Propuesta de acciones para fortalecer el enfoque de género en la nueva Política Nacional de Ciberseguridad (PNCS).

Diciembre, 2022.

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

Índice de contenido

I. Alcance de este informe

Esta propuesta se construye en base a dos informes: “Resultados de la Política Nacional de Ciberseguridad 2017-2022: avances y brechas sobre la inclusión del enfoque de género”, y “Diagnóstico actual sobre las nuevas demandas para incorporar la perspectiva de género en la Política Nacional de Ciberseguridad”.

Su objetivo es sugerir acciones concretas para fortalecer el enfoque de género en la nueva Política Nacional de Ciberseguridad (PNCS) que construya sobre los avances logrados en la anterior política, incorpore las urgencias y oportunidades detectadas por los especialistas en la materia, e incluya otras materias en las que se pueda seguir ahondando para que el país avance en una PNCS que fortalezca una visión de la ciberseguridad centrada en las personas y sus derechos, y que tenga especial atención con poblaciones en especial situación de vulnerabilidad como mujeres, adultos mayores, niños, niñas y adolescentes, disidencias sexuales y de género, y personas con discapacidad.

II. Enfoque de género interseccional: una herramienta para acercar la ciberseguridad a todas las personas

El género es el conjunto de ideas, representaciones, prácticas y prescripciones sociales elaboradas a partir de la diferencia anatómica entre los sexos. Pero el género es más que un poderoso 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. En ese contexto, el enfoque de género o análisis de género es una herramienta para analizar las diferencias de género y mitigarlas.

El enfoque de «transversalidad de la perspectiva de género» (*gender mainstreaming*) comenzó a aplicarse luego de la Conferencia de la Mujer de Beijing de 1995 y es un proceso de evaluación de las implicaciones para las mujeres y los hombres de cualquier acción planificada por los Estados, incluidas la legislación, las políticas o los programas, en todos los ámbitos y a todos los niveles. Su objetivo último es lograr la igualdad de género.

Por su parte, la perspectiva interseccional viene a enriquecer el enfoque de género, en tanto identifica 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 la persona en la sociedad, poniendo en escena las otras diferencias que nos constituyen, y enriqueciendo la noción de sujetos y poblaciones que son atravesados por atributos diversos. Así, una perspectiva de género interseccional es una metodología que permite complejizar la mirada a los problemas sociales ya que el análisis ahora considera múltiples sistemas de poder que hasta entonces se veían por separado y se convierte en una herramienta poderosa de análisis para diseñar e implementar políticas públicas centradas en la diversidad de personas.

Hasta ahora no existe 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 nacionales. De manera más tradicional, el enfoque de género ha sido comprendido desde las brechas de género en la fuerza laboral de la industria de ciberseguridad y en su gobernanza. Pero en los últimos años, desde las políticas públicas

relacionadas a la ciberseguridad, el enfoque de género se ha visto impulsado gracias a las corrientes llamadas humano-céntricas, que ven en las personas como el objeto referente de la ciberseguridad, y que se relacionan también con el enfoque de derechos humanos en la materia. En este contexto, **el enfoque de género interseccional comprende que las tecnologías y peligros cibernéticos para las personas no son neutrales al género y sus interseccionalidades y, por lo tanto, los impactos de las vulnerabilidades son distintos en función de las identidades y expresiones de género de las personas**.

Así, el enfoque de género interseccional en la institucionalidad de la ciberseguridad de un Estado **se convierte en una herramienta funcional para diseñar y desplegar una ciberseguridad centrada en las personas y sus derechos**. Esto significa, además, que esta perspectiva se debe convertir en un enfoque sistémico con el objetivo de impactar positivamente al mayor número de personas en toda su diversidad y complejidad de situaciones de vida.

III. Incorporación del enfoque de género interseccional en la PNCS y su plan de acción

A continuación, y de acuerdo con la evaluación de la política anterior, la visión de los expertos locales y los instrumentos de reciente aparición que generan sugerencias para la incorporación del género en las estrategias locales, se ordenan acciones concretas donde la próxima PNCS puede avanzar en concordancia con el contexto local.

Será, posteriormente, que la Coordinación Nacional de Ciberseguridad, de acuerdo con los procesos establecidos para el diseño de la PNCS y los énfasis que se quieran dar, incluido las posibilidades presupuestarias, el que decidirá qué incorporar y cómo hacerlo, incluido los actores gubernamentales que deben estar involucrados. Con todo, este documento trata de presentar las sugerencias desde una perspectiva amplia, de manera de darle un margen cómodo al tomador de decisión para poder incluir estas acciones.

La propuesta contiene tres partes: sugerencias para la política misma, indicaciones concretas para avanzar en el plan de acción, y precisiones para su aplicación.

a. Objetivos generales de la PNCS

La visión de género está estrechamente relacionada al papel que desempeña la ciberseguridad en la protección de los derechos humanos de las personas. En ese contexto, se debería avanzar en que, entre los objetivos de la estrategia, se reconozcan las necesidades diferenciadas de las personas en materia de ciberseguridad en función del género y otras interseccionalidades. Más específicamente, se puede determinar segmentos de población que están en una situación de mayor vulnerabilidad, entre ellas, por ejemplo: mujeres, adultos mayores, niños, niñas y adolescentes, disidencias sexo-genéricas y personas con discapacidad.

b. Gobernanza

Como diversos procesos de gobernanza de tecnología así lo demuestran, es vital que la nueva PNCS cuente con un marco claro de gobernanza que incluya la participación de todas las partes interesadas en la aplicación y revisión de la política para que, particularmente en este caso, sean una fuente de información sobre los aspectos diferenciados en los que una perspectiva de género puede mejorar la ciberseguridad de las personas.

Algunos actores que considerar para sus aportes sobre enfoque de género en la ciberseguridad:

Locales:
Derechos Digitales
ONG Amaranta
Fundación Datos Protegidos
Internet Society Chile (ISOC)
CEDI – Universidad de Chile
Alianza Chilena de la Ciberseguridad
Technovation Girls Chile

Internacionales:
WOMCY
Organización de los Estados Americanos (OEA) - Programa de Ciberseguridad del CICTE
Association for Progressive Communications (APC)

c. Ciber-resiliencia

Se refiere a las diversas medidas que el gobierno adoptará para proteger las infraestructuras, las redes, los sistemas, la información y a los usuarios de los ciberataques y las ciberamenazas. En este punto, respecto al enfoque de género interseccional en el contexto nacional, se propone incluir los siguientes objetivos y acciones.

N°	Objetivos	Acciones	Precisiones
1	Sensibilizar a públicos objetivos sobre habilidades y competencias de ciberseguridad desde una perspectiva de género interseccional, que permita acercar de forma coherente la tecnología a las personas, ayude a prevenir ataques informáticos, y mitigue la brecha de apropiación de tecnologías.	A. Campañas multiplataformas de sensibilización sobre ciberseguridad con un enfoque de género interseccional que lleguen a públicos objetivos y que sean continuos.	Basados en las campañas de la anterior PNCS, los especialistas apuntaron la necesidad que las campañas generen alianzas con organizaciones de base (tanto a nivel de sociedad civil como del propio Estado) para que lleguen a los públicos objetivos. Asimismo, se precisa la necesidad de que sea visada por una parte técnica para adecuar el lenguaje.
		B. Capacitaciones a nivel territorial para la creación de competencias y habilidades de ciberseguridad con enfoque de género interseccional.	De nuevo, con la idea de que llegue a público objetivos, se apunta a asociarse con diversas organizaciones desplegadas en el territorio (tanto del estado como, particularmente, de la sociedad civil que trabajan estos temas).
		C. En el mes de la ciberseguridad, los organismos partes de la institucionalidad de ciberseguridad nacional debe realizar acciones de difusión con particular énfasis en el enfoque de género y ciberseguridad	

2	Desarrollar competencias sobre los impactos diferenciados de los ataques informáticos con los actores Estatales relevantes en la materia. Esto para poder, por un lado, prevenir ataques y, por otro, desarrollar protocolos que ayuden a mitigar los daños.	A. Capacitaciones a los organismos pertenecientes a la institucionalidad de la ciberseguridad en Chile sobre cómo los incidentes de ciberseguridad tienen un impacto diferenciado diferente en las personas, a través de la aplicación de la metodología de género interseccional.	Estas capacitaciones deben incluir por cierto la violencia de género en línea (incluidos en especiales grupos en situación de alta vulnerabilidad social como mujeres en política, mujeres periodistas y mujeres defensoras de derechos humanos), pero no debe solo concentrarse en aquello: debe incluir el enfoque de género interseccional como herramienta para el análisis del impacto diferenciado de los ataques que afectan datos de personas.
3		B. Realizar ciberejercicios sobre incidentes de Ciberseguridad con perspectiva de género interseccional con diferentes comunidades interesadas para fomentar el conocimiento, investigación y difusión adecuada de brechas, vulnerabilidades y vías de mitigación encontradas en los sistemas nacionales.	En la PNCS anterior, se constató la participación 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. Si bien esta es una excelente acción que ojalá pueda ser replicada en los próximos años, se indica la necesidad de fomentar ciberejercicios donde se pueda determinar mejor el impacto diferenciado en las personas, utilizando el enfoque de género interseccional.

4	Informar sobre el avance anual de diversos aspectos relacionados sobre ciberseguridad y género en el país, que ayuden a alimentar las políticas públicas con evidencia.	A. Coordinación interministerial que incorpore de manera estandarizada indicadores de ciberdelitos y ciberseeguridad en los levantamientos de información que hacen de los públicos con los que trabajan.	En la PNCS anterior, se constató que en la Encuesta Nacional Urbana de Seguridad Ciudadana (ENUSC) se incluyó un set de preguntas vinculadas a los ciberdelitos, y en la sección que se refiere a victimizaciones ocurridas a través del uso de la tecnología informática e internet, se incluyó la pregunta sobre acoso y hostigamiento de carácter sexual.
		B. Creación de grupos focales para la medición continua de habilidades y competencias de ciberseguridad en grupos objetivos desde un enfoque de género, que permita crear indicadores de evolución y nuevas necesidades.	Esta acción puede ser un feedback esencial para el objetivo 1 de ciber-resiliencia planteado más arriba.
		C. Publicación de informe anual sobre avances y brechas de la ciberseguridad en grupos objetivos, desde el enfoque de género interseccional en la ciberseguridad.	Este informe debería alimentarse con las anteriores acciones de este objetivo como con otras fuentes que permitan el panorama más completo posible.
5	Adoptar medidas para incrementar la participación de mujeres en la ciberseguridad, tanto a nivel de gobernanza como a nivel de industria, de manera de mitigar la falta de profesionales en el área, pero también para mejorar la empleabilidad de mujeres en los próximos años.	A. Desarrollar un estudio tanto cuantitativo como cualitativo que determinen las brechas de incorporación de mujeres en la industria y gobernanza de ciberseguridad local e identifiquen las barreras sociotécnicas para su inclusión.	
		B. Facilitar una mesa técnica de múltiples partes interesadas (Estado, academia, industria, sociedad civil, sector técnico) que desarrolle un plan de acción que permita, a través de compromisos público-privados, aumentar	La PNCS no tenía ningún avance en temas de enfoque de género y ciberseguridad en la industria; parece urgente poder activar medidas en este ámbito.

		progresivamente el ingreso y desarrollo de mujeres en ciberseguridad, tanto en la industria como en la gobernanza.	

d. Respuesta a incidentes cibernéticos

Define la amplia gama de acciones que el gobierno tomará cuando se produzca un ciberataque. Por ejemplo, podría incluir el desarrollo de planes de contingencia, el suministro de herramientas y recursos a las fuerzas de seguridad, el apoyo a los afectados, etc. Las respuestas a los incidentes cibernéticos son fundamentales para las personas en situaciones de vulnerabilidad debido al género y otras interseccionalidades. En este aspecto, para la PNCS se propone:

N°	Objetivos	Acciones	Precisiones
1	Desarrollar protocolos en los organismos de la institucionalidad de ciberseguridad del Estado que tomen en cuenta el impacto diferenciado de los incidentes de ciberseguridad de acuerdo a un enfoque de género interseccional, a propósito de la obligación de incidentes de ciberseguridad por parte de la Administración del Estado.	A. CSIRT lidera el desarrollo y aplicación protocolos de análisis de impactos diferenciados sobre las personas debido a incidentes de ciberseguridad, de comunicación oportuna de estos impactos diferenciados, y de la gestión de los ciberincidentes de manera de activar mecanismos de mitigación adecuados y pertinentes.	A nivel de discusión legal, están ingresados en el Congreso al menos dos proyectos de ley (protección de datos personales y ley marco sobre ciberseguridad e infraestructura crítica de la información) que generarían nuevas oportunidades para elaborar protocolos similares a los anteriormente planteados.
		B. Realizar difusión y capacitaciones sobre estos protocolos en el sector privado interesado para fortalecer estándares sectoriales.	

e. Cibercrimen

Establece la forma en que el gobierno abordará la ciberdelincuencia, principalmente el desarrollo y la aplicación de la legislación sobre ciberdelincuencia y el apoyo a su cumplimiento por parte de las fuerzas del orden. Desde el enfoque de género, se propone:

N°	Objetivos	Acciones	Precisiones
1	Desarrollar competencias sobre la atención y manejo de investigaciones sobre casos de violencia de género online en Policías y Fiscalía	A. Capacitaciones a policías y fiscalía sobre violencia de género online y procesos de revictimización en la atención de casos, obtención de pruebas y cadena de custodia.	
2	Crear en conjunto con Fiscalía y Policías protocolos estandarizados, con perspectiva de género, sobre atención y gestión de casos de violencia de genero online.	B. Mesa de trabajo ampliada con policías y Fiscalía, sociedad civil y SernamEG para el diseño conjunto de protocolos estandarizados sobre atención de casos de violencia de género online, obtención de pruebas y su la cadena de custodia.	Muchas organizaciones de la sociedad civil que trabajan en Chile violencia de género online tienen experiencia concreta en casos de revictimización en el proceso de denuncia e investigación: una mesa ampliada con ellas para la creación de estos protocolos es vital para diseñarlos desde la evidencia. Asimismo, se puede hacer en coordinación con el SernamEG.
3	Avanzar en marcos legales y políticos que den protección jurídica a las ciberamenazas para grupos objetivos como, por ejemplo, la violencia de género en línea. También puede ser de interés la protección de la ciberseguridad para periodistas y defensoras de los derechos humanos.	C. Seguimiento y realizar aportaciones en proyectos de ley y otras políticas públicas relacionadas a violencia de género online.	

f. Cooperación internacional

Establece cómo trabajará el gobierno con otros gobiernos y organizaciones internacionales y regionales en cuestiones de ciberseguridad (colaboración para hacer frente a amenazas compartidas, promoción de valores, prioridades de política exterior, etc.). En este sentido, respecto al enfoque de género interseccional en la ciberseguridad, se propone:

N°	Objetivos	Acciones	Precisiones
1	Integrar las consideraciones de género interseccional en el debate internacional sobre las ciberamenazas.	Hacer el seguimiento y cooperar con discusiones internacionales sobre la ciberseguridad hechas en diferentes ámbitos como la OEA, la ONU y la Agenda Women, Peace, and Security, entre otros.	
2	Apoyar, fortalecer y articular procesos de cooperación y asistencia internacional en ciberseguridad y género	Establecer grupos de trabajo bilaterales y diálogos en ciberseguridad y género con países socios y amigos	