Muy buenas tardes a todos y todas,

Quiero darles la bienvenida al Primer Balance Anual de la Agencia Nacional de Ciberseguridad, saludando especialmente a la subsecretaria de Prevención del Delito, Carolina Leitao; señora Johana Álvarez Superintendenta de Insolvencia y Reemprendimiento al jefe nacional del Cibercrimen de la Policía de Investigaciones de Chile, señor Marcelo Wong; al coronel de Carabineros, señor José Riffo, a los representantes del H. Senado, de la H. Cámara de Diputados, del Poder Judicial y de los diversos servicios públicos y embajadas que hoy nos acompañan.

Antes de comenzar esta cuenta anual, quería revisitar un poco nuestra historia nacional en materia de ciberseguridad. Porque el trabajo no comenzó este año. Partió hace ya una década, cuando a comienzos del gobierno de la entonces presidenta Michelle Bachelet se tomó la decisión de iniciar el proceso de planificación primaria en ciberseguridad, creando para ello una comisión asesora presidencial: el Comité Interministerial sobre Ciberseguridad en abril de 2015. Ese comité, a su vez, aprobó la que fuera nuestra primera política nacional de ciberseguridad para el período 2017-2022, la que, junto a la Política de Ciberdefensa, proyectaron los cimientos sobre los cuales está construida hoy la Agencia Nacional de Ciberseguridad que es un componente, quizás el más importante, de nuestra gobernanza nacional de la seguridad digital.

Luego, le correspondió al presidente Sebastián Piñera comenzar a implementar varias de las 42 medidas de la Política, que buscaban satisfacer 5 objetivos estratégicos: infraestructura resiliente; derechos en el ciberespacio; cultura de la ciberseguridad; cooperación nacional e internacional; y promoción de la industria nacional.

En cumplimiento del primer objetivo estratégico, en el año 2018 se creó el CSIRT de Gobierno, y luego, a comienzos del año 2022, se ingresó al Congreso Nacional el proyecto de ley marco dio origen a nuestro marco regulatorio general y consolida este modelo de gobernanza.

Por ello, hacer un balance del primer año de funcionamiento de la Agencia Nacional de Ciberseguridad es una oportunidad no solo para dar cuenta del trabajo realizado en la última década, especialmente sobre los hitos alcanzados y los objetivos que hemos cumplido, sino que también es un espacio para visibilizar los desafíos que enfrentamos como país en materia de ciberseguridad, en un contexto en que lo digital ya es parte de la vida cotidiana de las personas, de la economía y del Estado.

La Agencia Nacional de Ciberseguridad nace a partir de la Ley Marco de Ciberseguridad, como una nueva institucionalidad pública especializada, técnica y con foco preventivo, cuyo propósito principal es fortalecer la seguridad y resiliencia del país frente a las crecientes amenazas en el entorno digital.

Como les decía, la Agencia es fruto del trabajo consistente y planificado de los últimos 10 años, que se transformó en una verdadera política de Estado transversal que fuere no solo apoyada por tres gobiernos consecutivos, sino que también recibió el sólido respaldo de la comunidad técnica, la sociedad civil, la academia y los gremios, porque fuimos capaces, como país, de comprender que la ciberseguridad dejó de ser un asunto técnico o sectorial. Hoy es una condición básica para la confianza, para la continuidad de los servicios esenciales, para el desarrollo económico y social y para el normal funcionamiento de nuestro país.

Este 2025 fue un año clave: pasamos a la puesta en marcha efectiva de una institucionalidad que ya está operando.

Rol y mandato

La ANCI tiene un mandato claro definido por la ley:

- Fortalecer la prevención, detección y respuesta frente a incidentes de ciberseguridad;
- Regular y fiscalizar a los servicios esenciales y operadores de importancia vital;
- Promover una cultura de ciberseguridad en el Estado, el mundo privado y la ciudadanía.

Este balance da cuenta de cómo hemos ido materializando ese mandato durante el año que ya acaba.

Principales hitos del año 2025

Durante este periodo logramos avances relevantes en distintos ámbitos.

En primer lugar, la instalación de la Agencia:

En segundo lugar, avanzamos en la implementación del sistema nacional de reporte de incidentes.

En tercer lugar, el primer listado de Operadores de Importancia Vital.

INSTALACIÓN DE LA AGENCIA

Hoy somos un servicio público completamente instalado. Contamos con una dotación inicial de 44 profesionales y especialistas, que son parte de la primera Agencia Nacional de Ciberseguridad de América Latina y el Caribe creada por ley.

La Agencia, para quienes no sepan, está estructurada orgánicamente con una subdirección nacional y cuatro divisiones (CSIRT Nacional, Jurídica, Vinculación con el Medio y Administración y Finanzas), que colaboran armónicamente en el ejercicio de las funciones públicas que le encomienda la ley; que nos permiten cumplir con los diversos objetivos que nos hemos propuesto (y también con aquellos que han surgido en el camino) y con las exigencias regulatorias que debe satisfacer cualquier organismo público: rendición de cuentas; acceso a la información pública; auditoría, control de legalidad, gestión de riesgos, compras públicas, cooperación y coordinación interinstitucional, entre otros.

El proceso de instalación lo realizamos, además, en medio del proceso de transición del modelo de gobernanza de la seguridad pública en Chile, que se materializó con la entrada en vigencia en abril recién pasado, de la ley que creó el Ministerio de Seguridad Pública -cuyas autoridades hoy nos acompañan- que es el ministerio a través del cual nos relacionamos con el Presidente de la República y con quien no solo compartimos un edificio, sino que también hemos desplegado esfuerzos conjuntos para contar con una infraestructura digital compartida, con un nivel de seguridad acorde a los riesgos que enfrentamos.

Con el ministerio, además, a través de sus subsecretarías, hemos suscrito diversos acuerdos o convenios de colaboración, como el convenio de transferencia de recursos desde el Plan Nacional contra el Crimen Organizado, para la dotación de infraestructura tecnológica de alto nivel o como los convenios para la ejecución de los recursos provenientes del préstamo BID que nos han permitido contar con capacidades humanas y tecnológicas en procesos críticos como la respuesta a incidentes de ciberseguridad a través del SOC, el desarrollo de las plataformas operacionales de la Agencia, o incluso, en la ejecución de los procesos participativos que hemos llevado a cabo este año en el proceso de calificación de Operadores de Importancia Vital.

Pero el proceso de instalación estaría incompleto si no hubiésemos realizado un esfuerzo por integrar a los otros poderes del Estado, a los órganos autónomos constitucionales, a los gremios, la academia y la sociedad civil. Porque, como ustedes muy bien saben, la ciberseguridad no distingue entre organismos públicos o privados, sino que opera como un ecosistema, altamente interconectado y dependiente entre sí.

Por eso, en este año suscribimos convenios con el Senado de la República, el Tribunal Constitucional y el Poder Judicial, los primeros organismos autónomos constitucionales que están dentro de los Regímenes Especiales de la Ley Marco de Ciberseguridad que decidieron convenir con la Agencia mecanismos de reporte de incidentes de ciberseguridad y de cooperación interinstitucional. El próximo año esperamos además suscribir convenio con los otros órganos autónomos constitucionales, con quienes ya estamos en conversaciones.

Con la sociedad civil organizada también hemos logrado avanzar en construir relaciones de confianza de largo plazo que vayan más allá de una iniciativa en particular. Por ello, este año hemos firmamos un acuerdo tripartito con la Alianza Chilena de Ciberseguridad y la Contraloría General de la República para capacitar a la ciudadanía y que ha sido un tremendo éxito; con la

Fundación Kodea que nos está apoyando en la incorporación de la ciberseguridad en la educación general básica y un acuerdo marco de cooperación la Alianza Chilena de Ciberseguridad, con quienes hemos realizado múltiples actividades durante todo el año que termina.

En este proceso de instalación ha sido clave la colaboración de los gremios de los sectores de la economía que son servicios esenciales, quienes jugaron un rol clave para permitirnos conocer y comunicarnos permanentemente con nuestros regulados.

Hoy veo a la mayoría de las directivas de los gremios y de la sociedad civil aquí presentes, por lo que aprovecho de expresarles públicamente nuestro agradecimiento y deseo de continuidad en el trabajo colaborativo en lo que viene.

Sistema nacional de reporte de incidentes

Hace 10 meses comenzó a regir comenzó a regir la obligación para todos los servicios esenciales, ya sean del sector público y privado, para que reportaran los ciberataques o incidentes significativos que sufrieran en sus redes o sistemas informáticos. Crear ese sistema fue una misión especialmente desafiante desde varias perspectivas.

Primero, necesitamos construir una plataforma de notificación que generara confianza, que fuera fácil de utilizar y, por sobre todo, que fuera segura. Era —y sigue siendo— imprescindible que la plataforma de reporte de incidentes de ciberseguridad sea robusta en términos de infraestructura; resiliente en caso de incidentes o ciberataques; y que dé certeza y seguridad a los regulados sobre la información que debían obligatoriamente compartir con la Agencia.

Para ello, conformamos un equipo de programación integrado completamente por mujeres, que consiguieron levantar la plataforma en pocas semanas, la que cumple con los atributos de integridad, confidencialidad y disponibilidad de la información especialmente sensible.

Nuestra plataforma fue el primer sistema informático del Estado, cuyo mecanismo de autenticación está basado en Clave Única, que cuenta con un segundo factor de autenticación, medida que nos permitió posteriormente recomendar a la Secretaría de Gobierno Digital del Ministerio de Hacienda, la utilización del 2FA en otros sistemas críticos de la gestión del Estado y hace solo unos días, la Comisión para el Mercado Financiero anunció su implementación en algunos de sus sistemas.

Aquí podemos apreciar claramente cómo la innovación en un órgano especializado en ciberseguridad termina generando cambios en otras instituciones y procesos críticos, que impactan positivamente en la seguridad digital de las personas.

El segundo desafío era contar con un esquema de notificación de incidentes que fuera sencillo para el usuario obligado a notificar. Porque tenemos que estar conscientes de algo muy importante. En ciberseguridad en Chile, los niveles de madurez son bien disímiles. Tenemos organizaciones especialmente preparadas y maduras que cuentan con equipos humanos especializados y recursos tecnológicos de vanguardia que les permiten notificar incidentes sin

ninguna dificultad. Pero, por otro lado, tenemos municipios distribuidos a lo largo del país, que no cuentan ni con esos recursos humanos ni tecnológicos, por lo tanto, la plataforma debía permitir a unos y a otros, cumplir fácilmente con la obligación legal de notificar los ciberataques o incidentes de impacto significativo que sufrieran.

Para ello, creamos una taxonomía de incidentes de ciberseguridad. En términos sencillos, nuestra taxonomía es un grupo de características que simplifica categorizar un incidente, responder a él de forma rápida, y analizarlo. Su principal objetivo es que el proceso de reporte sea lo más amigable posible. Se basa en los efectos visibles de un incidente, no en el detalle técnico. No se necesita ser especialista para reportar y además hemos acompañado a nuestros regulados con charlas permanentes y ofreceremos cursos certificados abiertos a toda la ciudadanía.

Incidentes y contexto de amenazas

Hasta 2024 teníamos una mirada parcial del escenario de la ciberseguridad en el país, ya que solo veíamos al mundo público a través del trabajo del entonces CSIRT de Gobierno. Hoy, gracias a la colaboración de todos ustedes estamos construyendo el mapa real de riesgos de ciberseguridad de Chile, lo que ha llevado a nuestro país a estar entre 20 países más ciberresilientes del mundo y debemos estar orgullosos de eso.

Hace solo unos días se publicó el "Informe de Ciberseguridad 2025: desafíos de vulnerabilidad y madurez para cerrar brechas en América Latina y el Caribe"; elaborado por el Banco Interamericano de Desarrollo y la Organización de los Estados Americanos (OEA), que identificó a nuestro país como el número 1 entre 30 países de América Latina y el Caribe. Especialmente por nuestros avances en áreas como la gobernanza, con la formación de una institucionalidad clara; la respuesta a incidentes, con la configuración de políticas definidas, y la amplia cooperación internacional que realiza nuestro país.

Además, este año entramos al top 20 de la ciberseguridad mundial. El ranking estonio NCSI puso a Chile en el lugar número 19 con un 85% de cumplimiento en el ponderado de factores, que incluye ítems como gobernanza en ciberseguridad, la lucha contra el cibercrimen y el aporte a la ciberseguridad global, marcando nuestro liderazgo en América y superando a países destacados por su madurez digital.

Ambos informes confirman que Chile ha avanzado de manera consistente en la construcción de una institucionalidad técnica, robusta e innovadora en ciberseguridad, pero también nos recuerda que el desafío principal de nuestro quehacer es llevar estas políticas a la práctica, fortaleciendo las capacidades operativas, la prevención y la coordinación con el sector privado y la ciudadanía.

Gracias al sistema de reporte, hoy contamos con información más completa y accionable. Los datos muestran que uno de los principales vectores de riesgo sigue estando en lo más básico: la gestión de contraseñas, el phishing y las brechas asociadas a factores humanos.

Esto refuerza una convicción clave: la ciberseguridad no es solo tecnología, es también cultura, procesos y personas. Por eso hemos puesto énfasis en difundir los "9 básicos" de la ciberseguridad como un estándar mínimo transversal, sobre lo que volveré más adelante.

A la fecha tenemos 3.258 número de instituciones inscritas en la Plataforma de Reporte de Incidentes y el sistema ha recibido más de 400 reportes de incidentes, provenientes tanto del sector público como del privado, lo que por primera vez nos permite tener una visión integral del riesgo cibernético del país.

Principales hallazgos: el problema mayor está en contraseñas.

Presentación de los 9 básicos.

PROCESO DE CALIFICACIÓN DE OIV

Un eje central del año fue el trabajo conjunto con los reguladores sectoriales para dar inicio al proceso de identificación y determinación con los Operadores de Importancia Vital, el cual decidimos dividir en dos etapas, la primera que concluyó hace algunos días y la segunda que comenzó el pasado 30 de noviembre y que debiera estar concluida el primer semestre de 2026.

Luego de un procedimiento administrativo que tomó un poco más de 6 meses, hace algunas semanas publicamos en el Diario Oficial el primer listado de Operadores de Importancia Vital pertenecientes a los cinco sectores más críticos del país: el sector eléctrico; las telecomunicaciones; los servicios digitales; el sector bancario y financiero; la salud y los organismos de la administración del Estado.

En total pasamos de un universo de 1.712 instituciones calificadas preliminarmente como OIV a un listado final de 915 organizaciones entre instituciones públicas y privadas repartidas de la siguiente manera:

	Final	% del universo
Energía	147	17%
Telecomunicaciones	29	3,80%
Digitales	413	0,70%
Financieras	34	18%
Salud	114	26,90%
Empresas públicas	20	69%
Organismos Administración del Estado	158	51%

Respecto del proceso de calificación me gustaría aprovechar de precisar uno de los criterios que se utilizaron en el proceso y que parece han sido comprendidos de maneras diversas por múltiples partes interesadas. Cuando nuestra ley identifica como uno de los criterios esenciales para ser calificado como OIV la "dependencia de redes y sistemas informáticos" es importante precisar que esto dice relación tanto con el normal funcionamiento de la organización (en términos de disponibilidad de sus redes y sistemas), como con el procesamiento, transmisión y transferencia segura de la información (es decir, preservando su confidencialidad, integridad y disponibilidad). En otras palabras, la dependencia no se evalúa únicamente respecto a la disponibilidad, sino que también respecto a la confidencialidad o integridad de la información. Que una organización sea madura en términos de disponibilidad, no garantiza que lo sea respecto a la protección de la confidencialidad o integridad de la información.

Finalmente, como una forma de avanzar en definir la forma en que los OIV deben cumplir con las obligaciones especiales que fija la ley marco, la semana pasada emitimos las dos primeras instrucciones generales que regulan el proceso de designación de los delegados de ciberseguridad de cada institución y las medidas necesarias que se deben adoptar para reducir el impacto y la propagación de un incidente de ciberseguridad, respectivamente.

Como se puede apreciar, durante el año 2025 logramos implementar las tres iniciativas imprescindibles para contar con una ley funcional: instalar un servicio público de calidad; contar con una plataforma segura de reporte de incidentes; y definir el primer universo de operadores de importancia vital. Pero no nos quedamos ahí. Gracias el enorme esfuerzo del equipo profesional de la Agencia, pudimos hacer mucho más.

Difusión, formación y cultura de ciberseguridad

Permítanme destacar algunos de las iniciativas más relevantes realizados en materia de difusión y formación. Participamos activamente en seminarios, charlas, encuentros técnicos y espacios de diálogo con empresas y organismos públicos.

Estas instancias han sido clave para explicar el nuevo marco legal, aclarar obligaciones, pero también para instalar una conversación profunda sobre ciberseguridad, sus riesgos y responsabilidades compartidas.

La organización de charlas conjuntas con otros organismos del Estado como el Ministerio de Salud, el Servicio Civil, la Superintendencia de Seguridad Social, el Instituto de Previsión Social, Carabineros de Chile, la Policía de Investigaciones, entre otras, y el acuerdo con la Contraloría, la Alianza Chilena de Ciberseguridad y la ANCI fueron los primeros pasos.

Impactamos directamente a más de 26 mil personas, quienes participaron distintas instancias educativas de manera presencial y virtual, incluyendo a las más de 800 personas que ya realizaron el curso que elaboramos con la Contraloría General de la República, la Alianza Chilena de Ciberseguridad y "Phising y fraude digital" disponible para todos los chilenos en el Centro de Estudios de la Administración del Estado y que cuenta con un certificado oficial tras realizarlo, por lo que los invito a cursarlo.

Además, hoy aprovecho de anunciar que durante enero lanzaremos un curso abierto, gratuito y certificado sobre respuesta de incidentes. El propósito es mejorar las capacidades de respuesta a incidentes en el sector público y privado nacional y estará enfocado en que profesionales, técnicos y especialistas aprendan a gestionar el proceso completo de un incidente de ciberseguridad, desde la prevención hasta el reporte de incidentes en la plataforma de la Agencia Nacional de Ciberseguridad.

Y finalmente en materia de educación, quiero destacar el compromiso de la dotación de la Agencia con los niñas, niños y adolescentes, ya que, en forma simultánea al cumplimiento de las funciones y responsabilidades propias de sus cargos, realizaron charlas presenciales en varios colegios de Santiago, interactuando con más de 1.150 menores de edad. Espero que en 2026 ese número que a algunos les puede parecer menor, pero que implica un gran esfuerzo para una dotación de 44 personas, siga creciendo.

Desde fines del año 2023, nos encontramos trabajando en el diseño de un Programa de Estudio en la especialidad de Ciberseguridad para la Educación Media Técnico-Profesional, en el marco de un convenio de colaboración y transferencia de recursos suscrito con la Secretaría de Modernización del Estado.

Este programa surge a partir de una necesidad país: la brecha existente de profesionales en ciberseguridad, y la convicción de que debemos generar oportunidades tempranas para los jóvenes, preparándolos desde la etapa escolar para una inserción efectiva en el mercado laboral.

Como parte de este proceso, se ha desarrollado el levantamiento de los primeros 10 perfiles ocupacionales en ciberseguridad, utilizando la metodología de Chile Valora, junto con la elaboración de planes formativos validados por SENCE, lo que permitirá avanzar en la creación de oportunidades concretas de certificación de personas en este ámbito estratégico.

Finalmente, durante el primer trimestre de 2026 iniciaremos un trabajo conjunto con el Ministerio de Educación para la elaboración de la propuesta de asignatura de ciberseguridad, la cual deberá ser presentada al Consejo Nacional de Educación. Paralelamente, avanzaremos en la generación de oportunidades de certificación en perfiles de ciberseguridad, enfocados en una primera etapa en los Encargados de Ciberseguridad del Estado.

Cooperación Internacional

Ser la primera Agencia de Ciberseguridad de la región es un privilegio que también conlleva responsabilidades y compromisos. Hoy estamos implementando un proyecto en conjunto con la Agencia Chilena de Cooperación Internacional para el Desarrollo (AGCID) y financiado por la Unión Europea para el "Fortalecimiento y desarrollo de capacidades en América Latina y el Caribe en materia de ciberseguridad", que busca mejorar la preparación en seguridad digital de la región tomando la experiencia chilena y europea como referencia. En este proyecto estamos trabajando de la mano con las autoridades nacionales de ciberseguridad de Argentina, Brasil, Ecuador, Colombia, Costa Rica, Jamaica, México, Panamá, Perú, República Dominicana, Trinidad y Tobago y Uruguay, en un esfuerzo inédito de cooperación e integración regional en ciberseguridad.

Para este primer año en materia internacional definimos nuestros objetivos estratégicamente con vocación de servicio público e impacto nacional e internacional, lo que nos permitió avanzar rápida y eficientemente. ¿El resultado? Hemos firmado convenios de colaboración con instituciones tan importantes como el Instituto Nacional de Ciberseguridad y el Centro Criptográfico Nacional del Centro Nacional de Inteligencia, ambos de España, donde somos invitados permanentes de sus principales conferencias anuales, e incluso hemos tenido el honor de dictar las conferencias inaugurales en algunos de esos eventos.

Adicionalmente, hemos fortalecido las relaciones bilaterales en materia de ciberseguridad con nuestros países aliados y socios de larga data especialmente en el caso del Reino Unido, Estados Unidos, Canadá, República Checa y España, a cuyos representantes diplomáticos hoy presentes agradezco el trabajo conjunto.

En los próximos meses esperamos suscribir nuevos convenios de cooperación con el resto de los países de la región y con las entidades de referencia a nivel mundial.

¿Qué nos depara el futuro?

Este año también deja desafíos claros que será necesario implementar el próximo año:

- Incrementar la dotación de la Agencia y el presupuesto de ciberseguridad tanto en el sector público como privado.
- Seguir fortaleciendo las capacidades técnicas en el Estado y en todas las instituciones que proveen servicios esenciales.

- Consolidar el cumplimiento del marco normativo.
- Mejorar la gestión del riesgo cibernético a nivel estratégico.
- Avanzar decididamente en cultura organizacional y formación de personas.
- Poner en práctica el plan de acción definido por el Comité Interministerial de Ciberseguridad
- E implementar funcionamiento del Consejo Asesor Multisectorial una vez que el Presidente de la República formalice la designación de sus seis integrantes.

Estos desafíos son de corto, mediano y largo plazo, por lo requieren continuidad, coherencia y colaboración y en esto el compromiso que ha mostrado Chile ha sido claro y constante durante la última década.

Cierre

Quiero cerrar agradeciendo profundamente al equipo de la Agencia Nacional de Ciberseguridad por su compromiso, profesionalismo y vocación de servicio público. Sin su trabajo, este primero año de funcionamiento –sin duda- no habría sido posible. Somos un servicio pequeño que, con determinación, profesionalismo, creatividad y una entrega sin límite ha permitido hacer todo lo que les he contado y mucho más.

Agradezco también a las instituciones públicas y privadas que han colaborado con este proceso, que se han abierto al diálogo público y privado y que han comprendido que la ciberseguridad llegó para quedarse. No es posible pensar en un futuro sin ciberseguridad.

Y en lo personal, agradezco al Presidente de la República, por la confianza de haberme encomendado la misión de liderar este primer año de vida y la instalación de la Agencia Nacional de Ciberseguridad y al Ministerio de Seguridad Pública y sus autoridades, por todo el trabajo conjunto realizado.

Ha sido un enorme privilegio conducir a la ANCI en su primer año de funcionamiento y estoy particularmente orgulloso del trabajo realizado.

Este primer balance refleja un primer paso sólido en la construcción de una institucionalidad moderna, técnica y al servicio del país. Tenemos mucho por delante, pero hoy Chile cuenta con una Agencia que está trabajando día a día para fortalecer la seguridad digital como un bien público esencial.

Muchas gracias a ustedes.