POLÍTICA NACIONAL DE CIBERSEGURIDAD

2023-2028

CICS Comité Interministerial sobre Ciberseguridad

Gobierno de Chile

gob.cl

POLÍTICA NACIONAL DE CIBERSEGURIDAD

2023-2028

CICS Comité Interministerial sobre Ciberseguridad

Gobierno de Chile

gob.cl

POLÍTICA NACIONAL DE CIBERSEGURIDAD

2023-2028

ÍNDICE DE CONTENIDOS

En los últimos diez años, Chile ha logrado posicionarse en varios rankings internacionales sobre competitividad digital, que dan cuenta de un país cuyo proceso de transformación digital se ha acelerado.

En el mismo período, nuestro país comenzó un proceso de planificación para afrontar los riesgos aparejados a la masificación en el uso de tecnologías de información y comunicaciones, el que dio lugar a la Política Nacional de Ciberseguridad para los años 2017 a 2022, la que orientó las acciones en ciberseguridad durante tres gobiernos consecutivos. En materia de ciberseguridad, Chile cuenta con una verdadera política de Estado.

En esta oportunidad, tengo el honor de presentar ante ustedes la nueva Política Nacional de Ciberseguridad para el período 2023-2028. Se trata de un instrumento con un enfoque integral, que da continuidad a los esfuerzos que venimos desarrollando en esta última década para salvaguardar nuestros activos digitales, proteger los derechos de nuestros ciudadanos y fortalecer la resiliencia de nuestras instituciones frente a las crecientes amenazas cibernéticas.

Al igual que la anterior, esta política es producto de la colaboración multisectorial entre el sector público, el sector privado, la academia y la sociedad civil, dado que la ciberseguridad se garantiza de mejor manera a través de un esfuerzo conjunto en el que participe toda nuestra sociedad. La política promueve la colaboración y la coordinación para aprovechar la experiencia de los distintos sectores con el propósito de prevenir riesgos en materia de ciberseguridad.

Para enfrentar los desafíos y las nuevas amenazas a la seguridad de las personas, la nueva Política Nacional de Ciberseguridad fija una hoja de ruta para la acción pública y privada que requiere acciones en el mediano plazo y está compuesta por cinco objetivos estratégicos: contar con una infraestructura resiliente, asegurar la protección de los derechos de las personas, fomentar una cultura de la ciberseguridad, promover la coordinación nacional e internacional y fomentar a la industria y la investigación científica.

Adicionalmente, en esta ocasión se han incorporado cuatro dimensiones transversales cuya finalidad es lograr que los cinco objetivos sean alcanzados con un enfoque de protección y promoción de los derechos de las personas y sus familias en Internet. La actual política incorporó dimensiones de equidad de género; protección de niños, niñas y adolescentes; protección al adulto mayor; y, protección del medio ambiente.

> ***Con esta nueva Política Nacional de Ciberseguridad esperamos avanzar a pasos firmes en la construcción de un espacio digital seguro para todas y todos.***

Para la implementación de la política se establece un plan de acción compuesto por un conjunto de medidas de corto plazo, cubriendo un periodo de dos años en lugar de cinco, como hacía la política anterior, lo que permitirá revisar el avance, evaluar la necesidad de mejoras y enmendar aquellas acciones que hayan sido implementadas de manera deficiente. Por lo anterior, el plan de acción será publicado de forma separada a la Política.

Con esta nueva Política Nacional de Ciberseguridad esperamos avanzar a pasos firmes en la construcción de un espacio digital seguro para todas y todos.

Gabriel Boric Font
Presidente de la República de Chile

A días de publicarse en el Diario Oficial la Política Nacional de Ciberseguridad 2023 -2028, que establece los objetivos estratégicos del Estado de Chile en esta materia para los próximos años, el Congreso Nacional despachó, de manera unánime, el proyecto de ley marco sobre ciberseguridad que crea la Agencia Nacional de Ciberseguridad. Así, Chile pasa a ser el primer país de América Latina y El Caribe en contar con una ley general y con una institucionalidad pública nacional de la ciberseguridad, que ayude a incrementar los niveles de madurez en este ámbito tan esencial de la vida de las personas.

La seguridad digital también se ha transformado en un desafío para el gobierno, la sociedad, las empresas y, también, para las personas. Se han incrementado considerablemente —tanto en número como en sofisticación— los incidentes y ciberataques que han afectado tanto a organizaciones del sector público como privado, e incluso, a particulares.

Por ello, contar con un nuevo instrumento de planificación política de la ciberseguridad es clave para nuestro país y ahora nos toca como sociedad avanzar en su correcta implementación, como una política de Estado, tal como nos comprometimos en el Programa de Gobierno. Así ocurrió en el segundo gobierno de la presidenta Michelle Bachelet, donde se estableció la primera política en materia de ciberseguridad, cuya implementación se mantuvo durante el gobierno del presidente Sebastián Piñera, incluyendo la presentación del proyecto de ley marco sobre ciberseguridad.

Hemos asumido como un desafío prioritario del gobierno del presidente Gabriel Boric Font, la seguridad digital, poniendo un fuerte énfasis en mejorar nuestra infraestructura tecnológica y en promover la protección de los derechos de las personas en el ciberespacio.

Para ello, con la creación de la Agencia Nacional de Ciberseguridad podremos enfocar los esfuerzos en proteger el normal funcionamiento en áreas tan sensibles como el sector eléctrico, el transporte o las telecomunicaciones, donde los efectos de un ciberataque pueden afectar a las personas en su vida cotidiana.

Porque estamos convencidos que cuando adoptamos medidas para proteger la seguridad digital no sólo estamos protegiendo computadores. Estamos protegiendo a las personas y a la sociedad en su conjunto. Como muchos y muchas han sostenido, la ciberseguridad dejó de ser una cuestión técnica y se transformó en un deber del Estado, que incluso nos permite enfrentar de mejor manera la criminalidad organizada trasnacional.

Porque estamos convencidos que cuando adoptamos medidas para proteger la seguridad digital no sólo estamos protegiendo computadores. Estamos protegiendo a las personas y a la sociedad en su conjunto.

Contar tanto con esta nueva Política Nacional de Ciberseguridad, como con la recientemente aprobada Ley Marco sobre Ciberseguridad, nos permitirá avanzar de manera mucho más contundente en construir un espacio digital seguro para que las personas pueden ejercer sus derechos y desarrollar sus actividades con normalidad y seguridad.

Manuel Monsalve Benavides
Subsecretario del Interior


01
INTRODUCCIÓN

1.Introducción

Las tecnologías de información y comunicaciones (TIC) juegan un papel fundamental en las actividades diarias y en el bienestar de las personas, en la generación de riqueza para los países, en la provisión de servicios básicos para las sociedades, y en la seguridad y soberanía de las naciones. Tanto la cantidad y variedad de usos que damos a las TIC como el número de personas con acceso han aumentado de forma acelerada en los últimos 20 años, generando nuevas oportunidades de desarrollo social y crecimiento económico. Sin embargo, la tecnología es inherentemente vulnerable. La mayor parte de las TIC no fueron diseñadas pensando en la seguridad de la información, posibilitando que diversos actores sean capaces de dañar a personas y organizaciones a través de estas tecnologías.

En abril de 2017, la entonces presidenta Michelle Bachelet lanzó la primera Política Nacional de Ciberseguridad de Chile, que contenía cinco objetivos de política pública en materia de ciberseguridad, y una serie de 41 medidas a ser implementadas entre los años 2018 y 2022. La Política fue confirmada por el gobierno del presidente Sebastián Piñera, progresando en el diseño de la institucionalidad y el fortalecimiento del marco regulatorio, y permitiendo al país avanzar de manera decidida en los retos que enfrentamos. Los desafíos se han diversificado y complejizado, y el escenario global cambia de forma acelerada, lo que hace necesario robustecer con celeridad las mismas áreas de protección consideradas en la primera política, y generar nuevas capacidades para adaptarnos a circunstancias distintas de las que se previeron hace cinco años.

El gobierno del presidente Gabriel Boric ha continuado con el proceso de implementación de la Política Nacional de Ciberseguridad 2017-2022 y ha impulsado la discusión del proyecto de ley marco sobre ciberseguridad, poniendo especial énfasis en la protección y defensa de los derechos de las personas, la equidad de género, y la profundización de la democracia. Se ha procurado brindar protección a aquellos grupos que se ven mayoritariamente afectados por la violencia digital y los ciberdelitos, teniendo en consideración que las amenazas del ciberespacio no impactan a todos por igual, siendo las principales víctimas las mujeres, niñas, niños, adolescentes, adultos mayores y disidencias sexogenéricas.

Para incrementar nuestro nivel de madurez en ciberseguridad, necesitamos contar con un ciberespacio libre, abierto, seguro y resiliente, tal como fue planteado en la primera Política Nacional de Ciberseguridad, que constituyó una política de Estado y, como tal, debe ser renovada.

La presente Política es el resultado de la participación de numerosos actores del mundo público y privado, que a través de audiencias públicas expresaron sus preocupaciones y visiones sobre los problemas y desafíos que conlleva la vida digital. La sociedad civil tuvo un rol fundamental en su elaboración a través de dos consultas ciudadanas, una previa y otra posterior a su redacción. Para su elaboración se siguieron las recomendaciones de la Unión Internacional de Telecomunicaciones (UIT)[1], se observó la experiencia de países similares y más avanzados, se consultaron diversas publicaciones internacionales[2] y se realizó una evaluación del proceso de implementación de las medidas de la primera Política. Esta segunda política representa tanto una continuación de los esfuerzos de la primera, como una readecuación del foco para los próximos años producto de la revisión de los cambios sucedidos desde entonces.

1.1. ¿Por qué necesitamos una Política Nacional de Ciberseguridad?

El siglo en curso probablemente verá más cambios que toda la historia de la humanidad, tanto en términos culturales como políticos y económicos. El calentamiento global acelera el cambio climático, acentuando climas extremos y aumentando la frecuencia y duración de eventos como sequías, inundaciones, tornados e incendios forestales. La disponibilidad de agua ha disminuido, lo que afecta la agricultura y disminuye nuestra capacidad para generar alimentos[3]. Todos estos cambios ya están afectando a nuestro país, y se espera que se aceleren durante este siglo.

La pandemia de SARS CoV-2 (COVID-19) ha producido, a abril de 2023, poco más de 6,8 millones de muertes en el mundo[4] y más de 52 mil muertes confirmadas en nuestro país[5]. Además del enorme costo social en términos de salud pública, la pandemia aceleró múltiples procesos de transformación digital. La productividad de la mayor parte de las sociedades se ha visto mermada de forma considerable durante varios años, lo que contribuye a una recesión económica en ciernes o declarada en decenas de países. Tal como ocurrió con la epidemia mundial de gripe de 1918, los efectos de la actual pandemia tardarán muchos años en desaparecer.

Finalmente, la inestabilidad política y económica que ha generado la guerra en Europa del Este nos pone en un escenario que no veíamos desde la segunda guerra mundial. Antes del conflicto, Ucrania producía el 10% del trigo, el 15% del maíz y el 13% de la cebada del mundo[6]. La escasez de grano generó durante varios meses aumentos de precios y ha contribuido al aumento de la inflación en muchas economías.

Todo lo anterior es relevante para nuestro país, pero ¿qué relación tiene con la ciberseguridad?

La ciberseguridad no es un fin en sí mismo. La ciberseguridad es una condición que, de existir, permite el uso pleno de Internet y de la web, herramientas habilitadoras y potenciadoras de las actividades humanas. Todos nuestros esfuerzos para enfrentar desafíos como el cambio climático y la pandemia de COVID-19, y para devolver la paz y la estabilidad política y económica al mundo, pueden verse facilitados o entorpecidos por la presencia o ausencia de las herramientas de comunicación provistas a través de las redes y sistemas informáticos.

En diciembre de 2003, la ***World Summit on the Information Society***, formada bajo el auspicio de la Organización de las Naciones Unidas (ONU), publicó una declaración de principios de la Sociedad de la Información luego de largas negociaciones con organizaciones privadas, públicas y representantes de la sociedad civil de todos los países congregados[7]. En el punto 4 de la declaración se afirma que ***"que todo individuo tiene derecho a la libertad de opinión y de expresión, que este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir información y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. La comunicación es un proceso social fundamental, una necesidad humana básica y el fundamento de toda organización social."***[8]. Es la satisfacción de esta necesidad humana básica y derecho humano fundamental la que hacemos posible a través de la ciberseguridad. Todo Estado tiene hoy el deber de generar las condiciones para permitirle a cada persona ejercer este derecho.

Veinte años después, en enero de 2023, el ***World Economic Forum*** publicó un reporte[9] donde presentan una serie de problemas sobre ciberseguridad, desde la perspectiva de expertos y líderes de negocio alrededor del mundo, destacándose los siguientes:

- La inestabilidad geopolítica global ha convencido a líderes y expertos por igual de la importancia de la gestión de los riesgos de ciberseguridad. 91% de los participantes del estudio creen que un incidente catastrófico de ciberseguridad es relativamente probable dentro de los próximos dos años.

- 43% de los líderes piensa que es probable que su organización sea atacada a través del ciberespacio dentro de los próximos dos años.

- Las preocupaciones sobre ciberseguridad y protección de datos personales están crecientemente influyendo en cómo y dónde operan los negocios. El nivel de ciberseguridad que cada país es capaz de mantener está siendo considerado por inversionistas para tomar decisiones sobre dónde invertir.

- La naturaleza de las amenazas en el ciberespacio ha cambiado. Tanto líderes de negocio como expertos en ciberseguridad creen que los atacantes se están concentrando en dañar los procesos de negocio, y en arruinar la reputación de las organizaciones.

Nuestra economía, la mayor parte del comercio internacional, nuestras actividades de ocio, los medios de comunicación masivos, las interacciones sociales y políticas, y la mantención y difusión de nuestra cultura: todas dependen fuertemente del acceso a Internet y a los medios y aplicaciones que posibilita. Es por eso que la primera versión de la Política Nacional de Ciberseguridad (2017-2022) fijó como objetivo para el 2022 el ***contar con un ciberespacio libre, abierto, seguro y resiliente***; por la misma razón, la nueva Política Nacional de Ciberseguridad (2023-2028) perseguirá el mismo objetivo.

1.2. Los desafíos en ciberseguridad en nuestro país

Chile tiene un nivel medio de madurez en ciberseguridad en el escenario internacional. En el Índice Mundial de Ciberseguridad de 2020[10], Chile se encontraba en el lugar 74 a nivel mundial, y en el 7° lugar en América (debajo de Estados Unidos, Canadá, Brasil, México, Uruguay y República Dominicana). En este índice, Chile se destaca por su avance en medidas legales, medidas organizacionales y de cooperación; sin embargo, se queda atrás en las medidas técnicas.

En el Índice Nacional de Ciberseguridad[11], desarrollado por Estonia y actualizado de forma continua, Chile se encuentra, al año 2023, en el lugar 53 entre 175 países, y en el 6° lugar en Latinoamérica y el Caribe, debajo de República Dominicana, Argentina, Paraguay, Perú y Uruguay. En este ránking, que consta de 12 áreas distintas, Chile se destaca en desarrollo de políticas de ciberseguridad; lucha contra el cibercrimen, y operaciones militares; pero se queda atrás en protección de servicios esenciales; protección de servicios digitales, gestión de crisis y protección de datos personales.

Los principales problemas que enfrentamos hoy en materia de ciberseguridad en nuestro país son:

1. **La insuficiente resiliencia de nuestras organizaciones e infraestructura.**
   Brechas de seguridad recientes en el país nos confirman la necesidad de fortalecer la protección de nuestra infraestructura de redes y sistemas; además de mejorar el entrenamiento y formación de los funcionarios públicos, así como de todas las personas en organizaciones que lo requieran. Para esto, es necesario monitorear nuestro ciberespacio de forma efectiva, especialmente la infraestructura de redes del sector público, de los servicios esenciales y los operadores de importancia vital.

2. **La falta de cultura de las organizaciones y de las personas sobre la importancia de la ciberseguridad.**
Esto, junto a la falta de conocimiento, lleva a que tanto las organizaciones como las personas no tomen medidas suficientes de protección en el ciberespacio. El desafío para el Estado es entregar alfabetización básica en ciberseguridad y generar conciencia de su importancia en cada persona, desde la segunda infancia hasta los adultos mayores, tanto en la educación básica y media, como en las organizaciones privadas, el sector público y la sociedad civil. Para abordar este desafío el Estado velará especialmente por los territorios más apartados.

3. **La falta de especialistas en ciberseguridad.**
Se estima que en Chile faltan alrededor de 28.000 especialistas en ciberseguridad para satisfacer las necesidades tanto del sector público como privado, y que en carreras relacionadas específicamente a la ciberseguridad, solo el 10% son cupos femeninos, cifra que se condice con el 15% de participación de mujeres en los puestos laborales de ciberseguridad que existen en el país[12]. La ausencia de mujeres en el mundo laboral y en las carreras relacionadas con computación e informática, tanto en centros de formación técnica como en universidades e institutos profesionales, encuentra su explicación en distintas condiciones sociales que desincentivan su participación, y no en una falta de interés de las mujeres en el área. Es necesario que el Estado genere las condiciones para disminuir estas brechas, incentivando que una mayor cantidad de personas escoja estudiar carreras relacionadas con la ciberseguridad y promoviendo un aumento de la participación femenina en el sector, especialmente considerando que las mujeres representan un 52,4% de la población chilena.

4. **La falta de sofisticación de nuestra demanda por ciberseguridad.**
Se estima que la industria de ciberseguridad en nuestro país realiza ventas anuales por alrededor de $350 millones de dólares, lo que representa un 0.11% del PIB de Chile[13]. La ciberseguridad es un área económica intensiva en capacidades, que a futuro podría representar una parte creciente de nuestro producto interno bruto, ayudar a posicionar a nuestro país en el escenario latinoamericano, e incluso fortalecer la confianza en nuestra economía, vista desde el exterior. Sin embargo, para que esto suceda, es necesario tener una demanda más amplia y sofisticada.

5. **El aumento de delitos en el ciberespacio.**
De acuerdo con la encuesta nacional urbana de seguridad ciudadana, durante los últimos años la tasa de denuncia de los delitos informáticos se ha incrementado progresivamente desde un 6,6% en 2017 a un 10,1% en 2021[14]. Este tipo de delitos pone en riesgo la seguridad y la confianza de las personas en el ciberespacio y es un fenómeno que debe abordarse desde una perspectiva preventiva y sancionatoria.

Nuestro país se ve afectado sin ninguna duda por las tendencias globales, pero además tiene problemas específicos. Hay grupos de atacantes que han estado muy activos en Latinoamérica y se han autoproclamado responsables de grandes filtraciones de datos que ocurrieron en 2022 y 2023. La cantidad de incidentes que se registran en la Red de Conectividad del Estado (la red de datos que presta conectividad a una parte importante del sector público) confirma que una de las preocupaciones fundamentales de los próximos meses debe ser el fortalecimiento de la infraestructura pública, así como la formación y entrenamiento del personal público, además de un robustecimiento de los servicios esenciales y operadores de importancia vital.

1.3. Los cinco objetivos de la Política Nacional de Ciberseguridad

Para enfrentar los problemas y los desafíos anteriores, la nueva Política Nacional de Ciberseguridad contiene cinco objetivos fundamentales:

1. **Infraestructura resiliente:**
   El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad y de desastres socioambientales, bajo una perspectiva de gestión de riesgos.

2. **Derechos de las personas:**
   El Estado protegerá y promoverá la protección de los derechos de las personas en Internet, a través del fortalecimiento de la institucionalidad existente en materia de ciberseguridad; y de la generación, adopción, y promoción de los mecanismos y las herramientas tecnológicas necesarias para que cada persona pueda integrarse a la sociedad y desarrollarse y expresarse plenamente.

3. **Cultura de ciberseguridad:**
   Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas, responsabilidad en el manejo de tecnologías digitales, y promoción y garantía de los derechos de las personas.

4. **Coordinación nacional e internacional:**
   El Estado creará una gobernanza pública para coordinar las acciones necesarias en ciberseguridad. Los organismos públicos y privados crearán, en conjunto, instancias de cooperación con el propósito de comunicar y difundir sus actividades en ciberseguridad, evitar la duplicación de trabajo y pérdida de recursos, y hacer eficientes los esfuerzos en esta área.
   En el ámbito internacional, el Estado se coordinará con países, organismos, instituciones y otros actores internacionales para permitir a nuestro país enfrentar de mejor manera las actividades maliciosas e incidentes en el ciberespacio.

5. **Fomento a la industria y la investigación científica:**
   El país promoverá el desarrollo de una industria de la ciberseguridad, que proteja a las personas y las organizaciones y que sirva a sus objetivos estratégicos. Para ello, fomentará la focalización de la investigación científica aplicada en temas de ciberseguridad, acorde a las necesidades del país.

La elección de los objetivos anteriores no es aleatoria: es posible establecer una relación entre ellos y las dimensiones definidas en al menos dos modelos internacionales en ciberseguridad[15].

Adicionalmente, la política incluye algunas dimensiones transversales con las que se busca proteger y promover la protección de los derechos de las personas y sus familias en Internet:

1. **Equidad de género:**
   Todas las iniciativas considerarán de manera preferente a las mujeres, tanto para aumentar su seguridad en el entorno digital, al ser ellas las principales víctimas de violencia digital, como para mejorar su inclusión, mediante acciones positivas dirigidas a corregir las inequidades existentes en nuestra sociedad. Ello, pues a pesar de representar a más del 50% de la población chilena, su participación en los puestos laborales de ciberseguridad que existen en el país apenas alcanza el 15%.

2. **Protección a la infancia:**
   Todas las iniciativas deben considerar protección preferente a niñas, niños y adolescentes.

3. **Protección al adulto mayor:**
   Todas las iniciativas deben considerar protección preferente a adultos mayores.

4. **Protección del medio ambiente:**
   Todas las iniciativas deben minimizar su impacto negativo sobre el medio ambiente.

A diferencia de la versión anterior de la Política, el Plan de Acción se publicará de forma separada pues contiene medidas que se implementarán a corto plazo, mientras que la Política es un instrumento de largo plazo. El propósito es permitir revisar el avance, proponer cambios y mejoras, y enmendar oportunamente el rumbo en caso necesario durante la implementación de la Política en vez de sólo al final de su vigencia. Cada medida tendrá una institución responsable de conducir los esfuerzos para lograr su implementación, y reportará al Comité Interministerial sobre Ciberseguridad de forma periódica los avances observados o la falta de ellos. Cada medida estará asociada a resultados claros y medibles, y a plazos de consecución.

El Comité Interministerial sobre Ciberseguridad sugerirá alternativas de seguimiento e implementación de la Política, y, asesorará el cumplimiento de sus medidas para conseguir los objetivos de política pública contenidos en este documento.

El gobierno podrá utilizar una serie amplia de medidas políticas, económicas, estratégicas y sociales para lograr la implementación de las medidas, y para generar las condiciones para hacer surgir un ecosistema de ciberseguridad en el país, en conformidad con las políticas delineadas en este documento.

El Estado incentivará progresivamente la investigación y desarrollo aplicados en ciberseguridad, y estimulará la inversión privada en el área, en conjunto con las instituciones de educación superior y centros de investigación nacionales. La investigación científica aplicada es un deber ineludible y necesario del Estado, para generar conocimiento que permita aumentar la eficiencia de los factoresproductivos, generar valor agregado sobre la mera extracción de materias primas, y proveer servicios que le entreguen al país ventajas en el contexto comercial internacional. La investigación en ciberseguridad es una condición necesaria para generar un ecosistema de ciberseguridad en nuestro país, y para cumplir con los objetivos de política pública contenidos en este documento.

1.4. Relación con otros objetivos nacionales

- **Política de ciberdefensa**

Nuestro país tiene una Política de Ciberdefensa vigente, publicada en marzo de 2018, aprobada mediante el decreto supremo N° 3, de 2017, del Ministerio de Defensa Nacional. En ella, se establecen dos prioridades:

1. **La cooperación internacional:**
   Chile colaborará con otros países y promoverá medidas de transparencia y confianza en instancias como la ONU, la OEA, UNASUR, y otros, en coordinación con el Ministerio de Relaciones Exteriores.

2. **El desarrollo de capacidades:**
   El sector de la Defensa Nacional desarrollará líneas de carrera en cada rama de las Fuerzas Armadas. Para ello, creará un Comando Conjunto de Ciberdefensa y un Centro de Respuesta a Incidentes de Seguridad Informática de Defensa (CSIRT de la Defensa Nacional).

Es importante mencionar que la ciberdefensa es fundamental para el cumplimiento de los objetivos nacionales de ciberseguridad, por lo que se debe propender a fortalecer las capacidades del país para enfrentar las ciberamenazas que puedan atentar contra la seguridad del país y poner en riesgo la soberanía nacional.

Adicionalmente, la Política de Ciberdefensa establece un principio de equivalencia: Chile podrá considerar ciberataques masivos sobre sus habitantes, su infraestructura o sus intereses como un ataque armado, en el contexto del Artículo 51 de la Carta de las Naciones Unidas. Este principio pone la infraestructura de comunicaciones de Internet al mismo nivel que la infraestructura considerada estratégica y vital para el país, como la red de transporte y la red de centros de salud, entre otros. La presente Política está en armonía con la Política de Ciberdefensa, y especifica objetivos de política pública que están en plena concordancia con los objetivos y prioridades de ese instrumento de planificación, particularmente en lo que respecta al objetivo de Coordinación Nacional e Internacional.

De igual forma, el sector de la Defensa Nacional realizará la reorganización orgánica que sea necesaria para el cumplimiento de sus funciones en el ciberespacio.

• Política Nacional de Inteligencia Artificial

Nuestro país posee también una Política Nacional de Inteligencia Artificial, publicada en diciembre de 2021 aprobada mediante el decreto supremo N°20, de 2021, del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación. En ella, se establecen cuatro principios transversales: Inteligencia Artificial (o IA) centrada en el bienestar de las personas, IA para el desarrollo sostenible, IA inclusiva, e IA globalizada y en evolución. En la Política se establecen además tres ejes:

1. **Factores habilitantes,** como el desarrollo de talentos, la infraestructura tecnológica y la promoción y fomento del uso masivo de datos para la toma de decisiones.

2. **Desarrollo y adopción,** donde se incluyen la investigación básica y aplicada, la transferencia tecnológica, innovación, emprendimiento, mejoramiento de servicios públicos, y desarrollo económico basado en tecnología, entre otros.

3. **Ética, aspectos normativos y efectos socioeconómicos,** donde se considera un conjunto amplio y heterogéneo de tópicos y áreas de discusión y reflexión, entre los cuales se encuentra: ciberseguridad, ciberdefensa, género, etc.

La presente política está en plena concordancia con los objetivos y ejes planteados en la Política Nacional de Inteligencia Artificial, particularmente en el primer eje sobre la formación y desarrollo de talentos, y la capacitación y concientización de las personas; lo planteado en el segundo eje sobre investigación aplicada, transferencia tecnológica, emprendimiento y mejora de los servicios públicos; y respecto al tercero, en referencia a la promoción de sistemas tecnológicos seguros y robustecimiento de la institucionalidad en ciberseguridad.

• Política Nacional contra el Crimen Organizado

Finalmente, nuestro país cuenta con una Política Nacional contra el Crimen Organizado, aprobada mediante decreto supremo N° 369, de 2022, del Ministerio del Interior y Seguridad Pública, con el propósito de disminuir la actividad delictiva de las organizaciones criminales que operan en Chile, a través de la acción planificada y coordinada de las instituciones del Estado. Esta política tiene tres objetivos fundamentales: desarticular bandas y organizaciones criminales, implementar medidas específicas para controlar diversos delitos y fortalecer la coordinación interinstitucional a través de la consolidación de un ecosistema de seguridad pública. El segundo de los objetivos anteriores menciona explícitamente el cibercrimen como una de las formas de delito a combatir.

Dentro de las medidas propuestas por la Política anterior está la elaboración de una nueva Política Nacional de Ciberseguridad para el período 2023-2028, la tramitación de un proyecto de ley marco sobre Ciberseguridad e Infraestructura Crítica, y desarrollar estrategias de prevención y educación digital.

La presente Política está en plena concordancia con la Política Nacional contra el Crimen Organizado, específicamente en lo que se refiere a la prevención de la comisión de delitos informáticos, a la generación de una cultura de ciberseguridad en nuestro país, y a la coordinación entre instituciones de gobierno e instituciones privadas. Una de las motivaciones de esta coordinación es el intercambio de información y la colaboración para evitar y combatir de mejor forma el cibercrimen.

POLÍTICA NACIONAL DE CIBERSEGURIDAD

2023-2028


02
OBJETIVOS

2. Objetivos de la Política Nacional de Ciberseguridad 2023-2028

2.1. Infraestructura resiliente

El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad y de desastres socioambientales, bajo una perspectiva de gestión de riesgos. Para ello, es necesario avanzar en el fortalecimiento de los elementos técnicos físicos y lógicos de nuestro ciberespacio, incluida nuestra creciente red de dispositivos conectados a Internet (Internet de las Cosas).

Para avanzar en este objetivo, es necesario:

1. Impulsar la tramitación del proyecto de ley marco sobre ciberseguridad e infraestructura crítica de la información, que crea la Agencia Nacional de Ciberseguridad, que opere como el órgano rector de la ciberseguridad en Chile, con facultades normativas, fiscalizadoras y sancionatorias, que ayude a incrementar el nivel de madurez institucional en ciberseguridad, tanto en el sector público como privado.

2. Crear el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional), para atender las necesidades y requerimientos de protección y recuperación ante incidentes en el sector público y privado que afecten a organismos considerados de importancia vital.

3. Fortalecer la resiliencia de nuestros servicios esenciales frente a incidentes de ciberseguridad. Las instituciones públicas y privadas que operen servicios considerados vitales deben mejorar su nivel de madurez en ciberseguridad y su capacidad de sobreponerse a brechas y ataques. El Estado entregará recomendaciones y lineamientos básicos que permita a las instituciones protegerse frente a los ataques más frecuentes o de mayor impacto.

4. Robustecer la resiliencia física de la red en Chile. El Estado, conforme a lo dispuesto en los cuerpos legales y reglamentarios pertinentes, promoverá en coordinación con el sector privado la priorización de la conexión de lugares previamente no conectados, o donde no exista redundancia de conexiones con al menos otros dos lugares.

5. Fortalecer el análisis de la información de red en el ciberespacio nacional, a través de la inversión en investigación científica aplicada en conjunto con el sector académico y la industria nacional, para colocar a Chile a la vanguardia en Latinoamérica en la generación de conocimiento y desarrollo de tecnología en ciberseguridad.

2.2. Derechos de las personas

El Estado resguardará y promoverá la protección de los derechos de las personas en Internet, a través del fortalecimiento de la institucionalidad pública en materia de ciberseguridad; y de la generación, adopción, y promoción de los mecanismos y las herramientas tecnológicas suficientes para que cada persona pueda integrarse a la sociedad y desarrollarse y expresarse plenamente, otorgando especial protección a mujeres, niñas, niños, adolescentes, adultos mayores y disidencias sexogenéricas. Todas las personas deberían poder hacer uso de Internet para comunicarse, trabajar, estudiar, y desarrollarse en lo personal, familiar y social en un entorno de equidad, inclusión, justicia y protección a la diversidad.

Para avanzar en este objetivo, es necesario:

1. Fortalecer el marco normativo sobre ciberseguridad y protección de datos personales, a través de la aprobación e implementación de la ley marco de ciberseguridad y la ley sobre protección de datos personales.

2. Generar instancias de capacitación para todos los funcionarios públicos en hábitos y medidas básicas de seguridad digital, que les permitan proteger la información de ciudadanos y ciudadanas que les es confiada y que administran a través de redes y sistemas computacionales.

3. Prevenir la comisión de delitos informáticos, con énfasis en aquellos que afectan a mujeres, niñas, niños y adolescentes, adultos mayores y disidencias sexogenéricas, debido a su mayor vulnerabilidad en el ciberespacio.

4. Identificar y corregir inequidades en el acceso y uso del ciberespacio producidas por la falta de conocimiento de seguridad digital en personas y grupos sociales en situaciones de mayor vulnerabilidad frente a incidentes.

2.3. Cultura de Ciberseguridad

Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas, responsabilidad en el manejo de tecnologías digitales, y promoción y garantía de los derechos de las personas. La protección de la sociedad va en directa relación con la capacidad que tenga cada persona de protegerse. Se requiere generar nociones y prácticas de ciberhigiene en la población, de forma que cada uno sea capaz de cuidar por sí mismo su identidad digital y su información.

Para avanzar en este objetivo, es necesario:

1. Diseñar e implementar un plan de concientización nacional sobre ciberseguridad y privacidad, para que todas las personas que usen un computador o teléfono inteligente, independientemente de la región del país en que se encuentren, adquieran nociones y prácticas de ciberhigiene. Este programa se enfocará especialmente en mujeres, niñas, niños, adolescentes, adultos mayores y disidencias sexogenéricas, así como en personas que vivan fuera de la Región Metropolitana y en otros grupos que podrían estar en desventaja frente al resto de la sociedad en términos de conocimiento sobre ciberseguridad; y en micro y pequeñas empresas.

2. Generar e implementar un plan matriz de introducción y mejora de la educación en ciberhigiene y ciberseguridad para el sistema de enseñanza básica, media científico-humanista y media técnico-profesional. En particular, este plan considerará evaluar la generación de especialidades para la educación media técnico-profesional y la incorporación de materias de ciberhigiene y ciberseguridad a especialidades afines a lo largo del país.

3. Fomentar una cultura de evaluación y gestión del riesgo, tanto en organizaciones públicas como privadas, que nos permita prepararnos frente a incidentes y desastres que puedan afectar gravemente a las personas de nuestro país, su bienestar, su salud, sus derechos, su identidad, sus bienes o la posibilidad de desarrollarse plenamente a través de Internet.

4. Promover la investigación científica aplicada en ciberseguridad para resolver problemas que nuestro país enfrentará en los próximos años debido al uso e implementación intensiva de tecnologías con aplicaciones insospechadas. Nuestro país no puede ser simplemente un consumidor pasivo de tecnologías desarrolladas en el exterior. Es responsabilidad del Estado generar las condiciones para resolver problemas técnicos complejos que requieran de investigación científica y que surjan de las necesidades y requerimientos de protección de nuestras personas y organizaciones.

2.4. Coordinación nacional e internacional

Para aprovechar de manera eficiente y eficaz los recursos disponibles, resulta indispensable la acción coordinada e intencionada hacia la consecución de los objetivos de política pública. Los organismos públicos y privados promoverán instancias de cooperación con el resto del sector público y de la industria, y con la futura autoridad nacional de ciberseguridad, con especial énfasis en la comunicación y difusión de los esfuerzos que se realicen en ciberseguridad, a fin de evitar la duplicación de trabajo y la pérdida de recursos. En el ámbito internacional, el Estado se coordinará y trabajará con países, organismos, instituciones y otros actores internacionales, para permitir a nuestro país enfrentar de mejor manera las actividades maliciosas e incidentes en el ciberespacio, y contribuir de esa forma a fortalecer su liderazgo regional en ciberseguridad.

Para avanzar en este objetivo, es necesario:

1. Generar instancias de colaboración y cooperación entre organizaciones públicas y privadas en diversos ámbitos, como educación, infraestructura, protección de derechos, fomento a la industria, y otras áreas relacionadas con la ciberseguridad que puedan ser de interés del país, con el propósito de dar a conocer las iniciativas en desarrollo y coordinarlas adecuadamente.

2. Establecer relaciones de cooperación con instituciones de ciberseguridad de países avanzados en el área para aprender sobre sus experiencias y traer experiencia relevante a la implementación de iniciativas o proyectos en ciberseguridad. Para ello, se desarrollará una estrategia de cooperación internacional mediante la cual se establezcan prioridades y líneas de acción específicas.

3. Aumentar la participación en instancias multilaterales, particularmente en el ámbito de las Naciones Unidas y la Organización de los Estados Americanos, como también en iniciativas de múltiples partes interesadas. De la misma forma, se potenciará el trabajo y colaboración en el marco del Convenio de Budapest.

4. Promover activamente la ciberdiplomacia, incentivando a nivel regional y global la discusión respecto a la aplicación de normas, derecho internacional, y medidas de fomento de la confianza en el ciberespacio, y el desarrollo de acuerdos bilaterales que refuercen la cooperación en ciberseguridad, y el respeto de los derechos humanos en el ciberespacio.

5. Coordinar la política internacional en materia de ciberseguridad. El Ministerio de Relaciones Exteriores será responsable de esta coordinación con el resto de los ministerios y agencias de gobierno.

2.5. Fomento de la industria y la investigación científica

El país promoverá el desarrollo de una industria de la ciberseguridad, que proteja a las personas y las organizaciones y que sirva a sus objetivos estratégicos. Este fomento se implementará a través de estímulos y fondos dirigidos a la oferta de servicios y productos en ciberseguridad, pero también a través de la generación de una demanda más sofisticada en ciberseguridad, de forma que nuestra industria pueda proteger de mejor forma a las personas y organizaciones, y servir mejor a los intereses del país.

Para avanzar en este objetivo, es necesario:

1. Focalizar la investigación aplicada respecto a aquellos problemas y necesidades en ciberseguridad tanto del sector público como privado. Para ello, se promoverá la creación de institutos de investigación científica aplicada y transferencia tecnológica en la materia, con

la finalidad de que potencien la ciberseguridad como un área preferente por parte del sector académico nacional, y que conecten las necesidades de las organizaciones y el sector público con el conocimiento científico existente.

2. Generar incentivos para el emprendimiento tecnológico en ciberseguridad, impulsado por las necesidades de las organizaciones privadas y públicas de nuestro país, particularmente por los Centros de Respuesta a Incidentes de Seguridad Informática (CSIRTs), al alero de grupos de investigación en universidades y centros de investigación. Estos incentivos no se restringirán al ámbito económico, serán amplios y se enfocarán especialmente en las regiones del país distintas de la Región Metropolitana.

3. Revisar los mecanismos de contratación de servicios de ciberseguridad por parte del Estado, para hacerlos más eficientes y expeditos, dando preferencia a la contratación de servicios de ciberseguridad ofrecidos por la industria local.

4. Promocionar los productos y servicios de las empresas locales en ciberseguridad a nivel nacional y en el extranjero, a través de fondos públicos y alianzas público-privadas, y generar incentivos económicos y tributarios para que las empresas existentes puedan ampliar su oferta de servicios en ciberseguridad y ofrecerla de forma preferente al Estado.

5. Fomentar la integración e inclusión de una transversalización de género en el desarrollo del ecosistema de ciberseguridad en nuestro país, generando medidas de acción positiva que permitan aumentar el número de mujeres en roles gerenciales y técnicos en ciberseguridad.

POLÍTICA NACIONAL DE CIBERSEGURIDAD

2023-2028


03
CONCLUSIONES

3. Gobernanza del país en ciberseguridad

3.1. Marco normativo

Nuestro país cuenta con un amplio conjunto de normas legales y reglamentarias que se relacionan directa o indirectamente con la ciberseguridad. Dentro de éstas destacan a nivel nacional nuestra propia Constitución Política de la República (artículos 8°, 19, 24, 39 y siguientes) y leyes como la ley N° 20.285, sobre acceso a la información pública; la ley N° 19.628, sobre protección de la vida privada; la ley N° 21.180, sobre transformación digital del Estado; la ley N° 21.113, que declara el mes de octubre como el mes nacional de la ciberseguridad; la ley N° 21.459, 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; la ley N° 21.521, que promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros, también denominada "ley FINTECH"; la ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma; la ley N° 19.974, sobre el Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia; la ley N° 18.168, ley general de telecomunicaciones; entre otras.

Adicionalmente, es posible destacar las siguientes normas: decreto supremo N° 83 del 2004, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos; decreto supremo N° 1.299 del 2004, del Ministerio del Interior y Seguridad Pública, que establece nuevas normas que regulan la Red de Conectividad del Estado que administra el Ministerio del Interior y fija los procedimientos, requisitos y estándares tecnológicos para la incorporación a dicha red de instituciones públicas; decreto supremo N° 1 del 2015, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica sobre sistemas y sitios web de los órganos de la administración del Estado; decreto supremo N° 533 del 2015, que crea el Comité Interministerial sobre Ciberseguridad, y su modificación mediante decreto supremo N° 579 del 2020, ambos del Ministerio del Interior y Seguridad Pública; decreto supremo N° 273 del 2022, del Ministerio del Interior y Seguridad Pública, que establece obligación de reportar incidentes de ciberseguridad; decreto supremo N° 14 del 2014, del Ministerio de Economía, Fomento y Turismo, que modifica el decreto supremo N° 181 del 2002, que aprueba el reglamento de la ley N° 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica; decreto supremo N° 24 del 2019, del Ministerio de Economía, Fomento y Turismo, que aprueba norma técnica para la prestación del servicio de certificación de firma electrónica avanzada; etc.

A su vez, existen normas sectoriales como la resolución exenta N° 1381, de 10 de agosto de 2020, de la Subsecretaría de Telecomunicaciones, que aprueba norma técnica sobre fundamentos generales de ciberseguridad para el diseño, instalación y operación de redes y sistemas utilizados para la prestación de servicios de telecomunicaciones; la resolución exenta N° 785, de 03 de noviembre de 2021, de la Subsecretaría de Redes Asistenciales que aprueba un Instructivo de seguridad de la información y ciberseguridad para el sector salud; de la Superintendencia de Casinos y Juegos cuya circular N°119, de abril de 2022, imparte instrucciones relativas a los lineamientos de ciberseguridad que deben observar las sociedades operadoras y las sociedades concesionarias de casinos de juego; de la Superintendencia de Pensiones que establece un Modelo de Gestión de Seguridad de la Información y Ciberseguridad; la norma de carácter general N° 454, de fecha 18 de mayo de 2021, de la Comisión para el Mercado Financiero que imparte instrucciones en materia de gestión de Riesgo Operacional y Ciberseguridad, así como de la realización periódica de autoevaluaciones en ambas materias en entidades aseguradoras y reaseguradoras; la directiva N°32, de fecha 05 de diciembre de 2018, de ChileCompra, que aprueba Recomendaciones para la contratación de servicios en la nube; entre otras.

Por último, a nivel internacional, se puede mencionar el Convenio sobre la Ciberdelincuencia, promulgado a través del decreto supremo N° 83 del Ministerio de Relaciones Exteriores, de 27 de abril del 2017, y la serie de normas ISO/IEC 27000 que han sido publicadas por el Instituto Nacional de Normalización (INN).

3.2. Institucionalidad actual y futura

La institucionalidad vigente en materia de ciberseguridad se encuentra distribuida en diversos organismos y entidades. Esto hace necesaria la coordinación estratégica de los distintos esfuerzos, de sus roles y funciones, y el establecimiento de prácticas y criterios técnicos comunes, con el objetivo de mejorar la eficiencia y eficacia en el ámbito de la ciberseguridad.

Es de público conocimiento que durante los últimos años nuestro país se ha visto afectado por una serie de incidentes y ataques de ciberseguridad. Esto, sumado a una dispersión normativa e institucional, ha generado la necesidad y urgencia de legislar al respecto. Así, con el reconocimiento de la ciberseguridad como un medio transversal para la protección de las personas, sus derechos, patrimonio y seguridad individual, el gobierno del presidente Gabriel Boric ha impulsado el Proyecto de Ley Marco sobre Ciberseguridad (Boletín N° 14.847-06), ingresado en el gobierno del presidente Sebastián Piñera.

Dicho proyecto ofrece una respuesta integral a los problemas y desafíos que la ciberseguridad impone, acorde al proceso de transformación digital en que se encuentra inmerso nuestro país, teniendo como ámbito de aplicación a todo el sector público y privado, con obligaciones de ciberseguridad diferenciadas por riesgos y tamaño. Reflejo de aquello es la obligación de determinar los servicios esenciales e identificar a los operadores de importancia vital. En cuanto a la institucionalidad, crea la Agencia Nacional de Ciberseguridad, el Consejo Multisectorial sobre Ciberseguridad, un CSIRT Nacional y el CSIRT de la Defensa Nacional, velando por su coordinación con otros CSIRT Sectoriales que se pudieran originar.

Finalmente, el proyecto de ley propone establecer obligaciones específicas en materia de ciberseguridad para el sector público y el sector privado, incorporando la dimensión de la educación, capacitación, buenas prácticas y ciberhigiene. Además, siguiendo las mejores y más actuales prácticas internacionales, busca fomentar la investigación de vulnerabilidades otorgando protección legal al hacking ético, y promover la notificación de incidentes de ciberseguridad. De aprobarse el proyecto de ley, Chile contará con un marco normativo y una autoridad nacional de ciberseguridad de vanguardia en la región y en el mundo.

Notas al pie

1. Guide to Developing a National Cybersecurity Strategy, 2nd edition 2021.

2. Como las guías y manuales del Cooperative Cyber Defence Centre of Excellence de la OTAN; la National Cyber Security Strategies de ENISA; el Modelo de Madurez de Capacidades de Ciberseguridad para Naciones de la Universidad de Oxford; y el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones;

3. IPCC, 2022: Summary for Policymakers [H.-O. Pörtner, D.C. Roberts, E.S. Poloczanska, K. Mintenbeck, M. Tignor, A. Alegría, M. Craig, S. Langsdorf, S. Löschke, V. Möller, A. Okem (eds.)]. In: Climate Change 2022: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change [H.-O. Pörtner, D.C. Roberts, M. Tignor, E.S. Poloczanska, K. Mintenbeck, A. Alegría, M. Craig, S. Langsdorf, S. Löschke, V. Möller, A. Okem, B. Rama (eds.)]. Cambridge University Press, Cambridge, UK and New York, NY, USA, pp. 3–33, doi:10.1017/9781009325844.001.

4. *https://www.worldometers.info/coronavirus/*

5. *https://www.gob.cl/pasoapaso/cifrasoficiales/*

6. *https://www.dw.com/en/five-facts-on-grain-and-the-war-in-ukraine/a-62601467*

7. *https://en.wikipedia.org/wiki/Right_to_Internet_access*

8. *https://www.itu.int/net/wsis/docs/geneva/official/dop.html*

9. Global Cybersecurity Outlook 2023, Insight Report, Enero 2023. World Economic Forum. En colaboración con Accenture. Ver *https://www.weforum.org/reports/global-cybersecurity-outlook-2023/*

10. Global Cybersecurity Index, de la International Telecommunication Union, es un ránking que mide "el grado de compromiso" de los 193 países miembros de la ITU con cinco pilares: jurídico, técnico, organizacional, de capacitación y de cooperación.
Ver *https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx*

11. National Cybersecurity Index (NCSI). Ver *https://ncsi.ega.ee*

12. Estudio #2: Estimación de la brecha de expertos en ciberseguridad en Chile. Coordinación Nacional de Ciberseguridad, enero de 2023. Disponible en *https://bit.ly/cnc-eb02*

13. Estudio #1: RFI de la industria de ciberseguridad en Chile. Coordinación Nacional de Ciberseguridad, diciembre de 2022. Disponible en *https://bit.ly/cnc-eb01*

14. Disponible en *https://www.ine.gob.cl/estadisticas/sociales/seguridad-publica-y-justicia/seguridad-ciudadana*

15. El Modelo de Madurez de la Capacidad de Ciberseguridad (CMM) del Centro Global de Capacidad en Seguridad Cibernética de la Universidad de Oxford (*https://gcscc.ox.ac.uk/the-cmm*), y también el Índice de Ciberseguridad Global (ICG) publicado por la Unión Internacional de Telecomunicaciones en 2020 (*https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-S.pdf*).

La Política Nacional de Ciberseguridad fue aprobada por S.E. el Presidente de la República, mediante Decreto Supremo N°164, de 16 de junio de 2023, publicado en el Diario Oficial de fecha 4 de diciembre de 2023.

El texto oficial en español de la Política está disponible en el siguiente enlace:
https://www.diariooficial.interior.gob.cl/publicaciones/2023/12/04/43717/01/2415658.pdf

La Política Nacional de Ciberseguridad 2023-2028 fue elaborada por el Comité Interministerial sobre Ciberseguridad, en cumplimiento del mandato establecido por el Decreto Supremo N°533, de 2015 y fue aprobada en la sesión del día 25 de mayo de 2023, siendo sus integrantes titulares los siguientes:

1. Manuel Monsalve Benavides, Subsecretario del Interior
2. Macarena Lobos Palacios, Subsecretaria General de la Presidencia
3. Heidi Berner Herrera, Subsecretaria de Hacienda
4. Victor Jeame Barrueto, Subsecretario de Defensa
5. Gloria de la Fuente González, Subsecretaria de Relaciones Exteriores
6. Jaime Gajardo Falcón, Subsecretario de Justicia
7. Claudio Araya San Martín, Subsecretario de Telecomunicaciones
8. Montserrat Castro Hermosilla, Subsecretaria (s) de Economía y Empresas de Menor Tamaño.
9. Willy Kracht Gajardo, Subsecretario de Minería
10. Luis Felipe Ramos Barrera, Subsecretario de Energía
11. Carolina Gainza Cortés, Subsecretaria de Ciencia, Tecnología, Conocimiento e Innovación
12. Luis Marcó Rodríguez, Director Agencia Nacional de Inteligencia

El Comité Interministerial sobre Ciberseguridad fue presidido por Daniel Álvarez Valenzuela.

Los representantes delegados fueron las siguientes personas:

1. José Inostroza Lara, Subsecretaría General de la Presidencia
2. Claudio Reyes Barrientos, Subsecretaria de Hacienda
3. Pablo Sierra Hormazabal y Juan Pablo Cortés Albornoz, Subsecretaría de Defensa
4. Felipe Cousiño Donoso, Pablo Castro Hermosilla y Magdalena Durán Reyes, Subsecretaría de Relaciones Exteriores
5. Gabriel Monsalve León, Subsecretaría de Justicia
6. Enoc Araya Castillo, Subsecretaría de Telecomunicaciones
7. Joan Romero Ubiergo, Subsecretaría de Energía
8. Constanza Alarcón Cuevas, Agencia Nacional de Inteligencia
9. Nicky Arenberg Nissin, Subsecretaría de Economía y Empresas de Menor Tamaño
10. Daniela Vera Puga y Gonzalo Arenas Sepúlveda, Subsecretaría de Ciencia, Tecnología, Conocimiento e Innovación

La Comisión Asesora del Comité Interministerial de Ciberseguridad fue liderada por Ingrid Inda Camino. La Secretaría Ejecutiva del Comité estuvo a cargo de Michelle Bordachar Benoit y el equipo de la Secretaría Ejecutiva estuvo integrado por Alejandra Ayala Díaz, Cristian Bravo Lillo, Bárbara Schneider Schiehl y Hernán Espinoza Medina.

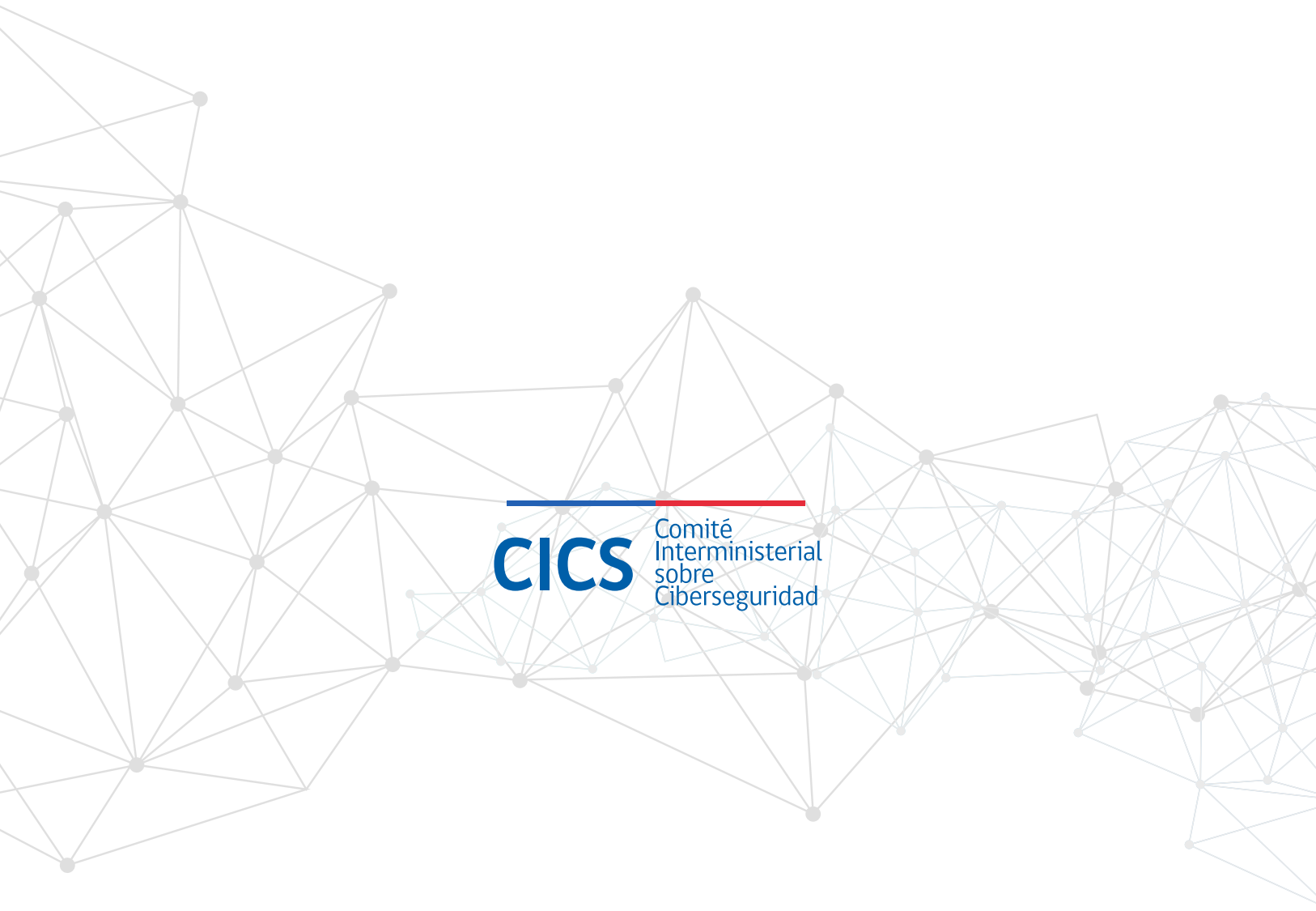
Participaron en audiencias públicas representantes de las siguientes organizaciones:

- Academia Politécnica Militar
- Alianza Chilena de Ciberseguridad
- Asociación Chilena de Tecnologías de la Información
- Asociación Nacional de Informáticos Municipales
- Centro Nacional en Sistemas de Información en Salud (CENS)
- ChileTelco
- CODELCO
- Consultora en Género Paz Peña
- Departamento de Ciencias de la Computación de la Universidad de Chile
- Derechos Digitales
- ENAP
- Fundación País Digital
- Fundación Soshisi
- Fundación Soymás
- Fundación Whilolab
- Hackada
- Instituto Milenio Fundamentos de los Datos
- NIC Chile
- Observatorio ALMA
- Red de Mujeres de Alta Dirección
- Universidad Andrés Bello

Se realizaron dos consultas públicas los días 3 de marzo y 8 de mayo de 2023, en las que participaron más de 1.000 personas.

Diseño y diagramación: Fredy Castillo V. / División de Gobierno Interior / Subsecretaría del Interior.

Año 2024, Santiago. Región Metropolitana. Chile.



CICS Comité Interministerial sobre Ciberseguridad

Subsecretaría del Interior
Gobierno de Chile

Subsecretaría de Defensa
Gobierno de Chile

Subsecretaría de Relaciones Exteriores
Gobierno de Chile

Subsecretaría de Justicia
Gobierno de Chile

Subsecretaría General de la Presidencia
Gobierno de Chile

Subsecretaría de Telecomunicaciones
Gobierno de Chile

Subsecretaría de Economía
Gobierno de Chile

Subsecretaría de Hacienda
Gobierno de Chile

Subsecretaría de Minería
Gobierno de Chile

Subsecretaría de Energía
Gobierno de Chile

Subsecretaría de Ciencia, Tecnología, Conocimiento e Innovación
Gobierno de Chile

Agencia Nacional de Inteligencia
Gobierno de Chile

POLÍTICA NACIONAL DE CIBERSEGURIDAD

2023-2028

CICS Comité Interministerial sobre Ciberseguridad

Gobierno de Chile

gob.cl