



Resultados de la Política Nacional de Ciberseguridad 2017-2022: avances y brechas sobre la inclusión del enfoque de género.

Diciembre, 2022.

Autora: Paz Peña O.
Consultora especializada en tecnologías y género.

Resumen ejecutivo

- El enfoque de género de la Política Nacional de Ciberseguridad (PNCS) 2017-2022 es una estrategia novedosa a nivel regional y, considerando un contexto internacional, fue un primer paso valorable para los tiempos en que fue diseñada.
- Con todo, el mayor problema es que la perspectiva no se traduce en mayores medidas en el plan de acción y solo es incluida en una medida de 41 en total.
- La única medida (N°18) que contempla explícitamente el enfoque de género (“Diseñar e implementar una campaña de ciberseguridad de carácter masivo y fomentar la implementación de programas de difusión estableciendo alianzas con los privados en campañas de sensibilización, con énfasis en sectores vulnerables y empleando perspectiva de género”), no se considera un avance, a pesar de reportarse cumplida. Esto, debido a que, si bien la campaña comunicacional existe, no tiene “énfasis en sectores vulnerables y empleando perspectiva de género”.
- Es importante constatar que hay un avance mucho más sustantivo en considerar la perspectiva de género interseccional que lo que originalmente estipulaba el plan de acción. De 41 medidas totales descritas en el plan de acción que representan el 100%, se constatan 7 medidas relacionadas al enfoque de género (17%), pero se registran avances solo en 6 (se excluye la N°18), que representan un 15% del total de medidas del plan de acción.
- Visto de manera particular, los avances son valorables, pero mucho de ellos aún optimizables desde una perspectiva técnica del enfoque de género.
- Se presentan avances del enfoque de género en la ciberseguridad en 4 de los 5 objetivos de la PNCS. El objetivo que cuenta con más acciones cumplidas que representan avances en enfoque de género es el objetivo “C: Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales”. En cambio, no se registra ningún avance en el objetivo "E: El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos". Una brecha preocupante si se considera que la inclusión del género en la fuerza laboral de la industria de la ciberseguridad es una de las perspectivas más tradicionales de la ciberseguridad.

Índice de contenido

I. Introducción y alcance de este informe	4
II. Breve contexto general.....	5
a. El enfoque de género.....	5
b. Enfoque de género en las políticas públicas	6
c. El enfoque de género en las políticas de ciberseguridad.....	7
III. El enfoque de género en la PNCS	9
IV. Evaluación de la PNCS desde el enfoque de género	10
a. Avances registrados en perspectiva general	10
b. Brechas registradas en perspectiva general	12
c. Avances y brechas específicas de las acciones cumplidas con enfoque de género	13
V. Conclusiones	21
VI. Bibliografía	22

I. Introducción y alcance de este informe

El propósito de este informe es analizar cómo ha avanzado el enfoque de género en la ciberseguridad de acuerdo con el cumplimiento del plan de acción de la Política Nacional de Ciberseguridad 2017-2022 (en adelante, PNCS). Para hacerlo, se analizó la política, su plan de acción y las respuestas de los actores estatales¹ respecto al cumplimiento de sus acciones asignadas.

Para evaluar de forma justa los avances de la PNCS respecto al enfoque de género, este documento toma dos caminos:

- Primero, brinda un breve contexto general de cómo ha avanzado esta perspectiva en el campo de la ciberseguridad y cómo ha sido incluida a nivel de políticas públicas en la materia a nivel internacional y regional, de manera de comprender el contexto general de dónde se ubica Chile hoy con su PNCS actual.
- Segundo, analiza los avances respecto al enfoque de género en todas las medidas que se consideran como cumplidas por los actores responsables de acuerdo con el plan de acción, de manera de ir mucho más allá de la acción N°18 que es la única que, en el 2017, nombraba explícitamente la perspectiva de género. Esto permite dar un diagnóstico más apegado a la realidad sobre los avances que en estos años se han tenido.

Ambas decisiones permiten poner en un contexto más apegado a lo real los avances y brechas particulares del enfoque de género en esta política pública y brinda, así, mejor información a los tomadores de decisiones de política pública.

Este reporte se divide en varias partes que van de lo general a lo particular, de manera de facilitar el entendimiento de la información, no importando el nivel de conocimiento que el lector tenga sobre asuntos de género y ciberseguridad. Así, la sección II es un breve contexto que presentará un panorama general de la importancia del enfoque de género, su aplicación en las políticas públicas y en cómo se ha impulsado esta aproximación en las políticas de ciberseguridad. En la sección III se caracteriza cómo la PNCS 2017-2022 abordó el enfoque de género para, en la parte IV, ahondar en profundidad en las medidas del plan de acción de la PNCS relativas al avance del enfoque de género, de acuerdo con las respuestas reportadas por los encargados oficiales de su cumplimiento. Finalmente, en la sección V se avanzan en conclusiones que permiten comprender el diagnóstico actual de la política de ciberseguridad en cuanto al enfoque de género.

¹ Es importante recalcar que este informe solo se basa en las respuestas que los responsables dieron respecto a los avances de la PNCS, por tanto, no se incluye ningún avance relacionado al enfoque de género que no haya sido reportado oficialmente por sus responsables. Esto permite que este informe esté ajustado a la metodología de evaluación de la PNCS, que se radica a las acciones planificadas y previamente estipuladas en el plan de acción.

II. Breve contexto general

a. El enfoque de género

El género es el conjunto de ideas, representaciones, prácticas y prescripciones sociales elaboradas a partir de la diferencia anatómica entre los sexos. El género, así, es una categoría que fluye y se moldea en las interacciones sociales respecto de lo que se entiende como masculino y femenino, por lo que el género responde más bien a espacios situacionales e históricos de nuestras sociedades, más que a una naturaleza inherente, esencialista e individual.

En este marco, de hecho, la Comisión Interamericana de Derechos Humanos ha definido la “expresión de género” como “la manifestación externa de los rasgos culturales que permiten identificar a una persona como masculina o femenina conforme a los patrones considerados propios de cada género por una determinada sociedad en un momento histórico determinado” (CIDH, 2008). Otro concepto importante y relacionado es el de identidad de género. De acuerdo a los Principios sobre la Aplicación de la Legislación Internacional de Derechos Humanos en Relación con la Orientación Sexual y la Identidad de Género (Principios de Yogyakarta), la identidad de género es la vivencia interna e individual del género tal como cada persona la siente profundamente, la cual podría corresponder o no con el sexo asignado al momento del nacimiento, incluyendo la vivencia personal del cuerpo (que podría involucrar la modificación de la apariencia o la función corporal) y otras expresiones de género, incluyendo la vestimenta, el modo de hablar y los modales. La identidad de género puede fluir entre lo masculino y femenino, no existe una norma absoluta que lo defina.

El género no se refiere únicamente a la diferencia cultural entre los sexos, sino también al poder: es más que un eficaz principio de diferenciación social, es un brutal productor de discriminaciones y desigualdades. Las ideas y prácticas de género jerarquizan a los seres humanos social, económica y jurídicamente. Por eso, la consecución de la igualdad de género es un campo de estudio teórico y práctico amplio que crecientemente ha ganado popularidad.

Las relaciones de género están, además, intersectadas e implicadas en otras relaciones sociales: de producción, etnicidad, nacionalidad, religión y otras de carácter generacional. El sistema de género como tal, por tanto, no está aislado en la sociedad, sino que se articula con otros sistemas de relaciones sociales: esto es lo que se llama la perspectiva interseccional del género.

En este contexto, el enfoque de género es una herramienta para analizar las diferencias de género, considerando sus intersecciones con otros sistemas de opresión, y mitigarlas de manera de lograr la igualdad de género. Esta última significa que la mujer, el varón y las diversas identidades de género disfrutan de la misma situación y tienen iguales condiciones para la plena realización de sus derechos humanos y su potencial de contribuir al desarrollo, político, económico, social y cultural y de beneficiarse de los resultados. La igualdad de género es, por lo tanto, la valoración imparcial por parte de la sociedad de las similitudes y diferencias entre géneros y de los diferentes papeles que cada uno juega (OEA, 2018).

El enfoque de género es útil en las políticas públicas que buscan superar las barreras que, particularmente, impiden a las mujeres lograr la igualdad de género en la sociedad en general.

b. Enfoque de género en las políticas públicas

Las políticas de igualdad de género han tenido su propia evolución. Durante mucho tiempo, se limitaron a garantizar la igualdad de trato de ambos sexos en la legislación, es decir, pretendía corregir la discriminación existente (en la legislación) y hacer a las y los ciudadanos formalmente iguales. Pronto se reconoció en base a la evidencia que la igualdad de derechos no significa necesariamente igualdad de oportunidades, ni siquiera igualdad de resultados, debido a las posiciones de partida estructuralmente diferentes a las que se enfrentan los individuos en la vida cotidiana. Desde la cuarta conferencia de las Naciones Unidas sobre la mujer celebrada en Pekín en 1995, las políticas de igualdad de género se han reorientado cada vez más hacia un enfoque más amplio y estructural de las desigualdades de género. Así, se introdujeron medidas específicas de igualdad de género (como la acción positiva², legislación, y mecanismos para abordar intereses específicos de las mujeres, investigación y formación) para mitigar la desigualdad estructural, aunque no jurídica, y promover la igualdad.

Además de las políticas específicas de igualdad de género que son irremplazables, éstas se han complementado con la llamada “integración de la perspectiva de género” (*gender mainstreaming* en inglés), un proceso de evaluación de las implicaciones para mujeres y hombres de cualquier acción planificada, incluidas la legislación, las políticas o los programas, en todos los ámbitos y a todos los niveles.

El enfoque de género en las políticas públicas es hoy parte fundamental de Estados modernos y democráticos y organismos intergubernamentales alrededor del mundo. Han recibido un impulso clave gracias a varios instrumentos internacionales sobre diversos aspectos de la igualdad de género, en particular, los principios consagrados en la Convención de las Naciones Unidas sobre la eliminación de todas las formas de discriminación contra la mujer (CEDAW) de 1979; la Declaración y Plataforma de Acción de Beijing de 1995 de la Cuarta Conferencia Mundial de las Naciones Unidas sobre la Mujer; los Objetivos de Desarrollo del Milenio (ODM) de las Naciones Unidas; y los "Objetivos de Desarrollo Sostenible" (ODS) de las Naciones Unidas³, entre otros. Por cierto, a nivel interamericano, la Comisión Interamericana de Mujeres (CIM) fue el primer organismo de carácter intergubernamental en el mundo fundado expresamente para luchar por los derechos civiles y políticos de la mujer en el continente. Es importante resaltar la labor realizada por la CIM para establecer normas sistemáticas en favor de los derechos de la mujer, como las Convenciones Interamericanas sobre Nacionalidad de la Mujer (Uruguay, 1933), Concesión

² Se llama acción positiva en igualdad de género al conjunto de medidas que se toman para corregir situaciones patentes de desigualdad que sufren las mujeres respecto a los hombres en diferentes ámbitos, como el laboral o el político.

³ La igualdad de género y el empoderamiento de todas las mujeres y niñas es un objetivo de 193 países del mundo, que lo aprobaron como el quinto Objetivo de Desarrollo Sostenible (ODS) en la Agenda 2030, en el año 2015.

de los Derechos Políticos a la Mujer (Colombia, 1948), Concesión de los Derechos Civiles a la Mujer (Colombia, 1948) y la Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer, “Convención de Belém do Pará” (Brasil, 1994).

De este modo, el enfoque de género se puede encontrar como método integral para lograr la igualdad de género en instrumentos y organismos múltiples, que van, a nivel global, por ejemplo, en la “Recomendación del consejo de la OCDE⁴ de 2015 sobre la igualdad de género en la vida pública” donde se “RECOMIENDA que los Miembros y no Miembros que se hayan adherido a la Recomendación (en adelante, los "Adherentes") incorporen la igualdad de género en el diseño, desarrollo, aplicación y evaluación de las políticas y presupuestos públicos pertinentes”. Y que también pasan, a nivel regional, a que se establezca en el Programa Interamericano como uno de sus objetivos primordiales (nº2): "Alentar a los Estados Miembros de la OEA a formular políticas públicas, estrategias y propuestas dirigidas a promover los derechos humanos de la mujer y la igualdad de género en todas las esferas de la vida pública y privada, considerando su diversidad y ciclos de vida" (OEA, 2018).

c. El enfoque de género en las políticas de ciberseguridad

El enfoque de género en la ciberseguridad es una materia de reciente formación y si bien existen avances impulsados por corrientes teóricas variopintas, no hay una definición transversal de la ciberseguridad desde el enfoque de género, ni más particularmente, modelos estudiados de cómo introducirlo en los distintos aspectos de las políticas y estrategias nacionales en la materia.

De manera más tradicional, el enfoque de género en este campo ha sido comprendido casi exclusivamente desde las **brechas de género en la fuerza laboral de la industria de ciberseguridad y en su gobernanza**. Esta aproximación, aunque insuficiente en aislamiento, sigue siendo fundamental. Y es que, a nivel mundial y según el ISC2 (2022a), las mujeres constituyen apenas el 24% de la fuerza laboral del área, lo que no solo se traduce en una brecha de desarrollo económico para las mujeres, sino también en una barrera para la propia industria de la ciberseguridad: existe una escasez mundial de 3,43 millones de trabajadores calificados en ciberseguridad (ISC2, 2022b). Además, tal como afirma la OEA (2022), esta escasez impacta directamente a los Estados ya que el desarrollo de la fuerza laboral en ciberseguridad es fundamental para que los países estén preparados para enfrentar conflictos en el ciberespacio. Por lo demás, como es ampliamente reconocido, el desafío actual en el mercado laboral no es solo contratar a más personas, sino también construir equipos más capaces, multidisciplinarios y diversos que estén preparados para una variedad de roles diferentes dentro de la ciberseguridad. En este contexto, y de acuerdo con la Asociación Chilena de Empresas de Tecnologías de Información A.G. (ACTI, 2021), solo el 15% de la fuerza laboral del área de ciberseguridad en Chile son mujeres.

Ahora bien, a nivel de gobernanza en políticas de ciberseguridad, como ha reconocido ONU Mujeres (2023), la participación de mujeres en la formulación de políticas y la toma de decisiones en materia de ciberseguridad es particularmente escasa, y las medidas adoptadas para mitigar las implicaciones de género de las inseguridades relacionadas con la ciberseguridad van a la zaga. Como explican Brown y Pytlak (2020), la participación en la

⁴ Organisation for Economic Co-operation and Development, donde Chile es miembro desde el 2010.

ciberpolítica es fundamental para la representación. Sin la participación plena e igualitaria de las mujeres, es improbable que sus puntos de vista estén representados o que su perspectiva se tome en serio en la ciberpolítica.

Con todo, en los últimos años, desde las políticas públicas relacionadas a la ciberseguridad, el enfoque de género se ha visto impulsado de forma mucho más sistémica gracias a las corrientes llamadas humano-céntricas, que ven en las personas como el objeto referente de la ciberseguridad (Deibert, 2018), y que se relacionan también con el enfoque de derechos humanos en la materia. En este contexto, **el enfoque de género va más allá de solo la brecha de género en la industria y su gobernanza, y comprende que las tecnologías y peligros cibernéticos para las personas no son neutrales al género y, por lo tanto, los impactos de las vulnerabilidades son distintos en función de las identidades y expresiones de género de las personas** (Sharland et. al., 2021). Asimismo, este enfoque se complementa con la perspectiva interseccional pues permite identificar un sistema de opresiones diversas -entre las que se encuentra el género, pero que incluye también la raza, la edad, la clase social, la discapacidad, entre otras- que jerarquizan a los sujetos en la sociedad, poniendo en escena las otras diferencias que constituyen a las personas y poblaciones que, por cierto, también afectan su desempeño en el campo de la ciberseguridad.

A nivel de políticas públicas internacionales en materia de ciberseguridad, los procesos multilaterales sobre ciberseguridad han comenzado recientemente a incluir declaraciones oficiales que llaman la atención sobre sus dimensiones de género, pero todavía de forma demasiado tímida y limitada, como fue el caso del informe final del Grupo de Trabajo Abierto (OEWG, en sus siglas en inglés) de la ONU sobre la evolución en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional (2019-2020). De hecho, a pesar de que varias delegaciones y otros organismos habían manifestado la necesidad de incorporar la perspectiva de género en la aplicación de las normas cibernéticas, crear capacidades sensibles al género y comprender mejor otros vínculos entre los marcos de ciberseguridad y de igualdad de género⁵, los avances fueron insatisfactorios: de hecho, el informe final del OEWG - si bien en su introducción destaca lo relevante de promover una participación y un liderazgo significativos de las mujeres en los espacios de elaboración de ciberpolíticas, además de la importancia de superar la "brecha digital de género"- los debates sobre el enfoque de género y lo que los Estados podrían hacer al respecto están prácticamente ausentes en las diferentes secciones del informe (Ferrari, 2021).

⁵ Ver, por ejemplo, las intervenciones en el debate de:

- El gobierno de Canadá: "Updated Canadian text proposals, November 2020". En: <https://front.un-arm.org/wp-content/uploads/2020/12/updated-canadian-text-proposals-nov-30.pdf>
- El gobierno de los Países Bajos: "The Kingdom of the Netherlands' response to the pre-draft report of the OEWG". En: <https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/UNGGE/The+Kingdom+of+the+Netherlands+%E2%80%99+Response+to+the+Pre-Draft+Report+of+the+OEWG.pdf>
- United Nations Institute for Disarmament Research (UNIDIR): "Advancing Gender Considerations in the Cyber OEWG". En: <https://unidir.org/commentary/advancing-gender-considerations-cyber-oewg>
- Women's International League for Peace & freedom (WILPF) & la Association for Progressive Communications (APC): "Joint Submission to the UN OEWG: Gender in International Cyber Security". En: https://www.wilpf.org/advocacy_documents/submission-to-the-un-open-ended-working-group-oewg/

Respecto a políticas y estrategias nacionales de ciberseguridad y su inclusión del enfoque de género, a nivel latinoamericano y hasta el 2020, además de Chile, solo Guatemala, Ecuador, Jamaica y República Dominicana han efectuado alguna referencia general y explícita sobre la perspectiva de género o a la equidad de género, pero ninguna estableció una hoja de ruta e indicadores para medir el progreso y estado de madurez de la ciberseguridad a la luz de esta perspectiva (Herrera & Peña, 2020).

III. El enfoque de género en la PNCS

En este contexto regional e internacional, el enfoque de género de la PNCS chilena ha resultado bastante novedoso.

La PNCS estableció un mandato estatal de velar por el respeto y promoción de los derechos fundamentales en el ciberespacio (página 12). También señala que, en materia de derechos fundamentales, se empleará “un enfoque de género, que permita hacer visible y enfrentar desigualdades que enfrentan los diversos grupos en el ciberespacio” (página 15).

Para Herrera Carpintero (2020), si se considera la estrategia nacional en perspectiva con las políticas de otros países latinoamericanos, “Chile ha sido el único que dispuso explícitamente la consideración de un enfoque de género en materia de ciberseguridad; en comparación, los demás países solo hicieron alusión a la consideración de una perspectiva general en materia de derechos humanos”.

Con todo, en el plan de acción de la PNCS, solo existe una acción específica (la N°18) que nombra el enfoque de género en forma explícita:

Objetivo C	Medida	Responsable
<p>Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.</p> <p>1. Una cultura de la ciberseguridad</p> <p>2. Sensibilización e información a la comunidad</p> <p>3. Formación para la ciberseguridad</p>	<p>18. Diseñar e implementar una campaña de ciberseguridad de carácter masivo y fomentar la implementación de programas de difusión estableciendo alianzas con los privados en campañas de sensibilización, con énfasis en sectores vulnerables y empleando perspectiva de género.</p>	<p>MSGG (CICS supervisor de la medida)</p>

IV. Evaluación de la PNCS desde el enfoque de género

Para evaluar los avances y brechas del enfoque de género en el plan de acción de la PNCS y dar una perspectiva más integral, se instó a los actores encargados de cumplir las medidas establecidas en el plan de acción a reportar si las medidas que se consideraban cumplidas o avanzadas consideraban el enfoque de género. Esto permitió analizar cómo la política había desarrollado esta perspectiva, más allá de la acción específica N°18.

Para dar cuenta de la evaluación integral, esta sección se subdivide en tres:

- Avances en el enfoque de género desde una perspectiva general, es decir, tomando en cuenta la totalidad del plan de acción de la PNCS.
- Asimismo, desde esta misma perspectiva de la totalidad del plan de acción, se da cuenta de las brechas generales más importantes.
- Y, por último, se analiza particularmente una por una las medidas del plan de acción donde se registran avances en la perspectiva de género, también incluyendo sus posibles brechas.

a. Avances registrados en perspectiva general

Efectivamente, se debe constatar que hubo más avances de la perspectiva de género que los que inicialmente el plan de acción previó. Esto es una buena noticia, porque demuestra que este enfoque se ha ido incluyendo de a poco en la política pública de la ciberseguridad, mucho más allá de los compromisos obligatorios.

Así, de 41 medidas descritas en el plan de acción que representan el 100%, se constatan 7 medidas relacionadas al enfoque de género (17%), pero **se registran avances solo en 6, que representan un 15% del total de medidas del plan de acción.**

Ahora bien, la única medida que explícitamente se refiere a una perspectiva de género, la acción N°18, a pesar de que se considera cumplida porque se trata de una campaña de carácter masivo, no se registra como avance en perspectiva de género puesto que, como se verá en la sección “Brechas registradas en perspectiva general” de este documento, el spot no tiene “énfasis en sectores vulnerables y empleando perspectiva de género” como mandataba el plan de acción.

Con todo, se presentan avances de la perspectiva de género en 4 de los 5 objetivos generales de la PNCS. **El objetivo que cuenta con más acciones cumplidas y que representan avances en enfoque de género, es el objetivo C: “Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales”.**

	Descripción objetivo	N° Acciones con enfoque de género	Acciones consideradas
A	El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos	1	34. Realizar ciberejercicios sobre incidentes de Ciberseguridad con diferentes comunidades interesadas para fomentar el conocimiento, investigación y difusión adecuada de brechas, vulnerabilidades y vías de mitigación encontradas en los sistemas nacionales (Objetivos A y C).
B	El Estado velará por los derechos de las personas en el ciberespacio	2	13. Actualizar normativa sobre delitos informáticos. 36. Incorporar en la Encuesta Nacional Urbana de Seguridad Ciudadana (ENUSC) un set de preguntas vinculadas a los ciberdelitos (Objetivos B y C).
C	Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales	4	16. Generar primer punto de difusión de información para el ciudadano sobre Ciberseguridad, basado en los diferentes canales electrónicos y redes sociales que ofrece internet. 21. Diseñar e implementar una campaña de ciberseguridad orientada a los adultos mayores, que considere medidas de capacitación y difusión. 34. Realizar ciberejercicios sobre incidentes de Ciberseguridad con diferentes comunidades interesadas para fomentar el conocimiento, investigación y difusión adecuada de brechas, vulnerabilidades y vías de mitigación encontradas en los sistemas nacionales (Objetivos A y C). 36. Incorporar en la Encuesta Nacional Urbana de Seguridad Ciudadana (ENUSC) un set de preguntas vinculadas a los ciberdelitos (Objetivos B y C).
D	El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales	1	23. Apoyar decididamente el establecimiento a nivel internacional de procesos de consultas políticas regionales, subregionales y multilaterales, con especial énfasis en la región.
E	El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos	0	Sin acciones

Con todo, es importante aclarar que constatar avances no significa que no existan brechas a superar en esas mismas metas cumplidas, las cuales se verá de forma general y particular en los próximos apartados de este documento.

b. Brechas registradas en perspectiva general

Se constatan dos brechas importantes desde una perspectiva general. Por un lado, como se ha explicitado, la mayor brecha de avance en el cumplimiento del plan de acción es la única medida (N°18) que consideraba explícitamente el enfoque de género, es decir, “diseñar e implementar una campaña de ciberseguridad de carácter masivo y fomentar la implementación de programas de difusión estableciendo alianzas con los privados en campañas de sensibilización, **con énfasis en sectores vulnerables y empleando perspectiva de género**”. Sin embargo, a pesar de que la campaña existe, no tiene el énfasis de perspectiva de género requerido, por lo que si bien se trata una meta cumplida en el plan de acción en tanto se realizó la campaña, no se la considera como un avance en el enfoque de género en este informe.

A continuación, se explicita la medida N°18, el detalle de la respuesta de los actores responsables y el análisis de ella desde el enfoque de género.

Objetivo C	Medida	Responsable	Detalle de la respuesta	Análisis desde el enfoque de género
Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales. 1. Una cultura de la ciberseguridad 2. Sensibilización e información a la comunidad	18. Diseñar e implementar una campaña de ciberseguridad de carácter masivo y fomentar la implementación de programas de difusión estableciendo alianzas con los privados en campañas de sensibilización, con énfasis en sectores vulnerables y empleando perspectiva de género.	MSGG (CICS supervisor de la medida)	El Departamento de Marketing perteneciente a la División Secretaria de Comunicaciones (SECOM), asesoró al Ministerio del Interior y Seguridad Pública en una campaña sobre la materia durante el 2018, la que contó con minutos otorgados por CNTV para la emisión por los canales de televisión abierta en horario prime. La campaña fue emitida en diciembre 2018 y enero 2019.	El spot hace una aproximación general a la ciberseguridad desde el punto de vista de la responsabilidad personal de las y los usuarios. Y aunque entre el casting hay dos mujeres, una de ellas adulta mayor, no es suficiente para brindar un énfasis en sectores vulnerables y empleando una perspectiva de género. Por ende, no da respuesta a las problemáticas de ciberseguridad

3. Formación para la ciberseguridad			Se indica link para acceder al spot de la campaña y su plan de medios.	más comunes de acuerdo al género e interseccionalidades más importantes de las personas. En este sentido, tampoco se aprecia en el plan de medios del spot, evidencia explícita que la selección de canales y horarios haya sido pensada para estos sectores.
-------------------------------------	--	--	--	---

Por otro lado, otra brecha importante es que **no se registra ningún avance en el objetivo general E de la política nacional, que dice: “El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos”**. Esto es preocupante sobre todo ya que, como se veía al inicio de este documento, la inclusión del género en la fuerza laboral de la industria de la ciberseguridad es una de las perspectivas más tradicionales de la ciberseguridad y el género.

c. Avances y brechas específicas de las acciones cumplidas con enfoque de género

A continuación, un análisis específico de las siete acciones relacionadas al enfoque de género del plan de acción, en las que se examinan por cada medida los avances y brechas de las acciones reportadas por los encargados de cumplir el plan de acción. Este examen es especialmente importante para poder no solo comprender lo que se ha logrado y, por ende, construir en la próxima PNCS sobre eso, sino también que permite que la próxima política pueda hacerse cargo también de esas brechas particulares.

N°	Medida	Responsable	Detalle de respuesta	Enfoque de género e interseccionalidades
1	13. Actualizar normativa sobre delitos informáticos	MISP - MINJUSTICIA	<p>Esta medida se cumple con la LEY 21.459</p> <p>Ley publicada en el Diario Oficial el 20.06.2022 que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.</p>	<p><i>Avances:</i></p> <p>En el Artículo 10 sobre "Circunstancias agravantes. Constituyen circunstancias agravantes de los delitos de que trata esta ley", incluye 2) Cometer el delito abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores.</p> <hr/> <p><i>Brechas:</i></p> <p>Las personas especialistas consultadas sobre la evaluación de la PNCS 2016-2022, insisten que los niveles de vulnerabilidad de las mujeres en Chile desde la perspectiva de la violencia de género online siguen siendo enorme.</p> <p>La violencia en línea contra la mujer ha sido entendida como “todo acto de violencia de género contra la mujer cometido, asistido o agravado en parte o totalmente por el uso de las tecnologías de las comunicaciones TIC, como teléfonos móviles y teléfonos inteligentes, Internet y redes sociales, plataformas o correo electrónico, contra una mujer porque ella es una mujer, o afecta a las mujeres desproporcionadamente” (ONU, 2018). Algunas de las últimas cifras en Chile, hablan de que la violencia en espacios digitales es común para la mayoría de las mujeres en el país (Ananías & Vergara, 2020).</p> <p>Más aún, las especialistas consultadas apuntan a que hay grupos en particular vulnerabilidad a</p>

N°	Medida	Responsable	Detalle de respuesta	Enfoque de género e interseccionalidades
				<p>ataques cibernéticos que siguen desprotegidos, como mujeres en política y mujeres periodistas (RELE, 2022).</p> <p>A nivel de legislación sobre violencia de género online, si bien hay discusiones legislativas (Boletín N°13.928-07, Boletín N°11.077-07), estas están estancadas y aún existe desprotección. Esta es considerada una brecha urgente en que la próxima PNCS debe avanzar para brindar una protección integral de ciberseguridad a las mujeres.</p>
2	16. Generar primer punto de difusión de información para el ciudadano sobre Ciberseguridad, basado en los diferentes canales electrónicos y redes sociales que ofrece internet.	MISP - MSGG (CICS supervisor de la medida)	Se han implementado varios canales de difusión articulados por el CSIRT (sitio web y redes sociales) teniendo presente distintos públicos objetivo. Además de participar en campañas públicas y asociaciones con privados.	<p><i>Avances:</i></p> <p>Se constatan campañas de prevención para el público objetivo de mujeres y adolescentes, integrando diversos peligros, muchos de los cuales constituyen violencia de género digital.</p> <p><i>Brechas:</i></p> <p>La terminología técnica de las campañas es problemática pues no está acorde a la discusión técnica nacional e internacional sobre violencia de género online. Esto ocurre, por ejemplo, al usar el término “porno venganza” (porque, como constata Sophie Maddocks (2019), rara vez se trata de una venganza y calificarlo de pornografía es asumir que la víctima dio un permiso tácito para consumir algo que fue creado, o difundido, sin consentimiento). También cuando se opta por un concepto mucho menos reconocido técnicamente como “abuso digital” cuando se</p>

N°	Medida	Responsable	Detalle de respuesta	Enfoque de género e interseccionalidades
				trata de violencia de género online, que puede inducir a ciertas confusiones a las víctimas al momento de informarse tanto sobre las protecciones legales como de los mecanismos de mitigación que las mismas plataformas pueden brindarle.
3	18. Diseñar e implementar una campaña de ciberseguridad de carácter masivo y fomentar la implementación de programas de difusión estableciendo alianzas con los privados en campañas de sensibilización, con énfasis en sectores vulnerables y empleando perspectiva de género.	Subsecretaria General de Gobierno	<p>El Departamento de Marketing perteneciente a la División Secretaria de Comunicaciones (SECOM), asesoró al Ministerio del Interior y Seguridad Pública en una campaña sobre la materia durante el 2018, la que contó con minutos otorgados por CNTV para la emisión por los canales de televisión abierta en horario prime. La campaña fue emitida en diciembre 2018 y enero 2019.</p> <p>Se indica link para acceder al spot de la campaña y su plan de medios.</p>	<p><i>Brechas:</i></p> <p>Como se constató anteriormente, el spot hace una aproximación general a la ciberseguridad desde el punto de vista de la responsabilidad personal de las y los usuarios. Y aunque entre el casting hay dos mujeres, una de ellas adulta mayor, no es suficiente para brindar un énfasis en sectores vulnerables y empleando una perspectiva de género. Por ende, no da respuesta a las problemáticas de ciberseguridad más comunes de acuerdo con el género e interseccionalidades más importantes de las personas. En este sentido, tampoco se aprecia en el plan de medios del spot, evidencia explícita que la selección de canales y horarios haya sido pensada para estos sectores.</p>

N°	Medida	Responsable	Detalle de respuesta	Enfoque de género e interseccionalidades
4	21. Diseñar e implementar una campaña de ciberseguridad orientada a los adultos mayores, que considere medidas de capacitación y difusión.	MDS (Senama) - MINECON (Mesa Capital Humano) (CICS supervisor de la medida)	<p>a) Noviembre, 2020</p> <p>SENAMA, en conjunto con la Subsecretaria del Interior, lanza campaña educativa sobre conciencia digital para adultos mayores. Ésta busca guiar y apoyar a los adultos mayores para evitar que sean víctimas de algún tipo de estafa cibernética. Consiste en seis cápsulas de videos que abordan la importancia de la privacidad en internet, explicando, por ejemplo, qué es la ciberseguridad, un ciberdelito, phishing, se presentan los tipos de delitos, cómo identificar una estafa y recomendaciones. La campaña se encuentra disponible en las redes sociales y en el sitio web www.concienciadigital.gob.cl</p> <p>b) Enero, 2021</p> <p>Dirigentes de personas mayores del país se capacitan en Ciberseguridad por medio de una Charla, organizada por el programa Escuela de Formación para Dirigentes Mayores de SENAMA. “Ciberseguridad y Redes Sociales, ¿cómo estar prevenidos?” fue el nombre de la charla realizada por el oficial de Seguridad de la información de la Universidad de Chile, Andrés Peñailillo, y donde participaron dirigentes mayores, de las 16 regiones del país. Entre los temas abordados destacaron: las redes más utilizadas, recomendaciones de seguridad, como, por ejemplo: para generar contraseñas seguras, además se habló de los distintos tipos de estafas por canales digitales, entre otros temas.</p>	<p><i>Avances:</i></p> <p>Uno de los públicos objetivos con mayor necesidad de capacitación en términos de ciberseguridad, los adultos mayores, ha sido abordado.</p> <hr/> <p><i>Brechas:</i></p> <p>Las capacitaciones son muy esporádicas y puntuales. Debe hacerse el esfuerzo de convertirlas a capacitaciones sistémicas para abordar aún más público.</p>

N°	Medida	Responsable	Detalle de respuesta	Enfoque de género e interseccionalidades
5	23. Apoyar decididamente el establecimiento a nivel internacional de procesos de consultas políticas regionales, subregionales y multilaterales, con especial énfasis en la región.	MINREL	<p>Ámbito OEA:</p> <p>En los días 26 y 27 de octubre de 2022 se realizó en la Ciudad de México la cuarta reunión del grupo de trabajo, presidida por México. Durante la reunión, Chile, con el apoyo de Canadá y México, presentó 4 nuevas medidas de fomento de la confianza, relacionadas con:</p> <ul style="list-style-type: none"> -Enfoque de género. -Implementación de las 11 normas voluntarias no vinculantes sobre comportamiento responsable de los Estados en el ciberespacio adoptadas por la Resolución 70/237 de la Asamblea General de las Naciones Unidas. -Derecho internacional. -Y promoción en el ámbito de las tecnologías de la información y las comunicaciones el trabajo y diálogo con las todas partes interesadas, como la sociedad civil, academia, sector privado, comunidad técnica, entre otros. 	<p><i>Avances:</i></p> <p>Entre las medidas impulsadas por Chile en el ámbito OEA, está el enfoque de género.</p> <hr/> <p><i>Brechas:</i></p> <p>Se puede seguir trabajando en el enfoque de género en otras políticas internacionales que hoy son claves en ámbitos de ciberseguridad: por ejemplo, la continuación de la discusión en el grupo de trabajo de composición abierta de la ONU (OEWG en inglés) sobre la seguridad de las tecnologías de la información y las comunicaciones y en su uso 2021-2025.</p>
6	34. Realizar ciberejercicios sobre incidentes de Ciberseguridad con diferentes comunidades interesadas para fomentar el	CSIRT	<p>Se han realizado ejercicios de simulación a cargo de CSIRT involucrando a los Encargados de ciberseguridad y de las áreas TI.</p> <p>Actividad permanente (Anual)</p>	<p><i>Avances:</i></p> <p>Se participa en Cyberwomen Challenge, que son actividades impulsadas por la OEA, en los cuales solo participan mujeres previa inscripción y se trata de ejercicios de ciberseguridad. Una de las ganadoras de estos Challenge incluso fue reclutada por el CSIRT debido a su alto conocimiento técnico.</p>

N°	Medida	Responsable	Detalle de respuesta	Enfoque de género e interseccionalidades
	conocimiento, investigación y difusión adecuada de brechas, vulnerabilidades y vías de mitigación encontradas en los sistemas nacionales.			<p><i>Brechas:</i></p> <p>El análisis de incidentes de ciberseguridad diferenciados de acuerdo al género aún es un pendiente que avanzar.</p>
7	36. Incorporar en la Encuesta Nacional Urbana de Seguridad Ciudadana (ENUSC) un set de preguntas vinculadas a los ciberdelitos.	Subsecretaría de Prevención del Delito	<p>En el marco de mejoras en la aplicación anual de la ENUSC, el año 2014 la entonces Subsecretaría, implementó un consejo de expertos que propuso realizar mejoras en la medición y contenido de la encuesta. Entre estas mejoras, se contempló un apartado de consulta de victimización por delitos cibernéticos, la sección y las tres preguntas involucradas se describen en el cuadro N° 1 (adjunto).</p> <p>En términos concretos, desde el año 2015 al 2021 la ENUSC, cuenta con indicadores de delitos cibernéticos descritos para el nivel país así como a nivel de regiones. De esta forma, la Subsecretaría de Prevención del Delito estaría cumpliendo con el compromiso descrito en la medida N°36 antes señalada. Como indicador de cumplimiento y/o medio de verificación, se encuentra disponibles tanto las bases de datos, como los informes de resultados de la encuesta de años 2015 a 2021, en los</p>	<p><i>Avances:</i></p> <p>En la sección de delitos cibernéticos (refiere a victimizaciones ocurridas a través del uso de la tecnología informática e internet) se incluyó la pregunta J8. Durante los últimos doce meses, ¿a usted o algún miembro de su hogar le sucedieron las siguientes situaciones?, ¿Cuántas veces? Entre las opciones está 05 - Acoso u hostigamiento a través de mensajes indecentes u obscenos, comunicaciones, imágenes no solicitadas o requerimientos de carácter sexual. / Para el año 2022, la Subsecretaria junto con el INE, harán una actualización del instrumento, que consideran delitos como el ciberacoso (ver respuesta subsecretario de prevención del delito).</p>

N°	Medida	Responsable	Detalle de respuesta	Enfoque de género e interseccionalidades
			<p>cuales se reporta el indicador de prevalencia de delitos cibernéticos. Esta información es de acceso público y puede ser descargada de los portales de información de la Subsecretaría y el INE: http://cead.spd.gov.cl/estudios-y-encuestas / https://www.ine.cl/estadisticas/sociales/seguridad-publica-y-justicia/seguridad-ciudadana</p> <p>Para el año 2022, la Subsecretaría en conjunto con el INE, organismo técnico que implementa la encuesta, se encuentran planificando una actualización en términos de diseño muestral y delitos abordados por el instrumento, teniendo como referencia encuestas de victimización a nivel internacional y propuestas regionales como la VICLAC, que cuenta con apoyo de UNODC. La propuesta de ésta última considera los siguientes delitos en cuadro N° 2 (adjunto).</p> <p>La determinación final de las modificaciones realizadas en el cuestionario serán parte de metodologías de revisión y formulación de preguntas realizadas por el INE y la validación de un comité asesor en temáticas de seguridad implementada por la subsecretaría.</p>	<p>Aquello es un avance importante en la brecha sobre datos de violencia de género online.</p> <p><i>Brechas:</i></p> <p>Más que una brecha, se constata que es importante ver los resultados de esta pregunta y coordinar respuestas de política pública adecuadas; además de evaluar el mismo desempeño de la pregunta en la encuesta, para ver si necesita mejoras.</p>

V. Conclusiones

El enfoque de género de la PNCS 2017-2022 es una estrategia novedosa a nivel regional y, considerando un contexto internacional, fue un primer paso valorable, aunque sin mayor profundidad al momento de traducirla al plan de acción. Esto último también se debe leer inserto en los propios tiempos históricos cuando fue diseñado el documento (2016-2017), donde tampoco desde el enfoque de género había mayor claridad de cómo avanzar más explícitamente en las políticas y estrategias nacionales de ciberseguridad.

En forma más particular, es interesante constatar que hay un avance mucho más sustantivo en considerar la perspectiva de género que lo que originalmente estipulaba el plan de acción, lo que probablemente se debe a que en estos últimos años ha habido un creciente interés de la opinión pública en cuestiones de género y tecnología, impulsadas por las problemáticas de la violencia de género en línea y también la digitalización masiva producida por la pandemia.

Esos avances son siempre una buena noticia, pero son aún insuficientes. Más aún, como se ve en la sección anterior, pueden ser optimizables desde un punto de vista técnico. Sobre todo, en consideración a los desarrollos que la perspectiva de género ha tenido en la ciberseguridad en este último tiempo y que han profundizado un amplio espectro de intereses en la materia, desde la brecha de género en el ámbito de la ciberseguridad, las dimensiones de la violencia de género en la ciberseguridad, las vulnerabilidades diferenciales a los ciberataques, el impacto diferencial de los ciberincidentes en función del género, la reconfiguración de los marcos de análisis de la ciberseguridad, hasta las políticas públicas internacionales en materia de ciberseguridad, entre otros.

El reto de la próxima PNCS será tomar estos avances, mejorarlos y profundizarlos, además de incorporar de forma transversal el enfoque de género. Para eso, será necesario trabajar con todas las partes interesadas relacionadas con la materia para comprender las brechas de género más urgentes que la política debe hacerse cargo, además de identificar las oportunidades que en Chile existen para apalancar el avance de la perspectiva de género en la ciberseguridad. Las condiciones para que el país siga siendo pionero en el enfoque de género en la ciberseguridad están plenamente dadas.

VI. Bibliografía

ACTI (2021). Mujeres representan solo el 15% de los trabajadores del área de ciberseguridad en Chile. <https://acti.cl/mujeres-representan-solo-el-15-de-los-trabajadores-del-area-de-ciberseguridad-en-chile/>

Ananías, C. & Vergara, K. (2020). Informe preliminar. Chile y la violencia de género en Internet: experiencias de mujeres cis, trans y no binaries. ONG Amaranta. <https://amarantaong.files.wordpress.com/2020/08/informe-proyecto-aurora.pdf>

Brown, D. & Pytalk, A. (2020) Why Gender Matters in International Cyber Security. Women's International League for Peace and Freedom and the Association for Progressive Communications <https://www.apc.org/en/pubs/why-gender-matters-international-cyber-security>

Comisión Interamericana de los Derechos Humanos (CIDH). 2008. Algunas precisiones y términos relevantes. Disponible en: <http://www.oas.org/es/cidh/lgtbi/mandato/precisiones.asp>

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

Ferrari, V. (2021) WHY SHOULD GENDER MATTER (MORE) FOR THE OEWG? *Cyber Peace & security Monitor*. Vol.01 N°10. 17 March 2021. <https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.10.pdf>

Herrera Carpintero, P. (2020). El enfoque de género en la Política Nacional de Ciberseguridad de Chile. *Revista Chilena De Derecho Y Tecnología*, 9(1), 5-32. <https://doi.org/10.5354/0719-2584.2020.51577>

ISC2 (2022a). (ISC)² Cybersecurity Workforce Study: Women in Cybersecurity. <https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx?la=en&hash=4C3B33AABFBFAFDDA211856CB274EBDDF9DBEB38>

ISC2 (2022b). The (ISC)² Cybersecurity Workforce Study. <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx>

Maddocks, S. (2019) "MI VIDA NO ES TU PELI PORNO": 5 RAZONES PARA NO USAR EL TÉRMINO "PORNOVENGANZA". *GenderIT*. <https://www.genderit.org/es/feminist-talk/mi-vida-no-es-tu-peli-porno-5-razones-para-no-usar-el-termino-pornovenganza>

OEA (2018). General Secretariat. Género, derechos y diversidad en la Secretaría General de la OEA / Secretaría General de la Organización de los Estados Americanos. (OAS. Documentos oficiales ; OEA/Ser.D/XV.20). <https://www.oas.org/es/cim/docs/GPAP-ES.pdf>

OEA (2022). Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades. https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf

OECD (2016), 2015 OECD Recommendation of the Council on Gender Equality in Public Life, OECD Publishing, Paris. <http://dx.doi.org/10.1787/9789264252820-en>

ONU (2018). Consejo de Derechos Humanos. Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias, acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos. A/HRC/38/47.

Peña, P. & Herrera, P. (2021). Género y Cibersguridad. CEDI.

RELE (2022). Mujeres periodistas y salas de redacción: avances, desafíos y recomendaciones para prevenir la violencia y luchar contra la discriminación / Pedro Vaca Villareal, Relator Especial para la Libertad de Expresión. v. ; cm. (OAS. Documentos oficiales; OEA/Ser.L/V/II). ISBN: 978-0-8270-7545-0

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