2026

Balance de Gestión Integral

Etapa 1: Principales resultados de la gestión 2025

MINISTERIO DE SEGURIDAD PÚBLICA
Agencia Nacional de Ciberseguridad

Gobierno de Chile
gob.cl

Principales resultados de la gestión 2025 según sus objetivos estratégicos de la Agencia Nacional de Ciberseguridad[1]

AUTORIDADES DEL SERVICIO	DEPENDE DEL MINISTERIO DE SEGURIDAD PÚBLICA
Michelle Bordachar Benoit, Directora Nacional (s)	Luis Cordero Vega, Ministro de Seguridad Pública Carolina Leitao Álvarez-Salamanca, Subsecretaria de Prevención de Delito Rafael Collado Gonzalez, Subsecretario de Seguridad Pública Michelle Bordachar Benoit, Director Nacional ANCI

Con el fin de identificar los principales logros en la gestión, para cada objetivo estratégico del Servicio se presenta una priorización de las acciones que se llevaron a cabo para dar cumplimiento a los desafíos enunciados por cada uno de ellos2

OBJETIVO ESTRATÉGICO
Desarrollar e implementar políticas y acciones públicas en materias de ciberseguridad, que permitan contar con un ciberespacio libre, abierto, seguro y resiliente, donde se proteja la seguridad del país, sus instituciones y los derechos de las personas.

ACCIÓN 1	NUBE DE PALABRAS
Fortalecimiento de la gobernanza nacional en ciberseguridad mediante la realización del primer Comité Interministerial de Ciberseguridad 2025, efectuado el 27 de marzo en La Moneda, con participación de los ocho representantes definidos por reglamento. Su objetivo es coordinar a los organismos del Estado en la implementación de la política sectorial y aprobar el Plan de Acción de la Política Nacional de Ciberseguridad 2023-2028, formalizado por Resolución Exenta N° 28 de 2025 de la ANCI. El plan contempla 15 medidas; en 9 la ANCI participa y en 3 lidera: metodología de evaluación de riesgos, fomento de ejercicios público-privados y reporte anual nacional. En	

[1] Las autoridades ministeriales y del servicio corresponden a aquellas vigentes al momento de emitir este informe
[2] La redacción de las acciones y justificación corresponde a un auto reporte elaborado íntegramente por el Servicio responsable de acuerdo con las directrices impartidas por la Dirección de Presupuestos

2025 se concretaron dos hitos: participación en el ejercicio del Coordinador Eléctrico y desarrollo de She Secures junto a la OEA, con foco en género e inclusión.	

ACCIÓN 2
Consolidación de la implementación de la Política Nacional de Ciberseguridad mediante el fortalecimiento de la institucionalidad, el desarrollo del marco normativo y la articulación de capacidades nacionales. En esta línea, durante 2025 se dictaron 5 de los 6 Reglamentos mandatados por la Ley Marco de Ciberseguridad, y las Resoluciones Exentas N° 2, 7, 24, 28, 50, 76 y 87, relativas al reporte de incidentes, la publicación de alertas tempranas y la calificación de Operadores de Importancia Vital. Estos avances se vieron reflejados en la mejor posición de Chile en evaluaciones internacionales que posicionaron a Chile como líder regional en el Informe de Ciberseguridad BID-OEA y dentro de los primeros 20 países del National Cyber Security Index (NCSI), que valoraron la entrada en videncia de la Ley, la puesta en marcha de la ANCI, la coordinación interministerial y la existencia de un Plan de Acción vigente establecido por el Gobierno Central.

ACCIÓN 3
Difusión de buenas prácticas normativas y técnicas en el marco de la Política Nacional de la Ciberseguridad. Para ello se apoyó la difusión de convocatoria del Diplomado Internacional en Ciberseguridad en conjunto con AGCID y se realizaron alrededor de 13 presentaciones y participaciones en jornadas técnicas en distintos países del mundo, tales como Estados Unidos, Uruguay, México, Panamá, República Dominicana, España, Reino Unido, Francia y Singapur. Estas acciones permitieron apoyar al fortalecimiento de las capacidades y cultura preventiva en el ecosistema de ciberseguridad mundial.

JUSTIFICACIÓN DE LAS ACCIONES
Las acciones que forman parte de este objetivo permiten dar forma a la Política Nacional de Ciberseguridad a través de medidas concretas, responsables institucionales y metas definidas para fortalecer la resiliencia digital, mejorar la coordinación estatal, proteger derechos en el entorno digital y consolidar capacidades frente a amenazas cibernéticas. Su enfoque intersectorial permite traducir lineamientos estratégicos en acciones públicas ejecutables, contribuyendo a un ciberespacio libre, abierto, seguro y resiliente. Estas acciones permiten fortalecer la gobernanza del país en materia de ciberseguridad, articulando a los diferentes actores relacionados a la materia y permitiendo mejorar la posición del país en el escenario internacional.

OBJETIVO ESTRATÉGICO
Asegurar la gestión oportuna y eficaz de los incidentes de ciberseguridad mediante la definición e implementación de protocolos y estándares, garantizando que los servicios esenciales cuenten con acceso continuo a una plataforma de reporte y cuenten con mecanismos de respuesta que permitan disminuir la probabilidad de pérdida en la continuidad operacional y en la confidencialidad e integridad de la información.

ACCIÓN 1	NUBE DE PALABRAS
Implementación de la obligación nacional de reporte de incidentes de ciberseguridad y habilitación operativa de la plataforma de notificación para servicios esenciales y organismos regulados. El 1° de marzo comenzó a regir la obligatoriedad de reporte de incidentes de ciberseguridad para servicios esenciales, para lo que la ANCI habilitó una plataforma especialmente diseñada, con altos estándares de seguridad. El universo de sujetos obligados no se encuentra definido en términos cerrados, ya que corresponde a todos los organismos del Estado y las instituciones privadas que prestan servicios en cualquiera de los 16 sectores regulados. Al cierre de 2025 se contaban 3.294 instituciones inscritas, y 410 reportes gestionados. El tiempo promedio de respuesta entre la apertura y el cierre de la gestión de un incidente significativo de ciberseguridad de 13,2 días. Además de la plataforma, la Agencia cuenta con un SOC disponible 24/7 para recibir reportes y alertas.	

ACCIÓN 2
Emisión de instrucciones generales para la inscripción, gestión y respuesta ante incidentes de ciberseguridad en servicios esenciales y operadores de importancia vital. En 2025 se dictaron cuatro Instrucciones Generales: IG N°1 (4 de junio) y las IG N°2, N°3 y N°4 (26 de diciembre). Las IG N°1 y N°2 aplican a servicios esenciales; las IG N°3 y N°4 a operadores de importancia vital. El seguimiento se activa ante incidentes con deber de reporte y, de revestir entidad suficiente, puede iniciarse un procedimiento sancionatorio conforme a la Ley N°21.663. Asimismo, se impartieron directrices sobre inscripción en plataforma, designación de responsables y adopción de medidas técnicas obligatorias. Estas disposiciones

refuerzan protocolos estandarizados y una respuesta coordinada y oportuna, reduciendo impacto y propagación de incidentes y resguardando la disponibilidad, confidencialidad e integridad de la información.

ACCIÓN 3

Monitoreo y consolidación del uso de la plataforma nacional de reporte de incidentes y fortalecimiento del sistema de gestión institucional. La incorporación progresiva de instituciones y la recepción sistemática de reportes permitieron generar información para la gestión coordinada de eventos de ciberseguridad. Entre marzo y diciembre de 2025 se registraron 414 reportes: 145 por compromisos de cuenta y 190 correspondientes a incidentes significativos. A partir del análisis del CSIRT Nacional se emitieron 179 alertas de fraude, 48 de vulnerabilidades y 11 de incidentes, difundidas para prevenir nuevos eventos. El sector que más reportó fue la Administración del Estado (227), seguido de servicios digitales (108), banca, finanzas y medios de pago (58), y salud y productos farmacéuticos (44).

JUSTIFICACIÓN DE LAS ACCIONES

Durante 2025 se implementó la obligatoriedad de reporte de incidentes de ciberseguridad para servicios esenciales y organismos regulados, habilitando una plataforma de soporte al proceso. La obligación rige desde el 1 de marzo de 2025 y permitió estandarizar procesos de alerta temprana, mejorar la trazabilidad de incidentes y fortalecer la coordinación entre instituciones y el CSIRT Nacional. La disponibilidad permanente del sistema contribuye a reducir tiempos de respuesta, prevenir la propagación de ataques y resguardar la continuidad operacional y la integridad de la información en servicios críticos. El universo de sujetos obligados no se encuentra definido en términos cerrados, ya que corresponde a las personalidades jurídicas de los 16 sectores regulados, estimadas en alrededor de 1 millón. Al cierre 2025 se registraban 3.294 organismos inscritos y 410 reportes gestionados. El sistema alcanzó un 98,753% de disponibilidad y un tiempo promedio de respuesta promedio entre la apertura y el cierre de un reporte de 13,2 días.

Así mismo, la Agencia emitió instrucciones complementarias sobre inscripción en la plataforma, designación de responsables de ciberseguridad y adopción de medidas técnicas obligatorias para contener incidentes. Estas disposiciones fortalecen protocolos estandarizados de gestión y respuesta, promoviendo una actuación coordinada y oportuna frente a eventos que puedan afectar servicios esenciales. La definición de roles, procedimientos y medidas mínimas contribuye a disminuir el impacto y la propagación de incidentes, asegurando mayores niveles de disponibilidad, confidencialidad e integridad de la información.

En 2025 se impartieron cuatro Instrucciones Generales: la IG N°1 fue publicada el 4 de junio, y las IG N°2, N°3 y N°4 el 26 de diciembre. Las IG N°1 y N°2 aplican a servicios esenciales, mientras que las IG N°3 y N°4 rigen exclusivamente para operadores de importancia vital. Los mecanismos de seguimiento y fiscalización se activan ante la ocurrencia de un incidente con deber de reporte y, si reviste suficiente entidad, puede iniciarse un procedimiento administrativo sancionatorio conforme a ley N°21.663.

OBJETIVO ESTRATÉGICO
Diseñar e implementar planes y acciones de formación ciudadana, que permitan generar concientización en las personas sobre el cuidado y prevención ante amenazas digitales a las cuales se ven expuestas.

ACCIÓN 1	NUBE DE PALABRAS
Diseño e implementación del ciclo de Charlas ANCI de Ciberseguridad 2025, orientado a la formación ciudadana en prevención de amenazas digitales, con énfasis en conocimientos prácticos sobre riesgos, reconocimiento de amenazas y medidas básicas de protección en el uso cotidiano de tecnologías. En el ámbito escolar se realizaron 11 charlas presenciales en 5 comunas de la Región Metropolitana (Peñalolén, La Florida, Renca, Recoleta y Quinta Normal). Especialistas del CSIRT Nacional visitaron 10 establecimientos y expusieron a estudiantes de Séptimo Básico a Cuarto Medio, alcanzando a 1.149 alumnos. En cada colegio se entregó la guía digital ?Riesgos y Prevención: Pérdida de privacidad en redes sociales?, dirigida a apoderados y disponible en la web institucional para su descarga.	

ACCIÓN 2
Desarrollo y difusión de la guía de "Los 9 básicos de la ciberseguridad" para la promoción de prácticas de autocuidado digital. Esta iniciativa se basó en el análisis de reportes institucionales que evidenció que el 41% de los casos correspondía a compromiso de cuentas y otros incidentes evitables mediante medidas simples. La guía propone nueve acciones: actualizar periódicamente, capacitar, minimizar privilegios, respaldar información, asegurar redes y equipos, monitorear en tiempo real, utilizar autenticación multifactorial y gestores de contraseñas. La estimación institucional indica que estas medidas podrían prevenir hasta el 90% de los incidentes reportados. Fue presentada por el director Daniel Álvarez Valenzuela en el último trimestre de 2025 y socializada con actores relevantes.

ACCIÓN 3
Ejecución de acciones de divulgación y educación digital para sensibilizar a la población sobre riesgos

emergentes en ciberseguridad.

Considerando el público diverso al que la ley mandata que la ANCI debe concientizar en materias de ciberseguridad, durante 2025 se realizaron acciones orientadas a la población general, a través de ciberconsejos en redes sociales, con recomendaciones prácticas sobre gestión segura de contraseñas, actualización de dispositivos y detección de fraudes.

Además, el 3 de noviembre de 2025 se lanzó el Curso de Phishing y Fraude Digital, desarrollado junto a la CGR y la Alianza Chilena de Ciberseguridad y alojado en el CEA de la CGR; a diciembre fue completado por más de 800 personas.

Por último, durante todo el año, se charlas online que convocaron aprox. 2.000 personas.

JUSTIFICACIÓN DE LAS ACCIONES

La ley Marco de Ciberseguridad establece entre las funciones de la ANCI el diseño e implementación de acciones de formación ciudadana para fortalecer y promover una cultura de ciberseguridad, ya que la ciberseguridad no es una materia de exclusiva responsabilidad de áreas técnicas, sino que requiere de la acción y concientización de los usuarios.

El análisis de los reportes de incidentes recibidos dio cuenta que sobre el 40% podría haberse evitado con medidas básicas como contraseñas robustas y doble factor de autenticación. Por esto, y considerando el alto grado de digitalización con que cuenta Chile, es cada vez más importante que conocimientos y herramientas de ciberseguridad sean transversales a toda la ciudadanía.

OBJETIVO ESTRATÉGICO
Desarrollar y ejecutar el procedimiento definido en la Ley N° 21.663 para la calificación de operadores de importancia vital, asegurando la identificación oportuna de las instituciones públicas y privadas cuya afectación tenga un impacto significativo en la seguridad y el orden público, o en la provisión continua y regular de servicios esenciales.

ACCIÓN 1	NUBE DE PALABRAS
Publicación e implementación del procedimiento de calificación de Operadores de Importancia Vital conforme a la Ley N°21.663, estableciendo etapas, criterios técnicos y coordinación con reguladores sectoriales para la emisión de informes. Su aplicación fortalece el marco regulatorio y la resiliencia ante incidentes que afecten el orden público o la continuidad de servicios esenciales. Por Resolución Exenta N°24 (30 de mayo de 2025) se inició el primer proceso y su calendarización. Luego, la Resolución N°50 (16 de septiembre) aprobó una nómina preliminar con 1.712 entidades, sujeta a consulta pública por 30 días. Finalmente, la Resolución N°87 (17 de diciembre) aprobó la nómina definitiva con 915 entidades. Durante el proceso se recibieron cerca de diez informes técnicos sectoriales, conforme al reglamento.	

ACCIÓN 2
Publicación e implementación del procedimiento de calificación de Operadores de Importancia Vital conforme a la Ley N°21.663, estableciendo etapas, criterios técnicos y coordinación con reguladores sectoriales para la emisión de informes. Su aplicación fortalece el marco regulatorio y la resiliencia ante incidentes que afecten el orden público o la continuidad de servicios esenciales. Por Resolución Exenta N°24 (30 de mayo de 2025) se inició el primer proceso y su calendarización. Luego, la Resolución N°50 (16 de septiembre) aprobó una nómina preliminar con 1.712 entidades, sujeta a consulta pública por 30 días. Finalmente, la Resolución N°87 (17 de diciembre) aprobó la nómina definitiva con 915 entidades. Durante el proceso se recibieron cerca de diez informes técnicos sectoriales, conforme al reglamento.

ACCIÓN 3
Publicación de la nómina oficial de Operadores de Importancia Vital en el Diario Oficial formalizando la identificación de organizaciones críticas pertenecientes a sectores estratégicos como energía, telecomunicaciones, salud, servicios financieros e infraestructura digital. La identificación formal de estos actores fortalece la capacidad estatal para prevenir impactos sistémicos ante incidentes cibernéticos y resguardar la seguridad nacional. Las 915 organizaciones calificadas se distribuyen sectorialmente en: 147 empresas eléctricas; 29 de telecomunicaciones; 413 de servicios digitales, infraestructura digital y TI; 34 del sector bancario, financiero y medios de pago; 114 prestadores de salud; 20 empresas públicas; y 158 organismos de la Administración del Estado.

JUSTIFICACIÓN DE LAS ACCIONES
La Ley define dos grupos de instituciones reguladas por la ANCI: servicios esenciales y Operadores de Importancia Vital. Estos últimos son aquellos Organismos de la Administración del Estado y empresas privadas que prestan servicios en alguno de los sectores definidos, que dependen de redes y sistemas informáticos y la afectación, interceptación, interrupción o destrucción de sus servicios, tenga impacto significativo en el funcionamiento del país. Es decir, aquellas instituciones que son más críticas para el día a día.

OBJETIVO ESTRATÉGICO
Garantizar el cumplimiento de los fines y disposiciones de la Ley N° 21.663, sus reglamentos, protocolos, estándares técnicos, e instrucciones generales y particulares emitidos por la Agencia a través del diseño de estrategias y mecanismos de fiscalización y sanción.

ACCIÓN 1	NUBE DE PALABRAS
Diseño e implementación de Instrucciones Generales que establecen obligaciones técnicas y operativas en reporte de incidentes, gestión de riesgos y adopción de medidas mínimas de ciberseguridad. Estas instrucciones traducen el marco legal en requisitos verificables y parámetros objetivos para evaluar el cumplimiento de las entidades reguladas. La definición de estándares obligatorios habilita la fiscalización, permitiendo supervisar la implementación efectiva de la normativa y sustentar medidas correctivas o sancionatorias ante incumplimientos. Asimismo, asegura trazabilidad institucional en la adopción de protocolos y estándares técnicos, facilitando la supervisión permanente de la Agencia. Se dictaron 4 instrucciones generales para todos los sujetos obligados y 13 particulares dirigidas a instituciones específicas, orientadas a fortalecer acciones preventivas y la gestión de incidentes.	

ACCIÓN 2
Establecimiento de la obligación de designar y registrar Delegados de Ciberseguridad como responsables formales ante la autoridad, definiendo funciones y responsabilidades asociadas al cumplimiento de la Ley N°21.663. La instrucción N° 3 del 26 de diciembre, definió el procedimiento para que se diera cumplimiento a esta obligación por parte de los Operadores de Importancia Vital.

ACCIÓN 3
Establecimiento de estándares técnicos mínimos y medidas obligatorias para la prevención y contención de incidentes de ciberseguridad, alineadas con los protocolos definidos en la Ley N°21.663.

Durante el primer año de funcionamiento de la Agencia no se publicaron estándares técnicos mínimos con sus respectivos mecanismos de verificación. Sin embargo, se realizó un estudio de los incidentes con mayor impacto y se identificaron las principales brechas de seguridad explotadas por los atacantes, dando origen a un estándar mínimo de recomendaciones de seguridad denominado "los 9 básicos" que corresponde a controles básicos que habrían permitido evitar más del 90% de los incidentes de alto impacto gestionados durante el 2025.

JUSTIFICACIÓN DE LAS ACCIONES

La estandarización de estas exigencias permite evaluar objetivamente el grado de cumplimiento normativo por parte de los sujetos obligados, reduciendo la discrecionalidad en los procesos de supervisión. Estos estándares constituyen un instrumento clave para el diseño de estrategias de fiscalización, al proporcionar criterios técnicos verificables que sustentan eventuales procesos sancionatorios y fortalecen la protección de servicios esenciales y activos críticos.

La definición de estándares obligatorios constituye un mecanismo habilitante para la fiscalización, al permitir supervisar la implementación efectiva de la normativa y sustentar la adopción de medidas correctivas o sancionatorias ante incumplimientos.

Este mecanismo permite asegurar trazabilidad institucional respecto de la adopción de protocolos y estándares técnicos, facilitando la supervisión permanente por parte de la Agencia. La identificación de responsables habilita procesos efectivos de fiscalización y fortalece la capacidad institucional para exigir cumplimiento y aplicar medidas correctivas cuando corresponda.

Al término del año 2025 finalizó el primer proceso de designación de OIV con un total de 915 regulados designados. Sin embargo, el registro de delegados estará finalizado en el primer trimestre 2026.

La estandarización de estas exigencias permite evaluar objetivamente el grado de cumplimiento normativo por parte de los sujetos obligados, reduciendo la discrecionalidad en los procesos de supervisión.

Estos estándares constituyen un instrumento clave para el diseño de estrategias de fiscalización, al proporcionar criterios técnicos verificables que sustentan eventuales procesos sancionatorios y fortalecen la protección de servicios esenciales y activos críticos.

OBJETIVO ESTRATÉGICO
Gestionar y operar la Red de Conectividad Segura del Estado para contar con una infraestructura de red con un alto nivel de disponibilidad y resiliencia, que permita el intercambio confidencial e íntegro de información para los organismos de la Administración del Estado.

ACCIÓN 1	NUBE DE PALABRAS
Implementación del reglamento de la Red de Conectividad Segura del Estado (RCSE) y definición de obligaciones operativas para organismos públicos conectados. La normativa estableció requisitos técnicos, uso obligatorio de dominios institucionales y medidas de seguridad perimetral, estandarizando la infraestructura digital estatal. La RCSE fue aprobada por Decreto Supremo N°293 (23 de septiembre de 2024) y publicada el 11 de abril de 2025, fecha desde la cual rige. Actualmente, cuenta con 57 organismos conectados directamente, con doble enlace para asegurar alta disponibilidad. El universo obligado asciende a 730 organismos. Además, 165 entidades se conectan indirectamente a través de organismos integrados, alcanzando una cobertura efectiva de 222 entidades.	

ACCIÓN 2
Operación y monitoreo centralizado de la infraestructura de conectividad y seguridad perimetral de la RCSE, incluyendo la administración de enlaces y servicios tecnológicos que permiten la interconexión segura entre organismos del Estado. El monitoreo continuo permite detectar anomalías, prevenir interrupciones y fortalecer la continuidad operacional de los servicios públicos conectados. Esta gestión centralizada incrementa la resiliencia de la infraestructura estatal y reduce riesgos que puedan afectar la confidencialidad e integridad de la información intercambiada. En el marco de su operación se registran los siguientes indicadores: disponibilidad global aproximada de 99,5% de uptime; disponibilidad mensual promedio por institución de 99,2%; y disponibilidad mensual por enlace, considerando enlaces primarios y redundantes de 99,5%.

ACCIÓN 3
Fortalecimiento de capacidades institucionales para la operación segura de la RCSE mediante acciones de soporte técnico y capacitación continua para responsables de ciberseguridad. En gestión de incidentes se registran aproximadamente 600 tickets asociados a eventos de conectividad, seguridad y operación, con el 100% de los casos gestionados conforme a los procedimientos establecidos, asegurando análisis, seguimiento y cierre. La infraestructura opera bajo un esquema de alta disponibilidad y redundancia, distribuida en dos datacenters, con enlaces nacionales e internacionales de respaldo. Cada institución conectada dispone de doble enlace, lo que permite mantener la operación ante contingencias y minimizar impactos en servicios críticos. La red es monitoreada 24/7 bajo procedimientos formales de gestión y escalamiento de incidentes, asegurando la continuidad operativa de los servicios digitales del Estado y un funcionamiento estable y resiliente.

JUSTIFICACIÓN DE LAS ACCIONES
La Red de Conectividad Segura del Estado fortalece la disponibilidad y resiliencia de la infraestructura estatal al asegurar condiciones homogéneas de seguridad y operación, favoreciendo el intercambio confiable y protegido de información entre instituciones públicas. Cierre


Gobierno
de Chile
gob.cl