género en un sentido más amplio— en los debates y foros internacionales sobre ciberseguridad.

¿Cuáles son las políticas y medidas que se están utilizando para una implementación con enfoque de género de las normas de las Naciones Unidas?

La participación de Canadá en los debates internacionales sobre ciberseguridad se guía por un enfoque feminista, reflejado en su Política de Asistencia Internacional Feminista.[168] Las áreas clave de acción de la política exterior canadiense son:

- Igualdad de género y empoderamiento de mujeres y niñas
- Dignidad humana
- Gobernanza inclusiva, incluyendo la democracia, los derechos humanos, el estado de derecho y el buen gobierno
- Paz y seguridad, mediante la promoción de procesos de paz inclusivos y la lucha contra la violencia basada en género[169]

Este enfoque puede considerarse una buena práctica para cuestionar las nociones tradicionales y centradas en el Estado de la ciberseguridad, que tienen menos capacidad para evaluar las necesidades, experiencias y capacidades interseccionales de las personas y comunidades. La visión de seguridad explícitamente centrada en las personas y que responde a cuestiones de género presente en la política exterior canadiense ofrece una base para redefinir la ciberseguridad, de manera que responda a las necesidades complejas, diferenciadas e interseccionales de las personas, basadas en el género, entre otros factores.[170]

A partir de esta comprensión de la seguridad que responde a cuestiones de género, Canadá ha elaborado una guía específica para integrar la igualdad de género en la implementación de las normas de las Naciones Unidas. Esta guía propone:

- El desarrollo inclusivo de una cultura mundial de ciberseguridad que aborde sus dimensiones de género [171] (véase la *Norma g*)
- La recogida de más datos relacionados con el género para apoyar políticas basadas en evidencia y abordar impactos diferenciados (véanse las *Normas f* y *g*)
- Que los Estados, al examinar toda información en casos de incidentes TIC, “realicen investigaciones sobre posibles impactos de género, y trabajen de forma

inclusiva con todas las partes interesadas para entender el contexto amplio de un incidente TIC, incluyendo su impacto en el disfrute de los derechos de las mujeres y las personas LGBTI" (véase la *Norma b*)

- Que los Estados consideren las amenazas diferenciales que enfrentan las mujeres y las personas de grupos minoritarios o vulnerables en el contexto de la ciberseguridad (véanse las *Normas c*, *d*, *f*, *g* e *i)*

- Que los Estados realicen auditorías de género de las políticas de ciberseguridad nacionales o regionales para identificar áreas de mejora (véase la *Norma e*)[172]

Canadá ha solicitado que el OEWG de las Naciones Unidas aborde las cuestiones de género, destacando la conexión entre los desarrollos en las TIC y la Agenda MPS, señalando que "las mujeres se ven afectadas de manera única y diferenciada por los conflictos y las amenazas a la paz y la seguridad internacionales".[173] Canadá ha propuesto que el OEWG dé prioridad a la igualdad de género, instando al grupo a abordar cómo proteger mejor a las personas defensoras de los derechos humanos, incluidas las activistas, frente a amenazas dirigidas mediante el uso de las TIC.[174]

El trabajo político más relevante de Canadá en materia de igualdad de género y ciberseguridad se encuentra en su recientemente actualizado Plan de Acción Nacional sobre Mujeres, Paz y Seguridad 2023–2029 (NAP).[175] El Plan de Acción Nacional amplía el enfoque tradicional de la Agenda MPS, centrado en los derechos, necesidades y vulnerabilidades de las mujeres en contextos de guerra y conflicto convencional, para incluir nuevas amenazas a la seguridad, como la VGFT, las campañas de desinformación y los ciberataques dirigidos contra mujeres constructoras de paz y defensoras de derechos humanos. El Plan Nacional de Acción coordina el trabajo en materia de igualdad de género y diversidad sexual de diez organismos federales, y orienta tanto la política interior como la política exterior de Canadá.

El Área de Enfoque 2 del Plan de Acción Nacional ("Seguridad, justicia y rendición de cuentas") aborda la ciberseguridad y las tecnologías disruptivas, incluyendo la VGFT, la desinformación y el uso indebido, el abuso y la perpetuación de estereotipos y sesgos dañinos mediante la inteligencia artificial. La estrategia propone un "enfoque transformador de género" para comprender estas amenazas emergentes y responder mejor a las necesidades de grupos demográficos diversos. En el marco de esta área temática, la estrategia incluye acciones como mejorar la sensibilización y las capacidades de los sectores de seguridad y justicia para enfrentar amenazas no tradicionales o emergentes.

En el Área de Enfoque 4 ("Violencia sexual y basada en género"), la VGFT y la desinformación con sesgo de género se enmarcan como amenazas a la seguridad nacional que afectan negativamente los avances en materia de igualdad de género. La igualdad de género se concibe, a su vez, como un componente central de la seguridad nacional; el Plan de Acción Nacional destaca la gravedad que tienen tanto para las personas como para el Estado las actividades maliciosas relacionadas con las TIC y los posibles actos internacionalmente ilícitos, como la interferencia electoral o la desinformación masiva. En respuesta, el Plan de Acción Nacional incluye compromisos para fortalecer la comprensión del Estado sobre las conexiones entre el extremismo violento, la desinformación y la violencia basada en género, así como su capacidad para responder a la VGFT.

Canadá ha financiado investigaciones[176] e iniciativas de desarrollo de capacidades[177] sobre las dimensiones de género en la ciberseguridad y ha desarrollado buenas prácticas para apoyar la participación de las mujeres en los debates sobre políticas de ciberseguridad y en la práctica técnica. Por ejemplo, como parte de sus iniciativas de desarrollo de capacidades en ciberseguridad a nivel global, Canadá ha financiado la participación de diplomáticas de las Américas en las reuniones del OEWG de las Naciones Unidas, en el marco del programa *Women in International Security and Cyberspace Fellowship* (véase el recuadro sobre "Buenas Prácticas"). Estas acciones para mejorar la representación de las mujeres en las delegaciones estatales ante el OEWG se acompañan de llamados a que los procesos de diplomacia cibernética de las Naciones Unidas sean más inclusivos con las partes interesadas. Canadá subraya especialmente el papel clave de la sociedad civil en la promoción de la igualdad de género.[178]

¿Cuáles son las lecciones aprendidas de este caso?

En términos generales, el enfoque adoptado por Canadá constituye un buen ejemplo de cómo los Estados pueden cuestionar y transformar los supuestos de género que subyacen a las normas, políticas y prácticas convencionales de ciberseguridad. Este enfoque permite a Canadá interpretar e implementar las 11 normas de las Naciones Unidas de manera que respondan a cuestiones de género, mediante su coordinación con la Agenda MPS.[179] Otros países de las Américas también han adoptado políticas exteriores feministas y han llevado esta perspectiva a los debates internacionales sobre ciberseguridad, haciendo un llamado a conectar estos esfuerzos con la Agenda MPS.[180]

La integración de la Agenda MPS y la ciberseguridad, tal como lo proponen diversas académicas y activistas feministas, permite promover concepciones más progresistas de la ciberseguridad que reconozcan y aborden las experiencias, necesidades y vulnerabilidades de hombres, mujeres, niños, niñas y personas de diversas identidades, expresiones y orientaciones sexuales de todas las edades. Por lo tanto, la incorporación de la ciberseguridad en la Agenda MPS —incluidos los planes de acción nacionales— representa una actualización necesaria para abordar de manera más efectiva las dimensiones digitales de los conflictos contemporáneos, permitiendo reconocer y enfrentar las amenazas que las tecnologías digitales y el ciberespacio suponen para la paz y los procesos de construcción de paz liderados por mujeres.[181]

3.2 Chile: Un enfoque con perspectiva de género en las estrategias nacionales de ciberseguridad

El caso de Chile ilustra cómo los Estados pueden integrar la perspectiva de género en la implementación de las normas de las Naciones Unidas (de forma explícita o implícita) a nivel nacional, a través de estrategias y planes de acción en ciberseguridad.[182]

¿Qué hace que este caso sea relevante para una ciberseguridad con perspectiva de género?

Las estrategias nacionales de ciberseguridad son documentos clave de política pública diseñados para abordar el panorama de ciberseguridad de un país. Son fundamentales tanto para la paz y seguridad internacionales[183] como para la implementación, a nivel nacional, de las 11 normas de las Naciones Unidas sobre el comportamiento responsable de los Estados en el ciberespacio. Chile fue el primer país de América Latina en integrar consideraciones específicas de género en su Política Nacional de Ciberseguridad (PNCS), y fue más allá que otras estrategias comparables que, en cambio, hacían referencias más generales a los derechos humanos.[184] En este sentido, el caso de Chile constituye un ejemplo práctico positivo de implementación que responde a cuestiones de género de las 11 normas. Asimismo, representa un ejemplo de buenas prácticas en políticas públicas, ya que el Estado llevó a cabo una evaluación de género de su estrategia de ciberseguridad con el objetivo de identificar áreas de mejora.

¿Cuáles son las políticas y las medidas que Chile está utilizando para una implementación con perspectiva de género de las normas de la ONU?

La PNCS de Chile 2017–2022 establece, entre sus objetivos, el mandato del Estado de proteger los derechos de las personas en el ciberespacio. El documento señala que estos esfuerzos tomarán especialmente en cuenta los derechos de los grupos vulnerables y que se utilizará un enfoque de género "que permita hacer visibles y enfrentar las desigualdades que enfrentan los diversos usuarios del ciberespacio".[185] La elaboración de una estrategia nacional de ciberseguridad que sitúe en el centro la protección de la seguridad de las personas y el ejercicio de los derechos humanos en el ciberespacio se alinea con una interpretación y una implementación con enfoque de género de la *Norma a*.

El trabajo de Chile para integrar las obligaciones de respetar, proteger y garantizar los derechos humanos, incluido el derecho a la libertad de expresión, como parte de su estrategia de ciberseguridad, destaca que "en los esfuerzos en materia de derechos fundamentales se considerarán especialmente los derechos de grupos vulnerables",[186] y constituye un ejemplo de implementación interseccional y con enfoque de género de la Norma e. La estrategia enfatiza la protección de los niños, niñas y adolescentes, personas de la tercera edad, personas con discapacidad y minorías étnicas, al tiempo que incorpora un enfoque de género.

Entre noviembre de 2022 y enero de 2023, la autoridad nacional de ciberseguridad de Chile, que opera bajo el Ministerio del Interior y Seguridad Pública, llevó a cabo una evaluación de la PNCS 2017–2022, que incluyó una evaluación externa de la política con un enfoque específico en género. Esta auditoría de género fue diseñada para evaluar la implementación de la política, identificar áreas de mejora e incorporar estos aprendizajes en la política de ciberseguridad posterior. La realización de una auditoría de género de la política existente se alinea con la implementación con perspectiva de género de las normas de las Naciones Unidas, y en este caso, en particular, con las *Normas a*, *e* y *g*.

En el caso de la *Norma a*, la auditoría proporciona una línea de base al evaluar si el enfoque de género está transversalizado en todos los niveles de la gobernanza y la cooperación en ciberseguridad. Para la *Norma e*, implica revisar las prácticas, políticas y leyes existentes en materia de ciberseguridad con el fin de evaluar su cumplimiento con la igualdad de género y los derechos humanos. En cuanto a la *Norma g*, la auditoría contribuye a evaluar hasta qué punto el género está integrado en el desarrollo de capacidades en ciberseguridad y en la construcción más amplia de una cultura global de ciberseguridad.

La evaluación señaló que la PNCS solo incluía una acción que mencionaba explícitamente el enfoque de género (la Acción 18), la cual tenía como objetivo desarrollar una cultura de ciberseguridad mediante, entre otras actividades, el lanzamiento de una campaña de ciberseguridad con énfasis en los sectores vulnerables y con perspectiva de género.[187] La evaluación externa observó que la campaña fue efectivamente implementada, pero careció del énfasis anunciado en los sectores vulnerables y en la perspectiva de género.[188]

La evaluación también adopta una visión amplia de las consideraciones de género dentro del plan de acción de la PNCS, evaluando avances y desafíos más allá de esta única acción. La evaluación concluyó que se observó un mayor avance en la integración de una perspectiva de género interseccional de lo que originalmente se había previsto en la PNCS. De las 41 medidas del plan de acción, se identificaron siete como relacionadas con el género. Asimismo, se registraron avances en la integración de la perspectiva de género en cuatro de los cinco objetivos generales de la PNCS. En particular, se observaron progresos en la incorporación de consideraciones de género en las acciones orientadas a promover la cultura y la educación en ciberseguridad (Objetivo C de la PNCS).

La evaluación también reconoció la promoción que ha hecho Chile de un enfoque de género en el marco de la OEA. Asimismo, recomendó que Chile contribuyera al trabajo sobre género en los espacios internacionales de ciberseguridad, como en los debates del Grupo de Trabajo de Composición Abierta (OEWG) de las Naciones Unidas sobre el uso de las TIC por parte

de los Estados. El papel activo de Chile en foros internacionales y regionales de ciberseguridad, abogando por perspectivas de género, puede verse también como la operacionalización de la *Norma a* en lo que respecta a la cooperación interestatal.[189]

Según la evaluación, también se registraron avances en la creación del primer punto de información para la ciudadanía sobre ciberseguridad a través de canales digitales. Asimismo, se desarrollaron y difundieron campañas de prevención dirigidas a los riesgos asociados con la VGFT, especialmente dirigidas a mujeres y adolescentes.[190] Se incorporaron preguntas relacionadas con la ciberdelincuencia en la Encuesta Nacional Urbana de Seguridad Ciudadana, con el objetivo de cerrar la brecha de datos sobre la violencia de género en línea. La inclusión de este tipo de violencia en los esfuerzos contra la ciberdelincuencia, combinada con la creación de mecanismos que faciliten el intercambio de información y la asistencia entre las organizaciones nacionales pertinentes, contribuye a reducir el espacio de operación para actores maliciosos en el ámbito de las TIC; esto puede considerarse alineado con los compromisos de la Norma d sobre cooperación para detener la ciberdelincuencia.

Si bien la evaluación identificó brechas en el análisis de los incidentes de ciberseguridad con enfoque diferenciado por género, también destacó que la implementación de la PNCS incluyó la realización de ejercicios de ciberseguridad con diversas comunidades, con el objetivo de incrementar el conocimiento sobre las brechas y vulnerabilidades en materia de ciberseguridad a nivel nacional. Estos ejercicios, combinados con campañas de sensibilización, constituyen un ejemplo de implementación con perspectiva de género de la Norma j ya que implican la inclusión de comunidades en los procesos de intercambio de información sobre vulnerabilidades en las TIC, el descubrimiento de vulnerabilidades diferenciadas ante incidentes cibernéticos, y la identificación de posibles medidas de mitigación.

La participación de Chile en el *Cyberwomen Challenge de la OEA* (véase el recuadro sobre "Buenas Prácticas") incluyó ejercicios de ciberseguridad, en los cuales una de las participantes –posteriormente contratada por el CSIRT nacional– demostró habilidades técnicas excepcionales. Esto representa un avance en la diversificación de los equipos CERT y CIRT nacionales y un paso hacia la paridad de género, un componente clave de la implementación con perspectiva de género de la *Norma k*. Las actividades de fortalecimiento de capacidades lideradas por la recientemente creada Agencia Nacional de Ciberseguridad, destinadas a fomentar la participación de más mujeres y niñas en el ámbito de la ciberseguridad,[191] también constituyen ejemplos de una implementación con enfoque de género de las normas en su conjunto.

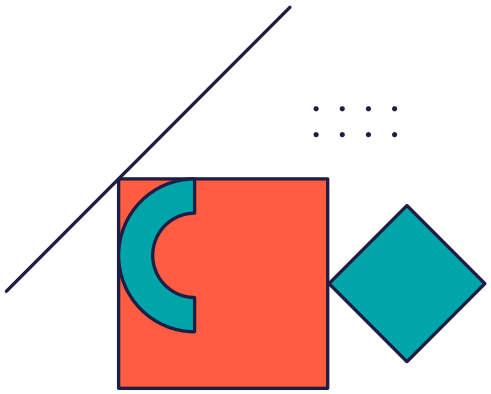
La Política Nacional de Ciberseguridad más reciente (2023–2028),[192] elaborada en paralelo a la evaluación por la autoridad nacional de ciberseguridad, demuestra una continuidad en la incorporación del enfoque de género en el ámbito de la ciberseguridad. Incluye un enfoque más holístico de la igualdad de género, estableciendo entre sus cinco objetivos estratégicos clave la necesidad de garantizar la protección de los derechos de las personas y transversalizar la equidad de género. Una brecha identificada en la evaluación de la PNCS 2017–2022 se relacionaba con la falta de medidas para fomentar la inclusión de género dentro de la industria nacional de ciberseguridad.[193]

La Política Nacional de Ciberseguridad 2023–2028 aborda la participación de las mujeres en el sector, destaca la necesidad de transversalizar el enfoque de género en el desarrollo del ecosistema de ciberseguridad,[194] e incluye medidas orientadas a aumentar el número de mujeres en cargos directivos y en funciones técnicas dentro del ámbito de la ciberseguridad.[195]

¿Cuáles son las lecciones aprendidas de este caso?

La experiencia de Chile ofrece un ejemplo valioso de cómo integrar el enfoque de género en su PNCS y su plan de acción, de una manera que se alinea con la interpretación y la implementación con enfoque de género de las 11 normas de las Naciones Unidas. Abordar necesidades y vulnerabilidades específicas de género frente a las amenazas cibernéticas en el marco de estrategias nacionales permite a los gobiernos coordinar mejor la incorporación del enfoque de género en distintos marcos jurídicos y de política pública.

Asimismo, incrementa la capacidad de los gobiernos para asignar recursos y experiencia técnica al desarrollo e implementación de marcos normativos con perspectiva de género, al enmarcar la igualdad de género como una prioridad de seguridad nacional.[196] El caso también ilustra los beneficios de realizar auditorías de género a las políticas existentes y de evaluar el progreso en la implementación de una ciberseguridad con enfoque de género a través de acciones y medidas concretas. La evaluación llevada a cabo por la autoridad nacional de ciberseguridad permitió dar continuidad a las actividades exitosas y promovió un enfoque de género más holístico e interseccional en la elaboración de la siguiente Política Nacional de Ciberseguridad.



Buenas prácticas relacionadas con la participación y desarrollo de capacidades en ciberseguridad

La brecha de género en la participación en todos los ámbitos de la ciberseguridad ha cobrado relevancia y se ha reconocido como un aspecto crítico para un enfoque de la ciberseguridad con perspectiva de género. Las investigaciones han demostrado que la brecha de género en la participación existe tanto en el sector de las TIC como en el campo específico de la ciberseguridad.[197] A nivel internacional, el OEWG afirmó que el fortalecimiento de capacidades en ciberseguridad debe respetar los derechos humanos y las libertades fundamentales, y ser universal, no discriminatorio, sensible al género e inclusivo.[198] Existen buenos ejemplos de este enfoque en el fortalecimiento de capacidades en ciberseguridad. La iniciativa *Women in International Security and Cyberspace Fellowship*, apoyada por Australia, Canadá, el Reino de los Países Bajos, Nueva Zelanda, el Reino Unido y los Estados Unidos, busca promover la participación significativa de las mujeres en las discusiones sobre ciberseguridad en el marco de las Naciones Unidas como componente de la igualdad de género, y apoyar al OEWG en la incorporación de una perspectiva de género en los debates sobre ciberseguridad [199] La beca ha sido reconocida por algunos Estados como una contribución significativa a la participación significativa y el liderazgo de las mujeres en el OEWG, apoyando a mujeres de 35 países para representar a sus Estados en las discusiones del grupo.[200]

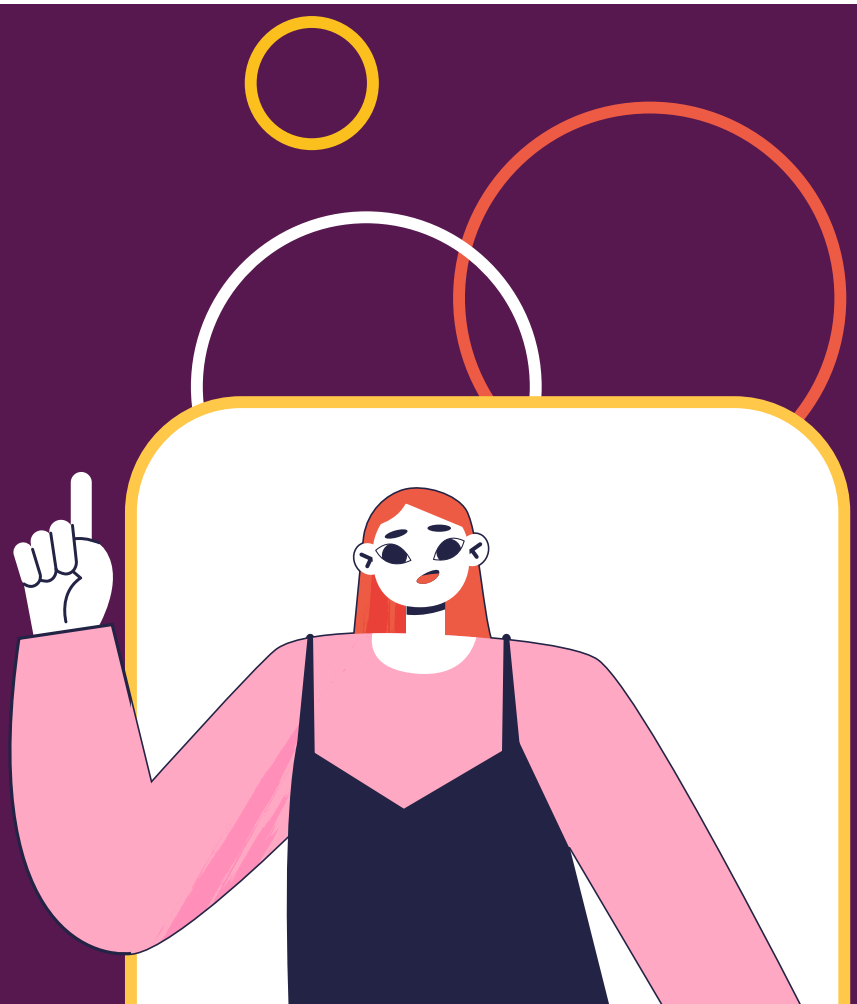
Her CyberTracks, una iniciativa respaldada por la Unión Internacional de Telecomunicaciones (UIT)[201], busca empoderar a mujeres de diferentes regiones en el ámbito de la ciberseguridad mediante formación especializada y mentoría en políticas y diplomacia, respuesta a incidentes y justicia penal. Esta iniciativa ofrece a las participantes acceso a formación, oportunidades de establecer redes de contacto y mentoría personalizada con líderes senior en ciberseguridad.

Diversos esfuerzos en América Latina y el Caribe destacan como buenas prácticas para abordar la brecha de género en ciberseguridad. La Red de Empoderamiento de Mujeres en Ciberseguridad (WiCE) del CICTE/OEA tiene

como objetivo impulsar un cambio en la industria de la ciberseguridad "creando una plataforma para que las mujeres colaboren, compartan conocimientos y se apoyen mutuamente".[202] Esta red, compuesta por más de 800 mujeres que trabajan en el ámbito de la ciberseguridad, busca equilibrar la distribución de oportunidades y recursos dentro del sector.

Específicamente, en el ámbito de la respuesta a incidentes —un entorno a menudo descrito como carente de diversidad en género, cultura y geografía[203]— el *Cyberwomen Challenge* anual de la OEA (actualmente reemplazado por la iniciativa SheSecures) se implementó entre 2018 y 2023 para fortalecer las habilidades en ciberseguridad de mujeres en la industria de las TIC en toda América Latina. Esta iniciativa buscaba cerrar tanto la brecha de diversidad como la de habilidades, contribuyendo finalmente a un panorama de ciberseguridad más seguro e inclusivo. A lo largo de estos años, más de 1 900 mujeres con experiencia en respuesta a incidentes, investigación de amenazas y seguridad de infraestructuras participaron en esta iniciativa. [204]

A nivel nacional, varias estrategias y políticas de ciberseguridad destacan la necesidad de mejorar las capacidades y fomentar una cultura de ciberseguridad que tenga en cuenta la perspectiva de género. Por ejemplo, el Objetivo 5.1 de la Estrategia Nacional de Seguridad de Ecuador (2022–2025)[205] y la Línea de Acción 6.2 del proyecto de Estrategia Nacional de Ciberseguridad de Uruguay se centran en desarrollar y fortalecer las capacidades cibernéticas. Cada una de estas políticas incluye una acción clave dedicada a promover el desarrollo de capacidades para grupos que enfrentan desigualdades y vulnerabilidades. [206] El análisis de estas medidas en el marco de las 11 normas de la ONU revela que la implementación con perspectiva de género (especialmente de las *Normas g* y *k*) requiere el fortalecimiento de capacidades y otras acciones orientadas a construir una cultura global de ciberseguridad inclusiva.



3.3 Costa Rica: Adopción de enfoques con perspectiva de género en ciberseguridad tras incidentes cibernéticos de gran alcance

Este caso ilustra cómo los incidentes maliciosos relacionados con las TIC pueden concienciar sobre las implicaciones en derechos humanos y género de la ciberseguridad, impulsando el compromiso para abordar estas inequidades a niveles nacional, regional e internacional.

¿Qué hace que este caso sea relevante para una ciberseguridad con perspectiva de género?

En 2022, Costa Rica sufrió importantes incidentes de ransomware que afectaron a organismos gubernamentales y comprometieron gran parte de la infraestructura crítica del país.[207] Los ataques provocaron la caída de sistemas, lo que generó graves interrupciones en la capacidad del gobierno para recaudar impuestos y aranceles aduaneros, así como para prestar servicios esenciales como la atención sanitaria. Se reprogramaron citas médicas, se perdieron o alteraron los cronogramas quirúrgicos, y el personal médico no pudo acceder al historial clínico de pacientes nuevos.[208] La respuesta de Costa Rica ante la COVID-19, incluyendo los sistemas de rastreo y seguimiento de contactos, también se vio afectada negativamente, ya que los registros médicos estuvieron temporalmente inaccesibles.[209] Los incidentes incluyeron además la exposición y filtración de datos personales y sensibles.[210]

Las investigaciones existentes sobre infraestructura, las divisiones de género en el trabajo social y de cuidados, y anteriores incidentes que afectaron infraestructuras críticas, indican que las operaciones dirigidas contra servicios esenciales afectan negativamente el acceso a la educación y a la atención sanitaria, entre otros sistemas. Las filtraciones de datos personales afectan no solo la privacidad de las mujeres y de las personas con diversas identidades, expresiones y orientaciones sexuales, sino también sus derechos sexuales y reproductivos, su dignidad y su desarrollo personal.[211]

¿Cuáles son las políticas y medidas utilizadas para la implementación con perspectiva de género de las normas de las Naciones Unidas?

La magnitud y gravedad de los incidentes en Costa Rica impidieron la recolección inmediata de datos detallados sobre sus efectos en los derechos humanos y las dimensiones de género. Sin embargo, testimonios documentados en la prensa evidenciaron los impactos humanos y de género de estos ataques. Una madre relató que no pudo acceder en línea a insumos especiales para su hijo autista de tres años, mientras que una docente denunció que pasó meses sin recibir su salario. Como consecuencia, tuvo que comprar materiales escolares con sus propios recursos, lo que le generó estrés y afectó los derechos de sus estudiantes.[212] Los incidentes de 2022 llevaron a Costa Rica a priorizar la ciberseguridad como un área clave en materia de políticas públicas.[213] Más importante aún, los ataques generaron conciencia sobre las implicaciones en materia de derechos humanos y de género derivadas de las fallas en ciberseguridad, y propiciaron un compromiso por abordar estas desigualdades. Las respuestas políticas adoptadas tras los incidentes incluyeron lo siguiente:

- Se adoptó la Estrategia Nacional de Ciberseguridad 2023–2027 con enfoque transversal de género e igualdad, elaborada tras un proceso de consulta con múltiples partes interesadas.[214] La estrategia aborda de forma directa los supuestos de género y otras desigualdades asociados a la ciberseguridad mediante

un enfoque centrado en las personas e inclusivo en términos de género. Esto se alinea con un enfoque con perspectiva de género de las Normas a y e, al fortalecer la ciberseguridad mediante una política nacional eficaz que promueve simultáneamente los derechos humanos.

■ La estrategia también busca abordar los riesgos e impactos diferenciados por género que generan las amenazas cibernéticas. Pretende responder a las necesidades complejas e interseccionales de las personas en Costa Rica, basadas en el género, la orientación sexual, la raza, la religión, la etnia, la clase social y otros factores. [215] En términos prácticos la Estrategia Nacional de Ciberseguridad tiene como objetivo:

- Establecer mecanismos de seguimiento y control para la gestión integral de riesgos de ciberseguridad, incluyendo indicadores que midan los impactos diferenciados por género. [216]

- Fortalecer el manejo de la información relacionada con incidentes de ciberseguridad y establecer la obligación de divulgar información oportuna y confiable sobre los riesgos de ciberseguridad, con especial atención a los riesgos asociados al género y otras interseccionalidades.[217]

■ La estrategia también incorpora la cooperación internacional en sus líneas de acción, incluyendo:

- La promoción de diversos aspectos interseccionales y de género, como la participación activa y efectiva de las mujeres en los debates internacionales sobre ciberseguridad internacional.

- El compromiso de incorporar un componente cibernético en los esfuerzos del Estado por implementar la Agenda MPS.

Esto se alinea con la implementación con perspectiva de género de las *Normas a* y *b* sobre cooperación internacional.

■ Costa Rica también publicó su postura nacional sobre la aplicación del derecho internacional en el ciberespacio, convirtiéndose en el segundo país de la región en hacerlo. El Ministerio de Relaciones Exteriores de Costa Rica presentó esta posición ante el OEWG de las Naciones Unidas en 2023, haciendo un llamado a una mayor protección de las infraestructuras críticas (*Normas f*, *g* y *h*) y reafirmando la importancia de considerar el impacto diferenciado por razón de género de las operaciones cibernéticas, ya que mujeres, niñas, personas LGBTQI+ y otros grupos vulnerables pueden ser particularmente objeto de usos malintencionados de las TIC (todas las normas).[218]

■ Según entrevistas, en el momento de los incidentes, el equipo encargado de la respuesta trabajó durante largas horas sin recibir compensación adicional. Tras los incidentes, se creó una Dirección de Ciberseguridad en el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. El personal de esta unidad creció a más de 20 personas, y el ministerio —ahora liderado por una mujer— también experimentó un aumento presupuestario.[219]

¿Cuáles son las lecciones aprendidas de este caso?

El caso de Costa Rica demuestra cómo, tras incidentes a gran escala, la ciberseguridad emergió como un área de relevancia política, y cómo el interés y el compromiso del país con los derechos humanos y los enfoques de género en ciberseguridad se fortalecieron.

A nivel nacional, el país implementó una estrategia de ciberseguridad con enfoque de género transversalizado. A nivel internacional, Costa Rica promovió una comprensión con perspectiva de género de la infraestructura crítica.[220] Si bien cuestiones como la paridad de género, la inclusividad y la diversidad dentro de los equipos encargados de responder a incidentes requieren una exploración más profunda, la respuesta de Costa Rica ante los incidentes reconoció la necesidad de que el Estado esté preparado para abordar adecuadamente los impactos diferenciados por razón de género de los incidentes cibernéticos.

De cara al futuro, es importante y necesario realizar investigaciones sobre el impacto diferenciado de los incidentes de ransomware según el género u otras interseccionalidades.

4. Ideas para la acción

Esta sección presenta propuestas de acción basadas en los hallazgos del informe.

La idea central consiste en que los Estados y las partes interesadas consideren aplicar el análisis y las preguntas orientadoras presentadas en este informe para una interpretación sensible al género y una implementación que responda a cuestiones de género de las 11 normas de conducta responsable de los Estados. Los Estados y los actores interesados pueden utilizar las preguntas orientadoras (véase la Sección 2) para desarrollar iniciativas de fortalecimiento de capacidades.

El resto de esta sección ofrece sugerencias más específicas para la acción a nivel internacional, regional y nacional. Si bien los Estados son el foco principal de estas propuestas, la implementación efectiva de las normas dependerá de la capacidad y voluntad de los gobiernos para consultar y colaborar de manera significativa con actores clave como el sector privado, la sociedad civil, la comunidad técnica y la academia.

4.1 Acciones a nivel internacional y regional

Gobernanza y diplomacia cibernética

■ Transversalizar una definición de ciberseguridad que responda a cuestiones de género en la participación y cooperación en espacios regionales e internacionales, con el fin de promover la estabilidad y la seguridad en el uso de las TIC.

■ Colaborar con organizaciones intergubernamentales y de normalización para diseñar normas técnicas de ciberseguridad que respondan a cuestiones de género, siguiendo las recomendaciones del informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos sobre los procesos de elaboración de normas técnicas en tecnologías digitales emergentes.[221]

■ Priorizar la protección del acceso al cifrado en la operacionalización, cooperación e implementación de las normas internacionales de ciberseguridad.

■ Cooperar para abordar la proliferación de herramientas cibernéticas que facilitan la violencia de género.

Agenda MPS y ciberseguridad

■ Sensibilizar sobre las conexiones entre la igualdad de género y la ciberseguridad, a fin de incorporar el debate sobre género y ciberseguridad en foros relevantes —por ejemplo, el Consejo de Seguridad de las Naciones Unidas—, en línea con el desarrollo de la Agenda MPS, abordando las dimensiones de género en la seguridad cibernética, digital y de las TIC.

■ Incluir a personas expertas y profesionales en políticas de la Agenda MPS en los procesos de gobernanza y formulación de políticas de ciberseguridad, para asegurar que estas reflejen los enfoques y principios de género, paz y seguridad.

Procesos inclusivos

■ Promover un enfoque multilateral de múltiples partes interesadas en los debates internacionales sobre ciberseguridad y fortalecer la participación y el apoyo a organizaciones de la sociedad civil, en particular a organizaciones de mujeres, LGBTQI+ y otras organizaciones de derechos humanos, en los debates internacionales sobre ciberseguridad.[222]

Desarrollo de capacidades

■ Priorizar el cierre de la brecha digital de género y la brecha de habilidades digitales.

- Alinear los esfuerzos de desarrollo de capacidades en ciberseguridad con las actividades de las agencias de las Naciones Unidas pertinentes, junto con la Agenda MPS.

- Basarse en los compromisos del Pacto Digital Mundial e implementarlos para abordar las barreras estructurales y sistémicas a la participación significativa; proporcionar conectividad digital segura y asequible para todas las mujeres y niñas; ofrecer oportunidades de educación e investigación en STEM de calidad e inclusivas; y promover la participación de mujeres y niñas en todos los roles y en todos los niveles.[223]

- Apoyar a las organizaciones de mujeres, personas LGBTQI+, otras organizaciones de derechos humanos, y a comunidades marginadas y minoritarias para que desarrollen la capacidad de participar de forma independiente en los procesos de gobernanza de la ciberseguridad, mediante financiación y acceso.

- Sostener, financiar y reforzar los esfuerzos de desarrollo de capacidades técnicas y políticas dirigidos específicamente a apoyar a las mujeres y a las personas con orientaciones sexuales, identidades y expresiones de género diversas para que accedan a carreras en el ámbito cibernético, conforme al enfoque basado en principios del OEWG sobre creación de capacidades.

- Promover el desarrollo de capacidades en ciberseguridad de manera inclusiva mediante formaciones periódicas y el intercambio de información sobre planes de emergencia que respondan a cuestiones de género.[224]

Medidas de fomento de la confianza

- Incorporar de forma transversal la perspectiva de género en las discusiones sobre CBMs a nivel regional y global.[225]

- Compartir información relevante sobre experiencias diferenciadas por género en relación con incidentes cibernéticos, fallos y prácticas.

- Compartir definiciones nacionales, estrategias de consulta y datos desglosados de manera interseccional y por género sobre los impactos de los incidentes cibernéticos, así como buenas prácticas en planes y respuestas de emergencia.

- Explorar mecanismos para el intercambio regular, entre regiones, de lecciones aprendidas y buenas prácticas sobre la integración de la igualdad de género en las CBMs.

4.2 Acciones a nivel nacional

Política cibernética

- Incorporar de forma transversal la perspectiva de género en las estrategias nacionales de ciberseguridad y sus planes de acción, e incluir objetivos concretos y medibles, así como indicadores relacionados con el género para el seguimiento y la evaluación de su implementación.[226]

- Integrar de forma transversal la ciberseguridad, la seguridad de las TIC y los derechos digitales en las políticas existentes sobre la Agenda MPS y, cuando corresponda, en los planes de acción nacionales.[227]

  - Impulsar la creación de capacidades cibernéticas para expertas/os en la Agenda MPS e incluirlas/os en los procesos de formulación de políticas de ciberseguridad.

- Generar, en consulta con socios multisectoriales, definiciones operativas que respondan a cuestiones de género, específicas al contexto, sobre ciberseguridad, infraestructura crítica y amenazas cibernéticas.

- Incorporar de forma transversal el enfoque de género en las acciones específicas a nivel internacional de la lista de comprobación para la implementación de las normas voluntarias y no vinculantes del comportamiento responsable de los Estados en el uso de las TIC (anexo A del Informe Anual de Progreso del OEWG 2021–2025 publicado en julio de 2024).

- Desarrollar planes de emergencia y procedimientos con perspectiva de género para responder a incidentes cibernéticos graves y operaciones sobre infraestructura crítica.

- Desarrollar e implementar marcos de protección de datos con enfoque de género que aborden las necesidades específicas de privacidad de mujeres y personas con diversas identidades, expresiones y sexualidades de género.[228]

- Incorporar de forma transversal la ciberseguridad, las TIC y los derechos digitales en la legislación nacional, en las políticas públicas y en los procesos jurídicos sobre derechos humanos.

- Proteger y promover la disponibilidad y el uso del cifrado mediante legislación nacional específica.

- Realizar una auditoría de género de la legislación, políticas y procedimientos existentes relacionados con la prevención, investigación y enjuiciamiento del ciberdelito y el terrorismo, incluido el apoyo a las víctimas, y modificarlos cuando sea necesario.

- Incorporar de forma transversal la perspectiva de género en los procesos existentes de gobernanza sobre no proliferación (licencias de exportación, regímenes de control de armas, etc.) y seguridad de la cadena de suministro de TIC.

- Desarrollar medidas para responsabilizar a actores no estatales que participen en actividades maliciosas relacionadas con las TIC —incluyendo la violencia de género facilitada por tecnologías —, de acuerdo con los estándares de derechos humanos y el debido proceso.

- Desarrollar procedimientos con enfoque de género, que respeten la privacidad y se ajusten a los derechos humanos, para evaluar solicitudes internacionales de cooperación en relación con delitos y terrorismo.

Recopilación de datos e intercambio de información

- Recopilar datos desagregados por género y otras dimensiones de igualdad sobre los efectos de los incidentes cibernéticos a nivel nacional, en consulta con organizaciones de la sociedad civil de mujeres, LGBTQI+ y de derechos digitales.[229]

- Realizar modelos de amenazas cibernéticas con equipos diversos y aplicar una perspectiva de género para comprender las vulnerabilidades cibernéticas y las posibles implicaciones en materia de igualdad de las distintas estrategias de respuesta.[230]

- Financiar investigaciones, en cooperación con el sector privado, la sociedad civil y la academia, sobre los efectos diferenciados de género no intencionados de las tecnologías emergentes, las funciones tecnológicas ocultas o maliciosas, y las prácticas de ciberseguridad.

Procesos inclusivos

- Involucrar y consultar de manera significativa a socios de múltiples partes interesadas —con especial atención a organizaciones de la sociedad civil que abogan por los derechos de las mujeres, personas LGBTQI+ y comunidades marginadas y minoritarias— para desarrollar, implementar y evaluar de forma colaborativa y transparente las políticas y prácticas de ciberseguridad.[231]

    - Evaluar y revisar continuamente la implementación del enfoque de género en las políticas de ciberseguridad, con el respaldo de una participación significativa de la sociedad civil.[232]

- Involucrar a actores especialistas en género a nivel nacional para amplificar sus voces en las discusiones internacionales sobre ciberseguridad.[233]

- Crear un mecanismo transparente de reporte de incidentes cibernéticos e intercambio de información entre el Estado, el sector empresarial y la sociedad civil, con rutas específicas para organizaciones centradas en género y sexualidad.

Cerrar la brecha digital de género

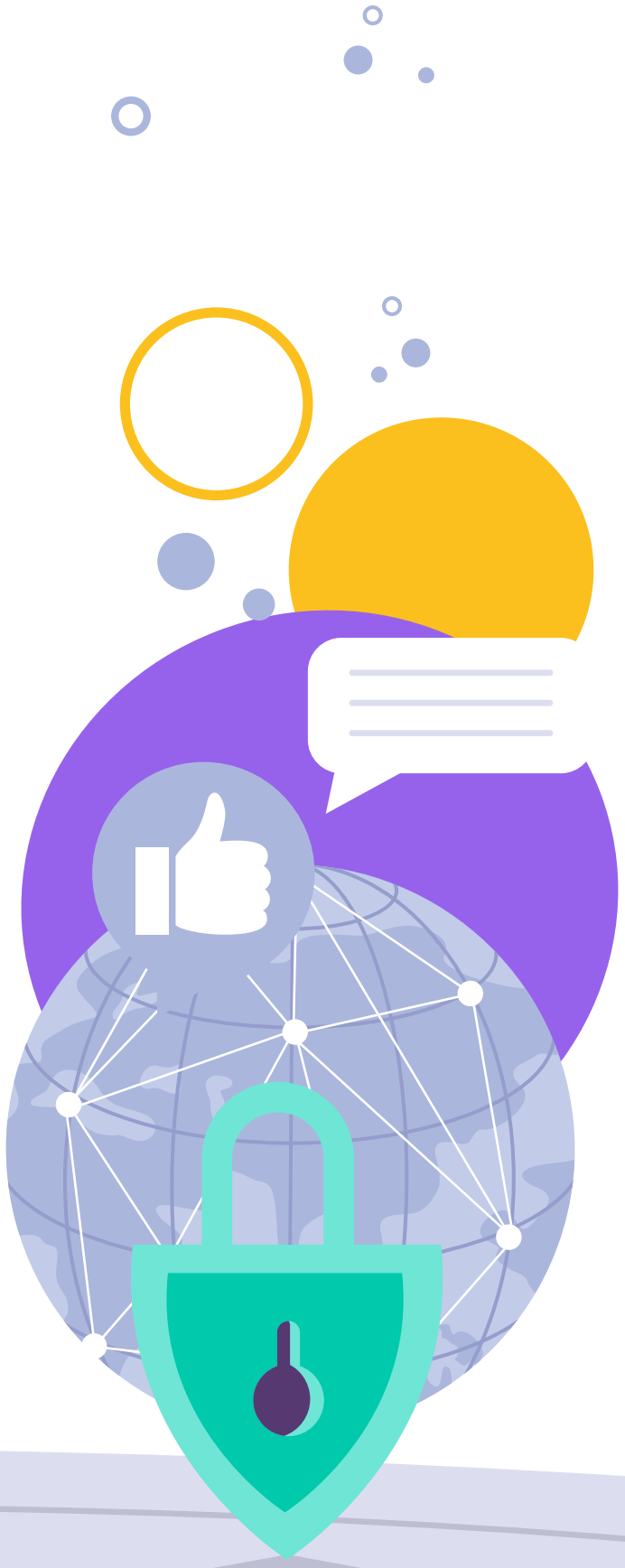
- Priorizar el cierre de las brechas de acceso digital, alfabetización y habilidades digitales con enfoque de género.

  - Cumplir con el compromiso del Pacto Digital Mundial de incorporar de forma transversal una perspectiva de género en las estrategias de conectividad digital para abordar las barreras estructurales al acceso digital significativo, seguro y asequible[234].

- Aspirar a la paridad de género en los equipos técnicos de personas expertas en ciberseguridad (incluidos los CIRT y CERT) y en la formulación e implementación de políticas digitales y de ciberseguridad.

  - Implementar políticas de recursos humanos que respondan a cuestiones de género, en consulta con trabajadoras y trabajadores de identidades, expresiones y orientaciones sexuales de género diversas.

- Desarrollar campañas de sensibilización sobre ciberseguridad en general y sobre riesgos diferenciados por género en colaboración con la sociedad civil.



Referencias

[1] Un incidente de ciberseguridad es "un ataque o intento de ataque contra una computadora o red que haya afectado, o potencialmente pueda afectar, la confidencialidad, integridad o disponibilidad de los datos o sistemas de la red". Gobierno de Nueva Zelanda, Oficina de Seguridad de las Comunicaciones (GCSB, por sus siglas en inglés), "Cyber Security Incidents", 2025, https://nzism.gcsb.govt.nz/resources/faq/cyber-security-incidents. Para definiciones adicionales, véase: https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cybersecurity-incidents; https://csrc.nist.gov/glossary/term/cybersecurity_incident.

[2] Allison Pytlak and Deborah Brown, *Why Gender Matters in Cybersecurity* (Association for Progressive Communications and Women's International League for Peace and Freedom, 2020), https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf;

Chatham House, "Gendered Hate Speech, Data Breach, and State Overreach", 24 de mayo de 2024, https://www.chathamhouse.org/2024/05/gendered-hate-speech-data-breach-and-state-overreach.

[3] Asamblea General, Informe del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, A/76/135, 14 de julio de 2021, https://docs.un.org/es/A/76/135 (párrafo 6).

[4] OEWG, Informe Sustantivo Final (2021),https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf. (disponible solo en inglés)

[5] OEWG (2021-2025), Informe anual sobre los progresos realizados (agosto de 2022), https://undocs.org/en/A/77/275.

[6] OEWG (2021–2025), *Informe anual sobre los progresos realizados* (agosto de 2023),, https://undocs.org/en/A/78/265. Véase también Australia et al., "Gender and the Future Permanent Mechanism" (20 February 2025), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Working_Paper_-_Gender_-_20FEB25_-Uploaded_Version.pdf

[7] Cybil, "Cerrando la brecha de género en la agenda de ciberseguridad -- América Latina y el Caribe", https://cybilportal.org/projects/addressing-the-gender-gap-in-the-cybersecurity-agenda-latin-america-and-the-caribbean/.

[8] OEA, "Grupo de Trabajo sobre Cooperación y Medidas de Fomento de la Confianza en el Ciberespacio", 2024, https://www.oascybercbms.org/index.php/es/

[9] Resolución 44/2023, *Boletín Oficial de la República de Argentina* (4 de septiembre de 2023), https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904; Gobierno de Chile, Política Nacional de Ciberseguridad 2023–2028, https://ciberseguridad.gob.cl/documents/4430/Pol%C3%ADtica_Nacional_de_Ciberseguridad_2023-2028.pdf; Costa Rica, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), Estrategia Nacional de Ciberseguridad 2023–2027 (2023), https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf; Ministerio de Telecomunicaciones y de la Sociedad de la Información, Estrategia Nacional de Ciberseguridad del Ecuador 2022-2025, 35, https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf.

[10] Entre septiembre y diciembre de 2024, las autoras tuvieron el agrado de dialogar con las siguientes personas expertas. No obstante, las conclusiones expuestas en el presente informe, así como cualquier error, son exclusivamente responsabilidad nuestra. Paz Peña, consultora independiente en género y tecnología, incluida su labor en la evaluación de la Política Nacional de Ciberseguridad de Chile (2017–2022); Paula Brenes, exdirectora de Gobernanza Digital del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica, durante los incidentes cibernéticos de mayo de 2022; Gezer Ramiro Molina Colomer, Director Nacional de Ciberseguridad, Costa Rica; Louise Marie Hurel, Investigadora asociada, Royal United Services Institute; Allison Pytlak, investigadora sénior y directora del Programa de Ciberseguridad, *Stimson Center*; Valentin Weber, Investigador sénior, *German Council of Foreign Relations*.

[11] Asamblea General, Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el contexto de la Seguridad Internacional, A/70/174, 22 de julio de 2025, https://docs.un.org/es/A/70/174

[12] International Cyber Policy Centre, *The UN Normas of Responsible State Behaviour in Cyberspace* (Australian Strategic Policy Institute, 2022), https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-Normas-of-responsible-state-behaviour-in-cyberspace.pdf.

[13] Geneva Centre for Security Sector Governance (DCAF), *Gender and Cybersecurity: A Policy Toolbox* (2023), https://www.dcaf.ch/sites/default/files/publications/documents/Gender_Cybersecurity_report_Jan2023.pdf.

[14] R.J. Deibert "Toward a Human-Centric Approach to Cybersecurity", *Ethics & International Affairs* 32, 4 (2018):411-424, doi:10.1017/S0892679418000618.

[15] J.-S. Hofstetter and P. Pourmalek, *Gendering Cybersecurity through the Women, Peace and Security* (Global Network of Women Peacebuilders and ICT4Peace Foundation, 2023), https://ict4peace.org/wp-content/uploads/2023/03/Gendering-Cybersecurity-through-WPS-Final-Report_March-2023.pdf.

[16] ONU Mujeres, "Concepts and definitions", https://www.un.org/womenwatch/osagi/conceptsandefinitions.htm; UNICEF Regional Office for South Asia, *Gender Equality: Glossary of Terms and Concepts (November 2017)*, https://www.unicef.org/rosa/media/1761/file/Gender%20glossary%20of%20terms%20and%20concepts%20.pdf; Canadian Institutes of Health Research, "What is gender? What is sex?" 28 April 2020, https://cihr-irsc.gc.ca/e/48642.html.

[17] Identidad de género "se define generalmente como una percepción interna y profunda del propio género. Puede coincidir o no con el sexo asignado al nacer." Expresión de género "se refiere a la forma en que las personas representan externamente su género, a través de sus acciones y su apariencia, como, por ejemplo, con su vestimenta, el habla y gestos. Algunos términos para describir la expresión de género son "masculino", "femenino" y "andrógino". Para muchas personas, su expresión de género coincide con las ideas que nuestras sociedades consideran adecuadas para su género. Para otras personas no es así. La expresión de género de una persona puede variar y es distinta de su identidad de género, orientación sexual y características sexuales." Libre e Iguales, Naciones Unidas, "Definiciones", https://www.unfe.org/know-the-facts/definitions/.

[18] Libres e Iguales, Naciones Unidas", https://www.unfe.org/know-the-facts/definitions. Véase también: Corte Interamericana de Derechos Humanos, Identidad de género, e igualdad y no discriminación a parejas del mismo sexo. Obligaciones estales en relación con el cambio de nombre, la identidad de género y los derechos derivados de un vínculo entre parejas del mismo sexo. Opinión Consultiva OC-24/17 (Serie A Nº 24), emitida el 24 de noviembre de 2017, https://www.corteidh.or.cr/docs/opiniones/seriea_24_esp.pdf

[19]Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *"Experto Independiente sobre orientación sexual e identidad de género"*, https://www.ohchr.org/en/special-procedures/ie-sexual-orientation-and-gender-identity. Véase también: Corte Interamericana de Derechos Humanos, Identidad de género, e igualdad y no discriminación a parejas del mismo sexo. Obligaciones estales en relación con el cambio de nombre, la identidad de género y los derechos derivados de un vínculo entre parejas del mismo sexo. Opinión Consultiva OC-24/17 (Serie A Nº 24), emitida el 24 de noviembre de 2017. https://www.corteidh.or.cr/docs/opiniones/seriea_24_esp.pdf

[20] "Se trata de términos de uso frecuente a escala internacional y en algunos contextos (aunque no en todos). Los términos que utilizan las personas para referirse a su orientación sexual, identidad de género, expresión de género y características sexuales, así como a la forma en que se habla de ellos, pueden depender del lugar, el idioma, la generación a la que pertenecen y a otros contextos culturales." Libres e Iguales, Naciones Unidas, "Definiciones", https://www.unfe.org/know-the-facts/definitions. Véase también: Corte Interamericana de Derechos Humanos, Identidad de género, e igualdad y no discriminación a parejas del mismo sexo. Obligaciones estales en relación con el cambio de nombre, la identidad de género y los derechos derivados de un vínculo entre parejas del mismo sexo. Opinión Consultiva OC-24/17 (Serie A Nº 24), emitida el 24 de noviembre de 2017, https://www.corteidh.or.cr/docs/opiniones/seriea_24_esp.pdf

[21] UNICEF Regional Office for South Asia, Gender Equality: Glossary of Terms and Concepts (November 2017), https://www.unicef.org/rosa/media/1761/file/Gender%20glossary%20of%20terms%20and%20concepts%20.pdf. Véase también UN Women, "Concepts and definitions", https://www.un.org/womenwatch/osagi/conceptsandefinitions.htm.

[22] Para reflexionar sobre la marginación de manera sensible al contexto, véase: Global Partners Digital (GPD), *Inclusive Cyber Norms Toolkit* (August 2023), https://www.gp-digital.org/wp-content/uploads/2023/08/Inclusive-Cyber-Normas-Toolkit_GPD.pdf.

[23]DCAF, *Gender and Cybersecurity*; Kimberle Crenshaw, "Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Colour", *Stanford Law Review* 43, 6 (1991): 1241–1299, https://doi.org/10.2307/1229039; Combahee River Collective, "A Black Feminist Statement", *Women's Studies Quarterly 42*, 3/4 (2014): 271–280, https://www.jstor.org/stable/24365010.

[24] Para tener una visión general sobre género y derecho internacional, véase: Kate Ogg y Susan Harris Rimmer, *Research Handbook on Feminist Engagement with International Law* (London: Edward Elgar Publishing, 2019); Hilary Charlesworth, Christine Chinkin y Shelley Wright, "Feminist approaches to international law", *American Journal of International Law 85*, 4 (1991): 613–645. Para más información sobre igualdad de género, derecho y las Américas, véase: https://www.oas.org/en/cim/.

[25]Véase, por ejemplo: Maysha Alam, *Inseparable but Not Interchangeable: Inclusion and Gender Sensitivity for Effective Peace Mediation* (United Nations University Centre for Policy Research, 2022), https://collections.unu.edu/eserv/UNU:8668/UNU_InclusivePeacebuilding.pdf.

[26]Véase: ONU Mujeres, *Plan Estratégico de ONU Mujeres 2022–2025* (Nueva York: Organización de las Naciones Unidas, 2021), https://www.unwomen.org/sites/default/files/2022-10/UN-Women-Strategic-Plan-2022-2025-brochure-es.pdf

[27] División para el Adelanto de la Mujer de las Naciones Unidas. *Transversalización de la perspectiva de género: estrategia para promover la igualdad de género,* (Nueva York: Naciones Unidas, 2001), https://www.un.org/womenwatch/daw/csw/GMS.PDF.

[28] Asamblea General, Informe del Consejo Económico y Social correspondiente a 1997, A/52/3, 18 de septiembre de 1997.

[29] UNIDIR, *Enfoques de Género en la Ciberseguridad: Diseño, defensa y respuesta* (Ginebra: UNIDIR, 2023), https://unidir.org/publication/enfoques-de-genero-en-la-ciberseguridad-diseno-defensa-y-respuesta/

[30]DCAF, *Gender and Cybersecurity.*

[31] Asamblea General, A/RES/78/213, 2023, https://docs.un.org/es/A/RES/78/213

[32]Hofstetter y Pourmalek, *Gendering Cybersecurity*; Anwar Mhajne and Crystal Whetstone, "A feminist cybersecurity: addressing the crisis of cyber (in) security", *International Affairs 100*, 6 (2024): 2341–2360.

[33]Cynthia Enloe, *Bananas, beaches and bases: Making feminist sense of international politics* (University of California Press, 2014).

[34]Cynthia Enloe, *Twelve feminist lessons of war* (University of California Press, 2023); UNIDIR, *Gender Approaches to Cybersecurity*; DCAF, *Gender and Cybersecurity*.

[35] DCAF, *Gender and Cybersecurity.*

[36] Los ciberdaños se definen como "efectos que se originan en el ciberespacio o se agravan en él, provocando disminución, daño o destrucción de áreas de valor humano, especialmente el cuerpo, la vida afectiva y la comunidad'. Chatham House, "Gendered hate speech, data breach and state overreach", 24 May 2024, https://www.chathamhouse.org/2024/05/gendered-hate-speech-data-breach-and-state-overreach/01-introduction.

[37]ONU Mujeres, "Repository of UN Women's work on technology-facilitated violence against women and girls", 2025,
https://www.unwomen.org/en/digital-library/publications/2024/10/repository-of-un-womens-work-on-technology-facilitated-gender-based-violence.

[38]Amnistía Internacional, "#Toxic Twitter – No permitas que un Twitter intoxicado silencie a las mujeres", 21de marzo de 2018, www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/; Plan International, *Free to Be Online? Girls' and young women's experiences of online harassment* (Surrey, UK: Plan International, 2020), https://plan-international.org/publications/freetobeonline.

[39]Nicola Henry and Rebecca Umbach, "Sextortion: Prevalence and correlates in 10 countries", *Computers in Human Behavior 158* (2024): 108298.

[40]T.J. Kasperbauer, "Protecting Health Privacy Even When Privacy is Lost", *Journal of Medical Ethics 46*, 11 (2019), http://doi.org/10.1136/medethics-2019-105880; Privacy International, "Why Does Reproductive Health Surveillance in India Need Our Urgent Attention?" 24 February 2020, https://privacyinternational.org/long-read/3368/why-does-reproductive-health-surveillance-india-need-our-urgent-attention; J. Davis, "300,000 Records Breached in Ransomware Attack on Pennsylvania Health System", Healthcare IT News, 26 July 2017, https://www.healthcareitnews.com/news/300000-records-breached-ransomware-Attack-pennsylvania-health-system; BBC News, "Trans Charity Mermaids UK 'Deeply Sorry' for Data Breach", 16 June 2019, https://www.bbc.co.uk/news/uk-48652970.

[41]Pytlak and Brown, *Why Gender Matters*, 9–12; Access Now, "Why Internet Shutdowns Are Even Worse for Women", 8 March 2023, https://www.accessnow.org/internet-shutdowns-international-womens-day/.

[42]Unión Internacional de Telecomunicaciones, "Brecha digital de género", 2023, https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-the-gender-digital-divide/.

[43] Como se indica en el informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, titulado "Justicia de género y libertad de expresión" (A/76/258, 2021), las disparidades en el acceso a Internet surgen a partir de otras disparidades a las que se enfrentan las mujeres en la sociedad y que se derivan de sus contextos económicos, sociales, políticos y culturales. Por ejemplo, la cultura y las normas suelen pasarse por alto y resultan especialmente relevantes en el contexto de la brecha digital de género. La barrera no radica únicamente en la asequibilidad, sino también en la autonomía económica y en cómo las mujeres perciben la relevancia de la tecnología. En algunas culturas rurales donde los grupos de mujeres son fuertes, un desafío clave radica en la falta de reconocimiento de que estos grupos podrían financiar su propia conectividad. Además, investigaciones documentan que el miedo al acoso, los riesgos a la reputación y el control masculino sobre los dispositivos de las mujeres limitan aún más el acceso y la participación equitativa de género en los espacios en línea. Véase también: APC, Bridging the Gender Digital Divide from a Human Rights Perspective (March 2021), https://www.apc.org/en/pubs/bridging-gender-digital-divide-human-rights-perspective-apc-submission-office-high; N. Sambasivan et al., "They Don't Leave Us Alone Anywhere We Go", *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (2019): 1–14, https://doi.org/10.1145/3290605.3300232.

[44]UNICEF clasifica estas actividades en tres grandes categorías de habilidades digitales: habilidades básicas, que incluyen tareas sencillas como mover archivos o carpetas; habilidades estándar, como trabajar con hojas de cálculo, crear presentaciones o configurar software; y habilidades avanzadas, que incluyen la capacidad de escribir código de programación. Para más información, véase: UNICEF, *Bridging the Gender Digital Divide* (May 2023), https://data.unicef.org/resources/ictgenderdivide.

[45]UNICEF, *Bridging the Gender Digital Divide.*

[46]United Nations Institute for Disarmament Research (UNIDIR), "Gender in Cyber Diplomacy", https://unidir.org/wp-content/uploads/2023/05/Gender-in-Cyber-Diplomacy_Factsheet.pdf; ISC2, *Women in Cybersecurity: Women in the Profession* (April 2024), https://www.isc2.org/Insights/2024/04/Women-in-Cybersecurity-Report-Women-in-the-Profession.

[47]Government of Australia, "Statement on Gender: Agenda Item 6, Open-Ended Working Group on Information and Communication Technologies", (2024), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Australia_-_agenda_item_6_-_statement_on_gender.pdf; Government of Canada, "Annex on Gender Considerations: Canadian Position Paper for the Open-Ended Working Group on ICTs (2021–2025)", (2021), https://documents.unoda.org/wp-content/uploads/2021/12/Canadian-position-paper-2021-25-OEWG-final-Dec-6_Annex-Gender-Considerations.pdf.

[48]Asamblea General, Informe del Grupo de Expertos Gubernamentales sobre el Avance del Comportamiento Responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional, A/76/135, 14 julio 2021, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

[49]OEWG, *Informe Sustantivo Final, 2021.*

[50]Asamblea General, "Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional", A/79/214, 22 de julio de 2024, https://docs.un.org/es/A/79/214

[51]UNIDIR, *Advancing Gender Considerations in the Cyber OEWG* (Geneva: UNIDIR, 2023), https://unidir.org/advancing-gender-considerations-in-the-cyber-oewg/; Gobierno de Suiza, "General views on the Zero Draft Report" (2022), https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/switzerland-comments-zero-draft.pdf; Gobierno de Chile, "Comentarios y sugerencias de Chile sobre el Borrador Cero del primer informe anual de progreso de Grupo de Trabajo de Composición Abierta (OEWG) 2021-2025 del Grupo de Expertos Gubernamentales sobre seguridad de las TIC, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/chile-comments-zero-draft.pdf; *Cyber Peace & Security Monitor 1, 7* (18 February 2020), https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.7.pdf.

[52]Asamblea General, OEWG, Chair's Summary, A/AC.290/2021/CRP.3, 10 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf; Government of Canada, "Canada's Proposal for the Report of the 2019–20 United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security", https://www.un.org/disarmament/wp-content/uploads/2019/09/canadian-position-Paper-oewg-en.pdf; General Assembly, A/7/275; Government of Italy, *Italian Position Paper on 'International Law and Cyberspace'* (December 2021), https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/italy-positionpaper-december2021.pdf; Government of Australia, "Australia's initial comments on the Zero Draft of the first annual progress report of the UN Open-Ended Working Group in the field of information and telecommunications in the context of international security 2021-2025", https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/australia-comments-zero-draft.pdf; Gobierno de Costa Rica, "Posición de Costa Rica sobre la Aplicación del Derecho Internacional en el Ciberespacio",, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/wp-costa-rica.pdf; Government of Canada, "Updated Canadian Text Proposals", (November 2020), https://front.un-arm.org/wp-content/uploads/2020/12/updated-canadian-text-proposals-nov-30.pdf; Government of Canada, "Canada's Proposal for the Work of the 2021-25 United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security", https://documents.unoda.org/wp-content/uploads/2021/12/Canadian-position-paper-2021-25-OEWG-final-Dec-6_Annex-Gender-Considerations.pdf.

[53]El informe desarrollará este concepto en las secciones siguientes. Véase, por ejemplo, el análisis de la *Norma g* y el recuadro sobre buenas prácticas relacionadas con la creación de capacidad en ciberseguridad.

[54]Australia et al., "Gender and the Future Permanent Mechanism" (20 February 2025), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Working_Paper_-_Gender_-_20FEB25_-Uploaded_Version.pdf.
See also:

"Working paper for a Programme of Action (PoA) to advance responsible State behavior in the use of ICTs in the context of international security", (2021), https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdfhttps://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf; Government of Canada, "Canada's Proposal for the Work of the 2021-25 United Nations Open-Ended Working Group"; CyberPeace Institute, "Statement on the Cyber Programme of Action", 11 July 2023, https://cyberpeaceinstitute.org/news/statement-cyber-programme-of-action/; Women's International League for Peace and Freedom, *Advancing a Global Cyber Programme of Action* (May 2022), https://reachingcriticalwill.org/images/documents/Publications/report_cyber-poa_final_May2022.pdf.

[55] UNIDIR, *The Role of Regional Organizations in Strengthening Cybersecurity and Stability: Experiences and Opportunities* (2021), https://unidir.org/files/publication/pdfs/the-role-of-regional-organizations-in-strengthening-cybersecurity-and-stability-experiences-and-opportunities-en-789.pdf.

[56] Cybil, "Cerrar la brecha de género en la agenda de ciberseguridad".

[57] OEA, "Medidas de Fomento de la Confianza en el Ciberespacio".

[58] OEA, "Medidas de Fomento de la Confianza en el Ciberespacio"; OEWG, Argentina et al., "Cyber CBMs in Action", https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/OEWG6-Joint-WP.pdfhttps://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/OEWG6-Joint-WP.pdf.

[59] Hofstetter y Pourmalek, *Gendering Cybersecurity.*

[60] Ibid.

[61] Consejo de Seguridad, S/RES/1325 (2000), https://docs.un.org/es/S/RES/1325(2000)

[62] UNIDIR, *System Update: Towards a Women, Peace and Cybersecurity Agenda* (Geneva: UNIDIR, 2023), https://unidir.org/wp-content/uploads/2023/05/UNIDIR_System_Update.pdf; ONU Mujeres, *Action Brief: Women, Peace and Cybersecurity—Promoting Women's Engagement in Cybersecurity* (UN Women Regional Office for Asia and the Pacific, 2020), https://asiapacific.unwomen.org/sites/default/files/Field%20Office%20ESEAsia/Docs/Publications/2020/06/Action%20Brief%20%20WPS%20%20CYBERSECURITY16620final.pdf; Hofstetter y Pourmalek, Gendering Cybersecurity; Anwar Mhajne y Alexis Henshaw, eds. Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions (Oxford University Press, 2024).

[63] Asamblea General, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Chair's Summary, A/AC.290/2021/CRP.3, 10 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

[64] ONU Mujeres, *Promoting Women's Peace and Security in the Digital World* (Bangkok: UN Women Regional Office for Asia and the Pacific, n.d.), https://asiapacific.unwomen.org/en/what-we-do/peace-and-security/promoting-womens-peace-and-security-in-the-digital-world.

[65] UNIDIR, *Actualización del Sistema: hacia una Agenda de Mujeres, Paz y Ciberseguridad* (Ginebra, 2023).

[66] Para los principales análisis académicos realizados hasta la fecha sobre la relación entre la ciberseguridad y la Agenda MPS, véase: Crystal Whetstone y K.C. Luna. "A Call for Feminist Insights in Cybersecurity Implementing United Nations Security Council Resolution 1325 on Women, Peace, and Security in Cyberspace", en *Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions* (2024), 25; Mhajne y Whetstone, "A feminist cybersecurity".

[67] Hofstetter y Pourmalek, *Gendering Cybersecurity.*

[68] Para obtener una guía paso a paso sobre la implementación y planificación de las normas cibernéticas en general, véase: International Cyber Policy Centre (ICPC), *Guidance on Implementation for ASEAN*, 2022.

[69] Comité Internacional de la Cruz Roja (CICR). "Género y Derecho Internacional Humanitario", 2024, https://www.icrc.org/es/derecho-y-politicas/genero-y-dih

[70] Asamblea General, Informe del Grupo de Expertos Gubernamentales sobre el Avance del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, A/76/135, 14 de julio de 2021 https://docs.un.org/es/A/76/135

[71] Asamblea General, OEWG (2021–2025), Borrador del Informe de Progreso Anual, A/AC.292/2024/CRP.1, 12 de julio de 2024. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_11_July_2024.pdf.

[72] Este informe también se fundamenta en el enfoque y en la guía para la implementación de normas elaborada por el Centro Internacional de Políticas Cibernéticas (ICPC, por sus siglas en inglés) titulada *Guidance on Implementation for ASEAN.*

[73] ICPC, *Guidance on Implementation for ASEAN*, 28; Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025, Letter from Chair, 20 February 2024, 2, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_20_February_2024.pdf.

[74] APC y Global Partners Digital, "Unpacking the GGE's framework on responsible state behaviour: Cyber norms", https://www.apc.org/sites/default/files/UnpackingGGGCyberNormas.pdf.

[75] ONU Mujeres, *Gender Mainstreaming: A Global Strategy for Achieving Gender Equality and the Empowerment of Women and Girls* (New York: UN Women, 2020), 5, https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2020/Gender-mainstreaming-Strategy-for-achieving-gender-equality-and-empowerment-of-women-girls-en.pdf.

[76] Hofstetter y Pourmalek, *Gendering Cybersecurity*; Australia et al., "Gender and the Future Permanent Mechanism".

[77] ONU Mujeres, "Facts and Figures: Economic Empowerment", https://www.unwomen.org/en/what-we-do/economic-empowerment/facts-and-figures; Toni Schmader and Katharina Block, "Why Do Women Care More & Men Couldn't Care Less?" *Dædalus 154*, 1 (2025): 82–97; European Institute for Gender Equality, "Gender Statistics Database", https://eige.europa.eu/gender-statistics/dgs/data-talks/covid-19-pandemic-reinforced-gender-inequalities-women-took-more-intensified-informal-care-and-housework-demands

[78] Pytlak y Brown, *Why Gender Matters.*

[79] Pavlina Pavlova, "Confronting Gendered Harm in Cyberspace Is Not a Matter of Social Justice – It's a National Security Imperative", Just Security, 17 February 2025, https://www.justsecurity.org/107353/gendered-harm-cyberspace-not-social-justice-a-security-imperative/; Mustafa Koroglu, Bridget R. Irwin and Karen A. Grépin, "Effect of power outages on the use of maternal health services: evidence from Maharashtra, India", *BMJ Global Health 4*, 3 (2019): e001372; Jianpeng Xiao et al., "Increased risk of multiple pregnancy complications following large-scale power outages during Hurricane Sandy in New York State", *Science of the Total Environment 770* (2021): 145359.

[80] Pavlova, "Confronting Gendered Harm in Cyberspace"; Australia et al., "Gender and the Future Permanent Mechanism".

[81] Pytlak y Brown, *Why Gender Matters*; Government of Canada, "Proposed Norms guidance text", https://front.un-arm.org/wp-content/uploads/2021/02/new-updated-Normas-guidance-text-feb-11-clean.pdf.

[82] Ioannis Agrafiotis et al., "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate", *Journal of Cybersecurity 4*, 1 (2018): tyy006.

[83] CyberPeace Institute, *Report of the Second Expert Meeting on Harms Methodology* (October 2024), https://cyberpeaceinstitute.org/wp-content/uploads/2024/10/Second-Expert-Meeting-Harms-Methodology-2024.docx.pdf.

[84] Véase Caso del Canal de Corfú, Reino Unido c. Albania, Sentencia sobre indemnización (1949), CIJ Rec 244, ICGJ 201 (CIJ 1949), 15 de diciembre de 1949, Naciones Unidas; Corte Internacional de Justicia.

[85] Michael N. Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law", *Chicago Journal of International Law*, https://cjil.uchicago.edu/print-archive/virtual-disenfranchisement-cyber-election-meddling-grey-zones-international-law.

[86] Elsa Hedling, "Gendered Disinformation", in *Feminist Foreign Policy Analysis* (Bristol University Press, 2024), 137–153.

[87] Asamblea General, Informe de la Relatora Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y expresión, A/78/288, 7 de agosto de 2023.

[88] Asamblea General,, A/78/288, 4.

[89] Dhanaraj Thakur et al., "An unrepresentative democracy: how disinformation and online abuse hinder women of color political candidates in the United States", Center for Democracy & Technology, 27 October 2022; Nukila Evanty y Fenny Tria Yunita, "Fake News and Violence against Women in Indonesia's Elections" en *Fake News and Elections in Southeast Asia* (Routledge, 2022) 63–83; Mytha Eliva Veritasia, Amalia Nurul Muthmainnah y Mathias-Felipe de-Lima-Santos, "Gendered disinformation: a pernicious threat to equality in the Asia Pacific", *Media Asia* (2024): 1–9; Ross Tapsell y Jananie Chandrarao, "Gendered Disinformation and Election Campaigning: A Malaysia Case Study", *Georgetown Journal of International Affairs* 25, 1 (2024): 193–199.

[90] Alexis Henshaw, *Digital frontiers in gender and security: Bringing critical perspectives online* (Policy Press, 2024); DCAF, *Online Actions, Offline Harms: Case Studies on Gender and Cybersecurity* (Geneva: DCAF, 2023), https://www.dcaf.ch/sites/default/files/publications/documents/Online-actions-offline-harms_EN-2nov2023.pdf.

[91] United Nations Institute for Disarmament Research (UNIDIR), *Unpacking Cyber Capacity-Building Needs: Part I – Mapping Foundational Cyber Capabilities* (Geneva: UNIDIR, 2023), 21–23, https://unidir.org/wp-content/uploads/2023/09/UNIDIR_Unpacking_Cyber_Capacity_Building_Needs_Part_1_Mapping_Foundational_Cyber_Capabilities.pdf

[92] ICPC, *Guidance on Implementation for ASEAN*, 37.

[93] ONU Mujeres, "Digital Abuse, Trolling, Stalking and Other Forms of Technology-Facilitated Violence Against Women: FAQs", 10 February 2025, https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women.

[94] En cuanto a cómo reflexionar sobre la marginación de manera sensible al contexto, véase: Global Partners Digital, *Inclusive Cyber Normas Toolkit* (August 2023), https://www.gp-digital.org/wp-content/uploads/2023/08/Inclusive-Cyber-Normas-Toolkit_GPD.pdf.

[95] Amanda Lenhart et al. 2016. *Online Harassment, Digital Abuse, and Cyberstalking in America.* (New York, NY: Data & Society Research Institute). www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf; V. Arasavva and A. Forth, "Personality, attitudinal, and demographic predictors of non-consensual dissemination of intimate images", *Journal of Interpersonal Violence* 37, 21-22 (2022); Rohini Lakshané, "Non-consensual intimate imagery: an overview," Take Back the Tech, 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4809632.

[96] Suzie Dunn, *Toward a Safer Internet: Minimizing the Impacts of Online Gender-Based Violence* (Centre for International Governance Innovation, 2021), https://www.cigionline.org/static/documents/SaferInternet_Paper_no_1_coverupdate.pdf; Anastasia Powell et al., "Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian adults", *Computers in Human Behavior* 92 (2018): 393–402; Julia Davidson et al., *Adult Online Hate, Harassment and Abuse* (UK Council for Internet Safety, 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811450/Adult_Online_Harms_Report_2019.pdf.

[97] Pranshu Verma, "How AI Fake Nudes are Ruining Teens' Lives", *The Washington Post*, 5 November 2023; Agnes Venema, "Deepfakes as a Security Issue: Why Gender Matters", Women in International Security, https://wiisglobal.org/deepfakes-as-a-security-issue-why-gender-matters/; Can Yavuz, "Adverse human rights impacts of dissemination of nonconsensual sexual deepfakes in the framework of European Convention on Human Rights: A victim-centered perspective", *Computer Law & Security Review 56* (2025): 106108.

[98] Mayssoun Sukarieh and Stuart Tannock, 'The Global Securitisation of Youth', Third World Quarterly (Vol. 39, No. 5, 2018),

pp. 854–70; Hassan, Ghayda, Sébastien Brouillette-Alarie, Séraphin Alava, Divina Frau-Meigs, Lysiane Lavoie, Arber Fetiu, Wynnpaul Varela et al. "Exposure to extremist online content could lead to violent radicalization: A systematic review of empirical evidence." *International journal of developmental science* 12, no. 1-2 (2018): 71-88.

[99] Clemmow, Caitlin, Bettina Rottweiler, Michael Wolfowicz, Noémie Bouhana, Zoe Marchment, and Paul Gill. "The whole is greater than the sum of its parts: Risk and protective profiles for vulnerability to radicalization." *Justice Quarterly* 41, no. 1 (2024): 140-166; OSCE. "Linkages between Violent Misogyny and Violent Extremism." Policy Brief. September 6, 2022 https://www.osce.org/files/f/documents/d/c/525297.pdf; Schuurman, Bart, and Sarah L. Carthy. "Citizens, Extremists, Terrorists: Comparing Radicalized Individuals with the General Population." Terrorism and Political Violence (2025): 1-20; Joana Cook, Eva Herschinger,

Seran de Leede, and Anna-Maria Andreeva, "Radicalisation and Gender – What Do We Know?", International Centre for Counter-Terrorism, University of Leiden (2024), https://icct.nl/sites/default/files/2024-11/Radicalisation%20and%20Gender%20What%20Do%20We%20Know%201.pdf

[100] Katharine Millar, *What Does It Mean to Gender Mainstream the Proposed Cybercrime Convention?* (Chatham House, 2022), https://chathamhouse.soutron.net/Portal/Public/en-GB/DownloadImageFile.ashx?objectId=5344&ownerType=0&ownerId=191233; UNIDIR, System Update; Aleksandra Dier and Gretchen Baldwin, *Masculinities and violent extremism* (International Peace Institute and UN Security Council Counter-Terrorism Committee Executive Directorate, 2022).

[101] UNIDIR, *Gender Approaches to Cybersecurity.*

[102] Consejo de Derechos Humanos, El derecho a la privacidad en la era digital, A/HRC/51/17, 4 de agosto de 2022, https://docs.un.org/es/A/HRC/51/17

[103] Electronic Frontier Foundation, "European Court of Human Rights Confirms: Weakening of Encryption Can Violate the Human Right to Privacy", EDRi, 28 March 2023, https://edri.org/our-work/european-court-of-human-rights-confirms-weakening-of-encryption-can-violate-the-human-right-to-privacy; Association for Progressive Communications (APC), *Feminist Principles of the Internet: Advocacy Brief on Privacy* (2023), https://genderit.org/FPI-paper-on-privacy; Asamblea General, Consejo de Dereches Humanos, The Right to Privacy in the Digital Age, A/HRC/51/17.

[104] Internet Society, "Encryption Is Essential for the LGBTQ+ Community", 1 November 2019, https://www.internetsociety.org/resources/doc/2019/encryption-factsheet-essential-for-lgbtq-community.

[105] Asamblea General, A/76/135. https://docs.un.org/es/A/76/135

[106] Banco Mundial, *Gender Dimensions of Cybersecurity: A Framework for Mainstreaming Gender in Cybersecurity Policy and Strategies* (Washington, DC: World Bank, 2024).

[107] Banco Mundial, *Gender Dimensions of Cybersecurity; Alison Gillwald and Andrew Partridge, Gendered Nature of Digital Inequality: Evidence for Policy Consideration* (Cape Town: Research ICT Africa, 2022), https://www.unwomen.org/sites/default/files/2022-12/BP.1_Alison%20Gillwald.pdf.

[108] UNICEF, "Bridging the Gender Digital Divide", May 2023, https://data.unicef.org/resources/ictgenderdivide.

[109] Consejo de Derechos Humanos, A/HRC/RES/32/13, 18 de julio de 2016, https://docs.un.org/es/A/HRC/RES/32/13

[110] Consejo de Derechos Humanos, A/HRC/RES/38/7, 5 de julio de 2018, https://docs.un.org/es/A/HRC/RES/38/7; Pytlak and Brown, *Why Gender Matters*.

[111] Consejo de Derechos Humanos, A/HRC/RES/38/5, 17 de julio de 2018, https://docs.un.org/es/A/HRC/RES/38/5

[112] Consejo de Derechos Humanos, A/HRC/RES/47/23, 16 de julio de 2021, https://docs.un.org/es/A/HRC/47/23

[113] Consejo de Derechos Humanos, A/HRC/RES/53/29, 18 de julio de 2023, https://docs.un.org/es/A/HRC/RES/53/29

[114] Asamblea General, A/RES/73/179, 21 de enero de 2019, https://docs.un.org/es/A/73/179

[115] Asamblea General, A/RES/78/213, https://docs.un.org/es/A/RES/78/213

[116] Consejo de Derechos Humanos, La aplicación práctica de los Principios Rectores sobre las Empresas y los Derechos Humanos a las actividades de las empresas tecnológicas, A/HRC/50/56, 21 de abril de 2022 https://docs.un.org/es/A/HRC/50/56

[117] Consejo de Derechos Humanos, A/HRC/50/56.

[118] Consejo de Derechos Humanos, A/HRC/50/56.

[119] Pavlina Pavlova, "Confronting Gendered Harm in Cyberspace is not a Matter of Social Justice – It's a National Security imperative". https://www.justsecurity.org/107353/gendered-harm-cyberspace-not-social-justice-a-security-imperative/

[120] Pavlova, "Confronting Gendered Harm in Cyberspace".

[121] Véase, por ejemplo, Cybersecurity and Infrastructure Security Agency, "Secure by Design", https://www.cisa.gov/securebydesign.

[122] Freedom Online Coalition, *FOC Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies* (2020), https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-on-the-Human-Rights-Impact-of-Cybersecurity-Laws-Practices-and-Policies.pdf; Association for Progressive Communications (APC), *Gender Approaches to Cybersecurity: Integrating Policy, Research, and Technical Standards Discussions* (2024), 13, https://www.apc.org/sites/default/files/genderapproaches-cyber.pdf.

[123] Millar, *What Does it Mean to Gender Mainstream?.*

[124] Para obtener información sobre cómo cerrar la brecha digital de género, véase: Gillwald and Partridge, *Gendered Nature of Digital Inequality*; World Bank Digital Development Partnership, "Closing Gender Gaps in Digital Development: A Practical Guide for Operational Teams", September 2023, https://documents1.worldbank.org/curated/en/099022924054584089/pdf/P1805721f6ca4402c1905b12c4337f89bb8.pdf; Hafsah Muheed, "The Gender Digital Divide Must be Bridged to Ensure We Leave No One Behind", UN Women Asia Pacific, 16 March 2023, https://asiapacific.unwomen.org/en/stories/feature-story/2023/03/the-gender-digital-divide; Alicja Pawluczuk, JeongHyun Lee and Attlee Munyaradzi Gamundani, "Bridging the gender digital divide: an analysis of existing guidance for gender digital inclusion programmes' evaluations", *Digital Policy, Regulation and Governance 23*, 3 (2021): 287–299.

[125] Pacto Digital Mundial. https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf; Gillwald and Partridge, *Gendered Nature of Inequality,* 27–31.

[126] Véase, por ejemplo: Marccus D. Hendricks and Shannon Van Zandt, "Unequal protection revisited: Planning for environmental justice, hazard vulnerability, and critical infrastructure in communities of color", *Environmental Justice 14,* 2 (2021): 87–97.

[127] Asamblea General, A/79/214, para. 14. https://docs.un.org/es/a/79/214

[128] Cecilia Gallais and Eric Filiol, "Critical infrastructure: where do we stand today? A comprehensive and comparative study of the definitions of a critical infrastructure." *Journal of Information Warfare 16*, 1 (2017): 64–87; Valentin Weber et al., "Mapping the World's Critical Infrastructure", DGAP, 22 November 2023, https://dgap.org/en/research/publications/mapping-worlds-critical-infrastructure-sectors.

[129]UNIDIR, *System Update.*

[130] Weber et al., "Mapping Critical Infrastructure".

[131] Gobierno de Costa Rica, "Posición Nacional sobre la Aplicación del Derecho Internacional en el Ciberespacio".

[132] Pavlova, *Confronting Gendered Harm in Cyberspace*; Priyanka Babbar et al., "Understanding and responding to the transit needs of women in Canada," Government of Canada, 2022, https://www.sshrc-crsh.gc.ca/society-societe/community-communite/ifca-iac/evidence_briefs-donnees_probantes/mobility_public_transit/grise-eng.aspx.

[133] Pytlak and Brown, *Why Gender Matters.*

[134] Centre for Feminist Foreign Policy, *Feminist Perspectives on the Militarisation of Cyberspace* (2023), 9, https://centreforfeministforeignpolicy.org/wordpress/wp-content/uploads/2023/06/CFFP_Briefing_Cybersecurity_final.pdf.

[135] Fundación Karisma, *Ciberataque a Sanitas: Impactos Diferenciales Sobre Mujeres Cuidadoras* (2024), https://web.karisma.org.co/ciberataque-a-sanitas-impactos-diferenciales-sobre-mujeres-cuidadoras/

[136] Anna Wellenstein and Maninder Gill, "Making infrastructure work for both women and men", World Bank Blogs, 28 August 2019), https://blogs.worldbank.org/en/voices/making-infrastructure-work-both-women-and-men

[137] Para una orientación práctica sobre consultas significativas y políticas de ciberseguridad inclusivas, véase: Global Partners Digital, *Inclusive Cyber Normas Toolkit.*

[138] APC, *Gender Approaches to Cybersecurity*; Australia et al., "Gender and the Future Permanent Mechanism".

[139] Julia Slupska and Leonie Maria Tanczer, "Threat modelling intimate partner violence: Tech abuse as a cybersecurity challenge on the internet of things", in *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (Emerald Publishing Limited, 2021), 663–688; Government of Canada, "Canada's Proposal for the Work of the 2021-25 United Nations Open-Ended Working Group".

[140] APC, *Gender approaches to cybersecurity: integrating policy, research and technical standards discussions*, https://www.apc.org/en/pubs/gender-approaches-cybersecurity-integrating-policy-research-and-technical-standards.

[141] Para una orientación práctica sobre cómo llevar esto a cabo, véase: Joyce Hakmeh et al., *A Principles-Based Approach to Cyber Capacity-Building* (Chatham House, June 2024), https://www.chathamhouse.org/sites/default/files/2024-06/2024-06-25-principles-based-approach-cyber-capacity-building-hakmeh-et-al.pdf.

[142] Asamblea General, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, A/AC.290/2021/CRP, 10 de marzo de 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf. Para orientación sobre cómo aplicar el enfoque basado en principios en el desarrollo de capacidades en materia de ciberseguridad, véase Hakmeh et al., *A Principles-Based Approach to Cyber Capacity-Building.*

[143] Pytlak and Brown, *Why Gender Matters.*

[144] Véase, por ejemplo: Louise Wignall et al., *Gender barriers to basic digital skills for employment in the ASEAN region: A review of promising practices* (Australian Council for Educational Research, 2024); Elodie Andrieu et al., *The role of education and skills in bridging the digital gender divide: Evidence from APEC economies* (Paris: OECD Publishing, 2019); Archita Misra, "Fostering digital skills in developing countries–what works?" Blavatnik School of Government, July 2022.

[145] "Las tecnologías de doble uso" son tecnologías que tienen tanto un uso militar o de seguridad nacional como un uso civil (por ejemplo, los satélites de posicionamiento global). En el ámbito de la ciberseguridad, las tecnologías de doble uso suelen referirse a herramientas de ciber-vigilancia, aunque el concepto se aplica de manera más amplia. Para más información sobre ciberseguridad y tecnologías de doble uso, véase: Amir Lupovici, "The dual-use security dilemma and the social construction of insecurity." *Contemporary Security Policy 42*, 3 (2021): 257–285.

[146]Joe Devanny and Grant Christopher, "Cyber arms control and counter proliferation: The limits of the possible", in *Research Handbook on Cyberwarfare* (Edward Elgar Publishing, 2024), 335–351.

[147]Christopher Parsons et al., *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry* (Citizen Lab, June 2019), https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/.

[148]Government of Canada, "Canada's Implementation of the 2015 GGE Normas", https://front.un-arm.org/wp-content/uploads/2019/11/canada-implementation-2015-gge-Normas-nov-16-en.pdf.

[149]Slupska and Tanczer, "Threat modelling intimate partner violence".

[150]Tamsin Rose and AAP, "Tracking devices increasingly used by DV offenders to 'stalk, harass, intimidate and monitor victims'" *The Guardian*, 25 June 2024,

https://www.theguardian.com/world/article/2024/jun/25/tracking-device-domestic-violence-offenders-stalking-apple-find-my-friends; New South Wales Government, "A safer NSW: Stronger protections for victim-survivors of domestic and family violence, 2 September 2024, https://www.nsw.gov.au/media-releases/a-safer-nsw-stronger-protections-for-victim-survivors-of-domestic-and-family-violence; Anastasia Powell, "New laws to tackle technology-based abuse in NSW are welcome. But police and courts also need to step up" *The Conversation*, 4 September 2024, https://theconversation.com/new-laws-to-tackle-technology-based-abuse-in-nsw-are-welcome-but-police-and-courts-also-need-to-step-up-238076.

[151]Government of Canada, "Canada's Proposal for the Work of the 2021-25 United Nations Open-Ended Working Group".

[152] Consejo de Derechos Humanos, Los derechos humanos y los procesos de establecimiento de normas técnicas para las tecnologías digitales nuevas y emergentes, A/HRC/53/42, 18 de septiembre de 2023, https://docs.un.org/es/A/HRC/53/42

[153]APC, *Principios feministas para Internet.* https://www.apc.org/es/pubs/principios-feministas-para-internet-version-2

[154] Para ejemplos de violaciones de bases de datos médicos, véase: Mao Frances, "Medibank: Hackers release abortion data after stealing Australian medical records, BBC, 10 November 2022, https://www.bbc.co.uk/news/world-australia-63579985; Tyler Griffin, "Perinatal and child registry data breach affects health info of million Ontarians", *The Canadian Press/City News*, 25 September 2023, https://toronto.citynews.ca/2023/09/25/perinatal-and-child-registry-data-breach-affects-health-info-of-3-million-ontarians/; Katie Kalubisch, "Planned Parenthood Under Attack by Anti-Abortion Hackers, Politicians", *Rolling Stone*, 31 July 2015, https://www.rollingstone.com/politics/politics-news/planned-parenthood-under-attack-by-anti-abortion-hackers-politicians-71311/.

[155] Véase, por ejemplo: Thomas Brewster, "A Massive Mobile Location Data Hack May Have Risked Gay People's Safety", *Forbes*, 10 January 2015, https://www.forbes.com/sites/thomasbrewster/2025/01/10/gravy-analytics-massive-mobile-location-data-hack-may-have-risked-gay-peoples-safety/; Reuters, "Grindr facing U.K. lawsuit over alleged data protection breaches", *NBC News*, 22 April 2024, https://www.nbcnews.com/nbc-out/out-news/grindr-facing-uk-lawsuit-alleged-data-protection-breaches-rcna148787; Hannah Crouch, "Transgender charity Mermaids fined £25k for data protection breach" *DigitalHealth*, 20 July 2021, https://www.digitalhealth.net/2021/07/mermaids-fined-ico-data-protection-breach/.

[156] Sheetal Kumar, "The missing piece in human-centric approaches to cyberNormas implementation: the role of civil society", *Journal of Cyber Policy 6*, 3 (2021): 375–393.

[157] Frost & Sullivan, *2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk* (International Information System Security Certification Consortium, 2017), https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx.

[158] UNIDIR, *Gender Approaches to Cybersecurity.*

[159] UNIDIR, *Gender Approaches to Cybersecurity.*

[160] Mika Kerttunen y Eneken Tikk, *Putting Cyber Normas in Practice: Implementing the UN GGE 2015 recommendations through national strategies and policies* (Cybil Portal, 2021), 99, https://cybilportal.org/wp-content/uploads/2021/11/Putting-Cyber-Normas-in-Practice.pdf; Asamblea General A/76/135, 16.

[161] Asamblea General, A/76/135.

[162] UNIDIR, "Gender in Cyber Diplomacy"; ISC2, "Women in Cybersecurity: Women in the Profession", 25 April 2024, https://www.isc2.org/Insights/2024/04/Women-in-Cybersecurity-Report-Women-in-the-Profession.

[163] Accenture, "Resetting Tech Culture, Accenture and Girls Who Code", 2020, https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-136/accenture-resetting-tech-culture.pdf; McKinsey and Company, *Women in the Workplace 2024*: *The 10th-Anniversary Report* (17 September 2024), https://www.mckinsey.com/featured-insights/diversity-and-inclusion/women-in-the-workplace#/; Michele Parmelee, "Empowering Women at Work", Deloitte, 25 April 2023, https://www2.deloitte.com/us/en/insights/topics/talent/work-life-balance-for-women.html.

[164] Valerie I. Sessa and Susan E. Jackson, "Diversity in decision-making teams: All differences are not created equal", in *Diversity in Organizations: New Perspectives for a Changing Workplace* (SAGE Publications, Inc., 1995), 133–156; Elizabeth Mannix and Margaret A. Neale, "What differences make a difference? The promise and reality of diverse teams in organizations", *Psychological Science in the Public Interest 6*, 2 (2005): 31–55; Gail Robinson and Kathleen Dechant, "Building a business case for diversity", *Academy of Management Perspectives 11*, 3 (1997): 21–31.

[165] Government of Canada, "Canada's Proposal for the Work of the 2021-25 United Nations Open-Ended Working Group".

[166] Gracias a Maja Romano, Liderazgo en producción y curación de contenido, APC, por sus valiosos comentarios editoriales sobre esta sección.

[167] UNIDIR, *System Update.*

[168] Government of Canada, "Canada's Feminist International Assistance Policy", https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/priorities-priorites/policy-politique.aspx?lang=eng.

[169] Government of Canada, "Canada's Feminist International Assistance Policy".

[170] APC, *A Framework for Developing a Gender-Responsive Cybersecurity Policy* (2023), https://www.apc.org/en/pubs/framework-developing-gender-responsive-cybersecurity-policy#tool.

[171] Government of Canada, "Updated Canadian Text Proposals".

[172] Government of Canada, "Updated Canadian Text Proposals"; Government of Canada, "Proposed Normas guidance text", https://front.un-arm.org/wp-content/uploads/2021/02/new-updated-Normas-guidance-text-feb-11-clean.pdf.

[173] Government of Canada, "Canada's response to questions in Chair's paper: February 2020 OEWG meeting", https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/canada-responses-to-oewg-chair-questions-Feb-26.pdf.

[174] Government of Canada, "Canada's Proposal for the Report of the 2019–20 United Nations Open-Ended Working Group".

[175] Government of Canada, "Foundations for Peace: Canada's National Action Plan on Women, Peace and Security – 2023 to 2029,"
https://www.international.gc.ca/transparency-transparence/women-peace-security-femmes-paix-securite/2023-2029-foundation-peace-fondation-paix.aspx?lang=eng.

[176] Véase Sarah Shoker, "Making Gender Visible in Digital ICTs and International Security", 2020, https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf; Pytlak and Brown, *Why Gender Matters.*

[177] Por ejemplo, el curso sobre Género y Ciberseguridad, ofrecido en colaboración con la Facultad de Derecho de la Universidad de Chile, tiene como objetivo brindar una perspectiva regional, integral y multidisciplinaria sobre la ciberseguridad desde un enfoque de género. Más información en: https://derecho.uchile.cl/noticias/220344/curso-genero-y-ciberseguridad-contara-con-becas-del-gobierno-de-canada.

[178] Government of Canada, "Canada's Proposal for the Work of the 2021-25 United Nations Open-Ended Working Group".

[179] UNIDIR, *System Update.*

[180] Véase, por ejemplo: "Intervención de México durante la tercera sesión sustantiva del OEWG sobre tecnologías de la información y seguridad internacional 2021-2025", https://documents.unoda.org/wp-content/uploads/2022/07/250722-Intervencion-Mexico-Sesion-apertura-OEWG-cotejo.pdf.

[181] Hofstetter and Pourmalek, *Gendering Cybersecurity,* 21.

[182] ICPC, *Guidance on Implementation for ASEAN.*

[183]Hofstetter and Pourmalek, *Gendering Cybersecurity.*

[184] Paloma Herrera Carpintero, "El enfoque de género en la Política Nacional de Ciberseguridad de Chile", Universidad de Chile, 22 December 2023, 11, https://orcid.org/0000-0001-6174-9822.
Pytlak and Brown, *Why Gender Matters.*

[185] Gobierno de Chile, National Cybersecurity Policy 2017-2022, 18 https://generoyparticipacion.interior.gob.cl/media/2023/02/Politica-Nacional-Ciberseguridad-2018-2022.pdf

[186] Gobierno de Chile, Política Nacional de Ciberseguridad 2017-2022, https://generoyparticipacion.interior.gob.cl/media/2023/02/Politica-Nacional-Ciberseguridad-2018-2022.pdf

[187] Paz Peña O., *Resultados de la Política Nacional de Ciberseguridad 2017-2022: Avances y Brechas sobre la Inclusión del Enfoque de Género* (Diciembre de 2022), 1, https://ciberseguridad.gob.cl/documents/4483/I.-Resultados-de-g%C3%A9nero-y-pol%C3%ADtica-nacional-de-ciberseguridad-2017-2022_final.pdf.

[188] Gobierno de Chile, *Evaluación de la Política Nacional de Ciberseguridad 2017–2022* (Santiago: Gobierno de Chile, 2022), https://ciberseguridad.gob.cl/documents/3/Evaluaci%C3%B3n_PNCS_2017-2022.pdf; Peña O., *Resultados de la Política Nacional de Ciberseguridad 2017-2022.*

[189] Véase, por ejemplo, Gobierno de Chile, "Comentarios y sugerencias de Chile sobre el Borrador Cero del primer informe anual de progreso de Grupo de Trabajo de Composición Abierta (OEWG) 2021-2025 del Grupo de Expertos Gubernamentales sobre seguridad de las TIC".

[190] Peña O., *Resultados de la Política Nacional de Ciberseguridad 2017-2022.*

[191] Por ejemplo, Feria de Mentorías en Ciberseguridad #GirlsinCyber, Foro #mujeresciber and She Hacks workshops for digital empowerment for girls and adolescents:
https://ciberseguridad.gob.cl/noticias/inscr%C3%ADbete-feria-de-mentor%C3%ADas-en-ciberseguridad-girlsincyber-y-foro-mujeresciber/; https://ciberseguridad.gob.cl/noticias/comienza-she-hacks-2024/.

[192] Gobierno de Chile, *Política Nacional de Ciberseguridad 2023–2028*, https://ciberseguridad.gob.cl/documents/4430/Pol%C3%ADtica_Nacional_de_Ciberseguridad_2023-2028.pdf.

[193] Peña O., *Resultados de la Política Nacional de Ciberseguridad 2017-2022.*

[194] Derechos Digitales, "Fostering Inclusive Cyber Normas: A Derechos Digitales Case Study," Global Partners Digital, https://www.gp-digital.org/fostering-inclusive-cyber-Normas-a-derechos-digitales-case-study/.

[195] J. Carlos Lara, "Las personas al centro: la apertura en las políticas de ciberseguridad", Derechos Digitales, 3 February 2023, https://www.derechosdigitales.org/20023/.

[196] Pytlak and Brown, *Why Gender Matters,* 21.

[197] Pytlak and Brown, *Why Gender Matters,* 15.

[198] General Assembly, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report, A/AC.290/2021/CRP.2, 10 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

[199] Government of Canada, "Canada's response to questions in Chair's paper".

[200] Australia et al., "Gender and the Future Permanent Mechanism".

[201] El proyecto Her CyberTracks está financiado por el Ministerio Federal de Asuntos Exteriores de Alemania y ejecutado conjuntamente por el Sector de Desarrollo de las Telecomunicaciones de la UIT y la Agencia Alemana de Cooperación Internacional (GIZ), en colaboración con la Oficina de las Naciones Unidas contra la Droga y el Delito y el Centro de Competencia Cibernética para América Latina y el Caribe (LAC4). See more at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Skills-Development/Her-CyberTracks.aspx.

[202] OEA, "OAS Launches WiCE Network of Women Cybersecurity Professionals", 12 June 2024, https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-038/24.

[203] Serge Droz, "Diversity and Cyber Resilience: Views of an Incident Responder", 24 March 2021, https://unidir.org/diversity-and-cyber-resilience-views-of-an-incident-responder/. Ministerio de Telecomunicaciones y Sociedad de la Información, Estrategia Nacional de Ciberseguridad de Ecuador 2022-2025, 35, https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf.

[204] OEA, "The Organization of American States and Trend Micro promote in Latin America the first edition of the security workshop 'Cyberwomen Challenge'", 1 June 2018, https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-035/18.

[205] Ministerio de Telecomunicaciones y Sociedad de la Información, *Estrategia Nacional de Ciberseguridad de Ecuador 2022-2025*, 35, https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf.

[206] Gobierno de Uruguay, *Estrategia Nacional de Ciberseguridad de Uruguay 2024–2030, AGESIC, Proyecto 2.0* (2024).

[207] Cyberlaw CCDCOE, "Costa Rica Ransomware Attack", 20 March 2023, https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022).

[208] Dina Temple-Raston and Sean Powers, "Son of Conti: Ransomware Tries Its Hand at Politics," *The Record*, 27 June 2022, https://therecord.media/son-of-conti; Matt Burgess, "Costa Rica's Ransomware Crisis Is a Global Wake-Up Call," Wired, 12 June 2022, https://www.wired.com/story/costa-rica-ransomware-conti/.

[209] Internet Governance Forum, IGF 2023: Best Practice Forum on Cybersecurity (November 2023), https://www.intgovforum.org/en/filedepot_download/56/26668.

[210] CyberPeace Institute, "Cyber Incident Tracer #HEALTH", https://cit.cyberpeaceinstitute.org/.

[211] Pytlak and Brown, *Why Gender Matters,* 12; Rebecca Emerson-Keeler, Amrit Swali and Esther Naylor, *Integrating Gender in Cybercrime Capacity-Building* (Chatham House, 2023), 3, https://www.chathamhouse.org/2023/07/integrating-gender-cybercrime-capacity-building.

[212] Carla Rosch, "A massive cyberattack in Costa Rica leaves citizens hurting", Rest of the World, 1 June 2022, https://restofworld.org/2022/cyberattack-costa-rica-citizens-hurting/.

[213] Louise Marie Hurel, *Accountability in Cyberspace: Lessons from and for Latin America* (Stimson Center, 2024), https://www.stimson.org/2024/accountability-in-cyberspace-lessons-from-and-for-latin-america/.

[214] El desarrollo de la estrategia implicó una consulta pública no vinculante y discusiones entre múltiples partes interesadas apoyadas por la Sección de Ciberseguridad del CICTE/OEA. Para más detalles, véase: Costa Rica, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) *National Cybersecurity Strategy 2023–2027* (2023), https://www.micitt.go.cr/sites/default/files/transparencia/consulta-publica/Informe%20MICITT-DGDCFD-DRII-INF-168-2023%20ENC-firmado.pdf.

[215] Costa Rica MICITT, *National Cybersecurity Strategy 2023–2027,* 27. Disponible en: https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf

[216] Costa Rica MICITT, *Estrategia Nacional de Ciberseguridad 2023–2027,* 32.

[217] Costa Rica MICITT, *Estrategia Nacional de Ciberseguridad 2023–2027,* 38.

[218] Gobierno de Costa Rica, "Costa Rica's Position on the Application of International Law in Cyberspace", https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/wp-costa-rica.pdf.

[219] Costa Rica también fue seleccionada para participar en el programa CyberTalents de la OEA, una iniciativa de pasantías que fomenta una mayor participación de mujeres en los CSIRT nacionales y públicos de los Estados miembros de la OEA y promueve la colaboración a través de la plataforma hemisférica CSIRT Américas.

[220] "Pytlak and Brown, *Why Gender Matters.*

[221] Asamblea General, Consejo de Derechos Humanos, A/HRC/53/42.

[222] ICT4Peace, *Advancing a Global Cyber Programme of Action* (May 2022), https://ict4peace.org/wp-content/uploads/2022/05/Report-Advancing-a-Global-Cyber-Programme-of-Action-Options-and-priorities.pdf; S. Perera, "White Paper on Feminist Internet Research", APC, 2022, https://www.apc.org/sites/default/files/firn-whitepaper-2022.pdf.

[223] Oficina de Tecnologías Digitales y Emergentes, Naciones Unidas, "Global Digital Compact", 2024, https://www.un.org/techenvoy/global-digital-compact.

[224] "Working-Paper to advance the ongoing Discussions within the United Nations Open Ended Working Group (OEWG) on Confidence Building Measures (CBM) in Cyberspace", https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/CBMS-workingpaper-2022.pdf.

[225] Asamblea General, OEWG 2021–2025, A/AC.292/2024/CRP.1, Annex B.

[226] Hofstetter and Pourmalek, *Gendering Cybersecurity.*

[227] Hofstetter and Pourmalek, *Gendering Cybersecurity.*

[228] APC, *Principios Feministas de Internet.*

[229] Pytlak and Brown, *Why Gender Matters.*

[230] Slupska and Tanczer, "Threat modelling intimate partner violence"; Government of Canada, "Canada's Proposal for the Work of the 2021-25 United Nations Open-Ended Working Group".

[231] Global Partners Digital, *Inclusive Cyber Normas Toolkit.*

[232] APC, *Gender and Cybersecurity Assessment Tool* (2023), 38.

[233] APC, *Gender and Cybersecurity Assessment Tool* (2023), 39; Media Foundation for West Africa, *Using the OEWG to open doors and build partnership for a secure and human-centric internet in Africa* (2022), https://www.mfwa.org/wp-content/uploads/2022/06/Policy-brief-on-African-Participation-in-OEWG-MFWA.pdf.

[234] Pacto Digital Mundial, 4.

Un enfoque novedoso para las 11 normas de la ONU sobre el comportamiento responsable de los Estados en el ciberespacio:

Directrices para una implementación con perspectiva de género

OEA | CICTE

UNIDIR