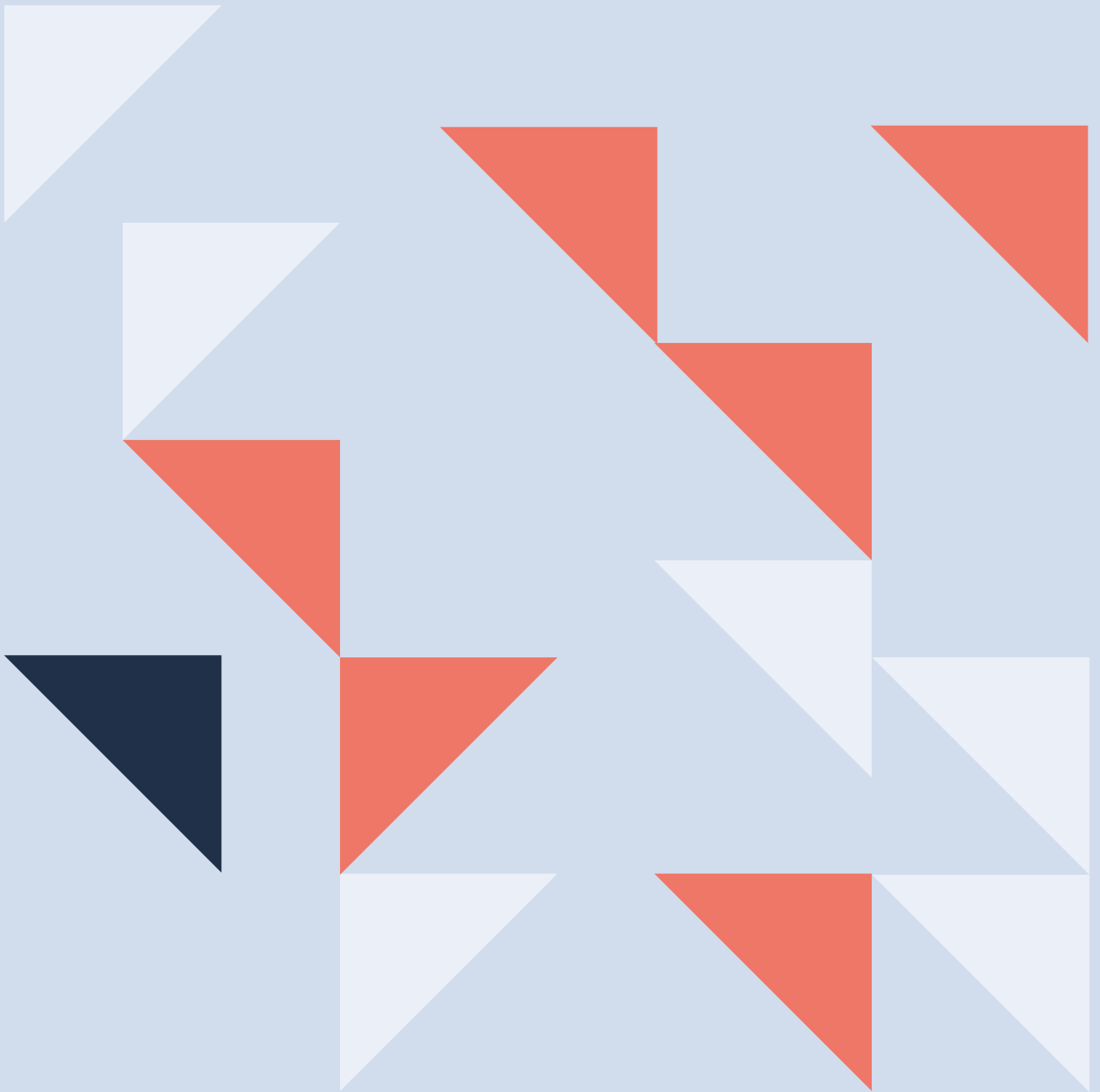


Promoción de cibernormas inclusivas: un estudio de caso de Derechos Digitales





En julio, GPD publicó la Guía para Cibernormas Inclusivas, un nuevo recurso pionero cuyo objetivo es apoyar y capacitar a personas que se encargan de la formulación de políticas y a otras partes interesadas para garantizar un enfoque plenamente inclusivo en el desarrollo e implementación de cibernormas.

Para ubicar y dar vida a las lecciones y principios clave establecidos en la Guía, se encargó a tres organizaciones de la sociedad civil que trabajan en América Latina (Derechos Digitales (América Latina), R3D (México) y Fundación Karisma (Colombia)) que escribieran estudios de caso, en los que describieran sus experiencias de defensa de la ciberseguridad y los derechos humanos.


A continuación se presenta el primer estudio de caso, realizado por Derechos Digitales, sobre Chile.

Antecedentes y contexto

En 2017, el Gobierno de la Presidenta Bachelet elaboró la primera Política Nacional de Ciberseguridad 2017–2022 (PNCS), en la que se establecieron las directrices del Estado de Chile para la salvaguardia de la seguridad de las personas y sus derechos en el ciberespacio. En 2018, el Presidente Piñera reafirmó la PNCS como política de Estado, lo que permitió avanzar en su implementación. Ese mismo año se presentó el proyecto de Ley Marco de Ciberseguridad e Infraestructuras Críticas como una de las medidas de la Política. La PNCS proporcionó una hoja de ruta para avanzar en la implementación de las normas acordadas internacionalmente con miras a garantizar un ciberespacio seguro para todas las personas, incluido el comportamiento responsable del Estado y la protección de las infraestructuras.

En agosto de 2022, el Gobierno anunció que elaboraría una nueva política nacional (2023–2028) para sustituir a la PNCS. Se anunció como una forma de proporcionar medidas más concretas para hacer frente a las amenazas y vulnerabilidades, que vendría a su vez acompañada de una nueva institución dedicada específicamente a la gestión de la ciberseguridad en el país, creada en la Ley Marco.

¿Qué objetivo tenía su organización al involucrarse en este proceso?



En el proceso de elaboración de la PNCS 2017–2022 hubo un notable nivel de apertura, transparencia y participación inclusiva, que incluyeron, en parte, a Derechos Digitales. Cuando se planteó la elaboración de una nueva política nacional, se esperaba no solo una participación similar, sino también una mayor inclusión. No obstante, pasado 2022 no había ningún proyecto de nueva política que sustituyera a la PNCS 2017–2022 ni que continuara su labor. Si bien, el proyecto de Ley Marco avanzaba en el Congreso, no fue hasta mediados de 2022 cuando se anunció la nueva política nacional, junto a una evaluación del desempeño de la política anterior (la PNCS 2017–2022).

Ante esta falta de información, Derechos Digitales y otros grupos **expresaron su preocupación** por el proceso de elaboración de la nueva política nacional: ¿Cómo se aplicarían sustancialmente las cibernormas internacionales? ¿Hasta qué punto sería diferente la participación en comparación con el **proceso anterior**, y cómo se impulsarían las consideraciones de género y de derechos humanos en el nuevo borrador? Estas eran las prioridades básicas que teníamos al inicio del proceso.



¿Qué ha sucedido (hasta la fecha)?

Las organizaciones de la sociedad civil, del mundo académico, de la comunidad técnica y del sector privado recibieron invitaciones para participar en audiencias públicas con el Comité Interministerial a principios de 2023 con el fin de aportar contribuciones para la redacción de la política nacional 2023–2028, y contribuir de forma constructiva y crítica al proceso mediante el examen de un documento de trabajo que sentaba las bases de la nueva política. Durante ese periodo supimos que había una evaluación en curso del primer proceso, y que la política nacional para 2023–2028 se redactaría en paralelo a esa evaluación.

El proceso prosiguió sin grandes alardes, pero dando cabida a la participación pública. La Primera Consulta Ciudadana sobre Ciberseguridad 2023 comenzó en marzo y la segunda, en mayo. Estas consultas, en forma de encuestas en línea, nos dieron acceso a una primera versión de la nueva política propuesta. Ambas se organizaron en función de las capacidades individuales y de la comprensión de los temas, en lugar de basarse en el grupo de interesados o en la afiliación institucional. A pesar de ser una encuesta accesible a todo público, la falta de difusión del proceso hizo que no se realizaran grandes esfuerzos de concientización. Así pues, el proceso seguía estando limitado a quienes tenían conocimiento de su existencia.

El esfuerzo por involucrar más explícitamente a las mujeres y las niñas se limitó a la primera consulta pública. Los resultados, **publicados** en abril, se inclinaron en consecuencia hacia los hombres de entornos más privilegiados. Solo el 37,2% de las personas que respondieron se identificaron como mujeres. Aunque este proceso se trata de un esfuerzo valioso, parece que este proceso no llegó a suficientes personas o comunidades para involucrarlas de forma efectiva, lo que podría afectar el resultado de las cuestiones percibidas como menos importantes, como el enfoque de género y la paridad. Tampoco observamos ningún análisis sobre el enfoque de género o la inclusión de niños, niñas y adolescentes, y los resultados no reflejan a los grupos marginados. Asimismo, no se hizo público un análisis comparable de la segunda consulta pública.

La ciudadanía en general conoció por fin el nuevo proyecto de política cuando el Presidente Boric anunció públicamente su finalización a finales de mayo de 2023. La nueva política nacional seguiría así con cinco objetivos básicos en línea con la anterior: el fomento de una infraestructura resiliente, los derechos en línea, una cultura de la ciberseguridad, la coordinación nacional e internacional, y la industria y la investigación en ciberseguridad. El anuncio no estuvo acompañado de una versión pública de la política finalizada ni de la evaluación de la política anterior (la PNCS 2017–2022). Tras el anuncio, gran parte del énfasis del Gobierno se puso en la tramitación del proyecto de Ley Marco.

Si bien reconocemos los pasos dados para mantener la participación pública a través de audiencias públicas, consultas públicas y un énfasis en las consideraciones de género, hubo una participación limitada en general y una falta de claridad sobre las etapas y los plazos de todo el proceso. Está previsto que la nueva política entre en vigor en el cuarto trimestre de 2023.

Recomendaciones

Para la sociedad civil

- **Es esencial mantener relaciones de confianza.** La capacidad de obtener información privilegiada sobre los procesos en curso suele requerir la existencia de vínculos con el personal involucrado, incluidas las personas presentes en iteraciones anteriores de los procesos políticos. Gracias a una buena comunicación y a nuestra franqueza en las conversaciones, pudimos intervenir en el proceso y obtener información relevante.
- **Transmitir las altas expectativas.** Dado que los procesos políticos largos pueden tener menos instancias de participación e inclusión, las autoridades y la población deben estar al tanto de las expectativas, a fin de fomentar el cambio y ayudar a dirigir los procesos hacia los resultados deseados.
- **Involucrar a otras partes interesadas.** Conocer a las diferentes partes interesadas y colaborar con ellas puede ser útil para conocer las preocupaciones comunes y profundizar en los procesos políticos. Para ello, es necesario dedicar tiempo y recursos y desplegar una amplia red para localizar y llegar a las comunidades afectadas que, en un principio, podrían no parecer partes interesadas obvias en la ciberpolítica. También es importante que estos esfuerzos permitan a las distintas partes interesadas relacionarse entre sí y crear sinergias entre ellas.

Para las instancias responsables de la formulación de políticas

- **Dar a conocer ampliamente los procesos,** con plazos e instancias claras para la participación pública. En el caso de Chile, esto ocurrió de manera limitada y el lanzamiento y la publicación de ciertos documentos no tuvo la difusión esperada.
- **Garantizar la inclusión y utilizar un lenguaje accesible** en las interacciones con las distintas partes interesadas con diferentes niveles de experiencia, especialmente con aquellas que tratan el tema por primera vez.
- **Servir de modelo de transparencia publicando las aportaciones de las partes interesadas.** A pesar de que en las consultas públicas para este proceso se hizo especial hincapié en la inclusión, hubiera sido útil publicar los aportes recibidos de las partes interesadas para saber si se llegó suficientemente a distintas comunidades. En el caso de las consultas públicas abiertas, si se refieren a personas y grupos específicos en situación de vulnerabilidad, las estadísticas y conclusiones deben garantizar el anonimato de las personas encuestadas.
- **Colaborar desde el principio, ampliamente y con frecuencia.** Aunque los procesos de implementación de ciberpolíticas y cibernormas parezcan muy técnicos, deben incluir a todas las partes interesadas y no solo a los representantes de las instituciones más comprometidas.