Red de Núcleos de Investigación Aplicada en Ciberseguridad: ciencia aplicada para la seguridad digital

1 | Objetivo

Incentivar la investigación nacional en materia de ciberseguridad aplicada, promoviendo la formación de una industria nacional con base científica y con la capacidad de proteger a personas e instituciones de ataques cibernéticos de diversa índole.

2 | Metas

- Para el año 2027, se proyecta la convocatoria a grupos y comunidades de investigación en ciberseguridad, a nivel nacional, a integrar los Núcleos de trabajo.
- Para el año 2030, la Red nutrirá a empresas nacionales de contenidos y directrices en materia de ciberseguridad. Además, elaborará insumos que informarán la toma de decisiones de política pública en torno a la materia señalada.
- Para el año señalado, de conformidad con el Modelo de Madurez de Capacidades de Ciberseguridad para Naciones (CMM), se proyecta el avance del país hacia la etapa 4 de avance en relación con la tercera dimensión del Modelo (Educación, Capacitación y Habilidades en Ciberseguridad).

3 | Métricas

- Identificar grupos y comunidades de investigación en ciberseguridad a nivel regional y nacional.
- Establecer convenios de cooperación entre el Ministerio de Ciencia y Tecnología, la Agencia Nacional de Ciberseguridad y las universidades que alojarán los Núcleos, para la ejecución de la propuesta.
- Definir estructura orgánica de la Red, estableciendo objetivos específicos, dinámicas de trabajo y espacios de encuentro y trabajo colaborativo entre los Núcleos que la integren.
- Recoger necesidades en materia de ciberseguridad que presenten empresas e instituciones privadas y estatales, con el fin de socializarlas con la Red.

4 | Contexto

El panorama actual en materia de nuevas tecnologías se caracteriza por su rápida y constante evolución. El surgimiento en los últimos años de fenómenos como la computación cuántica, la inteligencia artificial, la automatización de procesos críticos de gestión, entre muchos otros, da cuenta de la acelerada expansión y masificación de las tecnologías de información, hecho que implica una doble dimensión de análisis: por un lado, la posibilidad de facilitar las tareas de la vida diaria; por otro lado, nuevos riesgos y amenazas para la seguridad de la población.

Este último punto está directamente relacionado con la cada vez mayor presencia de la tecnología en el diario vivir de las personas, lo que va de la mano con la mayor vulnerabilidad de estas. Esto se ha manifestado en el altísimo número de intentos de ataque cibernético registrados en Chile: solo en el 2023, FortiGuard Labs informaba de más de 6.000 millones

de intentos de ataques (FORBES Chile, 2024), mismos que se han vuelto progresivamente más dirigidos y sofisticados.

En este escenario, la ciberseguridad se ha convertido en una de las prioridades de la agenda pública en torno a la seguridad. En esa línea, la actual Administración ha logrado avances significativos en la materia, como lo fue el lanzamiento de la Política Nacional de Ciberseguridad 2023-2028 y la creación de la Agencia Nacional de Ciberseguridad. Sin embargo, organismos e instrumentos internacionales han hecho ver que **aún existen áreas relacionadas a la cibe**rseguridad con muy escaso –o incluso nulo— desarrollo a nivel nacional. Entre ellos, por ejemplo, el *National Cyber Security Index* ha destacado la protección de infraestructura crítica digital, el manejo de crisis ante ataques cibernéticos y la investigación y desarrollo en ciberseguridad.

Respecto al último ejemplo, es relevante precisar qué entendemos por investigación y desarrollo en ciberseguridad. Al respecto, el Modelo de Madurez de Capacidades de Ciberseguridad para Naciones (CMM, por sus siglas en inglés) aborda el concepto en su factor NºD3.4, denominado "investigación e innovación en ciberseguridad", el que consiste en la "capacidad de una nación para llevar a cabo investigaciones avanzadas y promover la innovación en el campo de la ciberseguridad" (Ministerio de Ciencia, Tecnología, Fomento e Innovación; 2024). En este sentido, es posible concluir que el indicador no sólo da cuenta de una necesidad de avanzar en políticas públicas relacionadas con la investigación propiamente tal, sino que se requiere conectar a investigadores con las necesidades de la industria nacional, de modo tal de construir productos y servicios de base científico-tecnológica que permitan traer más desarrollo al país en general.

En este sentido, es relevante precisar que uno de los objetivos centrales de la Política Nacional de Seguridad corresponde al "fomento de la industria e investigación científica". Esto, con el subobjetivo de "focalizar la investigación aplicada respecto a aquellos problemas y necesidades de ciberseguridad tanto del sector público como privado" (Comité Interministerial de Ciberseguridad, 2023, p. 19). El presente instrumento de transformación viene a proponer una alternativa para concretar dicho objetivo, para así continuar con la expansión y profundización de políticas públicas en ciberseguridad llevadas a cabo por el gobierno.

5 | Intervención

En relación al contexto expuesto, se propone la creación de una Red de Núcleos de Investigación Aplicada en Ciberseguridad, dependiente de la Agencia Nacional de Seguridad, con el objetivo de articular a los grupos y comunidades que actualmente desarrollan investigación en ciberseguridad a nivel nacional. Esto, para conectarlos con las necesidades de la industria, tanto por parte de empresas privadas como estatales. Para su organización, se sugiere la siguiente estructura orgánica.

Los Núcleos se constituirán físicamente en universidades del país, a lo largo de todo el territorio nacional, luego del establecimiento de los correspondientes acuerdos de cooperación con las mismas. Se sugiere la definición, en primera instancia, de un Núcleo por región, los que tendrán la responsabilidad de llevar a cabo investigaciones y elaborar insumos en temáticas de ciberseguridad, aplicadas al mundo empresarial.

Cada uno de ellos se encargará de elegir entre sus integrantes a una Mesa Directiva, compuesta por cargos de presidencia, vicepresidencia y secretario o secretaria, la que se encargará de presidir reuniones periódicas del Núcleo, y registrar los acuerdos, problemáticas y necesidades que se releven en las mismas. Además, tendrá la responsabilidad de hacer llegar a los y las integrantes de cada Núcleo las conclusiones a las que se arribe en instancias superiores de debate, así como las comunicaciones que reciban por parte de otros miembros de la Red.

Dichas instancias superiores de debate corresponderán a Consejos Nacionales, que reunirán a todas las presidencias de los Núcleos de la Red en un espacio de diálogo, presidido por el director o directora de la Agencia Nacional de Seguridad. En estas instancias, se socializarán los avances y requerimientos de cada Núcleo, tanto respecto a sus investigaciones específicas, como a necesidades generales que cada uno detecte respecto a su trabajo. En adición a ello, se definirán planes de trabajo colaborativo entre los Núcleos y entre la Red y otras instituciones. Por último, se gestionará la elaboración de informes a solicitud de instituciones del Estado, respecto a temas de ciberseguridad, así como la formulación de recomendaciones de políticas públicas en la materia.

Por último, se propone que el financiamiento de la iniciativa descrita se concrete a través de un porcentaje del presupuesto asignado anualmente a la Agencia Nacional de Ciberseguridad.

6 | Resultados e impacto esperado

Se propone la entrada en funcionamiento de la Red para el año 2027. Para dicha fecha, se espera la convocatoria nacional para integrar los Núcleos de Trabajo. Ya para el año 2030, se proyecta que el trabajo de la Red incida directamente en la formulación de políticas públicas relevantes en torno a ciberseguridad, tanto elaborando informes para ello, como por medio del análisis de los resultados de sus investigaciones.

Con lo anterior, se espera que Chile continúe escalando en los índices internacionales sobre ciberseguridad, como ha sido la tendencia en los últimos años. Pero no solo eso: con la iniciativa descrita, se busca sentar las bases para una industria nacional en torno a la ciberseguridad, con una fuerte base científica, que permita situar al país en el escenario latinoamericano y mundial como un agente competitivo en la generación de conocimiento y tecnología de ciberseguridad.

Las cifras y proyecciones de expertos dan cuenta de la importancia del mercado de la ciberseguridad para el país. De hecho, se estima que la industria de la ciberseguridad en Chile genera ventas de alrededor de 350 millones de dólares al año (Comité Interministerial sobre Ciberseguridad, 2023). El instrumento de transformación propuesto iría en directo beneficio de aquello, al permitir proteger a la industria nacional de amenazas cibernéticas y al mismo tiempo dotándolas de los conocimientos técnicos necesarios para ofrecer productos con base científica. Así, la propuesta se traduciría en mayor desarrollo económico y científico para el país.

7 | Desafíos

En el proceso de concebir la implementación de la presente propuesta, se identifican dos desafíos fundamentales a los que podría enfrentarse: (1) el riesgo de complejizar aún más

la relación entre el Estado y la comunidad científica nacional, y (2) la dificultad para conseguir recursos que permitan financiar la iniciativa.

El primer desafío encuentra su origen en lo que académicos han calificado como la "crisis de la ciencia en Chile" (Lavandero, 2025). Hechos como los importantes recortes de presupuesto a programas de ciencia, tecnología, conocimiento e innovación en el país y la falta de incidencia académica en la planificación y toma de decisiones al respecto, permiten concluir que la situación actual para los y las investigadoras científicas es compleja, al no contar con apoyo efectivo y concreto de parte de la Administración. Al respecto, la Red de Núcleos debe ser considerada como una oportunidad de mejoras concretas, en dos dimensiones: primero, distribuir recursos directamente a proyectos de investigación y segundo, de contar con un canal directo de comunicación con las autoridades de gobierno encargadas de ciencia.

El segundo desafío, en torno a la necesidad de financiamiento económico de la Red, debe ser resuelto en las etapas de discusión correspondientes, en el marco de la definición del presupuesto anual de la Agencia Nacional de Ciberseguridad.

8 | Proyecciones

La necesidad de ciberseguridad es un imperativo que llegó para quedarse. El acelerado crecimiento y expansión de las tecnologías de la información se vincula estrechamente con la cada vez mayor dependencia de las personas a las mismas, y con justa razón: el ciberespacio es una dimensión fundamental de la vida diaria de la población. Esto trae consecuencias positivas relevantes, pero también nuevos riesgos y amenazas a la seguridad.

Gobiernos anteriores iniciaron la inserción de la ciberseguridad como una prioridad nacional, creando las primeras políticas nacionales de ciberseguridad. La actual Administración ha seguido el mismo camino, con avances técnicos y de gestión relevantes en la materia. Sin embargo, la investigación y el desarrollo sigue siendo un flanco abierto entre los avances señalados, lo que invita a idear estrategias que permitan vincular y aterrizar ambos conceptos. En este escenario, se propone la creación de la Red de Núcleos de Investigación aplicada en Ciberseguridad, como una forma de promover la articulación de la investigación ya existente en el país y su vinculación con las empresas del país.

Más allá de los desafíos que puede presentar la propuesta, esta representa una posibilidad de concertar objetivos definidos desde hace años por las autoridades del país: el fomento de la investigación focalizada en la necesidad de la industria, para así promover la industria nacional. Y es que la investigación es una oportunidad para la innovación, a nivel general. Y entre todos los desafíos que enfrenta el país a la fecha, la seguridad es quizás el que más requiere ser abordado así: ante su naturaleza, debe enfrentarse con originalidad. Fortalecer la investigación nacional es fundamental para ello.

9 | Bibliografía

Chile. Comité Interministerial sobre Ciberseguridad (2023). Política Nacional de Ciberseguridad 2023-2028. Disponible en: https://anci.gob.cl/documents/4430/Pol%C3%ADtica_Nacional_de_Ciberseguridad_2023-2028.pdf

Chile, Ministerio de Ciencia, Tecnología, Fomento e Innovación. (2024). Informe I+D en Ciberseguridad. Disponible en: https://api.observa.minciencia.gob.cl/api/datosabiertos/download/?uuid=2f7b883f-c8e8-4b05-999a-12f0486f24d9&filename=2024-ChileCybersecurityLandscape_vf.pdf

FORBES Staff. (2024). Chile registró 6.000 millones de intentos de ciberataques en 2023: menos que 2022 pero más sofisticados. FORBES Chile. Disponible en: https://forbes.cl/tecnologia/2024-03-25/chile-registro-6-000-millones-de-intentos-de-ciberataques-en-2023-menos-que-2022-pero-mas-sofisticados.

National Cybersecurity Index (2024). Chile. Disponible en: https://ncsi.ega.ee/country/cl/

Lavandero, S. (2025). Crisis de la ciencia en Chile: balance 2024 y desafíos para el 2025. La Tercera. Disponible en: https://uchile.cl/noticias/224243/crisis-de-la-ciencia-en-chile-balance-2024-y-desafios-para-el-2025