Propuesta de Política Nacional de Ciberseguridad 2023 - 2028

Comité Interministerial sobre Ciberseguridad

PNCS2-D4-20230503

Índice de contenidos

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 crecimiento social y económico. Sin embargo, la tecnología es inherentemente vulnerable. La mayor parte de las TIC no fueron diseñadas pensando en la seguridad de la información; esto ha posibilitado 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 2018 y 2022. La Política fue confirmada por el gobierno del presidente Sebastián Piñera, que avanzó en el diseño de la institucionalidad y el fortalecimiento del marco regulatorio, permitiendo al país avanzar de manera decidida en los desafíos que enfrentamos en materia de ciberseguridad. Sin embargo, esos desafíos se han diversificado y complejizado, y el escenario global ha cambiado de forma acelerada y nos obliga, como país, a 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 y con la discusión del proyecto de ley marco sobre ciberseguridad, poniendo especial énfasis en la protección y defensa de los derechos de las personas, en el avance hacia la igualdad de condiciones para la mujer, y en la profundización de la democracia. Para lograr esto, necesitamos contar con un ciberespacio libre, abierto, seguro y resiliente, tal como fue

planteado en la primera Política Nacional de Ciberseguridad, que es una política de Estado y, como tal, debe ser renovada.

La presente Política es fruto 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 públicas, 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 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 anterior 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[2]. 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[3] y más de 52 mil muertes confirmadas en nuestro país[4]. 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, incluido el nuestro. 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 en el resto del mundo 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[5]. La escasez de grano generó durante varios meses aumentos de precios y ha contribuido a 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 World Wide Web, herramientas habilitadoras y potenciadoras de todas las actividades humanas. Todos nuestros esfuerzos para enfrentar 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 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[6]. En el punto 4 de la declaración se afirma que "*todos [los seres humanos] tienen el derecho a la libertad de opinión y de expresión; este derecho incluye la libertad de tener opiniones sin interferencia y a buscar, recibir e impartir información e ideas a través de cualquier medio, no importando las fronteras. La comunicación es un proceso social fundamental, una necesidad humana básica, y el fundamento de toda organización*

social."[7] Es 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.

20 años después, en enero de 2023, el World Economic Forum publicó un reporte[8] donde presentan una serie de problemas desde la perspectiva de expertos en ciberseguridad y líderes de negocio alrededor del mundo, destacándose los siguiente:

- 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 los negocios operan, y en la decisión sobre qué países invierten. 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 está cambiando. 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, nuestros medios de comunicación masivos, nuestras 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 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 perseguirá el mismo objetivo.

1.2. Los desafíos en ciberseguridad en nuestro país

Chile ha logrado posicionarse a nivel medio en ciberseguridad en el escenario internacional. En el Índice Mundial de Ciberseguridad[9] de 2020, Chile se encontraba en el lugar 74 a nivel mundial, y en el 7mo. lugar en las Américas (debajo de Estados Unidos de América, 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[10], desarrollado por Estonia y actualizado de forma continua, Chile se encuentra en el lugar 53 entre 175 países, y en el 6to. 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 falta de conciencia de las personas y las organizaciones sobre la importancia de la ciberseguridad**. Esto, junto a la falta de conocimiento, lleva a que tanto las personas como las organizaciones 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 la tercera edad, tanto en la educación básica y media, como en las organizaciones privadas, el sector público, y la sociedad civil.

2. **La falta de especialistas en ciberseguridad**. Estimamos que faltan en Chile alrededor de 28.000 especialistas en ciberseguridad para servir las necesidades tanto del sector público como privado. Es necesario que el Estado genere las

condiciones para disminuir esta brecha, incentivando el que una mayor cantidad de jóvenes escojan estudiar carreras relacionadas con ciberseguridad.

3. **La falta de resiliencia de nuestras organizaciones e infraestructura**. Brechas de datos públicas y recientes en nuestro país nos confirman la necesidad de fortalecer la protección de nuestra infraestructura de redes y mejorar el entrenamiento y formación de nuestros funcionarios públicos, así como de todas las personas en organizaciones públicas o privadas que lo requieran. Para esto, es necesario monitorear nuestro ciberespacio de forma efectiva, especialmente la infraestructura de redes del sector público.

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 del país. La ciberseguridad es un área económica intensiva en capital humano, que podría a futuro representar una parte creciente e importante de nuestro producto interno bruto, podría ayudar a posicionar a nuestro país en el escenario latinoamericano, e incluso fortalecer la confianza en nuestra economía, vista desde el exterior. Para que esto suceda, sin embargo, es necesario tener una demanda más amplia y sofisticada.

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 nuestro país en el 2022 y 2023. La cantidad de incidentes que se registran en la Red de Conectividad del Estado (una 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.

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 materias 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.

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**: Los organismos públicos y privados deben establecer instancias de cooperación con el resto del sector público, de la industria, o de la autoridad institucional existente en ciberseguridad, con el propósito de comunicar y difundir sus esfuerzos en ciberseguridad, evitar la duplicación de trabajo y pérdida de recursos, y hacer eficientes los esfuerzos en ciberseguridad.

5. **Fomento a la industria**: 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.

Los objetivos anteriores representan pequeñas variaciones de los planteados en la primera política. La elección de estos objetivos no es aleatoria: es posible establecer una relación con las dimensiones que plantean al menos dos modelos internacionales en ciberseguridad[11].

Tal como en la primera versión, formará parte de esta política un Plan de Acción con un conjunto de medidas de corto plazo que la implementan. A diferencia de la versión anterior, el plan se publica de forma separada a la política y cubre un período de sólo dos años. El propósito es permitir revisar el avance, proponer cambios y mejoras, y enmendar el rumbo en caso necesario durante la vigencia 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 será el responsable de conducir el proceso de implementación de la Política, de requerir reportes de avance a las instituciones responsables, de generar condiciones favorables para la implementación de las medidas cuando éstas no existan, y en general de lograr la adecuada implementación de las 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 invertirá progresivamente en 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 factores productivos, 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

Nuestro país tiene una Política de Ciberdefensa vigente, publicada en marzo de 2018. En ella, se establecen dos prioridades para nuestro país:

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.
2. **El desarrollo de capacidades**: La Defensa desarrollará líneas de carrera en cada rama de las Fuerzas Armadas; creará un Comando Conjunto de Ciberdefensa; creará un CSIRT de Defensa; creará una Oficina de Ciberdefensa y Seguridad de la Información en el Ministerio de Defensa; y creará una reserva nacional de ciberdefensa.

Adicionalmente, 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 la Política de Ciberdefensa, particularmente en lo que respecta al cuarto objetivo, de Coordinación Nacional e Internacional.

Nuestro país posee también una Política Nacional de Inteligencia Artificial, publicada en noviembre de 2021. 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 3 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 capacitación y concientización a 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.

2. Objetivos de Política Pública 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-of-Things, o IoT).

Para avanzar en este objetivo, es necesario:

1. Crear una 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 sea considerado 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. Para las instituciones que no tengan recursos suficientes, el Estado entregará recomendaciones y proveerá recursos gratuitos mínimos que les permitan protegerse de forma básica frente a los ataques más frecuentes o de mayor impacto.

4. Fortalecer la resiliencia física de la red en Chile. El Estado deberá coordinar y priorizar con el sector privado la conexión de lugares previamente no conectados, o donde no exista redundancia de conexiones con al menos otros dos lugares.

5. Fortalecer el monitoreo y 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 protegerá y promoverá la protección de los derechos de las personas en Internet, a través del fortalecimiento de la institucionalidad existente en materias 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, jóvenes, personas de la tercera edad y disidencias sexogenéricas.Cada persona podrá 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 de protección a los datos personales y de ciberseguridad, a través de la aprobación e implementación de la ley sobre protección de datos, y la aprobación de la ley marco de ciberseguridad.

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

3. Generar medidas de acción positiva para favorecer y fortalecer la incorporación de la mujer en todo el quehacer de protección de nuestro ciberespacio..

4. Proteger y prevenir la comisión de delitos informáticos que afectan a las personas, sus derechos y su patrimonio.

5. 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 más desfavorecidos.

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 todos nosotros va en directa relación con la capacidad de cada uno de protegerse. Necesitamos generar nociones de higiene digital en todas las personas de nuestro país, de forma que cada persona sea capaz de cuidar por sí misma su identidad digital y su información.

Para avanzar en este objetivo, es necesario:

1. Diseñar e implementar un plan de concienciación nacional sobre ciberseguridad y privacidad, para que todas las personas en nuestro país que usen un computador o teléfono inteligente adquieran nociones de higiene digital,. Este programa se enfocará especialmente en mujeres, niñas, niños, jóvenes, personas de la tercera edad y disidencias sexogenéricas, y en otros grupos que podrían estar en desventaja frente al resto de la sociedad en términos de conocimiento sobre ciberseguridad.

2. Generar e implementar un plan matriz de introducción y mejora de la educación en higiene digital y ciberseguridad para el sistema de enseñanza básica, media científico-humanista y media técnico-profesional. En particular, este plan considerará de manera preferente la generación de carreras de nivel técnico para la educación media técnico-profesional.

3. Fomentar una cultura de evaluación y gestión del riesgo, tanto en organizaciones públicas como privadas, que nos permita estar preparados 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. Fomentar la investigación científica aplicada en ciberseguridad, para resolver problemas que nuestro país tendrá en los próximos años a raíz del uso e implementación de tecnologías con aplicaciones insospechadas. Nuestro país no puede ser simplemente 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

Los organismos públicos y privados deben establecer instancias de cooperación con el resto del sector público, de la industria, o de la autoridad nacional de ciberseguridad, con el propósito de comunicar y difundir sus esfuerzos en ciberseguridad, evitar la duplicación de trabajo y pérdida de recursos, y hacer eficientes los esfuerzos en ciberseguridad. Tenemos que coordinar mejor nuestros esfuerzos e intencionarlos hacia la consecución de estos objetivos de política pública..

En el aspecto internacional, el Estado debe coordinarse y trabajar 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 entre organizaciones públicas y privadas en educación, infraestructura, protección de derechos, fomento a la industria, y otras áreas relacionadas con la ciberseguridad que puedan ser de interés del país, todo con el propósito de relevar 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, fomentando 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.

2.5. Fomento de la industria

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. Crear institutos de investigación científica aplicada y transferencia tecnológica en materias de ciberseguridad, que realicen investigación sobre aquellos problemas y necesidades en ciberseguridad tanto del sector público como privado, que potencien la ciberseguridad como un área de investigación

preferente por parte del sector académico nacional, y que conecten las necesidades de las organizaciones y el sector público con el conocimiento científico existente en materia de ciberseguridad.

2. Generar incentivos para el emprendimiento tecnológico en ciberseguridad, impulsado por las necesidades de las organizaciones privadas y públicas de nuestro país, y 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 serán amplios y no se restringirán al ámbito económico

3. Revisión de los mecanismos de contratación de servicios de ciberseguridad por parte del Estado, para hacerlos más eficientes y expeditos.

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.

3. Gobernanza del país en ciberseguridad

3.1. Marco normativo

Nuestro país cuenta con un amplio conjunto de normas legales y reglamentarias que tienen relación 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, Ley FINTEC; 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, hallamos los siguientes Decretos: D.S. N°83/2005, aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos; D.S. N°1.299/2004, 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; D.S. N°1/2015, aprueba norma técnica sobre sistemas y sitios web de los órganos de la administración del Estado; D.S. N°533/2015, crea el Comité Interministerial sobre Ciberseguridad y su modificación mediante Decreto N°579 de fecha 07 de enero de 2020; D.S. N°273/2022 que establece obligación de reportar incidentes de ciberseguridad; D.S. N°14/2014 que modifica el Decreto N°181 de 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; 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 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; 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 encuentra 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 necesario 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 con una dispersión normativa e institucional, ha plasmado la necesidad y urgencia de legislar al respecto. Así, con el reconocimiento de la ciberseguridad como un vector transversal para la protección de las personas, sus derechos, patrimonio y seguridad individual, el gobierno del Presidente Boric ha impulsado fehacientemente el Proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información (Boletín N° 14.847-06).

Dicho proyecto ofrece una respuesta integral a los problemas y desafíos que la ciberseguridad impone, 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 identificación de los operadores de importancia vital, acorde al proceso de

transformación digital en que se encuentra inmerso nuestro país. En cuanto a la institucionalidad, crea la Agencia Nacional de Ciberseguridad, un CSIRT Nacional y el CSIRT de la Defensa Nacional, en coordinación con otros CSIRT Sectoriales que se pudieran crear.

Finalmente, el proyecto de ley busca establecer obligaciones específicas al Estado y al sector privado en materia de ciberseguridad, incorporando la dimensión de la educación, capacitación, buenas prácticas e higiene digital, además de proteger legalmente el hacking ético y promover la notificación de incidentes de ciberseguridad. De aprobarse el proyecto de ley, Chile contará con una autoridad nacional de ciberseguridad de vanguardia en la región y en el mundo.

Notas

1. Guide to Developing a National Cybersecurity Strategy, 2nd edition 2021.
2. 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.
3. https://www.worldometers.info/coronavirus/.
4. https://www.gob.cl/pasoapaso/cifrasoficiales/.
5. https://www.dw.com/en/five-facts-on-grain-and-the-war-in-ukraine/a-62601467.
6. https://en.wikipedia.org/wiki/Right_to_Internet_access.
7. https://www.itu.int/net/wsis/docs/geneva/official/dop.html.
8. 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/.
9. 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.
10. National Cybersecurity Index (NCSI). Ver https://ncsi.ega.ee.
11. 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).