MARCO PARA EL DESARROLLO DE UNA POLÍTICA DE CIBERSEGURIDAD QUE RESPONDA A LAS CUESTIONES DE GÉNERO: HERRAMIENTA DE EVALUACIÓN

APC
ASOCIACIÓN PARA EL PROGRESO DE LAS COMUNICACIONES

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

Esta publicación ha sido desarrollada y producida por APC con un importante apoyo de la investigadora externa Paz Peña.

Coordinación y edición: Verónica Ferrari y Paula Martins (APC)
Edición: Alan Finlay
Corrección: Lori Nordstrom (APC)
Traducción: Clio E. Bugel
Diseño y compaginación: Cathy Chen (APC)

Publicado por APC 2023

APC desea agradecer a las personas y organizaciones siguientes por los comentarios, el tiempo y la experiencia aportados para realizar esta publicación:

- Kerry-Ann Barrett, Katya Vera Morales, Orlando Garcés Corzo y todo el equipo del Comité Interamericano contra el Terrrorismo (CICTE), Organización de los Estados Americanos (OEA)
- Hija Kamran, Karla Velasco Ramos, Erika Smith, hvale vale y todo el equipo del Programa de Derechos de las Mujeres de APC
- Gabriela Montes de Oca, experta independiente
- Nanjira Sambuli, Miembro para Tecnología y asuntos internacionales de la Fundación Carnegie para la paz internacional
- Daniela Schnidrig, directora de participación nacional y activismo de Global Partners Digital
- James Shires, Isabella Wilkinson, Amrit Swali, Joyce Hakmeh y todo el equipo del Programa de seguridad internacional de Chatham House
- Tatiana Tropina, profesora asistente, ISGA, Universidad de Leiden
- Francisco J. Vera Hott, Director del programa Justicia y responsabilidad global, Open Society Foundations

Reconocimiento 4.0 Internacional (CC BY 4.0)
https://creativecommons.org/licenses/by/4.0/deed.es_ES

ISBN 978-92-95113-63-3
APC-202306-GAPS-R-ES-DIGITAL-353

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

I. INTRODUCCIÓN A ESTA HERRAMIENTA DE EVALUACIÓN

Esta herramienta de evaluación ofrece sugerencias detalladas y recomendaciones concretas para quienes se proponen la tarea de desarrollar políticas de ciberseguridad con un enfoque de género. Este documento se construye a partir del trabajo previo de APC desde proyectos de investigación hasta campañas de activismo, en cuanto al desarrollo de un concepto de ciberseguridad basado en derechos humanos, así como en el área de la violencia de género en línea, y la ciberseguridad y las cuestiones de género. El trabajo forma parte de un marco diseñado para prestar apoyo a los y las responsables de formular políticas, y a las organizaciones de la sociedad civil a la hora de crear políticas de ciberseguridad desde una perspectiva de género.[1]

Este marco también incluye dos documentos más y sugerimos que, quienes utilicen esta herramienta de evaluación los consulten antes de poner en práctica los principios y procesos aquí esbozados. Los otros dos documentos son:

- Un análisis de la literatura existente que explora cuál es el lugar que ha tenido la ciberseguridad como espacio de género en la investigación.[2]
- Un documento que identifica normativas, reglas y directrices que pueden servir de apoyo a las personas responsables de formular políticas de ciberseguridad y la comunidad de activistas de esta área que busquen promover la adopción de un enfoque de género en los debates nacionales y multilaterales sobre ciberseguridad.[3]

1. En esta herramienta de evaluación, las políticas de ciberseguridad nacional y las estrategias nacionales de ciberseguridad se consideran sinónimos. Los principios del marco se pueden aplicar también, con algunos ajustes, a las leyes de ciberseguridad, e incluso a las regulaciones del campo.
2. APC. (2022a). *Marco para el desarrollo de una política de ciberseguridad que responda a las cuestiones de género: Análisis de las publicaciones existentes.* https://www.apc.org/es/node/38847/
3. APC. (2022b). *Marco para el desarrollo de una política de ciberseguridad que responda a las cuestiones de género: Normativas, reglas y directrices.* https://www.apc.org/es/node/38852/

Tomando como base el Modelo de madurez de la capacidad de ciberseguridad de las naciones (CMM, por su sigla en inglés),[4] esta herramienta de evaluación ofrece una metodología de análisis que considera el grado de madurez de las políticas nacionales en cada país. El foco se fija en las tres primeras etapas de maduración – que se conocen como "inicial", "formativa" y "consolidada" – ya que son las más importantes para incidir en políticas. Este marco , como parte de su enfoque analítico,también adapta una herramienta para evaluar las estrategias nacionales de ciberseguridad desde la perspectiva de los derechos humanos que desarrolló Global Partners Digital (GPD).

Las recomendaciones aquí presentes son necesariamente generales y es preciso adaptarlas a cada contexto específico para que tengan sentido y se pueda ver el poder transformador de concebir la ciberseguridad desde un enfoque de género. Si bien nuestro foco está puesto en el proceso de desarrollo de políticas a nivel nacional, los principios del enfoque de género también se pueden aplicar en foros y debates regionales o globales de ciberseguridad multilateral.

Esperamos que este abordaje sea de utilidad para, entre otros actores, las personas a cargo de formular políticas y para la sociedad civil que se propongan elaborar un marco de políticas de ciberseguridad resiliente, valioso y relevante para su país.

¿De qué hablamos cuando hablamos de etapas de maduración en este documento?

La CMM define etapas de maduración para todas las dimensiones y los factores de la capacidad de ciberseguridad de un país. En este documento nos centramos sobre todo en las políticas nacionales de ciberseguridad que, al igual que cualquier otro desarrollo político, tienen un proceso evolutivo determinado por factores contextuales tales como los recursos institucionales y nacionales, la voluntad política y las capacidades y conocimientos de las personas a cargo de la formulación de políticas. Si bien es difícil señalar exactamente en qué etapa están los procesos políticos en cuanto a la capacidad de ofrecer una respuesta amplia y significativa a las necesidades de ciberseguridad de toda la gente, se suele hablar de "etapas de madurez". La etapa de desarrollo de las políticas de ciberseguridad en la que se encuentra tu país actualmente puede ser producto de una mezcla de diferentes fases.

4. Global Cyber Security Capacity Centre. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM) - 2021 Edition.* https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

Resumen de términos claves

Apoyándonos en el análisis sobre la literatura existente[5], en este documento utilizamos las definiciones siguientes:

Género: Conjunto de ideas, representaciones, prácticas y prescripciones sociales que se basa en las diferencias anatómicas entre los sexos. Estas ideas y prácticas conforman jerarquías sociales, económicas y legales en la sociedad que generan discriminación y desigualdad.

Inclusión de la cuestión de género: El proceso de evaluación de las consecuencias que puede tener cualquier tipo de acción planeada para mujeres y hombres, ya sean leyes, políticas o programas, en todas las áreas y a todo nivel. El objetivo final es alcanzar la igualdad de género.

Perspectiva interseccional: La perspectiva interseccional identifica un sistema de opresiones diversas e interconectadas – entre ellas el género, pero también se incluyen la raza, la religión y la clase social, entre otras – que a veces genera complejas jerarquías sociales, económicas y otras entre las personas que integran una sociedad. Rara vez sucede que los individuos se encuentren sujetos a una forma de opresión en sí misma.

Feminismo: El feminismo es un enfoque diverso e interdisciplinario sobre el tema de la igualdad y la equidad basándose en el género, la expresión de género, la identidad de género, el sexo y la sexualidad.

5. APC. (2022a). Op. cit.

II. ¿QUÉ IMPLICA CONCEBIR LA CIBERSEGURIDAD DESDE UNA PERSPECTIVA DE GÉNERO?

Concebir las políticas de ciberseguridad desde una perspectiva de género no implica sólo tener en cuenta los derechos de las mujeres – se trata de una herramienta para el desarrollo de políticas que se enfoquen, en general, en los derechos humanos de las personas en el entorno en línea. Con esto queremos decir que se trata de una perspectiva según la cual la ciberseguridad debe responder a las necesidades complejas, diferenciadas e interseccionales de la gente teniendo en cuenta factores tales como el género, la orientación sexual, la raza, la religión, la etnicidad, las capacidades, la clase social y la filiación política, entre otros.

No se trata de una medida agregada a una política ya creada, sino de un cambio sistémico del concepto de ciberseguridad. Se alienta a crear y usar datos interseccionales y de género desglosados y con más matices a fin de poder tomar decisiones políticas más informadas, más significativas y con mayor impacto.

También fomenta una reevaluación del concepto de ciberseguridad, que hasta ahora se enfocaba en el lado técnico de la ciberseguridad, basándose a menudo en la defensa nacional, o en las necesidades del sector privado. Al reformular la manera en que un país concibe la ciberseguridad, se aumenta la resiliencia del sistema de seguridad nacional.

¿En qué consiste la ciberseguridad desde una perspectiva de género?

Concebir la ciberseguridad desde un enfoque de género implica algo más que pensar simplemente en el impacto que tiene la ciberseguridad en las mujeres. Se trata también de tener en cuenta las discriminaciones y desigualdades interrelacionadas que se basan en la orientación sexual, la raza, la etnicidad, las capacidades, la clase social y la orientación política. La ciberseguridad con perspectiva de género tiene en cuenta los diferentes riesgos e impactos de las amenazas cibernéticas a fin de poder responder a necesidades, prioridades y percepciones complejas y diferenciadas, con base en el género y otros factores.

Conceptos erróneos más comunes

Qué decir cuándo alguien dice:

- **El género es una "cuestión de mujeres":** No. El concepto de género se refiere a las jerarquías sociales, políticas y económicas que se han ido desarrollando y que desempoderan, o empoderan a los individuos según su identidad de género. También se relaciona con las intersecciones entre esta identidad y otras jerarquías o poderes y con el desem-poderamiento, basándose en la raza, la religión y la clase social, entre otras cosas.
- **La ciberseguridad es solamente una cuestión técnica:** No. La tecnología y las políticas relativas a la tecnología no son "neutras". Más bien contribuyen a exaltar las jerarquías de poder social, económico y político que generan discriminación y desigualdades, o pueden servir para mitigarlas.
- **La ciberseguridad es "ciega al género":** No. Si bien las políticas de ciberseguridad deben apuntar a mitigar las desigualdades interseccionales y la discriminación basada en el género que se encuentran en la sociedad, sólo pueden servir para ello si se reconoce la existencia de esas desigualdades y se desarrollan formas de remediarlas. Las buenas políticas de ciberseguridad no son ciegas, sino sensibles al género.
- **"El feminismo es sólo para las mujeres":** No. El feminismo es un abordaje social y político para realizar un análisis sistemático y generar un cambio estructural en la sociedad, a fin de volverla más igualitaria y respetuosa de los derechos humanos y la dignidad. Los hombres también pueden ser feministas.

III. ¿POR QUÉ ES IMPORTANTE CONCEBIR LA CIBERSEGURIDAD DESDE UNA PERSPECTIVA DE GÉNERO?

Creemos que concebir la ciberseguridad desde una perspectiva de género es fundamental para crear políticas que fomenten los derechos humanos en línea. Se trata de una perspectiva desde la cual la ciberseguridad debe responder a las necesidades complejas y diferenciadas de las personas cuando hay una intersección de sistemas de opresión basados en factores como el género, la orientación sexual, la raza, la etnicidad, las capacidades y la clase social, entre otros. Sin embargo, el desafío consiste en demostrar que la perspectiva de género no es simplemente un "asunto de mujeres". Para ello, tenemos que ofrecer evidencia sólida de que se trata de un abordaje técnico y político transformador de las prácticas de ciberseguridad, centrado en la diversidad de pueblos y comunidades.

Tal como se puede ver en el análisis de la literatura existente, que acompaña a esta herramienta de evaluación[6], existe un debate en la intersección entre género y ciberseguridad. Si bien aún no es fácil encontrar consensos sobre el tema[7], resulta aún más difícil encontrar ejemplos generales de políticas nacionales de ciberseguridad desde una óptica de género. En América Latina y el Caribe, por ejemplo, se identificó a Chile, Guatemala, Ecuador, Jamaica y República Dominicana como países que, hasta cierto punto[8], cuentan con políticas de ciberseguridad nacional

6. APC. (2022a). Op. cit.
7. Sin embargo, hay señales de acuerdo en algunas áreas, como la necesidad de cerrar la brecha digital de género, la necesidad de acabar con la violencia de género en línea y en otros ámbitos, facilitada por la tecnología, y la necesidad de una mayor diversidad en el sector de la ciberseguridad y, en general, el de la tecnología. Por ejemplo, puedes consultar las Conclusiones acordadas en la sesión 67a de la Comisión sobre la Condición Jurídica y Social de la Mujer, de Naciones Unidas (CSW67): https://www.unwomen.org/en/csw/csw67-2023/session-outcomes
8. Por ejemplo, la estrategia actual de República Dominicana (2022-2030) no incluye referencias al género. Sin embargo, la estrategia previa de ciberseguridad (2018-2021) incluía referencias a la equidad de género. Puede ver más detalles en: https://cncs.gob.do/wp-content/uploads/2020/02/Decreto-230-18.pdf

con “alguna referencia general y explícita a una perspectiva de género o equidad de género, pero ninguno (de ellos) consolidó un mapa de ruta o indicadores para medir el progreso y la madurez del Estado en términos de ciberseguridad alineada a esta perspectiva”.[9] Un mapeo inicial de APC identificó también algunas referencias al género en las estrategias de ciberseguridad de países como Eswatini, Islandia y Nigeria (como se verá, con mayor detalle, más adelante en esta sección).

Por este motivo, creemos que es esencial ofrecer algún tipo de reflexión colectiva sobre la importancia de incluir un enfoque de género en las políticas de ciberseguridad nacional. Con este objetivo – y tal como se ve en la nota metodológica de la sección IV – realizamos entrevistas y organizamos talleres[10] con especialistas, para entender mejor por qué es importante adoptar una perspectiva de género en las políticas de ciberseguridad y en qué se diferencia este enfoque de los procesos tradicionales de formulación de políticas de ciberseguridad.

Los y las especialistas presentaron argumentos de peso y convincentes por los cuáles es importante adoptar una perspectiva de género:

- **El enfoque de género beneficia a la gran mayoría de las personas:** Una política de ciberseguridad con perspectiva de género implica que, desde el inicio, en cada paso del diseño, la implementación y la evaluación de las medidas de ciberseguridad a cargo del gobierno, la meta es generar un impacto positivo en el mayor número posible de personas en toda su diversidad y en toda la complejidad de las situaciones de la vida. No es una medida agregada a una política ya diseñada, sino que adopta la forma de un cambio sistémico. Esto se debe a que, para tener ese impacto positivo, la ciberseguridad desde un enfoque de género considera que las amenazas a la ciberseguridad afectan a las personas de diversas formas según su género y diferentes opresiones cruzadas como la raza y la clase social, y esto requiere especial consideración en las deliberaciones sobre ciberseguridad. Una consecuencia de esto es que, al adoptar una perspectiva de género para la ciberseguridad, se suele dar respuesta simultáneamente a muchas de estas opresiones que afectan a grupos vulnerables. Así, se puede pensar que la adopción de un enfoque de género en ciberseguridad constituye una forma de generar un cambio sistémico en el desarrollo de políticas.
- **El enfoque de género refuerza los derechos humanos y aumenta la seguridad nacional:** Sin este enfoque sistemático de las políticas de ciberseguridad, que incluye reunir datos correctamente desglosados sobre género y otros desafíos

9. Herrera Carpintero, P., & Peña Ochoa, P. (2021). *Género y Ciberseguridad.* Centro de Estudios en Derecho Informático, Facultad de Derecho, Universidad de Chile.
10. En los talleres utilizamos la definición de ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT): “La ciberseguridad es una colección de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, enfoques sobre gestión de riesgos, acciones, capacitación, mejores prácticas, garantías y tecnologías que se pueden usar para proteger el ambiente, la organización y los bienes cibernéticos de usuarios/as. La organización y los bienes de los/as usuarios/as incluyen los dispositivos informáticos conectados, el personal, la infraestructura, las aplicaciones, servicios, sistemas de telecomunicaciones y la totalidad de la información trasmitida y/o almacenada en el entorno cibernético. La ciberseguridad trata de garantizar el alcance y mantenimiento de las propiedades de seguridad de la organización y los bienes del/a usuario/a contra riesgos de seguridad relevantes en el ciberambiente. Los objetivos generales de seguridad son: disponibilidad, integridad, que puede incluir autenticidad y no repudio; y confidencialidad.” https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

interseccionales, grandes segmentos de población quedan vulnerables frente a peligros cibernéticos, lo que ayuda a ciberdelincuentes y otros actores maliciosos a explotar estas brechas de información y puntos ciegos. En otras palabras, si los y las responsables de tomar decisiones claves de seguridad no cuentan con políticas sensibles a las cuestiones de género, tomarán decisiones basándose solamente en suposiciones e información parcial, o incompleta. La consecuencia es que se debilita tanto la seguridad nacional, como los derechos humanos.

Nuestras consultas generaron también cuatro ideas que se relacionan entre sí y subrayan las diferencias entre la ciberseguridad concebida desde una perspectiva de género y los abordajes tradicionales para la elaboración de políticas de ciberseguridad. A diferencia de lo que sucede en los procesos tradicionales de desarrollo de políticas de ciberseguridad:

- **La perspectiva de género es explícita en su condición de abordaje interseccional:** Hay que entender el género como parte de un sistema complejo de opresiones interrelacionadas. Resulta fundamental reconocer esas opresiones interseccionales para conocer y comprender los riesgos y las necesidades que enfrentan sujetos (o individuos) complejos en el contexto de la ciberseguridad. La perspectiva de género también reconoce la necesidad de aceptar diversas prácticas y necesidades de seguridad que son significativas para las experiencias interseccionales, incluyendo prácticas de cuidado.[11]
- **El enfoque de género le da poder de acción a las personas:** El enfoque de género reconoce la importancia de contar con sujetos activos que tienen el poder de actuar en el proceso de creación de un ambiente en línea seguro. En otras palabras, además de reconocer a las personas desde una perspectiva interseccional y de género, y de reconocer las opresiones que esto puede implicar, el abordaje de género no considera a las personas como receptores/as pasivos/as de las medidas de ciberseguridad. Esta concepción es contraria a la percepción tradicional de la ciberseguridad, que subraya la pasividad de los sujetos incluso mediante el uso de conceptos tales como la "vulnerabilidad".
- **El enfoque de género pone en primer plano la igualdad y la justicia social en el proceso de elaboración de políticas:** Utilizando una lente feminista, el enfoque de género pone en primer plano los derechos humanos, así como

11. Las prácticas de cuidado, desde una perspectiva feminista, se realizan a través de las relaciones sociales, reconociendo las conexiones que existen entre lo personal y lo estructural – entre nuestras experiencias encarnadas y las normas culturales, instituciones y políticas que gobiernan el apoyo a las prácticas de atención y cuidados; y el cuidado siempre implica relaciones de poder. Ver Hoover, E. (2019, 29 October). Learning to care as a feminist. *openDemocracy*. https://www.opendemocracy.net/en/transformation/learning-care-feminist.
Al reconocer que la experiencia en línea y fuera de línea son indisociables, el cuidado digital constituye una manera de ocuparse de la seguridad digital desde la perspectiva del cuidado diario, y admitir que lo que afecta nuestros datos también tiene impacto sobre nuestro cuerpo. El concepto de cuidado digital supone que cuidar los datos también implica cuidar el cuerpo, y este cuidado debe ser diario, como un hábito, una cultura, una política. La idea del cuidado digital se propone resguardar el miedo, no alimentarlo. En términos metodológicos, el trabajo de cuidado digital toma la afección como principal conductor para el aprendizaje, confiando en ella como una poderosa forma de estructurar intercambios y generar transformaciones. Además, en el cuidado digital, el trabajo en torno de la seguridad se realiza desde una perspectiva integradora, entendiendo que las diferentes esferas del campo de la seguridad (física, digital, sicosocial, etc.) están estrechamente ligadas entre sí. Puedes leer más sobre este asunto en: https://fase.org.br/wp-content/uploads/2022/10/Digital-care-and-philanthropy.pdf

principios democráticos tales como la participación, la transparencia y la responsabilidad.

- **El enfoque de género reconoce el potencial transformador del proceso de elaboración de políticas:** El enfoque de género reconoce que los procesos de elaboración de políticas pueden ser transformadores y desafiar supuestos que tal vez ya no funcionen. Por ejemplo, cuestiona la distinción normativa entre las realidades en línea y fuera de línea, se propone reflexionar sobre las responsabilidades individuales y colectivas en lo relativo a la seguridad en línea de grupos e individuos, y amplía lo que es relevante para el debate sobre ciberseguridad. También reconoce que el diseño de soluciones tecnológicas no es neutro, y que a menudo contribuye a "invisibilizar" a las personas oprimidas.

Algunos ejemplos de políticas de ciberseguridad con una perspectiva de género[12]

Aunque es difícil encontrarlos, hay algunos ejemplos de políticas que intentan incorporar una perspectiva de género a las políticas de ciberseguridad. La lista incluye:

Estrategia nacional de ciberseguridad de Chile (2017-2022)[13]

- Este documento destaca que el país diseñará e implementará campañas de sensibilización con el énfasis puesto en los grupos vulnerables y la implementación de una perspectiva de género. Además, como objetivo, esta política de ciberseguridad subraya que todas las medidas propuestas en el documento deben ser diseñadas e implementadas desde una perspectiva de derechos humanos y que, para alcanzar esta meta, el país deberá poner el foco en cuestiones de género, lo que dejará a la vista las desigualdades que afectan a diversos grupos en el ciberespacio y permitirá encontrar maneras de resolver esas situaciones.

12. APC desea agradecer a Maia Levy Daniel, investigadora externa, que se ocupó de realizar este mapeo.
13. La estrategia completa, en español, se encuentra en: https://www.cnc.cl/wp-content/uploads/2020/02/Pol%C3%ADtica-Nacional-Ciberseguridad.pdf; puede ver más sobre la perspectiva de género en la política de ciberseguridad de Chile en este artículo, también en español, de Paloma Herrera Carpintero: https://rchdt.uchile.cl/index.php/RCHDT/article/view/51577/61679 Cuando se estaba terminando este documento, se debatía en Chile una nueva política de ciberseguridad actualizada. Se esperaba la publicación de la política nacional para fines de mayo de 2023, luego de una consulta pública. En una entrevista sobre este asunto, el Coordinador nacional de ciberseguridad Daniel Álvarez destacó que el género era uno de los temas transversales de la nueva estrategia. Puedes leer más sobre este tema en: https://www.df.cl/df-lab/transformacion-digital/coordinador-nacional-adelanta-los-principales-ejes-de-la-nueva-politica

Estrategia nacional de ciberseguridad de Ecuador (2022-2025)[14]

- De acuerdo con la meta estratégica relativa al aumento de la conciencia sobre ciberseguridad, la estrategia propone específicamente el desarrollo de programas que incluyan "una perspectiva que tenga en cuenta la equidad de género".

Estrategia nacional de ciberseguridad de Eswatini (2022-2027)[15]

- La estrategia se basa en la Estrategia Nacional de Desarrollo desde 2022, cuyo objetivo es responder a las dimensiones fundamentales de la calidad de vida, incluyendo la equidad de género. Sus objetivos estratégicos incluyen la creación de una sociedad de la información segura para Eswatini mediante el desarrollo de campañas nacionales de sensibilización hechas a medida y estudios "dirigidos a todos los grupos de usuarios/as, en particular los vulnerables y de riesgo, como los niños y las niñas, las mujeres, las personas mayores y otros grupos vulnerables."

Estrategia nacional de ciberseguridad de Nigeria (2021)[16]

- En el capítulo sobre fortalecimiento del marco legal y regulatorio, la estrategia incluye una sección sobre "derechos de género en línea" que reconoce los derechos y la importancia de la participación activa de las mujeres en el uso del ciberespacio. La estrategia consiste en "promover la inclusividad y la participación activa de las mujeres en el ciclo de vida completo de las actividades de nuestro ecosistema cibernético" y se compromete a eliminar "los obstáculos que impiden el acceso a las mujeres". Según el documento, una de las prioridades del gobierno de Nigeria es combatir la violencia en línea contra las mujeres. También se habla de promover la conciencia sobre la seguridad en línea y la educación de las mujeres, así como el "desarrollo de un foro multisectorial para guiar el desarrollo de iniciativas de protección y participación de género en línea", junto con el compromiso de brindar el apoyo necesario para que las organizaciones lleven a cabo iniciativas de promoción de las cuestiones de género a fin de reforzar la militancia, generar mecanismos para empoderar a las mujeres y crear oportunidades en el ecosistema de la ciberseguridad.

14. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf
15. https://www.esccom.org.sz/about/strategy/Eswatini%20National%20Cybersecurity%20Strategy%202022-2027.pdf
16. https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf?ref=benjamindada.com

Estrategia nacional de ciberseguridad de Islandia (2022-2037)[17]

- En su introducción, este documento subraya la necesidad de adoptar valores interdisciplinarios y considerar la diversidad y la inclusión de las personas afectadas, por ejemplo, en relación a la educación, el género, la edad y el contexto cultural.
- La estrategia enfatiza la cooperación, la diversidad y la inclusión "ya que la ciberseguridad es para todos y todas, y todo el mundo debería poder participar" y establece que "se prestará particular atención al aumento de la participación de las mujeres en este sentido".

Estrategia nacional de ciberseguridad de Jamaica (2015)[18]

- La estrategia incluye como objetivo que "se implementen medidas para proteger a los grupos vulnerables en el ciberespacio". Las actividades relativas a este objetivo para el mediano a largo plazo incluyen la implementación de programas para promover la adopción de prácticas seguras en línea por parte de los grupos vulnerables, incluyendo a los niños y niñas, las mujeres y las personas mayores, entre otros/as.

Estrategia nacional de ciberseguridad de España (2019)[19]

En la sección sobre ciberseguridad en la esfera internacional, al detallar los objetivos de la colaboración, la estrategia española menciona que el país "colaborará con la capacitación de otros Estados, prestando particular atención a las mujeres y las personas jóvenes, y promoverá la creación de canales de intercambio de información y experiencias, fomentando la adopción de acuerdos bilaterales y multilaterales en este campo para esos propósitos".

17. https://www.stjornarradid.is/library/04-Raduneytin/Haskola---idnadar--og-nyskopunarraduneytid/Icelandic%20National%20Cybersecurity%20Strategy%202022-2037.pdf
18. https://www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf
19. https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Estrategia nacional de ciberseguridad de Singapur (2021)[20]

- El documento establece que el gobierno trabajará con todos los grupos de interés para apoyar a los y las jóvenes, las mujeres y las personas profesionales que estén en el medio de su carrera a fin de que puedan seguir la carrera en ciberseguridad.
- Para poder "crear una reserva robusta de talentos cibernéticos", la estrategia destaca la necesidad de "atraer diversos talentos": "Aparte de la juventud, el gobierno está tratando de atraer más mujeres y profesionales calificados/as de ámbitos afines para que se unan a la industria de la ciberseguridad". El gobierno, además, "trabajará estrechamente ligado a la industria y junto con socios internacionales para alentar a las chicas a optar por programas de formación en ciberseguridad e inspirar a las mujeres a asumir roles en el área de la ciberseguridad".
- La Agencia de Ciberseguridad de Singapur, siguiendo esta estrategia, lanzó SG Cyber Women, una iniciativa para alentar a más mujeres a hacer una carrera del ámbito de la ciberseguridad.

20. https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021

IV. NOTA SOBRE METODOLOGÍA

Esta herramienta de evaluación fue creada en base a investigación teórica y entrevistas en profundidad con especialistas en el área del género y la ciberseguridad de diferentes regiones y contextos. Como ya hemos dicho, este documento se basa y es respaldado por el análisis sobre la literatura y el documento sobre normativa existente. Como parte de la metodología, también organizamos una sesión durante RightsCon 2022 que sirvió como una primera oportunidad para recolectar impresiones y comentarios sobre esta herramienta, y para hacer una lluvia de ideas con un grupo diverso de participantes sobre cómo incorporar el enfoque de género en las políticas de ciberseguridad.

Durante 2023, especialistas en género y ciberseguridad de diferentes sectores fueron invitados a revisar el texto, realizar aportes y sugerir cambios. Por último, en mayo de 2023 organizamos un taller de respuestas y comentarios con responsables de políticas de ciberseguridad que trabajan a nivel nacional y regional en África, durante el cual se analizaron las recomendaciones claves del texto.[21]

Cuando no existe un marco específico para analizar el género en las políticas de ciberseguridad, uno de los desafíos más difíciles consiste en encontrar un lenguaje común que tenga sentido para un amplio abanico de grupos de interesados/as de diferentes regiones.

Teniendo esto en cuenta, decidimos utilizar el Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CMM), creado por el Centro de seguridad cibernética global de la Universidad de Oxford.[22] El CMM es un marco desarrollado para analizar la madurez de la capacidad de ciberseguridad de un país a través de cinco dimensiones y en diferentes etapas de madurez (ver más abajo). Si bien el modelo no considera la dimensión de género y se trata de un abordaje

21. APC desea agradecer a Collaboration on International ICT Policy for East and Southern Africa (CIPESA) y Media Foundation for West Africa (MFWA) por su colaboración en la organización de este taller.
22. Global Cyber Security Capacity Centre. (2021). Op. cit.

abierto al examen crítico, su amplia adopción a través de las diversas regiones hace que valga la pena trabajar con él. Este modelo ha sido adoptado e implementado en más de 80 países del mundo entero gracias a la Organización de los Estados Americanos (OEA), el Banco Mundial, la Unión Internacional de Telecomunicaciones (UIT), la Commonwealth Telecommunications Union y el Global Forum on Cyber Expertise. También ofrece un lenguaje común que puede ser estratégico para enmarcar las conversaciones en torno de las cuestiones de género, además de constituir un modelo en etapas que puede ayudar a guiar la inclusión de un enfoque de género en las políticas de ciberseguridad, según el contexto nacional. Una de las conclusiones a las que se llegó a raíz de las entrevistas exhaustivas fue que el enfoque de género en la ciberseguridad constituye un trabajo de largo alcance, ya que su incorporación en mayor o menor escala depende de las condiciones culturales y políticas de cada país. Ello implica que existen diferencias evidentes entre los países a la hora de evaluar la incorporación del género en las estrategias nacionales de ciberseguridad : algunos tienen niveles de madurez más altos que otros. Teniendo en cuenta estos argumentos, el CMM es una buena herramienta en cuanto a su adaptabilidad a las diferentes realidades que viven las personas que lo utilizan.

También adaptamos el documento "Assessing National Cybersecurity Strategies from a Human Rights Perspective"[23], elaborado en 2022 por Global Partners Digital (GPD). El documento identifica seis componentes esenciales para el desarrollo de una política nacional de ciberseguridad y brinda recomendaciones generales sobre lo que debería incluirse en esos componentes desde una perspectiva de derechos humanos. Los derechos humanos y el enfoque de género para la ciberseguridad se relacionan entre sí: ambos consideran que las personas deben ser el centro de cualquier estrategia en la materia. En este sentido, el marco que presenta GPD ofrece un espacio habilitante que sirve de base y se puede adaptar al enfoque de género.

Como ya se dijo, esta herramienta de evaluación va acompañada de otros dos recursos desarrollados antes que este documento.[24] Dichos recursos constituyen un punto de referencia para nuestro debate aquí y han informado buena parte de nuestra reflexión contextual sobre el tema del género y la ciberseguridad. Los documentos son:

Análisis de la literatura existente

El análisis de la literatura existente explora la manera en que se ha tratado la ciberseguridad como espacio de género en la investigación, a fin de contribuir a promover una política de ciberseguridad más sensible al género. En este análisis, encontrarás:

23. Global Partners Digital. (2022). *Assessing National Cybersecurity Strategies from a Human Rights Perspective.* https://www.gp-digital.org/wp-content/uploads/2022/04/Assessing-NCSS-from-human-rights-perspective.pdf
24. Ambos se pueden encontrar aquí: https://www.apc.org/en/pubs/framework-gender-cybersec

- Importantes conceptos sobre género.
- Un contexto general sobre el desarrollo del concepto de ciberseguridad como espacio de género.
- Conexiones entre el surgimiento de los derechos humanos en la ciberseguridad y la perspectiva de género, y los conceptos transversales más prevalentes en las diversas investigaciones que tienen en cuenta al género en los varios campos de la ciberseguridad.
- Debate sobre alguno de los tópicos donde esté más presente la perspectiva de género en la ciberseguridad.

Normativa, reglas y directrices

Existen herramientas, agendas y marcos relevantes en los que se pueden apoyar quienes se dedican al activismo en el área de la ciberseguridad cuando se trata de promover una perspectiva de género en el debate nacional, o multilateral, sobre ciberseguridad. Dichos recursos se pueden utilizar como fuente de información, o para generar coherencia política con los compromisos existentes de un gobierno con la igualdad de género. Este documento presenta un resumen sobre los instrumentos más relevantes:

- La Convención para la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW)
- La Declaración y la Plataforma de Acción de Beijing
- La Agenda Mujeres, paz y seguridad (MPS)
- Los documentos resultantes de la Cumbre Mundial sobre la Sociedad de la Información (CMSI)
- La Agenda 2030 para el Desarrollo Sostenible y los Objetivos de Desarrollo Sostenible (ODS)
- Los informes y resoluciones del Consejo de Derechos Humanos de Naciones Unidas
- Las iniciativas de la Unión Internacional de Telecomunicaciones (UIT)
- Los procesos de ciberseguridad de la Asamblea General de Naciones Unidas.

V. ¿A QUIÉN SE DIRIGE ESTA HERRAMIENTA DE EVALUACIÓN?

Nuestro objetivo es que este marco – la herramienta de evaluación, el análisis de la literatura existente y el resumen de la normativa, las reglas y las directrices – sea de utilidad para diferentes públicos y de diferentes maneras. El público objetivo principal son las personas a cargo de las políticas que trabajan en la elaboración de estrategias y políticas de ciberseguridad, al igual que las organizaciones de la sociedad civil que trabajan en ciberseguridad y se dedican al activismo a nivel nacional. El siguiente grupo al que se dirige esta herramienta son las organizaciones regionales que influyen sobre las políticas de ciberseguridad a nivel nacional, y las organizaciones internacionales que elaboran guías para crear estrategias nacionales de ciberseguridad. También pretendemos ser de utilidad para ambos públicos cuando participan en espacios globales relacionados con estos temas y en los debates multilaterales. Por último, esperamos que sea útil, en general, para las organizaciones de la sociedad civil y la comunidad de investigación involucradas en cuestiones de género y ciberseguridad.

VI. CÓMO USAMOS EL MODELO DE MADUREZ DE CAPACIDADES EN CIBERSEGURIDAD PARA LAS NACIONES (CMM)

El CMM considera que el desarrollo de las políticas de ciberseguridad consiste en cinco etapas diferenciadas de madurez: inicial, formativa, consolidada, estratégica y dinámica. También articula cinco dimensiones que constituyen el amplio rango de capacidades que debe tener un gobierno para asegurar la ciberseguridad de manera eficiente. Esas dimensiones son:

1. Desarrollar una estrategia y política de ciberseguridad.
2. Fomentar una cultura de ciberseguridad responsable en la sociedad.
3. Construir la capacidad y el conocimiento en ciberseguridad.
4. Crear marcos legales y regulatorios eficientes.
5. Controlar los riesgos mediante normativas y tecnologías.

Por último, cada dimensión tiene cuatro aspectos a ser considerados: desarrollo de la estrategia, contenido, implementación y análisis[25], y participación internacional.

Esta herramienta de evaluación adapta este modelo para ayudar a las personas responsables de formular políticas y a las organizaciones de la sociedad civil a buscar la manera de introducir una perspectiva de género en sus procesos de elaboración de políticas nacionales de ciberseguridad. Nuestro foco está puesto en:

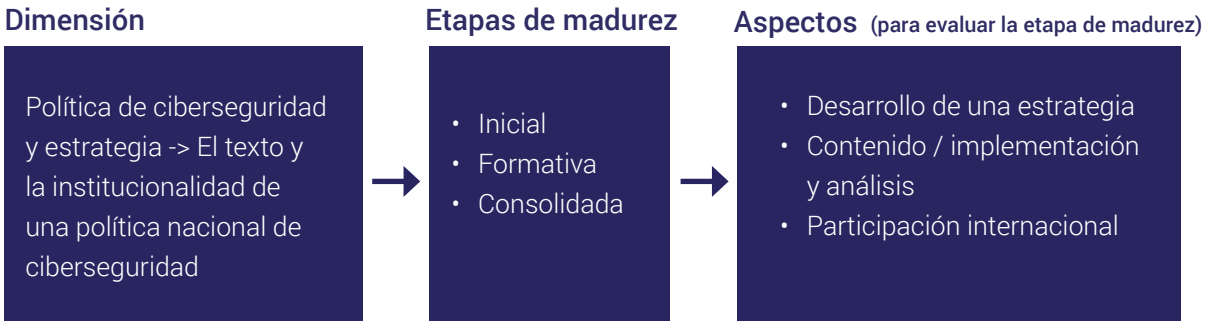
25. A diferencia de la CMM, en esta herramienta de evaluación se funde el aspecto del contenido con el de la implementación y la revisión. El motivo es práctico: es necesario contar con el contenido de la estrategia nacional de ciberseguridad para garantizar que haya un mecanismo de monitoreo, coordinación y análisis de la política. En este sentido, esta herramienta une todos estos aspectos en uno sólo, ya que funciona de manera transversal con la recomendación de incluir la dimensión de género y, sugiere hacerlo, sobre todo, en la etapa formativa de la política, recomendando mecanismos de coordinación, supervisión y análisis.

- La estrategia nacional de ciberseguridad, que constituye un factor de la dimensión "Desarrollo de una política y estrategia nacionales de ciberseguridad" del CMM.
- Las tres primeras etapas de madurez: inicial, formativa y consolidada.

En las dos etapas restantes y finales del CMM ("estratégica" y "dinámica"), se cuenta con que ya se ha publicado una política nacional de ciberseguridad y se ha establecido un marco institucional. En este documento, nos referimos a esas dos últimas fases como la "visión" que se debe alcanzar con una política nacional de ciberseguridad que considere que el enfoque de género es una parte esencial de su desarrollo.

Como se establece el CMM:

> La estrategia nacional de ciberseguridad [Factor D.1.1 de la dimensión 1] es esencial para incluir la agenda de la ciberseguridad en el gobierno porque ayuda a dar prioridad a la ciberseguridad como área política de importancia, establece las responsabilidades y mandatos de actores claves gubernamentales y no gubernamentales, y guía la asignación de recursos hacia los problemas y las prioridades emergentes de la ciberseguridad.[26]



El Cuadro 1 resume las tres primeras etapas de madurez, destacando los objetivos claves a los que se debe apuntar en cada una. En vez de la palabra "estrategia", que se utiliza en el CMM, nos referimos a "política". El resto de este documento trata sobre recomendaciones de acción para alcanzar las metas de cada una de estas etapas.

26. Global Cyber Security Capacity Centre. (2021). Op. cit.

Inicial

Generar conciencia entre las partes interesadas, sobre la importancia de concebir la ciberseguridad desde una perspectiva de género.

Desarrollo de una estrategia

Entender los riesgos y amenazas para la ciberseguridad nacional desde una perspectiva de género.

Contenido / implementación y análisis

Analizar los marcos legales y las políticas que pueden responder a las necesidades y los desafíos de género planteados antes, al menos en forma parcial.

Participación internacional

Mapear el conocimiento y la participación del gobierno en los debates internacionales sobre género y ciberseguridad, u otros temas relacionados con esto, como la gobernanza en internet y el género, género y STEM (ciencia, tecnología, ingeniería y matemáticas), y ciberdelitos desde la perspectiva de género.

Formativa

Incluir la perspectiva de género en los diversos aspectos estratégicos de la política de ciberseguridad y su plan de acción.

Desarrollo de una estrategia

Realizar una evaluación nacional de riesgos para recolectar información y evidencia sobre los riesgos interseccionales que enfrentan las personas en el contexto de la ciber-seguridad, identificando las brechas que hay en los mecanismos de seguridad actuales.

Habilitar mecanismos de consulta inclusiva.

Contenido / implementación y análisis

Influir sobre los diferentes componentes del desarrollo de una política nacional de ciberseguridad, brindando incluso contenidos sobre género.

Garantizar que el plan de acción priorice las acciones enfocadas en la cuestión de género.

Participación internacional

Participar, junto con las autoridades en los foros y procesos regionales y globales a fin de iniciar, o profundizar, la comprensión sobre ciberseguridad y género en el contexto internacional.

Consolidada

Participar activamente en la evaluación de los resultados de la política y participar en la cooperación nacional e internacional para fortalecer el concepto de ciberseguridad con perspectiva de género.

Desarrollo de una estrategia

Evaluar si las acciones de implementación de las políticas cumplen con las metas propuestas y presentar pruebas para apoyar cualquier mecanismo de seguimiento que sea necesario.

Contenido / implementación y análisis

Generar instancias de diálogo, intercambio de conocimientos y cooperación mutua con otras políticas públicas que puedan estar relacionadas con el género o la ciberseguridad.

Participación internacional

Facilitar instancias de conocimiento sobre la participación del gobierno en foros regionales e internacionales, consultar aportes y tratar de coordinar el posicionamiento de la cuestión de género en la ciberseguridad.

VISION

Después de estas tres etapas:

Todos los grupos de interés consideran que la perspectiva de género es estratégica.

La perspectiva de género en la ciberseguridad tiene un impacto tangible y positivo en la solidez y la resiliencia de la infraestructura frente a los ataques, ha reforzado los derechos humanos para toda la diversidad de las personas del ciberespacio, y ha tenido un impacto positivo en las principales culturas vinculadas a la ciberseguridad tanto a nivel empresarial, como social.

El país se convierte en un paladín de la perspectiva de género en ciberseguridad a nivel regional e internacional.

EL GÉNERO EN LA POLÍTICA NACIONAL DE CIBERSEGURIDAD

¿A qué nos referimos como etapas de madurez en este documento?
La CMM define etapas de madurez para todas las dimensiones y factores de la capacidad de ciberseguridad en un país. En este documento, nos centramos en las políticas nacionales de ciberseguridad, que, como todo desarrollo de políticas, pasa por un proceso evolutivo que es definido por factores contextuales, incluyendo los recursos institucionales y del país, la voluntad política y las habilidades y conocimientos de las personas responsables de las políticas. Si bien es difícil determinar exactamente dónde se encuentran los procesos de políticas en términos de brindar una respuesta integral y significativa a las necesidades de ciberseguridad para todas las personas, hablamos en general de “etapas de madurez”. La etapa actual del proceso de desarrollo de políticas en tu país podría ser en realidad una mezcla de diferentes etapas.

A. LA ETAPA INICIAL

En esta etapa, el debate sobre ciberseguridad y género es nuevo para la mayoría de los/as interesados/as. Por lo tanto, el objetivo de esta fase es generar conciencia entre los grupos de interés sobre la importancia de concebir la ciberseguridad desde una perspectiva de género.

Aspecto de desarrollo de una estrategia

Aunque en esta etapa aún no existe una política nacional de ciberseguridad, es probable que ya se esté planificando el desarrollo de una estrategia. El foco de desarrollo de la estrategia debe ser doble: primero, entender los riesgos y amenazas de ciberseguridad nacional desde una perspectiva de género mediante un investigación y un proceso de consulta inclusivo; y segundo, una vez comprendidos y asumidos los riesgos y las amenazas, sensibilizar sobre la importancia de contar con una perspectiva de género para la ciberseguridad, así como los riesgos y amenazas identificados entre los/as interesados/as a cargo de formular políticas.

Estos procesos de consulta constituyen una manera de construir evidencia que tenga impacto en las decisiones políticas específicas que se tomen y definir lo que se debe priorizar e incluir. Para generar dicha evidencia, puedes llevar a cabo las diferentes acciones que se describen a continuación. Las mismas no siguen ningún orden en particular y hay que evaluar su utilidad según las posibilidades contextuales de cada país.

RECOMENDACIÓN

Identificar una o un defensor del género y la ciberseguridad dentro del gobierno:

Ese defensor o adalid no tiene que ser experto/a en género, sino más bien, una persona que crea firmemente que es esencial incorporar esta perspectiva en las políticas nacionales de ciberseguridad a fin de responder a los desafíos del país. Esta persona tampoco tiene que trabajar en ciberseguridad. Su presencia destranca procesos y guía iniciativas.

Enmarcar una perspectiva de género amplia para la ciberseguridad:

Hay que destacar que, si bien los asuntos tales como la participación de las mujeres y la violencia de género en línea son fundamentales, el concepto de ciberseguridad con perspectiva de género es mucho más amplio que eso y

también cubre cuestiones tales como los diferentes riesgos e impactos que tienen las amenazas cibernéticas según el género y otras interseccionalidades; las diferentes necesidades, prioridades y percepciones de ciberseguridad según el género y otros factores; y cómo debe ser la capacitación en ciberseguridad desde la perspectiva interseccional de género. Un abordaje de ciberseguridad con perspectiva de género consiste en entender la ciberseguridad desde los impactos interseccionales que tienen sus políticas. Esto significa que la perspectiva de género aplicada al campo de la ciberseguridad puede ser relevante a muchos otros organismos o ministerios de un gobierno.

Las preguntas claves para esta fase de desarrollo estratégico son:

- ¿Cuáles son los riesgos y consecuencias que implican algunas amenazas específicas en el ciberespacio para las figuras públicas, la comunidad de periodistas y activistas por los derechos humanos, y las personas marginadas o vulnerables a causa de su género, raza, religión, etnicidad, capacidades, clase social, filiación política, u orientación sexual?
- ¿Cuáles son las capacidades, las necesidades y las prioridades de los diferentes géneros y sus interseccionalidades en lo que se refiere a la ciberseguridad?
- ¿Cómo incide la normativa de género en el diseño de la ciberseguridad en tu país?
- ¿Cuáles son las brechas de género y de conocimiento sobre ciberseguridad que existen hoy en tu país?
- ¿Cuáles son los actores relevantes de diferentes sectores comprometidos a adoptar la perspectiva de género en el área de la ciberseguridad?

Un mapeo general sobre un amplio rango de grupos de interés

Es esencial encontrar voces que puedan ayudar a entender cómo impacta el género en la ciberseguridad de cada país. Tal como se constató en el análisis de la literatura que viene junto con esta herramienta de evaluación, hay muchos nodos en ciberseguridad en los que se ha estudiado el género.[27] Se recomienda utilizar esos nodos como punto de partida para identificar actores y grupos de interés que ya estén trabajando en áreas relacionadas con el género y la ciberseguridad, o en un campo relevante para este tópico (ver Cuadro 2).

.

En esta etapa, hay que recordar que rara vez hay muchos actores trabajando directamente en cuestiones de género y ciberseguridad, de modo que resulta estratégico ampliar las consultas a fin de incluir actores que puedan interesarse en el tema de la ciberseguridad, como las organizaciones que trabajan con los

27. Analizar la sección "Critical nodes of cybersecurity for a gender perspective" del análisis de la literatura que forma parte de este marco: APC. (2022a). Op. cit.

Cuadro 2: ¿Qué actores trabajan a nivel local en cuestiones relativas al género en el área de la ciberseguridad?	
Actores	Nodos críticos de ciberseguridad desde una perspectiva de género
Sociedad civil Sector técnico Sector privado Academia Organismos y departamentos estatales	• La brecha de género en el campo de la ciberseguridad (industria y política) • Las dimensiones de la violencia de género en la ciberseguridad • Vulnerabilidades diferenciadas frente a ciberataques (acceso a internet y capacidades digitales; factores demográficos en el comportamiento relativo a la ciberseguridad) • Impacto de incidentes cibernéticos diferenciado en base al género • Reconfiguración de los marcos de análisis de la ciberseguridad • Infraestructura de internet autónoma y feminista[28] • Políticas públicas internacionales de ciberseguridad

derechos de las mujeres y derechos sexuales, o con jóvenes, asuntos de raza o etnicidad, entre otras áreas interseccionales. Este mapeo te permitirá identificar socios estratégicos potenciales que puedan participar en las numerosas acciones necesarias para introducir una perspectiva de género en las políticas de ciberseguridad, incluyendo la sensibilización y la capacitación.

Conciencia de género y ciberseguridad entre los diversos grupos de interés identificados

En esta fase es esencial sensibilizar acerca de la relación fundamental que existe entre el género y la ciberseguridad, ya que puede ser que más adelante esto forme parte de la planificación de las acciones de capacitación formal, en la etapa formativa de la estrategia nacional de ciberseguridad. Las partes interesadas se pueden agrupar en dos grandes categorías – las que saben sobre género y asuntos interseccionales, y las que saben sobre ciberseguridad – y el foco de los procesos de sensibilización será diferente para cada una.

28. Por más información sobre infraestructuras feministas, se puede consultar: Toupin, S., & Hache, A. (2015). Feminist autonomous infrastructures. In A. Finlay (Ed.), *Global Information Society Watch 2015: Sexual rights and the internet*. APC & Hivos. https://www.giswatch.org/index.php/en/internet-rights/feminist-autonomous-infrastructures; Zanolli, B., Jancz, C., Gonzales, C., Araujo, D., & Prado, D. (2018.) Feminist infrastructure and community networks: An opportunity to rethink our connections from the bottom up, seeking diversity and autonomy. In A. Finlay (Ed.), *Global Information Society Watch 2018: Community networks*. APC & IDRC. https://www.giswatch.org/en/infrastructure/feminist-infrastructures-and-community-networks

Generar conciencia sobre la importancia de la ciberseguridad entre actores que trabajan con cuestiones de género, o derechos de las mujeres, y otros asuntos interseccionales relacionados

Rara vez las partes interesadas que trabajan con estos asuntos saben sobre ciberseguridad, o consideran que las políticas nacionales de ciberseguridad sean un espacio de activismo importante. El trabajo con estos actores para generar conciencia sobre la importancia de la ciberseguridad tiene múltiples beneficios: aumenta su interés en la ciberseguridad, lo que puede traducirse en proyectos tales como iniciativas de capacitación o investigación a fin de generar evidencia para las políticas; fortalece las relaciones entre los diversos actores; y genera lenguaje y conocimiento técnico de ciberseguridad entre los actores, de forma que pueden participar no sólo en el diseño de las políticas, sino también en su implementación. Uno de los resultados más importantes de este proceso es que ayuda a identificar y mapear los riesgos y desafíos contextuales e interseccionales que afectan a las personas desde una perspectiva de género, lo que a su vez alimenta el proceso de elaboración de políticas.

Generar conciencia sobre la importancia de que los actores del campo de la ciberseguridad tengan una perspectiva de género

El análisis de la literatura existente que acompaña a esta herramienta de evaluación identifica varios aspectos de la ciberseguridad en los que el género es importante. Se recomienda introducir la cuestión de género con el foco puesto en esos aspectos.

Ambos procesos serán importantes al pasar a la etapa formativa, en la que se podrán sentir los beneficios de contar con actores informados en los debates.

Consulta internacional

Es probable que, en esta etapa inicial, tengas que pedir consejo sobre estrategias de ciberseguridad a diferentes socios internacionales, tales como las personas responsables de formular políticas de otros países, la comunidad académica, expertos/as de las instituciones, o especialistas de la sociedad civil. Es importante mapear los y las diversos/as especialistas que pueden prestar apoyo a un país en esta área. Por ejemplo, puede haber gobiernos que tengan como misión la incorporación del género en las políticas públicas y ellos pueden asesorar en cuanto a buenas prácticas en esa área. Como se vio en el análisis de la literatura, también hay muchos/as profesionales y organizaciones que trabajan en la Agenda Mujeres, Paz y Seguridad y por ello tienen una relación más estrecha con la ciberseguridad, de manera que pueden brindar lineamientos y sugerencias. También hay que tener en cuenta al sector privado, ya que muchas compañías han aumentado la diversidad en los equipos que trabajan en la industria de la ciberseguridad. Estos actores pueden informar el proceso de elaboración de políticas y también son aliados potenciales para las futuras negociaciones en foros globales.

Las Organizaciones e instituciones internacionales pueden colaborar en el proceso de elaboración de políticas

Cada vez hay más instituciones que trabajan y generan evidencia sobre la importancia de tener un concepto de ciberseguridad basado en cuestiones de género. Estas son sólo algunas de las que puedes consultar:

- Asociación para el Progreso de las Comunicaciones (APC) – https://www.apc.org
- Global Partners Digital (GPD) – https://www.gp-digital.org
- Chatham House – https://www.chathamhouse.org[29]
- Instituto de las Naciones Unidas para la Investigación sobre el Desarme (UNIDIR) – https://unidir.org[30]
- Liga Internacional de las Mujeres por la Paz y la Libertad (WILPF) – https://www.wilpf.org/
- Centro de Ginebra para la Gobernanza del Sector de la Seguridad (DCAF) – https://www.dcaf.ch

b. El aspecto de los contenidos/implementación y el análisis

En la etapa inicial, el aspecto del "contenido" implica conseguir evidencia local, analizar las investigaciones locales y globales disponibles sobre la cuestión de género y ciberseguridad, y analizar los documentos de política nacional y global que sean relevantes para tu trabajo..

RECOMENDACIÓN

Recolectar estudios de casos, informes y ejemplos de políticas:

Buscar informes relevantes para tu contexto nacional y que reflejen la investigación y los procesos de desarrollo de políticas a nivel global. Asegúrate de reunir informes que abarquen un concepto amplio de género y otras interseccionalidades (por ejemplo, orientación sexual, raza y clase social). Analiza políticas de género en otras áreas que puedan tener impacto en tu trabajo, por ejemplo, sobre políticas de acción afirmativa en las carreras de ciencias, tecnología, ingeniería y matemáticas, o políticas relativas a la violencia de género en línea. Vale la pena tomar nota del vocabulario y las expresiones específicas que te parezcan de utilidad.

29. https://www.chathamhouse.org/about-us/our-departments/international-security-programme/understanding-gender-and-cybersecurity
30. https://unidir.org/programmes/gender-and-disarmament

Conseguir pruebas

El objetivo de la etapa inicial es reunir evidencia sobre la situación de la ciberseguridad en el contexto local. Por ese motivo, la clave está en conseguir un amplio abanico de estudios e informes que muestren la relevancia que tienen el género y otras interseccionalidades para la ciberseguridad a nivel local, y lo mismo se aplica a las campañas de sensibilización referidos anteriormente, que sirven para identificar los riesgos y desafíos. El mapeo de actores también es útil porque permite identificar el trabajo de reunir pruebas cuantitativas y cualitativas relevantes para nuestro proceso de elaboración de políticas.

Sin embargo, cuando hay poca evidencia local publicada – lo que es común, ya que el tópico es muy nuevo aún – puedes crear estudios de caso enfocados en este tema a fin de documentar el impacto interseccional de los mecanismos de ciberseguridad en el contexto local. Los recursos que tengas determinarán el alcance de la investigación. Por ejemplo, si desarrollas estudios de caso sólo en un campo específico, como puede ser el impacto que tiene la ausencia de una perspectiva de género en los Equipos de Respuesta ante Emergencias Informáticas (CSIRT, por su sigla en inglés),[31] el impacto de género en incidentes específicos tales como el ransomware o la filtración de datos, o el impacto afirmativo de las políticas de acción sobre las carreras de ciencias, tecnología, ingeniería y matemáticas. Pero, al presentar esos estudios de caso, tendrás que enmarcarlos como ejemplos dentro de un abordaje más amplio de las cuestiones de género integradas a las políticas de ciberseguridad.

Si bien el objetivo, en esta etapa, consiste en reunir evidencia local para apoyar el proceso de elaboración de políticas, los estudios regionales e internacionales se pueden usar para entender mejor los desafíos que enfrentan los países del mundo entero en esta área.

Otra parte importante del aspecto del "contexto" es el análisis de las políticas y estrategias nacionales relativas a la ciberseguridad (por ejemplo, estrategias digitales nacionales, o estrategias nacionales en el área de la inteligencia artificial). Es necesario que comprendas si realmente reflejan prioridades específicas de género, y en caso afirmativo, en qué medida es así. También tienes que analizar políticas de campos interseccionales que sean relevantes para la ciberseguridad desde una perspectiva de género, como las estrategias de género, las políticas de inclusión y diversidad, y las de ciencias, tecnología, ingeniería y matemáticas. Además, tendrás que revisar los marcos legales relevantes tales como aquellos que se refieren a la violencia de género en línea, o la legislación sobre la protección de datos.

31. Equipos de técnicos/as y otros/as expertos/as creados para responder ante problemas o incidentes de seguridad.

c. El aspecto de la participación internacional

RECOMENDACIÓN

Mapear la forma en que el gobierno participa en debates internacionales relevantes:

Mapear el conocimiento y la participación del gobierno en los debates internacionales sobre género y ciberseguridad, u otros temas internacionales. El mapeo debe incluir una buena comprensión sobre la participación del gobierno en los foros y espacios de ciberseguridad y gobernanza de internet donde se trata el tema de las mujeres y las tecnologías de información y comunicación (TIC).

Este aspecto explora el alcance de la participación del gobierno y otros grupos relevantes de interesados/as, como la sociedad civil o las empresas, en los debates y foros internacionales sobre políticas de ciberseguridad.[32]

Si bien se puede esperar que haya cierta participación en los foros sobre ciberseguridad, es probable que, al menos en lo que se refiere al gobierno, la participación no implica promover la perspectiva de género para la ciberseguridad. Sin embargo, es importante mapear este compromiso y cuáles son los foros implicados. También es importante la participación de los/as interesados/as en foros relacionados, como los de gobernanza de internet, o los debates sobre género y TIC. Al realizar este mapeo, entenderás mejor la brecha de conocimiento de algunos grupos de interés claves en el proceso de elaboración de políticas y dónde es necesario reforzar ese conocimiento.

32. Para ampliar el contexto, puedes ver la publicación acompañante sobre las normativas, reglas y directrices internacionales existentes relativas al género y la ciberseguridad: APC. (2022b). Op. cit.

B. ETAPA FORMATIVA

En esta etapa, ya están mapeadas las prioridades de un enfoque de género aplicado a las políticas de ciberseguridad para tu contexto local gracias a investigaciones sobre el contexto, campañas de sensibilización y recolección de evidencia local sobre riesgos y desafíos. Esta etapa implica trabajar con la evidencia para asegurar que tus hallazgos influyan y modelen el esbozo del una política y un plan de acción de ciberseguridad.

a. El aspecto del desarrollo de una estrategia

El CMM reconoce que, en la etapa formativa, el proceso de desarrollo político ya está iniciado y se ha articulado un primer esbozo de política nacional de ciberseguridad. Además, ya hay acuerdo sobre la necesidad de realizar procesos de consulta con grupos de interés claves, durante los cuales se debatirá el texto del documento en proceso de elaboración. Hay dos aspectos del desarrollo de la estrategia que deben considerarse con cuidado:

Evaluación nacional de riesgo

Antes de desarrollar contenidos para la política, es importante elaborar una evaluación nacional de riesgos. Esto puede arrojar información valiosa para el desarrollo, la ejecución y la evaluación de una política. Los gobiernos suelen utilizar evaluaciones de riesgo para los procesos de elaboración de políticas.

Es importante que esta evaluación identifique los riesgos específicos que pueden enfrentar los individuos debido a su género, u otras opresiones interseccionales relacionadas. Buena parte de la evidencia para esta evaluación nacional de riesgos ya se consiguió en la etapa inicial. Sin embargo, puede ser que se hayan identificado brechas en relación a una mayor participación. Es posible que también tengas que realizar una evaluación mucho más amplia para mapear todos los riesgos que enfrentan otros sectores y actores a los que no involucraste en la etapa inicial.

La evaluación nacional de riesgos crea una imagen general de riesgos relacionados entre sí que sirve para que las políticas resultantes respondan adecuadamente a los riesgos identificados. En este punto, podrías articular el resumen del documento sobre políticas aprovechando lo que ya has desarrollado y ver si ya puedes identificar alguna brecha.

Mecanismos de consulta

Los mecanismos de participación para consultar sobre los borradores de las políticas son importantes. Constituyen una forma de reforzar la confianza y la colaboración entre las partes interesadas que reciben el impacto de las políticas

de ciberseguridad. Deben ser inclusivas y facilitar los aportes del sector, la comunidad de especialistas y el público en general.

Hay que poner en marcha diferentes mecanismos, como reuniones y procesos en línea para enviar aportes para la elaboración de las políticas. Dichos mecanismos deben adecuarse a las capacidades y los recursos de las partes interesadas. Los mecanismos también deben darles tiempo para analizar los borradores y hacer aportes.

Dedica tiempo a decidir qué mecanismos de participación son importantes. Estos procesos son importantes porque hay que gestionar las expectativas de los diferentes grupos de interés desde el arranque. Los mecanismos y las limitaciones de la participación tienen que ser transparentes para todas las partes interesadas y, para evitar un desequilibrio entre las voces de diferentes sectores de cada grupo, es necesario diseñar procesos y espacios de consulta ampliamente representativos, incluyendo la aclaración de cómo se convoca, dónde es la convocatoria y cómo se facilitan las conversaciones.

Debes contemplar mecanismos que aseguren responsabilidad, para garantizar la incorporación de todos los aportes y hacer que todas las partes interesadas estén al día en cuanto al estado del proceso y a la forma en que se van incorporando sus aportes. Si los procesos de participación son inclusivos y bien pensados, servirán para que los/as interesados/as se comprometan con las políticas y el éxito de su implementación.

En cuanto al llamado a participar en las consultas, tienes que asegurarte de incluir a las partes interesadas que involucraste en la etapa inicial. Esto garantiza la

RECOMENDACIÓN

Diseña cuidadosamente los procesos de participación para garantizar la inclusión:

Elaborar una perspectiva de género para aplicarla a la ciberseguridad no consiste solamente en reunir responsables políticos en torno de una mesa, sino en realizar una amplia consulta sobre el asunto. Piensa en quienes deben participar en el debate desde una perspectiva de género e interseccional. Esto puede incluir individuos de todos los organismos de gobierno, ONG que trabajan con grupos marginados, o asociaciones comerciales. Los principales departamentos de gobierno que podrías incluir en el proceso son aquéllos que trabajan con derechos de las mujeres y las personas LGBTQIA+, protección de la infancia, inclusión digital, promoción de la igualdad y la diversidad, y combate contra la desinformación.

Prestar atención a las dinámicas de poder:

Pensar en los procesos de participación, prestando particular atención a las dinámicas de poder y a la manera de asegurar que los grupos más vulnerables se hagan oír. Si hay reuniones presenciales, plantear preguntas prácticas tales como "¿Qué distancia tienen que recorrer los y las participantes para llegar hasta aquí?" Si las reuniones son en línea, ten en cuenta el costo que deben asumir algunas personas para poder participar, por ejemplo, el pago de datos móviles.

continuidad y la representación de las personas más afectadas por amenazas del área de la ciberseguridad.

Participación de la sociedad civil

Desde la perspectiva de la sociedad civil, estos mecanismos de consulta constituyen una oportunidad para presentar los riesgos y amenazas a la ciberseguridad desde una perspectiva de género y para defender prioridades políticas específicas en este sentido. Los mecanismos de consulta también ofrecen una excelente oportunidad para evaluar los resultados probables de las políticas y su implementación.

La sociedad civil debe considerar el uso de mecanismos de consulta como una oportunidad para coordinar con otras organizaciones, a fin de presentar un frente común. Los actores tendrán que mapear la evidencia disponible a favor de la adopción de un abordaje interseccional y de género de la ciberseguridad, para poder comunicar claramente los riesgos y desafíos para las comunidades interseccionales. La relación entre género y ciberseguridad se debe presentar como algo más que una "cuestión de mujeres" a fin de evitar cualquier resistencia que surja en los debates, y para mostrar, además, que la perspectiva de género tiene relevancia intersectorial. En este sentido, los nodos más comunes de ciberseguridad y género que se presentan en el análisis sobre la literatura existente pueden ser una base que guíe la intervención de la sociedad civil.[33] Por último, la sociedad civil debe realizar una adaptación estratégica de sus pruebas y sus posturas al lenguaje técnico de los debates sobre ciberseguridad, para que los y las responsables de formular las políticas vean la relación entre ciberseguridad y género como algo más natural.

33. Los nodos esenciales de la ciberseguridad desde un punto de vista de género son: la brecha de género que hay en el campo de la ciberseguridad (industria y política); las dimensiones de la violencia de género en el área de la ciberseguridad; vulnerabilidades diferentes frente a ciberataques (acceso a internet y conocimientos digitales; factores demográficos en el comportamiento de ciberseguridad); la diferencia de impacto de los incidentes cibernéticos según el género; reconfiguración de los marcos de análisis sobre ciberseguridad; infraestructura de internet feminista y autónoma; y políticas públicas internacionales sobre ciberseguridad.

b. El aspecto de los contenidos/implementación y el análisis

RECOMENDACIÓN

Ofrecer un amplio marco de argumentos políticos:

Muchos/as especialistas concuerdan en que las personas a cargo de tomar decisiones políticas necesitan otros argumentos, más allá de los específicos de ciberseguridad y género, para poder unir voluntades políticas. Entre las sugerencias que proponen, destacan la posibilidad de unirse a:

- Compromisos regionales e internacionales. Por ejemplo, qué relación tienen la ciberseguridad y el género con los Objetivos de Desarrollo Sostenible, o la Agenda Mujeres, Paz y Seguridad creada por Naciones Unidas.[34]
- Economía digital. Crear argumentos y mostrar indicadores de que esta perspectiva permite fortalecer la economía digital – por ejemplo, en cuanto a facilitar la participación de las mujeres en el mercado de trabajo, y la diversidad empresarial.[35]
- Cooperación internacional. Muchos países y foros internacionales de ciberseguridad pueden tener un interés particular en incluir el género en la ciberseguridad; su experiencia, pericia y apoyo pueden ser fundamentales para las personas a cargo de tomar decisiones a nivel local.

Incluir las perspectivas de todos los grupos de interés involucrados:

- Garantizar que se tengan en cuenta las necesidades y perspectivas del amplio abanico de grupos de interés que hayas involucrado durante el proceso de desarrollo estratégico. Ponerlas a disposición en forma de breves resúmenes para las personas a cargo de formular políticas, a fin de que sea fácil recurrir a ellas y utilizarlas como referencia.

34. Puedes leer más sobre estas conexiones en APC. (2022a). Op. cit.
35. Ver, por ejemplo: Organización para la Cooperación y el Desarrollo Económicos (2018). *Bridging the Digital Gender Divide: Include, upskill, innovate*. https://www.oecd.org/digital/bridging-the-digital-gender-divide.pdf

En esta etapa formativa, hay un borrador con el contenido de las políticas que debería reflejar las prioridades y circunstancias específicas del país en cuanto a la ciberseguridad, incluyendo aquéllas que se plantean desde una perspectiva de género.

En esta fase, es importante recordar que la perspectiva de género es una parte intrínseca del marco de derechos humanos con el cual están comprometidos la mayoría de los gobiernos. Nos referimos a esto como una manera de abordar el desarrollo de políticas basándose en derechos.[36] Por ejemplo, ONU Mujeres ha declarado que es fundamental relacionar la inclusión de género con los abordajes de desarrollo de políticas basados en derechos, ya que la igualdad de género, la no discriminación por la identidad sexual y de género, y el acceso a la salud y los derechos sexuales y reproductivos constituyen principios fundamentales y universales de derechos humanos.[37] Es importante aclarar este vínculo ante los y las responsables de la formulación de políticas porque pone de relieve el hecho de que el gobierno ya se comprometió anteriormente a implementar un enfoque de género en las políticas de ciberseguridad. También es importante tomar nota de las relaciones entre las políticas de ciberseguridad y otras, como las políticas nacionales de TIC, o de banda ancha, para ver si hay que realizar cambios a fin de que la perspectiva de género aplicada a las políticas de ciberseguridad sean coherentes entre todos los espacios políticos nacionales.

El documento "Assessing National Cybersecurity Strategies from a Human Rights Perspective",[38] elaborado por Global Partners Digital (GPD), ofrece una sólida base para construir desde allí una perspectiva de género. El documento de GPD identifica seis componentes esenciales que se incluyen sistemáticamente en las recomendaciones para desarrollar una política nacional de ciberseguridad y, a su vez, ofrece recomendaciones generales sobre los elementos básicos que deben incluirse en esos componentes, desde una perspectiva de derechos humanos. Esas recomendaciones están adaptadas en el Cuadro 3 para ayudar a las personas responsables de las políticas y las organizaciones de la sociedad civil a incorporar una perspectiva de género en sus estrategias nacionales de ciberseguridad.

En relación a la implementación y el análisis, durante la etapa formativa se empieza a desarrollar un plan de acción coordinado para implementar las políticas de ciberseguridad. En general, el diseño de la implementación se hace recién después de acordado el documento final sobre las políticas e idealmente incluye a todas las partes interesadas, incluyendo al sector privado y la sociedad civil.

---

36. Brown, D., & Esterhuysen, E. (2017). *A rights-based approach to cybersecurity: A pipe dream or a critical means to a secure and stable internet?* APC. https://www.apc.org/sites/default/files/IGF17-_A_rights-based_approach_to_cybersecurity_-_recommendations_201807018.pdf; APC. (2020). *APC policy explainer: A human rights-based approach to cybersecurity*. https://www.apc.org/en/pubs/apc-policy-explainer-human-rights-based-approach-cybersecurity
37. UN Women. (2020). Gender mainstreaming: A global strategy for achieving gender equality and the empowerment of women and girls. https://www.unwomen.org/en/digital-library/publications/2020/04/brochure-gender-mainstreaming-strategy-for-achieving-gender-equality-and-empowerment-of-women-girls
38. Global Partners Digital. (2022). Op. cit.

Cuadro 3: Componentes esenciales de las políticas de ciberseguridad, identificados por Global Partners Digital, y recomendaciones adaptadas, elaboradas por APC

	Marco, visión, objetivos y definiciones	Roles y responsabilidades	Resiliencia cibernética
Componentes esenciales de las políticas de ciberseguridad, identificados por Global Partners Digital	Aquí se define la visión de ciberseguridad, las metas y los objetivos de las políticas mismas de ciberseguridad, y se establecen las definiciones de términos claves tales como "ciberseguridad".	Aquí se establecen los mecanismos de gobernanza política a través de los roles y responsabilidades de los diferentes actores en la ciberseguridad	Aquí se establece un amplio rango de acciones que el gobierno deberá llevar a cabo para proteger la infraestructura, las redes, los sistemas, la información y también a los/as usuarios/as, frente a ciberataques y ciberamenazas. Pueden ser desde ejercicios de ciberseguridad y la creación de CSIRT, hasta investigación, capacitación, etc.
Recomendaciones adaptadas, elaboradas por APC	Para contar con una política de ciberseguridad sensible al género, la visión de la ciberseguridad debe reconocer explícitamente el papel que tiene la ciberseguridad en la protección de los derechos humanos de las personas. Como lo sugiere GPD, esto se debe reflejar en los objetivos y en una definición de ciberseguridad coherente con los marcos internacionales de derechos humanos. En relación, más específicamente, a la perspectiva de género, deberían registrarse avances al menos en cuanto a que los objetivos políticos reconozcan las diferencias y la interseccionalidad de las necesidades de seguridad de las diversas personas. Al utilizar este marco, y teniendo en cuenta las condiciones nacionales, se pueden promover objetivos concretos y mensurables en el plan de acción.	Es esencial que haya un compromiso claro y fuerte con la gobernanza multisectorial para poder contar con una estrategia de ciberseguridad exitosa. En este contexto, las organizaciones de la sociedad civil que trabajan con género y otros asuntos interseccionales relevantes deben involucrarse en la implementación y el análisis de las políticas para que se adopte un enfoque de género adecuado para la ciberseguridad, y para dar pruebas del éxito o fracaso de dicha adopción.	Además de los principios de legalidad y proporcionalidad necesarios para cumplir con los derechos humanos, que son de particular importancia en relación a las vulnerabilidades relativas al género y otras interseccionalidades, el plan de acción para construir "ciberresiliencia" puede ser amplio, según las necesidades nacionales. Entre las medidas a contemplar figuran: • El compromiso de que los modelos de riesgo de la infraestructura clave del gobierno incorporen una perspectiva d para proteger los derechos de las personas según sus necesidades diversas. El gobierno debe considerar la posibilidad de ofrecer sesiones de capacitación con las partes interesadas sobre el aporte que puede significar el hecho de contar con una perspectiva de género para desarrollar esos modelos y crear un plan de respuesta inmediata frente a los incidentes. • Promover marcos jurídicos y políticos que ofrezcan amparo legal contra ciberamenazas de género a las mujeres, la comunidad de periodistas y la de defensores/as de los derechos humanos. • Campañas de información: la gente debe tener información confiable, inmediata y adecuada sobre seguridad digital, incluyendo detalles sobre los riesgos más comunes que corren. • Igualdad y diversidad: la creación de incentivos para garantizar que las mujeres que trabajan en la academia, la industria y también en el gobierno puedan hacer carreras de ciencia, tecnología, ingeniería y matemáticas, que puedan integrarse a la fuerza de trabajo en ciberseguridad y también a los espacios de políticas de ciberseguridad.

	Respuesta ante incidentes cibernéticos	Ciberdelito	Cooperación Internacional
Componentes esenciales de las políticas de ciberseguridad, identificados por Global Partners Digital	Se trata del amplio abanico de acciones que llevará a cabo el gobierno cuando ocurra un ciberataque. Por ejemplo, puede incluir el desarrollo de planes de contingencia, ofreciendo herramientas y recursos para los organismos a cargo de hacer que se cumplan las leyes, o apoyo a las personas afectadas.	Los detalles de cómo hará el gobierno con los ciberdelitos, así como el desarrollo de la legislación sobre ciberdelitos y el apoyo para su implementación.	Esta detalla cómo el gobierno trabajará con otros gobiernos y organizaciones internacionales y regionales en temas de ciberseguridad (colaboración para abordar amenazas compartidas, promoción de valores, prioridades de política exterior, etc.).
Recomendaciones adaptadas, elaboradas por APC	Tiene que haber respuestas ante los ciberincidentes conforme a los principios de la legalidad y la proporcionalidad. Además, entre otras medidas que dependerán de las necesidades nacionales, se puede proponer lo siguiente: • Planes especiales de contingencia basados en un análisis de género e interseccionalidad que protejan a las personas más vulnerables de algunos tipos de ataques específicos. • Provisión de recursos para apoyar la infraestructura de los grupos identificados en el análisis de género e interseccional que hayan sido víctima de ciberataques a causa de su trabajo.	Además de que las definiciones de ciberdelito deben alinearse con las normativas de derechos humanos, deben también involucrar, por lo menos, lo siguiente: • Revisar el marco legal y las políticas públicas que puedan responder a los diversos ataques en línea por cuestiones de género en el contexto local, como la intrusión o disrupción en dispositivos o redes personales, doxeo, ciberacoso y difusión no consensuada de imágenes íntimas. • Capacitar a la policía de ciberdelitos en relación a la violencia de género en línea. • Obligación de la policía de ciberdelitos de obtener datos desglosados que incluyan ataques en línea por razones de género cuando se denuncia un ciberdelito.	La cooperación internacional en ciberseguridad debe basarse en el respeto y fortalecimiento de los derechos humanos y en una internet abierta, libre y segura. De igual manera, los gobiernos deben considerar el ciberespacio como un espacio libre de violencia de género y comprometer esfuerzos para erradicarla. Además, la cooperación internacional debe centrarse en lo siguiente: • Incorporar consideraciones de género como parte integral del debate sobre amenazas cibernéticas. • Integrar debates sobre los aspectos legales de la paz, la seguridad y la justicia internacionales para comprender el impacto de las operaciones cibernéticas maliciosas en los grupos vulnerables. • Adoptar un enfoque de múltiples partes interesadas para generar confianza, paz y estabilidad en el ciberespacio. • Trabajar en el desarrollo de capacidades con un enfoque centrado en las personas e integrando la perspectiva de género.[39]

39. Si deseas conocer más de los principios en los que debería basarse la capacitación, puedes consultar el reporte sustantivo final (2021) del del Grupo de Trabajo de Composición Abierta (OEWG) sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

RECOMENDACIÓN

Sugerir textos políticos específicos sobre género y ciberseguridad:

Proponer la incorporación de textos, palabras y expresiones específicas que hayas recolectado en la fase de investigación. Si bien no hay garantías de que el texto se mantenga en el documento final, constituye un punto concreto de referencia para el debate.

Influir en los planes de implementación y análisis:

Después de desarrollar el documento de políticas, es necesario desarrollar un plan de acción para implementar dichas políticas. Este es otro de los procesos importantes en los que quien sea el defensor de la cuestión de género debe tratar incidir. Puntos claves a tener en cuenta:

- Sugerir cuáles pueden ser los actores a cargo del cumplimiento, monitoreo, evaluación y análisis, y quién tiene los conocimientos y capacidades necesarias para asumir esas responsabilidades. Confirmar que entienden claramente por qué se necesita una perspectiva de género en ciberseguridad. Considerar la posibilidad de negociar por adelantado con quienes tengan interés de asumir dichas responsabilidades.
- Proponer acciones concretas con objetivos medibles de corto, mediano y largo plazo, con un prespuesto estimado posible. Como sucede con todos los presupuestos, las actividades de menor costo para el gobierno tendrán más posibilidades de volverse prioritarias.
- Formular acciones basadas en la infraestructura y los programas ya implementados por el gobierno u otros grupos de interés. La continuidad de estas actividades, o su fortalecimiento pueden constituir una excelente excusa para volverlas prioritarias.

En la etapa formativa, el aspecto clave del plan de acción es la disponibilidad de recursos adecuados para la implementación de las políticas y para establecer mecanismos de monitoreo y análisis.

Hay que considerar al plan de acción como un área estratégica de intervención porque constituye una verdadera posibilidad de que los compromisos que figuran en las políticas nacionales de ciberseguridad dejen de ser meras palabras y se vuelvan reales. Esto es de particular importancia, ya que podría ser tentador incluir cuestiones de género en las políticas con fines meramente publicitarios.

c. Aspecto de la participación internacional

En la etapa inicial, habrás mapeado la participación del gobierno en los foros globales de ciberseguridad y habrás determinado si las cuestiones de género están presentes o no en esos debates, y si lo están, hasta qué punto. Ahora es el momento de rever ese mapeo para ver si es necesario realizar algún ajuste. Según lo que hayas concluido en cuanto al conocimiento del gobierno sobre la perspectiva de género aplicada a la ciberseguridad y cómo se traduce eso en su participación en foros internacionales, puedes considerar varias medidas de capacitación para los/as delegados/as gubernamentales que incluyen encuentros, sesiones de formación y seminarios sobre género y ciberseguridad, y cooperación internacional para iniciar o profundizar el conocimiento sobre el tema.

RECOMENDACIÓN

Hacer que los y las responsables de formular políticas se sientan capaces de participar en foros internacionales:

Tomando como base el mapeo de foros de ciberseguridad realizado durante la fase inicial, hay que capacitar a las personas a cargo de formular políticas designadas para que puedan participar en esas instancias y su participación valga la pena. Muchos de esos foros cuentan con mecanismos de participación en línea, pero es probable que sea necesario contar con un presupuesto aparte para que asistan en persona. Se recomienda que quienes participan por primera vez tengan un/a m entor/a, que puede ser una organización de la sociedad civil, que los familiarice con los mecanismos y procesos del foro.

C. ETAPA CONSOLIDADA

En esta etapa, la estrategia nacional de ciberseguridad y su plan de acción ya están en marcha. El objetivo clave ahora es participar activamente en la evaluación del impacto de las políticas, así como la actuación del gobierno en los foros internacionales y los mecanismos de cooperación bilateral o multilateral.

a. Aspecto de desarrollo de una estrategia

En esta etapa, ya debería practicarse el monitoreo y evaluación de las políticas para verificar que se cumple el plan de acción. Hay dos casos posibles: uno en el cual las políticas implementadas incorporan la cuestión de género en grados diversos, y otro en el que no es así. En ambos casos, los y las responsables de la formulación de políticas y otras partes interesadas tienen que reunir pruebas concretas para analizar la capacidad de respuesta de las políticas y el plan de acción ante los desafíos de ciberseguridad en el contexto del género.

A continuación, se debe elaborar un informe diagnóstico que muestre claramente cuáles son las brechas y sugiera formas de remediarlas, para presentar ante los mecanismos de monitoreo y evaluación. Esto se puede complementar con otras presentaciones a las partes interesadas, a fin de mostrar transparencia.

Además de presentar pruebas ante los mecanismos, se puede evaluar la posibilidad de llevar a cabo otras acciones de sensibilización. Por más información sobre este asunto, vuelve a la etapa inicial en este documento, en particular la sección de desarrollo de estrategias.

RECOMENDACIÓN

Promover un ciclo contínuo de evaluación y análisis:

En esta etapa, deberían estar en marcha los mecanismos de monitoreo y evaluación de las políticas, para verificar si se cumple el plan de acción. Los y las responsables de la formulación de políticas y otros grupos de interés tienen que reunir evidencia concreta de cómo responden las políticas y el plan de acción a los desafíos de ciberseguridad. El análisis de las políticas tiene que identificar claramente las brechas que haya en el texto de las mismas o en su implementación, y contar con un plan de acción concreto de cómo resolver esas situaciones. Es necesario construir un ciclo cnostante de monitoreo y análisis que se adicionará al plan de implementación.

b. Aspecto de los contenidos/implementación y el análisis

La estrategia nacional de ciberseguridad debe incorporar y/o apoyar objetivos políticos más generales, como la protección de niños y niñas, la promoción de los derechos humanos, el combate contra la desinformación, y la promoción de la igualdad, diversidad e inclusión digital, entre otros. Es de vital importancia generar instancias de diálogo, intercambio de conocimiento y cooperación entre organismos de gobierno que tengan interés en la adopción de una perspectiva de género para la ciberseguridad para poder entender si las políticas les parecen eficientes.

RECOMENDACIÓN

Generar cooperación intersectorial y diálogo entre los departamentos y los/as funcionarios/as de gobierno:

La estrategia nacional de ciberseguridad debe incorporar y/o apoyar objetivos políticos más generales, como la protección de niños y niñas, la inclusión digital, la promoción de los derechos humanos, la igualdad y la diversidad, y el combate contra la desinformación. Desarrolla estrategias y procesos para que las personas que trabajan en esas áreas dialoguen sobre los problemas y desafíos que puedan estar enfrentando y compartan aprendizajes claves de la implementación de las políticas, así como el impacto que tiene en su trabajo.

c. Aspecto de participación internacional

En esta etapa, la participación del país en foros regionales e internacionales es mucho más activa. Es importante crear instancias de colaboración entre las diversas partes interesadas en esos foros, incluyendo al gobierno, la sociedad civil y el sector privado, de modo de presentar un frente común en relación al género y la ciberseguridad.

RECOMENDACIÓN

Trabajar en conjunto con diferentes grupos de interés para crear un frente común en los foros internacionales:

En esta etapa, la participación del país en foros regionales e internacionales es mucho más activa. Sin embargo, existen varias dinámicas de poder en juego en esos foros, donde la perspectiva de los países del Sur global suelen ser marginalizadas por los países más poderosos. Las personas responsables de formular políticas deberían considerar la posibilidad de trabajar con la sociedad civil y los grupos del sector privado que estén comprometidos con el enfoque de género aplicado a la ciberseguridad a fin de fortalecer la voz de esos países marginados en los foros.

D. OTRAS ETAPAS: ESTRATÉGICA Y DINÁMICA

En estas dos etapas, todas las partes interesadas deben considerar a la perspectiva de género en ciberseguridad como una herramienta estratégica y clave, al menos para:

- Evaluar regularmente los diferentes daños que le pueden causar los incidentes de ciberseguridad a los individuos.
- Hacer que las evaluaciones de riesgo en relación a la ciberseguridad sean más completas, matizadas y diversas.
- Reevaluar y, si es necesario, realizar cambios en los abordajes a fin de que las políticas y las prácticas sirvan para enfrentar las amenazas cibernéticas de manera más general.
- Evaluar y reforzar la diversidad en la industria de la ciberseguridad.

De esta manera, la perspectiva de género en ciberseguridad tiene un impacto tangible en el desarrollo de una infraestructura robusta y resiliente para prevenir ataques, fortalecer los derechos humanos para la diversidad de las personas en el ciberespacio, y crear una cultura de ciberseguridad resiliente tanto en la sociedad, como en el mundo corporativo.

Estos factores ayudarán al país a convertirse en un adalid del enfoque de género aplicado al desarrollo de políticas de ciberseguridad en los foros regionales e internacionales, y sus políticas servirán como modelo a ser utilizado por otros.

APC
ASOCIACIÓN PARA
EL PROGRESO DE
LAS COMUNICACIONES

MARCO PARA EL DESARROLLO DE UNA POLÍTICA DE CIBERSEGURIDAD QUE RESPONDA A LAS CUESTIONES DE GÉNERO: HERRAMIENTA DE EVALUACIÓN