Reporte de Resultados de Audiencias Públicas para Segunda Política Nacional de Ciberseguridad

Comité Interministerial sobre Ciberseguridad

PNCS2-D2-20230502

Este documento es responsabilidad de la Coordinación Nacional de Ciberseguridad (CNC), en la Subsecretaría del Interior.

Este documento debe ser visualizado en línea en la URL bit.ly/pncs2-d2, o escaneando el código QR; una versión en papel podría estar desactualizada.

Índice de contenidos

Introducción

Las tecnologías de información y comunicaciones (TICs) juegan un papel fundamental en las actividades diarias y 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.

El 27 de abril de 2017, la presidenta Michelle Bachelet lanzó la primera Política Nacional de Ciberseguridad de Chile ("Política" o "PNCS"), cuyo objetivo principal fue contar con un ciberespacio libre, abierto, seguro y resiliente. La política contenía cinco objetivos políticos para el Estado en materia de ciberseguridad, y una serie de 41 medidas a ser implementadas en cuatro años, entre 2018 y 2022. Los cinco ejes de la política anterior fueron:

A. Infraestructura resiliente, con el propósito de contar con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos.

B. Derechos digitales, con el objetivo de fortalecer los mecanismos de protección de los derechos de las personas en el ciberespacio.

C. Cultura de ciberseguridad, con el propósito de desarrollar una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.

D. Cooperación internacional, donde la meta es establecer relaciones de cooperación en ciberseguridad con otros actores y participar activamente en foros y discusiones internacionales.

E. Fomento de la industria, con el objetivo de promover el desarrollo de una industria de la ciberseguridad, que sirva tanto a las personas y organizaciones como al desarrollo económico del país.

La PNCS permitió al país avanzar de manera decidida, durante tres administraciones, en los desafíos que nuestro país enfrentó en materia de ciberseguridad. Sin embargo, esos desafíos se han complejizado y agravado, y el escenario global ha cambiado de forma acelerada y nos obliga, como país, a adaptarnos a circunstancias distintas de las que vimos hace media década.

Antecedentes

La elaboración de la primera Política Nacional de Ciberseguridad 2017-2022, fue un proceso participativo, donde se acogieron las observaciones de diferentes actores de la industria para incorporar en el documento. El éxito de este proceso llevó a que el Comité Interministerial sobre Ciberseguridad acordara la realización de actividades que fueran participativas, definiendo las audiencias públicas como un mecanismo deseable y conveniente para el cumplimiento.

Se realizaron seis sesiones, entre el 5 de enero y el 30 de marzo del 2023, a las cuales fueron invitados diversos exponentes de la sociedad civil, academia, y gremios, entre otros. El lugar de realización de estas audiencias fue el Salón 200 del Palacio de La Moneda, los días jueves de 15:00 a 18:00 horas.

Con la finalidad de enfocar la discusión a los puntos relevantes para la actualización de la Política, se les compartió previamente a los asistentes un borrador del documento con bases para la discusión. Los expositores dispusieron de 20 minutos cada uno para realizar comentarios y observaciones al respecto.

Detalle de las audiencias

Todas las audiencias se realizaron en el Salón 200, en el Palacio de la Moneda:

N°	Fecha	Invitado	Representantes
1°	05/01/2023	*Asociación Chilena de Tecnologías de Información*	-Thierry de Saint Pierre -Rodrigo Ríos -Carlos Bustos
		Alianza Chilena de Ciberseguridad	-Alejandra Moya -Claudio Magliona -Guillermo Carey

N°	Fecha	Invitado	Representantes
		Fundación País Digital	-Pelayo Covarrubias -Juan Luis Núñez
2°	12/01/2023	*Fundación Sochisi*	-Rodrigo Reveco
		Fundación Whilolab	-Carlos Montoya
		Red de Mujeres de Alta Dirección	-Ana María Castro -Claudia Álvarez
		Derechos Digitales	-Juan Carlos Lara -Isidora Ruggeroni
		Asociación Nacional de Informáticos Municipales	-Pablo Benavides
3°	19/01/2023	*Instituto Milenio Fundamentos de los Datos*	-Claudio Gutiérrez -Marcelo Arenas
		Academia Politécnica Militar	-Óscar Rodríguez
		Centro Nacional en Sistemas de Información en Salud (CENS)	-May Chomali -Priscila Vergara
		Universidad Andres Bello	-Romina Torres
4°	*26/01/2023*	*CODELCO*	-Soledad Bastías
		ENAP	-Helvecia Castro -Cristóbal Hammersley
		Observatorio ALMA	-Jorge Ibsen

N°	Fecha	Invitado	Representantes
		Liebherr	-Fabiola Arzic
5°	*09/03/2023*	*Hackada*	-Natalia Erika Pérez Muñoz -Bárbara Palacios
		Departamento de Ciencias de la Computación de la Universidad de Chile	-Alejandro Hevia -José Miguel Piquer
		Consultora en género	-Paz Peña
6°	*30/03/2023*	*ChileTelco*	-Eilat Nachari -Alfie Ulloa -Claudio Anabalon
		Fundación Soymás	- Bárbara Etcheberry Araos - Miguel Socias Pérez
		NIC Chile	- Patricio Poblete Olivares - Eduardo Mercader Orta - Guillermo Lama Antola

Observaciones

En los siguientes puntos se detallan las observaciones realizadas por los invitados a los 5 objetivos de la política. Es importante destacar que se han incluido todos los documentos que nos han compartido los invitados en el momento que fue solicitado, y reflejan las opiniones que manifestaron en las audiencias.

Objetivo 1: Infraestructura resiliente

A continuación se detallan las observaciones recibidas por los invitados respecto al objetivo A de la política. Es importante señalar que los comentarios se exponen textualmente conforme fueron recibidos; por lo que, cualquier omisión a alguna agrupación y/o comentario se debe a que no hizo referencia al objetivo específico.

El texto del objetivo es el siguiente:

> ***Infraestructura resiliente:*** *El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos*

A continuación se detallan las observaciones recibidas por los invitados respecto al objetivo A de la política. Es importante señalar que los comentarios se exponen textualmente conforme fueron recibidos; por lo que, cualquier omisión a alguna agrupación y/o comentario se debe a que no hizo referencia al objetivo específico.

Alianza Chilena de Ciberseguridad

Sugerimos que se considere coordinar las medidas para regular y salvaguardar la infraestructura crítica de Chile, debido a que el estado regulatorio podría estar en un mejor nivel para garantizar la protección de diversos sectores y entidades críticas para la prestación de los servicios esenciales del país, entre ellos, servicios bancarios y financieros, organismos de la administración del Estado, agua potable, electricidad, transporte, etc. Estamos conscientes que ciertos sectores han tenido grandes avances, pero se necesita llevar estos avances a todos los incumbentes.

En el ámbito internacional esto ha ocurrido, por ejemplo, en Europa, dónde desde el año 2008 se cuenta con normativa para la protección de la infraestructura crítica europea, y que es complementaria a los marcos generales o específicos en materia de ciberseguridad, recientemente representados por la "Security of Network and Information Systems Directive 2" del año 2022.

En el mismo sentido, los esfuerzos europeos por actualizar la normativa que protege a la infraestructura crítica europea, a través de la propuesta de una "Critical Entities Resilience Directive", no obstan al hecho de que un marco normativo robusto en materia de ciberseguridad se encuentra integrado por: a) la protección de la infraestructura, sectores y entidades críticas; y b) marcos regulatorios comunes relativos a ciberseguridad, y especiales relativos, por ejemplo, a sistemas de certificación, finanzas, comercio electrónico, privacidad, entre otros.

En Estados Unidos, por su parte, el marco regulatorio e institucional para la protección de la infraestructura crítica es inclusive más robusto que el europeo, debido a que contempla 16 sectores críticos cuya salvaguarda se encuentra en manos de la "Cybersecurity and Infrastructure Security Agency" (CISA).

Así, la importancia de la creación de una Agencia Nacional de Ciberseguridad para la administración y control sobre el marco regulatorio en materia de ciberseguridad y protección de la infraestructura crítica es evidente. Por ello, recomendamos que la Agencia sea un órgano de la Administración del Estado descentralizado, con patrimonio y personalidad jurídica propia, cuyos cargos directivos se concursen por el Servicio Civil por el sistema de Alta Dirección Pública, y de carácter técnico, tal como ocurre en otras jurisdicciones.

ACTI

Promover la colaboración entre instituciones en forma estructurada para compartir en tiempo real información y en el largo plazo experiencias y mejores prácticas. Desarrollar el concepto de ISACs sectoriales para un esquema más sistémico y complementar con el eje D.

- Incorporar los conceptos de Ciberseguridad IOT y nube (en línea con el eje E)
- Implementar el concepto de Cyber Range nacional
- Focalizarse en ciberseguridad no en cobertura.
- Avanzar en la regulación y protección de la infraestructura crítica de Chile.
- Ir más allá de la infraestructura

Fundación Sochisi

La masificación del uso de las tecnologías digitales y la información contenida en ellas ha impactado evidentemente el desarrollo de los países, desde la forma en que se relacionan y comunican los diferentes actores hasta nuevas formas de producción e integración de los países a nivel global. Este fenómeno importa beneficios para el desarrollo sustentable de los países, pero también riesgos que pueden afectar los derechos de las personas, infraestructuras críticas de información e intereses vitales del país, a nivel nacional e internacional.

Estos riesgos, propios del desarrollo, donde los datos y la información en poder de los actores de la sociedad se convierten en un activo, tienen el potencial de impactar negativamente la seguridad pública, los derechos fundamentales, e inclusive comprometer la seguridad externa del país a través de actividades tales como el espionaje y los ciberataques llevados a cabo por otros países, grupos organizados, o por sujetos individuales.

También parece relevante dar espacio a la noción de amenaza híbrida en cuanto ella puede servir como un puente entre los intereses de la seguridad pública nacional. Está noción de amenaza y bilidad permite conectar hechos que aparentemente no tienen

la misma naturaleza pero que afectan la seguridad pública o la ciberdefensa del país. En ese sentido el Profesor Carlos Galán define las amenazas híbridas: acciones coordinadas y sincronizadas —con origen habitualmente, pero no solo, en los servicios de inteligencia de los agentes de las amenazas— que atacan deliberadamente vulnerabilidades sistémicas de los Estados y sus instituciones a través de una amplia gama de medios y en distintos sectores objetivo (políticos, económicos, militares, sociales, informativos, infraestructuras y legales) utilizando el ciberespacio como la herramienta más versátil y adecuada para sus propósitos.

En un contexto de esa naturaleza los atentados físicos (por ejemplo a trenes) que se correlacionan con ataques cibernéticos, por ejemplo ataques de desinformación más atentados a infraestructuras críticas acompañado de hackeos, inclusive la guerra híbrida que hoy es una realidad.

No contar con esta noción especialmente pensando en un plazo como 2028 impide que haya una visión sistémica omnicomprensiva de ciertas amenazas que hoy están presentes en nuestra realidad, ella permitiría además una coordinación pública y privada más estrecha en caso de ocurrencia de hechos de esta naturaleza, donde la comunicación estratégica juegue un papel fundamental.

Derechos Digitales

Lo que se menciona es sobre fortalecimiento de servicios esenciales y de resiliencia física. Estamos asumiendo por el lenguaje amplio que esto pasa no solamente por recomendaciones, sino por exigencias formuladas desde la autoridad para el cumplimiento de estándares mínimos de seguridad desde la Agencia. Allí donde eso es necesario es importante que sea explícito en la política.

También se habla de la perspectiva de gestión de riesgos. A diferencia de la política anterior, no hay mención de las iniciativas de identificación de los riesgos o de la identificación de las infraestructuras críticas, que sí sería competencia de la Agencia. Sería bueno saber cómo se abordará antes de que la Agencia tome esa facultad.

Nos preguntamos si continuará el estímulo a la creación de CSIRTs y CERTs y sus instancias de colaboración. También, sobre la institucionalidad para responder a preocupaciones más habituales sobre phishing y otras formas de ataque. El CSIRT de gobierno está haciendo un importante trabajo de difundir información, pero por lo que hemos escuchado aquí, el rango de posibles formas de ataques es bastante más grande.

Instituto Milenio Fundamentos de los Datos

El documento no menciona los servicios esenciales; debieran incluirse las bases de datos y data centers dentro de estas.

Ciberseguridad y soberanía nacional (en particular seguridad de datos y soberanía nacional).

Academia Politécnica Militar

En el objetivo N°1 dice: "El Estado entregará....recursos gratuitos mínimos que le permitan protegerse de forma básica...." Se estima importante definir el nivel de criticidad de la organización para la entrega de recursos.

El objetivo N°1 dice: "Creación de una ANCS, que opere como organismo rector... con facultades normativas, fiscalizadoras y sancionatorias...", sin embargo, no queda claro si tendrá facultades específicas para apoyar o centralizar los esfuerzos de las instituciones estatales.

Las IP deben mejorar su nivel de madurez en ciberseguridad y su capacidad de sobreponerse a brechas y ataques.

Fortalecer la resiliencia física de la red en Chile.

Creación de ANCS... incrementar el nivel de madurez en ciberseguridad en el sector público.

Universidad Andrés Bello

Respecto de este objetivo, es necesario detallar los utilities que son cubiertos y que, dada su naturaleza, demandan un apartado por cada uno. Un ejemplo de ellos es el Coordinador Eléctrico Nacional – quienes trabajan con Estándar de ciberseguridad para el sector eléctrico.

En este punto puede ser relevante el factor d1.3 de protección a la infraestructura crítica del modelo de madurez de las capacidades propuesto por Oxford, que considera entre otros la capacidad de identificación de Infraestructura Crítica, las capacidades para diseñar requerimientos regulatorios, operacionalización basada en estándares, tal como el NIST para Infraestructura Crítica que considera la identificación, la protección, la detección, la respuesta y el plan de recuperación. ciberseguridad NIST Fuente: https://nvlpubs.nist.gov/.

Importante mencionar, acorde a noticias relacionadas a la próxima estrategia nacional de ciberseguridad de Estados Unidos, se demarcan regulaciones mandatorias a muchas industrias de infraestructura incluido el sector de defensa y seguridad nacional.

CODELCO

- Se sugiere indicar cómo se definirá un servicio esencial y cómo se abordará los temas de ciberdefensa asociado a temas de seguridad nacional.
- Se sugiere incorporar el concepto de cadena de suministro, es relevante considerar que un servicio esencial puede verse afectado por un incidente sufrido por algún proveedor de cadena de suministro.
- Se sugiere incorporar el concepto de convergencia IT/OT.
- Se sugiere incorporar el concepto de detección, respuesta y recuperación, se menciona bastante de medidas de prevención y protección, sin embargo, es clave la detección oportuna y estar preparado para responder y recuperarse de un incidente. Todo lo anterior, dado que cada vez es más probable sufrir un ciberataque y es relevante tener los mecanismos de detección y recuperación frente a un ciberataque.
- Se recomienda que existan mecanismos de difusión y colaboración en materias de ciberseguridad con un enfoque sectorial y cumplimiento de estándares internacionales de seguridad de la información y marcos de trabajo probados.

ENAP

Definir y exigir obligaciones de una infraestructura de la información robusta y resiliente, no sólo aplicable a las tecnologías de la información (TI), sino también a las tecnologías de la operación (OT), que sustentan la implementación de redes industriales para soportar y dar continuidad a los procesos operativos en la cadena productiva, de las empresas pertenecientes a los sectores industriales en general, y aún más preponderante, en aquellas además vinculadas a la infraestructura estratégica imprescindible para el adecuado funcionamiento de nuestro país.

En este contexto se vuelve fundamental, definir algunas consideraciones para desmitificar que las redes industriales de tecnologías de la operación (OT), que se encuentran aisladas de Internet y de la red administrativa de tecnologías de información (TI), no se encuentran expuestas a ciberataques, estableciendo que dichas redes OT igualmente se encuentran expuestas a posibles ciberataques de forma dirigida, inclusive con malware específicamente desarrollados para vulnerar los protocolos de comunicación propios de las redes industriales.

Por lo anterior, se hace necesario considerar como referencia las definiciones aplicadas en Canadá, España y Reino Unido, entre otros, y encauzar el cumplimiento de estándares internacionales de ciberseguridad, tales como IEC 62.443 (que entre otros importantes aspectos, establece directrices de cumplimiento para los licenciantes de Sistemas de Control Industrial), el Framework de Ciberseguridad NIST (definido el año 2012 a petición del Presidente Obama para ser implementado precisamente por las empresas definidas como infraestructura crítica para el país) y el NERC CIP (aplicable a las empresas eléctricas en USA).

Hackada

Infraestructura resiliente, en el documento en este apartado menciona el permitir mantener funcionando los servicios considerados esenciales en caso de ataques a través de internet como de desastres naturales. Realizamos la observación considerando además las problemáticas generadas por los humanos de forma intencional como el robo de cables y los actos vandálicos sobre las redes de transporte de información.

Departamento de Ciencias de la Computación de la Universidad de Chile

Considerar discutir, diseñar y proponer políticas para el manejo, incluyendo búsqueda activa, detección y reporte, de vulnerabilidades por parte de organismos de inteligencia, policiales o militares. Esto a la luz de que dichas vulnerabilidades pueden utilizarse como armas en operaciones de ciberataques, algo que ya ha sido frecuentemente discutido en foros y organismos internacionales. Los países pueden decidir buscar vulnerabilidades y no reportarlas, para usarlas como armas en ciberoperaciones, o alternativamente, reportarlas para segurizar a sus propios ciudadanos, con la desventaja que dichas vulnerabilidades reportadas no podrán ser usadas en las operaciones (pues serán arregladas luego del reporte). Chile debiera tener una política pública que exprese una postura al respecto.

Objetivo 2: Protección de Derechos de las Personas

El texto del objetivo es el siguiente:

> *Protección de los derechos de las personas: El estado velará por los derechos de las personas en el ciberespacio*

A continuación se detallan las observaciones recibidas por los invitados respecto al objetivo B de la política. Es importante señalar que los comentarios se exponen textualmente conforme fueron recibidos; por lo que, cualquier omisión a alguna agrupación y/o comentario se debe a que no hizo referencia al objetivo específico.

Alianza Chilena de Ciberseguridad

Hacer hincapié en la regulación y protección de la infraestructura crítica del país, salvaguardando así la prestación de los servicios esenciales del país y el legítimo ejercicio de los derechos de las personas tanto en el espacio físico como digital.

Propender y fomentar el cumplimiento regulatorio por parte de las diversas industrias, a través del establecimiento de mecanismos o herramientas de "compliance" adicionales y complementarios que inviten a las empresas a dar cumplimiento a la normativa, tales como certificaciones o la adopción de códigos de conducta, que aseguren de esta manera un mejor y eficiente despliegue de recursos económicos y humanos por parte de las autoridades, quienes normalmente no poseen las capacidades técnicas y económicas suficientes para garantizar, por sí solas, la correcta implementación del marco regulatorio.

Otorgar espacios de colaboración público-privada abiertos también a otros grupos de interés, tales como la academia o la sociedad civil, que permitan la elaboración de marcos comunes y autorregulatorios adicionales y complementarios para la protección de la privacidad de las personas y la ciberseguridad del país. La adopción de este tipo de marcos autorregulatorios genera un alto nivel de cumplimiento por parte de aquellas entidades que participen en su elaboración, y permiten que los estándares puedan ser actualizados más eficiente y rápidamente en comparación con la elaboración de otros cuerpos normativos (reglamentos, leyes, etc.). En EE. UU este tipo de mecanismos ha sido promocionado por el National Institute of Standards and Technology, creando estándares de replicación internacionales, tales como el "Cybersecurity Framework" de EE. UU.

Considerar explícitamente como un lineamiento transversal la protección de los derechos a la privacidad y protección de datos personales, que guíe el desarrollo e implementación de las medidas que sean adoptadas gracias a la Política, permitiendo que exista coherencia sistemática entre ellas y, de este modo, no resulten derechos en la práctica minimizados. Así, temas como la proporcionalidad de los mecanismos de protección y evitar medidas de supervigilancia masivas o demasiado invasivas debieran ser algunas de las medidas o lineamientos a tener en cuenta en la elaboración de la Política.

ACTI

Como ACTI hemos dicho en otros foros que la protección de datos personales es un eje fundamental del ecosistema de ciberseguridad; defiende la dignidad y la libertad de

las personas a la vez que entrega un marco legal que permite ser visto como un polo atractivo para la exportación de servicios e inversión extranjera.

Fundación País Digital

Evitar la duplicidad regulatoria y la multiplicidad de normativas sectoriales. Debemos avanzar en la unicidad normativa, a fin de evitar que cada regulador saque su propia normativa y que pueda entrar en contradicción o conflicto entre ella.

Fundación Sochisi

Sería interesante dar mayor profundidad sobre el rol de la identidad digital en Chile, más allá que contemos con una ley (de firma) 19.799 que trae aparejada una tecnología ya superada en la industria. La interoperabilidad transfronteriza y también la utilización de tecnologías en la nube debe ser promovida para potenciar los servicios en línea, con una transaccionalidad razonable. Resulta estratégico para el país controlar la verificación de identidad a través de las herramientas digitales disponibles como la clave única y actualizar la ley de firma 19.799 a las nuevas realidades de la industria de la identidad digital. Ello en cuanto el estado tiene un deber de habilitar a las personas para que puedan participar en igualdad de condiciones en los mercados de la sociedad digital, accediendo a bienes y servicios del mismo modo quienes pueden pagar tecnologías privadas para dichos fines. En ese sentido referirse a el estado como un garante e impulsor de herramientas de identidad digital para que ni igualdad de condiciones puedan acceder las personas sería una solución pertinente.

También creemos que es posible hacer una referencia más explícita la responsabilidad de garante que tiene el Estado respecto de las personas sus derechos en especial de aquellos grupos que no pueden cuidarse a sí mismos como los niños niñas y adolescentes así como también adultos mayores y otros grupos de personas que han sido históricamente discriminadas.

Autodeterminación informativa de menores de edad se ve fuertemente afectada por ciertas tecnologías de ofimática que perfilan a sus usuarios y predicen su comportamiento en ese sentido es interesante conocer una sentencia tribunales alemanes quién prohíbe el uso de esas aplicaciones en la nube, ya que ellas no recaban en el procesamiento de los datos, el consentimiento de los alumnos y por ello han estimado que "Las instituciones públicas en Alemania tienen una responsabilidad especial con respecto a la admisibilidad y trazabilidad del procesamiento de datos personales".

Red de Mujeres de Alta Dirección

Medición continua de las diversas brechas de género: mujeres que estudian o trabajan en alguna de las ramas dedicadas a la ciberseguridad y sus motivaciones; conocimiento de los ataques de género en la red; capacitación de agentes de los distintos poderes públicos así como de la empresa privada para considerar el enfoque de género, en sus compras, desarrollo y evaluaciones.

El citado estudio de UNIDIR propone una serie de recomendaciones como:

- Los creadores de estándares deben evaluar el alcance de la igualdad de género en los estándares de seguridad cibernética, incluida la participación significativa, el contenido y el lenguaje de los estándares, y los efectos de género directos e indirectos. El primer paso hacia esto es la recopilación de datos desglosados por género a lo largo de la política y la práctica de ciberseguridad.

- Desarrollar una política más amplia para aumentar la participación de las mujeres en ciencia, tecnología, ingeniería y matemáticas (STEM). Además, es importante elevar el perfil y el valor de las habilidades y la experiencia en ciberseguridad más allá de STEM (por ejemplo, comunicaciones, ética, gobernanza legal). Todas las partes interesadas en la seguridad cibernética deben contrarrestar las percepciones y los estereotipos de género dañinos, y deben apoyar los cambios organizacionales y culturales que valoran las diversas actividades y capacidades.

- Las medidas legales de ciberseguridad deben incorporar una perspectiva de género en el desarrollo, implementación, supervisión y evaluación de leyes pertinentes. Las medidas legales deben estar respaldadas por un proceso legislativo abierto y participativo que involucre a todas las partes interesadas, especialmente a los grupos y organizaciones de la sociedad civil

- que promueven los derechos de las personas con identidades de género marginadas y subrepresentadas.

- Todas las organizaciones, tanto en el sector público como en el privado, deben impartir capacitación sobre "género y seguridad cibernética" para profesionales y formuladores de políticas. Esta formación debería incorporar un doble enfoque en (a) la igualdad de género, diversidad e inclusión en el lugar de trabajo y (b) el desarrollo de una perspectiva de género en la ciberseguridad como una habilidad profesional. Esta capacitación proporcionará una

introducción práctica al género como un elemento de la política, asegurando que la experiencia en género sea un aspecto fundamental y respetado de la práctica profesional y la formulación de políticas de seguridad cibernética.

- Los Estados que participan en los procesos de seguridad cibernética de la ONU podrían apoyar y financiar el desarrollo de un conjunto de herramientas de capacitación cibernética y de género y exigir que las organizaciones del sector público y los contratistas del sector privado lo utilicen cuando sea posible. Los actores no estatales en la academia y, en particular, la sociedad civil podría contribuir con su experiencia en el desarrollo de un conjunto de herramientas, mientras que los actores corporativos podrían implementar versiones modificadas y utilizar la influencia comercial para garantizar que otros también lo hagan. Los Estados también podrían utilizar el conjunto de herramientas para fomentar la cooperación interestatal en materia de ciberseguridad.

Derechos Digitales

Consideramos idóneo tomar desde una perspectiva de ciberseguridad las obligaciones del Estado chileno de proteger, respetar, remediar y promover derechos fundamentales en relación con el ciberespacio.

Es ideal no solamente la intervención del Estado en el fortalecimiento de los marcos de protección, sino también la participación continua en el resguardo de los derechos de las personas en otras instancias legislativas, tales como la modificación de los marcos de persecución penal, de la regulación para la protección de infraestructuras críticas, de las reglas para las actividades de inteligencia, de las políticas públicas sobre vigilancia en espacios públicos o las reglas sobre intercambios de información con fines de seguridad (u otros) entre entidades públicas.

Lo anterior está vinculado tanto a las medidas legislativas como a la implementación y ejecución de la ley, en la priorización de la actividad policial, y en la formulación de políticas de promoción de derechos fundamentales. Entendemos que hay ahí una sobreposición con una estrategia o agenda digital más amplia, pero en cualquier caso ese estímulo al uso de tecnologías para el ejercicio de derechos requiere la perspectiva de seguridad.

También está vinculado con la creciente digitalización de servicios del Estado y la ley de modernización digital. Nos parece necesario allí enfatizar las perspectivas de seguridad en torno a iniciativas para la digitalización en materias como la “identidad digital” o el despliegue de tecnologías de decisión automatizada, con múltiples aristas de seguridad tanto de la información como de los derechos de las personas.

Asociación Nacional de Informáticos Municipales

Leyes de privacidad más robustas: En nuestra experiencia, las mismas instituciones (tanto financieras como de otras naturalezas) suelen emplear colección agresiva de datos, como cookies persistentes o localización geográfica. Dichas prácticas exponen innecesariamente al usuario en casos de hackeo o intersección de tráfico, lo que hace el elaborar crímenes de phishing más fácil para los perpetradores. Muchos datos personales son fácilmente accesibles a través de una búsqueda en Google gracias a esta recolección y exposición indiscriminada de datos, como nombre completo de las víctimas, RUTs, números de teléfono personales, cuentas de redes sociales, nombres de familiares, entre otros.

En lo que respecta ya a temas de ciberseguridad dentro del estado y de las instituciones públicas, consideramos que la mayor parte del tema se reduce a la implementación generalizada y fiscalizada de buenas prácticas:

Evitar subcontratar servicios que colecten datos, almacenen, o hagan transitar información interna de las instituciones del estado a través de servidores extranjeros localizados en países con legislaturas pobres de privacidad informática, particularmente los Estados Unidos. Eso incluye compañías conocidas por colectar datos agresivamente, como Google y Microsoft.

Utilizar protocolos de comunicación implementados por el estado de forma interna, con expertos de ciberseguridad involucrados, encriptación total con keys en posesión exclusiva del estado—jamás de compañías privadas, y mucho menos extranjeras—y buenas prácticas en general, tales como el uso de consistente de canales de comunicación unificados (no saltar de correo a WhatsApp, de WhatsApp a llamada, y de llamada a correo), empleo de contraseñas robustas, y autenticación de dos factores.

Desviar el tráfico de ser necesario cuando se sabe que los datos enviados son particularmente sensibles, quizá mediante el uso de un VPN o proxy hosteado por el propio estado en servidores internos.

Instituto Milenio Fundamentos de los Datos

Sobre los derechos digitales, la protección de datos está muy relacionada y debieran ser temas muy estrechamente relacionados. Sobre el programa de capacitación básica para todos los funcionarios públicos, creemos que sería interesante revisar/mejorar protocolos existentes sobre identidad digital.

Ciberseguridad y democracia: revisar y mejorar protocolos de autenticación actuales. Publicación de datos y privacidad (e.g., MINSAL, SERVEL). La criptografía de llave

pública nos permite desde los años 70 el mostrar que uno conoce un secreto sin revelarlo.

Academia Politécnica Militar

Protección de los datos personales y de ciberseguridad Capacitación básica para todos los funcionarios públicos, hábitos de seguridad digital.

Universidad Andrés Bello

- Importante la operacionalización de las leyes que actualmente están vigentes, tal como:
    - Generar programa de capacitación para públicos y privados con certificación y habilitación con fecha de caducación para quienes realicen tratamiento de datos desarrollen sistemas que almacenen/procesen data alineación a estándares de programación segura.
    - Auditorías que muestren evidencias de mecanismos que demuestren su apego a la normativa y leyes de protección de datos, así como a estándares de programación segura que no atenten contra la confidencialidad/integridad de los datos por desconocimiento/error. Por ejemplo, evidencia de mecanismos necesarios para satisfacer el requerimiento de “derecho al olvido" o de programación segura.
- Forzar cumplimiento de estándares en proveedores de soluciones tecnológicas con acceso a datos protegidos:
    - ISO27001 - proteger la confidencialidad: encriptación - proteger la integridad de los datos: acceso a datos: auditabilidad - trazabilidad
    - MDR . IEC62443 parte 4 dicta sobre los requerimientos de desarrollo del producto y los requerimientos de seguridad técnica para los componentes que lo conforman.
- Cruzar con los lineamientos de la Política Nacional de Inteligencia Artificial que buscan regular la equidad y el derecho a la explicación de manera que no pongan en riesgo el objetivo asociado a protección de datos.
- Auditorías de "mitigación de sesgos" o “mecanismos como transparencia algorítmica" que pueden poner en riesgo la privacidad de los datos.

- Ataques a las fuentes de datos de los que aprenden sistemas basados en aprendizaje automático (envenenamiento de fuentes de datos).

CODELCO

Se recomienda generar un programa de capacitación y especialización para aquellos organismos que deban fiscalizar y sancionar la comisión de delitos informáticos o incumplimiento a la política, por ejemplo, disponer de especialistas analistas forense, peritos de ciberseguridad que puedan certificar o acreditar la comisión de un delito en el espacio cibernético.

ENAP

Reinstituir el carácter de Dato Privado de carácter Personal al Rut, restringiendo de manera progresiva dentro de un período definido y acotado, su uso en protocolos de validación, al exigir como llave de entrada tanto lógica para el ingreso a trámites en línea de servicios públicos y privados como física para el acceso presencial. En este mismo alcance, se hace necesario incluir el número de documento y la clave única, que desde hace ya bastante tiempo y a la fecha, también son solicitados e inclusive registrados y almacenados, desconociendo el nivel de resguardo de todos estos supuestos identificadores únicos. Y por cierto, no es posible dejar de mencionar la indiscriminada habilitación de aplicaciones denominadas bajo el concepto de "rutificadores" que facilitan la obtención del Rut y en ocasiones también, posibles domicilios válidos, a partir de la coincidencia de nombre y apellidos del titular de dichos datos, que sí le hacen identificable y por tanto, caen dentro del concepto de datos de carácter personal que son privados y deben ser protegidos, según lo definido en la ley N° 19.628 de Privacidad y Protección de Datos de Carácter Personal.

Hackada

Realizamos también la observación sobre el tema de apoyo a las víctimas de los diversos ataques que se mencionan en el documento, en especial al momento si la víctima es una persona natural la cual no tiene conocimiento para saber cómo asesorarse y protegerse en esta situación.

Respecto al punto de Ingeniería social el vector de ataque no siempre es digital, Ingeniería social abarca todo aspecto de la manipulación, puede ser desde una llamada de teléfono, un correo malicioso, un WhatsApp malicioso, SMS malicioso, o una persona que nos contacte en persona por ejemplo en la calle u oficina y nos engañe.

Objetivo 3: Generación de una cultura de ciberseguridad

El siguiente es el texto del objetivo:

> *Generación de una cultura de ciberseguridad: Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales*

A continuación se detallan las observaciones recibidas por los invitados respecto al objetivo C de la política. Es importante señalar que los comentarios se exponen textualmente conforme fueron recibidos; por lo que, cualquier omisión a alguna agrupación y/o comentario se debe a que no hizo referencia al objetivo específico.

Alianza Chilena de Ciberseguridad

Sugerimos que las iniciativas y medidas que se propongan en la Política referidas a la generación de una cultura de ciberseguridad contemple la participación de todos los actores del ecosistema, incluyendo a entidades tanto públicas como privadas, organizaciones de la sociedad civil, la academia e, inclusive, organismos internacionales. Un mundo globalizado e interconectado requiere de la colaboración de todos los actores, con el objeto de desplegar responsable y eficazmente los recursos tanto públicos como privados.

Por su parte, sugerimos que esta participación amplia también alcance a la generación y financiación de investigación y desarrollo en ciberseguridad, incluyendo a entidades privadas. La redacción actual de las bases de discusión podría dar a entender que esta generación y financiación de investigación sólo afectaría al sector público, en el entendido que la Política es elaborada por este.

ACTI

En un esquema lineal nos vamos a tardar demasiado, hay que generar un plan de acción out of the box para reducir el gap con iniciativas como por ejemplo: Generar profesionales o re-educar/ re-convertir profesionales a esta línea de acción (identificar profesionales más cercanos) bajo un esquema tipo NICE; Promover inmigración de profesionales; y carreras técnicas muy integradas al sector productivo.

Falta acercar este tema a la gente común, está en un ámbito tecnológico específico pero falta acercarla (democratizar) a la ciudadanía y al negocio (directorios).

Informar y generar índices de niveles de madurez (CIS/NIST) gastos e inversión que sirvan de guía para las distintas organizaciones, verticales y tamaños de empresas.

Debe ser armónico con la hoja de ruta en los ámbitos “talentos y competencias en ciberseguridad” y “cultura ciberseguridad”

Fundación País Digital

Queremos hacer énfasis en la educación en ciberseguridad. La formación de capital avanzado es complejo en el mundo. El desafío es cómo enseñar ciberseguridad; no vemos reflejado este punto en el borrador. En otros países vemos elementos de formación transversales.

Fundación Whilolab

Apuntan a un vacío de educación en ciberseguridad. No existen iniciativas públicas de educación de ciberseguridad. Esto debe estar presente en la PNCS v2.

Se propone el salir con publicidad en todas las pequeñas pantallas que existen en lugares pequeños: centros de atención primaria de salud, municipalidades, etc. Para esto hay que generar material que sea difundible. Se propone educar a los imputados en las cárceles en ciberseguridad.

Derechos Digitales

Se menciona un plan de concientización nacional sobre ciberseguridad y privacidad. Parece una medida demasiado concreta considerando que la política anterior incluía en términos más amplios la concientización y desconocemos si ese proceso es evaluado favorablemente. Además debemos considerar el rol de distintos órganos, incluida la eventual Agencia de Protección de Datos.

En el segundo punto hay dos objetivos distintos. Uno está relacionado con la mejora de la educación formal en sus distintos niveles en relación con “higiene digital y ciberseguridad”, y el otro se refiere a la generación de carreras. Ese punto merece separarse, como también abordar cuál es el panorama actual de la formación en ciberseguridad.

Asociación Nacional de Informáticos Municipales

- Intervención en las instituciones financieras:
    - Suponiendo que la mayoría de los casos de phishing se dan en la forma de fraudes bancarios, particularmente colectando contraseñas de los usuarios mediante mensajes de texto, whatsapps, redes sociales, y links fraudulentos. Capacitar a los usuarios es algo que pareciera ya estar haciendo, pero consideramos el educar a todos en ciberseguridad una

visión idealista; muchas personas pueden no estar interesadas en asumir la responsabilidad de tomar medidas de protección personal de carácter informático, o son personas de tercera edad cuya capacidad de adquirir dichos conocimientos es limitada. El estado debería acercarse a las instituciones bancarias del país, e incentivar o responsabilizar legalmente a dichas entidades para implementar medidas de seguridad más robustas. Sin ir más lejos, la mayoría de los bancos que operan en el país, no ofrecen autenticación de dos factores, y no permiten usar contraseñas de más de 8 caracteres tampoco.

- Importancia de la educación:
    - Importancia de incluir en los planes de estudio transversalmente la educación en ciberseguridad. No solo en temas técnicos y de fraude, sino también en ciberbullying, grooming, y otros riesgos similares.
    - Abordar la ciberseguridad también en la educación no formal. Talleres, mentorías y otros. Aquí abarcamos todos los grupos etarios.
    - La mesa plantea que los planes de estudio transversalmente se tienen que incluir la educación en Ciberseguridad desde primer ciclo básico, incluso antes y llegar a básica, media y superior, en tal planteamiento podemos agregar que no debe ser solamente en lo técnico, sino que tiene que incluir trabajos en responsabilidad comunitaria y conciencia/educación cívica. Pero no hay que olvidar que también hay una educación no formal y que justamente son los municipios quienes más la generan, con talleres y monitorias de toda índole, por ejemplo alfabetización digital para adultos mayores prácticamente en todos los municipales se hacen, se hacen también para aquellas personas que no terminaron su educación media, hay reforzamiento de asignaturas formales, preuniversitarios, deportivos y muchos otros que siempre son gratuitos por lo que tienen alta convocatoria. Entonces, ahí es donde la educación no formal podría ser un aporte a la ciberseguridad se podría incluir como módulo más dentro de esta amplia gama de oferta de educación no formal que actualmente existe. Hay que considerar que esa educación no formal abarca todos los grupos etarios y también heterogéneos: niños, adultos mayores, mujeres trabajadoras temporeras, etc., todos los años se ejecutan, por lo tanto, puede ser un aporte a la ciberseguridad y hasta ahora no se ha considerado dentro de la política.

Instituto Milenio Fundamentos de los Datos

En la generación de cultura, para los días que corren, debería ser un plan de conciencia nacional sobre el mundo digital. Sugieren fuertemente incluir dentro del plan matriz formación sobre datos.

Atracción y retención de talento.

- Plan de toma de conciencia nacional sobre ciberseguridad y privacidad para la población [sobre el mundo digital]
- Plan matriz de "higiene digital y ciberseguridad" para todos los niveles del sistema educativo [especialmente datos]
- Generar y financiar I+D en ciberseguridad

Academia Politécnica Militar

- En el objetivo N°3, Generar e implementar un Plan Matriz, como Academia Politécnica Militar nos parece interesante estar incorporados en el Plan Matriz para el sistema de enseñanza superior de las FFAA.
- En el objetivo N°3, dice: Generar y financiar I+D en CS, como Academia Politécnica Militar nos parece interesante incorporarnos a estos círculos virtuosos para potenciar la investigación en CS.
- Generar e implementar un plan matriz...enseñanza media-técnico- profesional y superior.
- Generar I + D en ciberseguridad... círculos virtuosos entre la academia, la industria y el sector público.

Universidad Andrés Bello

Considerar modelos internacionales respecto del tipo de profesional en el área de ciberseguridad - Enisa[1] publicó el 19 de septiembre del 2022 el marco de trabajo para definir las habilidades necesarias para los diferentes perfiles que son necesarias tanto para la investigación como para otras habilidades.

[1] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

CODELCO

- Se sugiere incorporar la generación de una cultura de ciberseguridad o Incorporar el concepto de prevención y generación de cultura de ciberseguridad desde edad pre-escolar incluyendo a profesores, padres y/o cuidadores en este programa de concientización.
- Se sugiere generar programas de concientización desde edades tempranas con foco en crear una cultura de ciberhigiene.
- Se sugiere generar canales de apoyo para víctima de ciberdelitos (sextorsión, suplantación de identidad, entre otros)
- Se recomienda fomentar la generación y creación de carreras que cubran los aspectos de ciberseguridad OT, para proporcionar talento a aquellas organizaciones que utilizan sistemas de control industrial y automatización.

ENAP

Dentro del contexto del Mes de la Ciberseguridad, instituir actividades formales de formación y concientización a la comunidad, estratificados por grupos etarios, por ejemplo, a través de programas comunales organizados por las Municipalidades, que incluyan no sólo los conceptos de riesgos cibernéticos en toda su magnitud (Ingeniería Social, Grooming, Bullying, Sexting, etc.), sino que también, impartan los conocimientos necesarios para prevenirlos, abordando la ciber-higiene y la ciber-ética.

Por otra parte, se sugiere agregar dentro de los objetivos de cultura y obtención de información, la desinformación, como es el caso de las Fake News que podrían ser utilizadas, por ejemplo para generar un descontento masivo que redunde en una inestabilidad social y económica con una amenaza híbrida, que lleve a la desconfianza en las instituciones, mediante la perjudicial aplicación de inteligencia artificial para emitir falsos videos usando la imagen de figuras referentes para fundar credibilidad y movilización hacia pendencias.

Adicionalmente, se propone analizar la determinación de sanciones y reconocimientos, según el actuar diligente de las empresas públicas y privadas, en el contexto de la ciberseguridad, por ejemplo, ante la oportuna notificación de incidentes, la colaboración inter-empresas para prevenir la propagación de malware, entre otras.

Hackada

En Cultura en Ciberseguridad se comentó que podría existir la posibilidad de agregar asignaturas en educación media y superior enfocadas en Ciberseguridad para que los alumnos tengan conciencia de los posibles vectores de ataque y vulnerabilidades que puedan existir en nuestro día a día, tales como estafas por redes sociales, extorsión, fraudes, entre otros. Además, se comentó que podría culturizarse a padres, apoderados y a la tercera edad en temas de ciberseguridad con el mismo fin de lo mencionado anteriormente.

Departamento de Ciencias de la Computación de la Universidad de Chile

Se sugiere potenciar la existencia de becas para estudiantes de educación superior en áreas técnicas o profesionales (relacionadas a ingeniería) en el área de ciberseguridad, aunque también se recomienda considerar áreas afines (periodismo, derecho, etc) si siguen temáticas relevantes a ciberseguridad.

Potenciar la educación en programación para estudiantes en etapa escolar, focalizando en capacitación efectiva de docentes en programación en general, y ciberseguridad, en particular.

Objetivo 4: Cooperación y coordinación nacional e internacional

El texto del objetivo es el siguiente:

> *Cooperación y coordinación nacional e internacional: El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales*

A continuación se detallan las observaciones recibidas por los invitados respecto al objetivo D de la política. Es importante señalar que los comentarios se exponen textualmente conforme fueron recibidos; por lo que, cualquier omisión a alguna agrupación y/o comentario se debe a que no hizo referencia al objetivo específico.

Alianza Chilena de Ciberseguridad

Especialmente, consideramos relevante que la Política contemple espacios permanentes de compartición de información entre el sector público y privado, y fomente el diálogo y la correlación de esfuerzos dentro del sector privado, permitiendo que de esta forma la relación entre este y el sector público se realice a través de puntos únicos de contacto eficientes y eficaces, y plataformas abiertas de transparencia de iniciativas y medidas tanto públicas como privadas que puedan ser robustecidas o

replicadas por actores interesados. En la misma línea, sugerimos en específico que se promueva adicional y complementariamente la adopción de acuerdos reconocidos regulatoriamente entre el sector privado y público para compartir información, conocimientos y experiencias resguardando la confidencialidad para los participantes.

En el ámbito internacional, sugerimos que se tomen en consideración los avances alcanzados a través del Acuerdo de Asociación de Economía Digital "DEPA" entre Chile, Nueva Zelanda y Singapur, en materia de ciberseguridad. Además, recomendamos que las menciones a países específicos se realicen responsablemente. Por ejemplo, según el más reciente Cybersecurity index (ITU) y el NCSI, existen otros países mejor posicionados (Alemania, España, entre otros) en materia de ciberseguridad, y por ello por lo que sugerimos que los esfuerzos que la Política en cooperación internacional estén centrados y justificados en este tipo de países.

Sugerimos que, en materia de una política internacional de ciberseguridad, como la mandatada por la Política de 2017-2022, y una política o medidas de ciberdefensa, se tome en consideración el desarrollo de iniciativas estratégicas o diplomáticas asociadas a ciberdefensa y se evite, en aquel sentido, que estas herramientas de ciberdefensa mantengan artificialmente un entorno o sistemas inseguros para los ciudadanos que vulneren sus derechos.

Finalmente, sugerimos que se mencione entre las medidas a ser adoptadas las normas internacionales ampliamente aceptadas en la industria de ciberseguridad, tales como la serie ISO 27000, de manera de bien referenciar los esfuerzos, tanto gubernamentales, de empresas privadas y sobre todo de las PYMES.

ACTI

Potenciar la implementación de aspectos concretos de los acuerdos internacionales a través del intercambio concreto. Es decir, se observa un avance importante en la firma de acuerdos, pero esto no necesariamente se ha traducido en aspectos concretos de intercambio de información de amenazas, de vulnerabilidades, mejores prácticas, tecnologías.

Mejorar la coordinación de todos los actores público, privado, academia.

Fundación País Digital

Experiencia comparada. Resulta relevante basarnos en las mejores experiencias actualmente vigentes. Podríamos tomar como referencia el Global Cybersecurity Index de la ITU y seguir ejemplos como el de España o Alemania, que se encuentran bien posicionados.

Fundación Sochisi

Podría sortear las tensiones interinstitucionales qué se dan a partir de la defensa de la nación con intereses de seguridad pública. En este sentido hay trabajos del Parlamento Europeo que atienden el tema de forma más profunda.

Red de Mujeres de Alta Dirección

Ciberseguridad y enfoque de género: marco internacional

- En UNIDIR, la institución autónoma dentro de ONU que realiza investigaciones sobre desarme y cuestiones de seguridad internacional, se anida el Grupo de Trabajo de Composición Abierta (OEWG) que propone que la igualdad de género y la participación significativa de las mujeres deberían estar en el centro de la paz y la seguridad internacionales en el ciberespacio.

- Varias delegaciones que participan en el Grupo de trabajo de composición abierta (OEWG) de las Naciones Unidas sobre desarrollos en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional han declarado la necesidad de incorporar la perspectiva de género en la implementación de normas cibernéticas y la creación de capacidad sensible al género, así como una mejor comprensión de los vínculos entre la ciberseguridad y los marcos de igualdad de género.

- La subrepresentación de las mujeres en estas áreas refuerza los sesgos existentes y amenaza la igualdad de género en la seguridad cibernética. Lograr la igualdad de género en 'salas de reuniones' puede resultar insuficiente, si no hay apoyo para las aspiraciones de las mujeres para trabajos científicos en laboratorios o "detrás de una pantalla".La Unión Internacional de Telecomunicaciones (ITU) creó un Grupo de Experto de Mujeres para Estandarización como parte de sus esfuerzos para alcanzar el Objetivo de Desarrollo Sostenible de la ONU (ODS) número 5 sobre igualdad de género y empoderamiento de la mujer.

Derechos Digitales

Falta: Coordinación y coherencia interna para no impulsar cambios legislativos contrarios a lo que la ciberseguridad demanda.

Falta: Mención explícita a la forma en que se desarrollan posturas nacionales de política exterior, relacionada íntimamente con parte del diagnóstico, y donde también la participación multisectorial es útil.

Falta: Hacer explícita la forma de coordinación y coherencia gubernamental para las posturas de Chile en foros internacionales como:

- El (segundo) Grupo de trabajo de composición abierta sobre la seguridad en el uso de las tecnologías de la información y las comunicaciones en la Primera Comisión de la ONU.
- El Comité Especial encargado de elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos.
- La participación en foros diplomáticos como la Freedom Online Coalition no debiera encontrar puntos de disenso o de falta de mutua comprensión con las representaciones en otros foros como la Unión Internacional de Telecomunicaciones.

Academia Politécnica Militar

El objetivo N°4 dice; "Generar instancias de colaboración públicas...en educación..., sin embargo, no queda explícito como retendrán el talento. Este es un problema actual en las instituciones de las FFAA.

- Reportar las IP, las iniciativas desarrolladas en ciberseguridad a la institucionalidad existente.
- Establecer relaciones de cooperación con ciberseguridad en países avanzados.

Universidad Andrés Bello

- Considerar posicionar a Chile como líder latinoamericano en las 5 dimensiones del CMM de Oxford.
- Considerar un organismo coordinador de la red de centros de investigación, de escalamiento, de difusión que monitorea y ayuda al cumplimiento de la Política nacional de ciberseguridad y se coordina con diferentes organismos del Estado para facilitar el avance de la investigación en ciberseguridad en Chile a favor de los diferentes estamentos del País, incluido las faltas de capacidades humanas en materia de investigación avanzada en ciberseguridad.
- Considerar Foro Nacional de Ciberseguridad que fortalezca a Chile en el círculo de difusión/colaboración internacional de investigación en temas de ciberseguridad permitiendo que realice Intercambio de experiencias con otros países en materia de ciberseguridad, con énfasis en la implementación y

evaluación de estrategias y políticas, con grupos de trabajo en investigación avanzada con colaboración internacional.

CODELCO

Se sugiere fomentar la reportabilidad de incidentes entre entidades internacionales, que permitan tomar medidas preventivas frente a formas de ataques ya materializadas en otros países.

ENAP

Establecer acuerdos de colaboración con instituciones internacionales, a partir de la definición de programas de pasantía, que fomenten el intercambio de nuevos profesionales próximos a iniciarse en el campo laboral de la ciberseguridad, para que desarrollen actividades laborales en entidades internacionales con un mayor nivel de madurez en dicho contexto, donde puedan adquirir nuevos conocimientos y por sobre todo aprender de su experiencia en el desempeño de tareas propias de los distintos perfiles de ciberseguridad requeridos, tanto para la gestión como para la operación, en lo que se refiere a la implementación de un sistema de gestión de seguridad de la información y ciberseguridad.

Objetivo 5: Fomento a la industria de ciberseguridad

El siguiente es el texto del objetivo:

> *Fomento a la industria de ciberseguridad: El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos*

A continuación se detallan las observaciones recibidas por los invitados respecto al objetivo E de la política. Es importante señalar que los comentarios se exponen textualmente conforme fueron recibidos; por lo que, cualquier omisión a alguna agrupación y/o comentario se debe a que no hizo referencia al objetivo específico.

Alianza Chilena de Ciberseguridad

Sugerimos que entre las medidas a ser propuestas en la Política se consideren y establezcan roles específicos para las entidades que participan de la industria de ciberseguridad. Especialmente, y siguiendo las mejores prácticas internacionales, recomendamos fomentar que la industria participe en la implementación de la futura ley marco sobre ciberseguridad, a través del reconocimiento de mecanismos o herramientas que inviten a los sujetos regulados al compliance regulatorio.

Además, recomendamos que explícitamente se fomente el desarrollo y la mantención de sistemas o softwares seguros, a través de incentivos económicos, tributarios, de compliance o regulatorios, para incentivar que la industria busque producir software y sistemas con cada vez menos vulnerabilidades, traduciendo lo anterior en entornos más seguros para los ciudadanos y el ejercicio legítimo de sus derechos.

ACTI

- Incorporar los conceptos de IOT y Nube al ecosistema.
- Promover la compra de servicios de seguridad con componentes locales
- Desarrollar convenios marco para servicios de ciberseguridad
- Vincular la industria local con Ministerio de Interior y Ministerio de Defensa

Fundación País Digital

Reconocimiento expreso del principio de neutralidad tecnológica, puesto que ha sido uno de los pilares fundamentales en el desarrollo del ecosistema digital y es imprescindible su vigencia y aseguramiento en temas de ciberseguridad.

Formación de capital humano avanzado. Debemos avanzar en este aspecto para soportar las necesidades de la industria y para convertir a Chile en un exportador de servicios.

Creación de instituciones que impulsen la investigación y desarrollo en ciberseguridad.

Derechos Digitales

Está bien. Innova en relación a la instalación de industrias extranjeras.

Deja fuera la demanda del sector público como fuente de estímulo a la industria nacional

Asociación Nacional de Informáticos Municipales

Recursos: Capital humano, político, tecnológico y financiero.

- Lo más complejo para abordar este tipo de proyectos es no contar con una institucionalidad interna para abordar estos temas.
- Dependencia del criterio político del momento.

- Falta de RR.HH. Experto, falta de capacitación y de concientización.
- Requerimiento de Recursos focalizados

Instituto Milenio Fundamentos de los Datos

Los Fondecyt son proyectos de boutique, y por tanto están absolutamente alejados de la realidad.

Se plantea el problema de cómo se deciden los proyectos a los que se asignan recursos (Fondef, Fondecyt, etc.) Se aclara desde ciencia que ninguno de los proyectos son revisados internamente, todos tienen revisores externos. → ¿Cómo conectamos los problemas que identifica el Estado con lo que quiera investigar la academia? No tenemos un músculo de identificación de problemas, como existe también en la UE.

La PNCS puede funcionar como un generador de incentivos para los temas de I+D en ciberseguridad.

Academia Politécnica Militar

El objetivo N°5 dice: "Crear institutos de transferencia tecnológica…en materias de CS…que realicen investigación aplicada…en necesidades que tenga la industria y el sector público, como Academia tenemos previsto hacerlo con las FFAA (Empresas Estratégicas de Defensa), sin embargo es interesante como Ejército recibir y entregar transferencia tecnológica a estos institutos civiles.

Crear institutos de transferencia tecnológica entre la industria y la academia en materias de ciberseguridad que realicen investigación aplicada en aquellas necesidades que tenga la industria.

Universidad Andrés Bello

Considerar Posicionar a Chile como líder latinoamericano en las 5 dimensiones del CMM de Oxford.

Considerar un organismo coordinador de la red de centros de investigación de:

- Infraestructura compartida nacional que permita investigar desarrollar y probar algoritmos/modelos/productos del segmento ciberseguridad para diferentes Industrias optimizando recursos.
- Tal como lo realizado para 5G considerar Centro de escalamiento y nuevos negocios en torno a resultados de investigación en ciberseguridad. Mecanismo

para facilitar el desarrollo de la industria de productos y servicios de base científica-tecnológica en el área de ciberseguridad en Chile que ayude a posicionar al País en innovación, la investigación aplicada y el desarrollo tecnológico en ciberseguridad Potenciando la Investigación aplicada en Chile.

Para posicionar a Chile acorde al modelo de Oxford se recomienda considerar lo siguiente:

- Para alcanzar el nivel de madurez “establecido” a 4 años en materias de investigación avanzada en ciberseguridad, la estrategia nacional de ciberseguridad y el plan operativo debe indicar explícitamente y estar en operación lo siguiente:
    1. actividades de investigación que deben realizarse en el País,
    2. los recursos y procesos requeridos para realizar las actividades de investigación en ciberseguridad,
    3. las fuentes de financiamiento adecuadas para realizar estas actividades,
    4. los actores regionales e internacionales con los que se realice investigación además de mostrar evidencia de redes de colaboración regional/internacional con prácticas y desarrollos,
    5. las métricas y sus valores que permiten medir el rendimiento de las acciones de investigación en ciberseguridad y cómo se ha progresado.
- Para alcanzar un nivel de madurez “estratégico” a 8 años se requieren ya establecidas y en funcionamiento con mediciones de progreso lo siguiente:
    1. las comunidades alrededor de las áreas prioritarias de investigación en ciberseguridad
    2. evidencia de que el apartado en I+D de la estrategia nacional en ciberseguridad está funcionando completamente
    3. los aportes de financiamiento para contribuir a la I+D en ciberseguridad
    4. los consorcios internacionales de I+D e inversión para construir capacidades de innovación en materias de investigación en ciberseguridad.

5. los riesgos emergentes en ciberseguridad que están siendo abordados, mostrando evidencia de que son regularmente medidos y usados para actualizar la estrategia nacional y en particular el apartado de programas de investigación en ciberseguridad.

- Para alcanzar un nivel de madurez "dinámico" a 12 años en materias de investigación en ciberseguridad, deben existir evidencias

    1. en los rankings relevantes de que Chile está en el cuadrante de líder en investigación e innovación en ciberseguridad.
    2. de los debates internacionales en los que Chile está aportando en el desarrollo de los planes estratégicos regionales de I+D en ciberseguridad.
    3. de una unidad de observación que identifique los problemas emergentes alrededor de nuevos tipos de tecnología o amenaza
    4. de actividades I+D para prepararse a amenazas futuras.
    5. de generación de las mejores prácticas en I+D en ciberseguridad.

Fuentes tomadas del CCMM de Oxford.

CODELCO

- Se recomienda fomentar la incorporación y desarrollo de proveedores de ciberseguridad con el foco OT (tecnologías de la operación) para que puedan atender a aquellas industrias donde en su core de negocio utilicen tecnologías de control industrial y sistemas de automatización industrial.
- Se sugiere evaluar la homologación y cumplimiento de estándares de seguridad de la información y ciberseguridad internacionales, al igual que marcos de trabajo probados para diversas industrias.

ENAP

Definir y ofrecer algunos beneficios, por ejemplo incentivos tributarios a aquellas empresas de servicios de ciberseguridad, que realicen contribución directa y tangible a la mejora de la ciberseguridad en las Pymes, considerando que éstas no cuentan con suficientes recursos que les permita hacerse cargo de la materia, aun cuando frecuentemente son parte fundamental de la Cadena de Suministros para Grandes Empresas, que a pesar de contar con mecanismos de protección ante ciberataques, llegan a verse expuestas por las vulnerabilidades de sus proveedores, habiendo casos

mundialmente conocidos de impacto considerable a prestigiosas empresas de renombre internacional, a propósito de haber utilizado como vector de ataque a uno de sus “pequeños proveedores”.

Hackada

Se comentó la posibilidad de revisar una alternativa para los investigadores de descubrimiento de vulnerabilidades, que el gobierno pudiese generar algún plan para los investigadores y trabajara en conjunto con ellos para que no todos los descubrimientos se consideren un delito, que si se encuentran aprobados por el gobierno se puedan realizar, además que el gobierno se beneficiaría con la seguridad de sus sistemas al descubrir brechas que poseen. También evaluar la posibilidad de tener un catastro de todos los investigadores que quisieran apoyar en el descubrimiento de vulnerabilidades.

Departamento de Ciencias de la Computación de la Universidad de Chile

Mejorar los incentivos para investigación, vía fondos Fondecyt, Fondef, o similares, focalizados en el área ciberseguridad.

Anexos

- [ ] Minuta de observaciones “Asociación Chilena de Tecnologías de la Información”
- [ ] Minuta de observaciones “Alianza Chilena por la Ciberseguridad”
- [ ] Minuta de observaciones “Fundación País Digital”
- [ ] Minuta de observaciones “Red de Mujeres Alta Dirección”
- [ ] Minuta de observaciones “Asociación Nacional de Informáticos”
- [ ] Minuta de observaciones “Derechos Digitales”
- [ ] Minuta de observaciones “Academia Politécnica Militar”
- [ ] Minuta de observaciones “Universidad Andrés Bello”
- [ ] Minuta de observaciones “Centro Nacional de Sistemas de Información en Salud “CENS””
- [ ] Minuta de observaciones “Instituto Milenio”
- [ ] Minuta de observaciones “Codelco”
- [ ] Minuta de observaciones “Empresa Nacional del Petróleo “ENAP””
- [ ] Minuta de observaciones “HACKADA”
- [ ] Informe consultoría de género “Propuesta de acciones para fortalecer el enfoque de género PNCS”