Diagnóstico de especialistas sobre las prioridades de la perspectiva de género en la nueva Política Nacional de Ciberseguridad.

Diciembre, 2022.

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

Índice de contenido

I. Alcance de este informe

Este informe busca ordenar los objetivos sobre el enfoque de género interseccional que diversos especialistas entrevistados diagnosticaron como prioridad para la nueva Política Nacional de Ciberseguridad (PNCS).

Para recoger la información, se hicieron entrevistas en profundidad a actores sociales locales de las diversas partes interesadas en la materia, con experiencia en enfoque de género, de manera de comprender su visión de los problemas, desafíos, urgencias y oportunidades de la nueva política. Es importante aclarar que no todos los actores entrevistados habían participado en la primera política ni, al momento de entrevistarlos, conocen la evaluación que el gobierno ha hecho de ella. En este sentido, su visión está basada primeramente en su experiencia profesional como, secundariamente, en su experiencia limitada con el desarrollo de la PNCS.

Asimismo, los resultados de este documento no reemplazan un proceso de participación más abierto que debe habilitar el Estado para poder recoger, de manera participativa, visiones diversas y descentralizadas de cómo avanzar en la perspectiva de género en la política de ciberseguridad. Con todo, debe ser leído como una primera prospección que muestre posibles vías donde poner énfasis en la PNCS de acuerdo con las necesidades locales.

II. Sobre la perspectiva de género

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 y otras jerarquías sociales.

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, un reto para que esta perspectiva se convierta en un enfoque sistémico de la PNCS con el objetivo de impactar positivamente al mayor número de personas en toda su diversidad y complejidad de situaciones de vida.

III. Entrevistados

- Paloma Herrara, investigadora CEDI, Universidad de Chile.
- Patricia Peña, académica, ICEI, Universidad de Chile.
- Francisco Vera, especialista en políticas nacionales de ciberseguridad.
- Cecilia Ananías, ONG Amaranta.
- Jessica Matus, Fundación Datos Protegidos.

IV. Análisis de resultados

En general, hay una sensación de que esta nueva PNCS puede ser una oportunidad para poder encaminar un fortalecimiento de la perspectiva de género en la materia. No obstante, se comprende que es ésta es una de las diversas políticas digitales que existen en el Estado, y muchos apuntan a la necesidad que estas políticas no solo estén coordinadas en una institucionalidad coherente, sino también en la adopción transversal de la perspectiva de género interseccional. En este caso, se advierte, la PNCS podría estar parchando los vacíos que las otras políticas tienen debido a un desarrollo que ha sido ciego a la perspectiva de género interseccional.

a. Objetivos inmediatos de la PNC respecto a la perspectiva de género

En base a las entrevistas, se puede concluir al menos cuatro objetivos generales inmediatos que esta política debiera tener respecto al fortalecimiento de la perspectiva de género:

- **Sensibilizar al público general**, sobre habilidades y competencias de ciberseguridad desde una perspectiva de género interseccional, que permita acercar de forma coherente la tecnología a las personas.

- **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.

- **Crear, profundizar y/o estandarizar indicadores a nivel estatal sobre diversos aspectos relacionados sobre ciberseguridad y género en el país,** que ayuden a alimentar las políticas públicas con evidencia.

- **Incrementar la participación de mujeres en la industria de la ciberseguridad,** tanto a nivel técnico como profesional, para mitigar la falta de profesionales en el área, pero también para mejorar la empleabilidad de mujeres en los próximos años.

Estos objetivos, si llegan a permear lo macro de las políticas y llegan efectivamente hacia el día a día de las personas, puede tener efectos inmediatos en su bienestar y desarrollo personal como económico.

b. Acciones y oportunidades

Dentro de estos objetivos, las personas entrevistadas entregaron precisiones críticas y oportunidades que la nueva política de ciberseguridad puede trabajar:

Objetivo:
Sensibilizar al público general, sobre habilidades y competencias de ciberseguridad desde una perspectiva de género interseccional, que permita acercar de forma coherente la tecnología a las personas.

Línea:
- Ciber-resiliencia

Comentarios:
A nivel generacional, se pueden analizar las diversas brechas de habilidades y competencias que, en especial mujeres, tienen respecto al uso de tecnología. Por ejemplo, se señala que en niñas y jóvenes su falta de conocimiento de ciberseguridad muchas veces viene de la mano con la falta de una educación sexual integral, donde cuestiones tan fundamentales como el consentimiento están ausentes de la conversación y sus comportamientos. Distinto es el caso de mujeres adultas, donde las múltiples jornadas de trabajo (formal / informal y doméstico) no les permite el tiempo suficiente para comprender el funcionamiento de internet y se enfrentan a las tecnologías desde las inseguridades. A nivel de adulto mayor, hay una sensación generalizada que no existe una alfabetización digital para ellos, y su relación con las tecnologías muchas veces depende de terceras personas o servicios, lo que los pone en mucha vulnerabilidad.

Por lo demás, a lo anterior se tiene que incluir otras interseccionalidades, sobre todo la brecha urbana/rural. En los espacios rurales muchas veces la interacción con internet es a base de ofertas zero-rating o de solo usar chats de mensajería debido a la cobertura de internet, por lo que navegar por el resto de Internet es casi imposible y derechos como el acceso a la información se ven mermados.

Oportunidades:
- La sensibilización debe hacerse con una perspectiva de género interseccional.
- Asimismo, debe no solo tener una perspectiva generacional, sino también adoptar otras perspectivas de grupos que necesitan capacitaciones urgentes, como mujeres en pymes incorporadas a la economía digital.
- El principal objetivo debe ser conectarse con la ciudadanía, por lo que debe considerar múltiples formas de hacerlo. Por ejemplo, campañas multiplataformas como también crear materiales de capacitación en formato diverso.
- Para que la sensibilización funcione, es clave el esfuerzo colaborativo que se debe hacer, por un lado, con los diversos ministerios y servicios del Estado (a nivel centra y regional= que trabajan con mujeres de distinta edad o que desarrollan un foco particular con ellas, además de personas adulto mayor, niños, niñas y adolescentes, como con personas con discapacidad. Asimismo, es necesario extender puentes con diversas organizaciones de sociedad civil que trabajan temas de tecnología y género y que tienen llegada a los diversos públicos objetivos de manera territorial.

Objetivo:
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.

Línea:
- *Ciber-resiliencia*
- *Respuesta a incidentes cibernéticos*

Comentarios:
Existe una sensación general que a nivel de Estado se puede hacer mucho más para desarrollar competencias que permitan prevenir y mitigar daños producidos por los impactos diferenciados que tienen los ataques informáticos desde una perspectiva de género.

Por un lado, se apunta a que un organismo como CSIRT puede jugar un papel clave liderando el desarrollo de buenas prácticas, protocolos y estándares de ciberseguridad respecto a los impactos diferenciados de los ataques informáticos desde una perspectiva de género, no solo enfocándose al problema real de la violencia de género online, sino también a otros ataques como filtraciones masivas de datos personales y sensibles. Asimismo, puede avanzar en protocolos que ayuden a un análisis adecuado y pertinente al momento del reporte de incidentes de ciberseguridad por parte de la Administración del Estado.

Asimismo, se señala repetidamente a un problema que se está transformado en estructural: la falta de protocolos de atención desde una perspectiva de género por parte de las policías y Fiscalía para atender casos de violencia de género online y gestionar de manera prudente la obtención de pruebas y el cuidado de su cadena de custodia.

Oportunidades:
- Los organismos pertenecientes a la institucionalidad de la ciberseguridad en Chile deben capacitarse en cómo los incidentes de ciberseguridad afectan de forma diferente a las personas, y para eso es importante aplicar la metodología de género interseccional. Además, deben desarrollar protocolos de análisis que tomen en cuenta este impacto diferenciado de los incidentes de ciberseguridad, de comunicación de estos impactos diferenciados, y de gestión de los ciberincidentes de manera de activar mecanismos de mitigación adecuados y pertinentes.
- Policías y Fiscalía pueden avanzar en capacitación sobre violencia de género online y procesos de revictimización.
- 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.

Objetivo:
Crear, profundizar y/o estandarizar indicadores a nivel estatal sobre diversos aspectos relacionados sobre ciberseguridad y género en el país, que ayuden a alimentar las políticas públicas con evidencia.

Línea:
- Ciber-resiliencia
- Respuesta a incidentes cibernéticos

Comentarios:
Diversos actores señalan que hay una falta de estadísticas y de indicadores sobre diversos aspectos de género y ciberseguridad que permitan avanzar en políticas públicas más decididas y basadas en evidencia. Además, los indicadores son vistos como la forma de poder ver de forma más concretas los avances de la política y las nuevas necesidades.

Asimismo, se apunta a que necesitamos estadísticas, pero también investigación cualitativa continua sobre diversos aspectos, como:
- Conectividad en base a género, pero, por sobre todo, sobre todo habilidades y competencias.
- Número y gestión sobre denuncias de violencia de género online.
- Empleabilidad de mujeres en ciberseguridad y barreras sociotécnicas para su incorporación.

Oportunidades:
- Se pueden seguir refinando y estandarizando los datos de ciberdelitos respecto a cuestiones de violencia de género online.
- Es importante medir continuamente habilidades y competencias de ciberseguridad desde una perspectiva de género interseccional que permita crear indicadores de evolución y nuevas necesidades.
- Es importante, además, hacer una coordinación interministerial que incorpore de manera estandarizada indicadores de ciberseguridad en los levantamientos de información que hacen de los públicos con los que trabajan.

Objetivo:
Adoptar medidas para incrementar la participación de mujeres en la industria de la ciberseguridad, tanto a nivel técnico como profesional, para mitigar la falta de profesionales en el área, pero también para mejorar la empleabilidad de mujeres en los próximos años.

Línea:
- Ciber-resiliencia

Comentarios:
Tanto en el mundo como en Chile, hay una escasez de especialistas para trabajar en la industria en las que se apunta a que en el rubro de las Tecnologías de la Información (TI) las mujeres representan el 25% de la fuerza laboral. Sin embargo, las cifras muestran que en carreras relacionadas específicamente a la ciberseguridad, solo el 10% son cupos femeninos, lo que se condice con el 15% de participación de mujeres en los puestos laborales de ciberseguridad que existen en el país.

Se necesita comprender la oferta amplia de empleos que implica la ciberseguridad, desde habilidades técnicas como la instalación de cable de fibra óptica, peritaje forense, pasando por el diseño UX que será clave para prevenir ataques y abogados que puedan otorgar una mirada legal y de derecho, a los propios analistas de riesgos de ciberseguridad; y, desde allí, fomentar programas estatales como industriales para fomentar un círculo virtuoso.

Oportunidades:
- La empleabilidad de mujeres en ciberseguridad es una forma concreta de fortalecer su desarrollo económico.
- En los últimos años distintos espacios de mujeres en ciberseguridad han florecido, los que ayudan a establecer una conversación entre las propias profesionales de la industria sobre sus necesidades.
- Es necesario crear estudios cuantitativos y cualitativos que identifiquen las barreras sociotécnicas de la incorporación de mujeres a la industria local y trabajar en una mesa técnica de múltiples partes interesadas que desarrolle un plan de acción que permita, a través de compromisos público-privados, aumentar progresivamente el ingreso y desarrollo de mujeres en ciberseguridad.