DIARIO OFICIAL
DE LA REPÚBLICA DE CHILE
Ministerio del Interior

I SECCIÓN

LEYES, REGLAMENTOS, DECRETOS Y RESOLUCIONES DE ORDEN GENERAL

Núm. 44.218 | Miércoles 6 de Agosto de 2025 | Página 1 de 5

Normas Generales

CVE 2677012

MINISTERIO DE SEGURIDAD PÚBLICA

Agencia Nacional de Ciberseguridad

IMPLEMENTA ACUERDO DEL COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD, QUE APRUEBA PLAN DE ACCIÓN DE LA POLÍTICA NACIONAL DE CIBERSEGURIDAD 2023-2028

(Resolución)

Núm. 28 exenta.- Santiago, 11 de julio de 2025.

Vistos:

Lo dispuesto en el decreto con fuerza de ley Nº 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fijó el texto refundido, coordinado y sistematizado de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la ley Nº 19.880 de bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado; en el decreto supremo Nº 164, de 2023, del Ministerio del Interior y Seguridad Pública, que Aprueba la Política Nacional de Ciberseguridad 2023-2028; en la ley Nº 21.663, marco de ciberseguridad; en el decreto supremo Nº 275, de 2024, del Ministerio del Interior y Seguridad Pública, que Aprueba el Reglamento de Funcionamiento del Comité Interministerial sobre Ciberseguridad; y en las resoluciones Nº 36, de 2024, y Nº8, de 2025, ambas de la Contraloría General de la República, que fijan normas sobre exención del trámite de toma de razón.

Considerando:

1. Que, de acuerdo con lo dispuesto en el decreto con fuerza de ley Nº 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado, los órganos de la Administración del Estado deben cumplir sus funciones coordinadamente y propender a la unidad de acción, evitando la duplicidad o interferencia de funciones.

2. Que, a través del decreto supremo Nº 533, de 2015, del Ministerio del Interior y Seguridad Pública, se creó el Comité Interministerial de Ciberseguridad, a quien se le encomendó la misión de proponer una Política Nacional de Ciberseguridad, sugerir alternativas de seguimiento a su avance e implementación, y asesorar en la coordinación de acciones, planes y programas en materia de ciberseguridad de los distintos actores públicos y privados en la materia.

3. Que, mediante decreto supremo Nº 164, de 2023, del Ministerio del Interior y Seguridad Pública, se aprobó la Política Nacional de Ciberseguridad 2023-2028, que estableció entre sus objetivos fundamentales, la coordinación nacional e internacional, en virtud de la cual "(...) los organismos públicos y privados crearán, en conjunto, instancias de cooperación con el propósito de comunicar y difundir sus actividades en ciberseguridad (...)"

4. Que, con fecha 8 de abril de 2024, se publicó en el Diario Oficial la ley Nº 21.663, marco de ciberseguridad, la cual tiene por objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los órganos de la Administración del Estado y entre éstos y los particulares. En tal contexto, la referida ley creó la Agencia Nacional de Ciberseguridad, como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, de carácter técnico y especializado, y le encomendó, entre otras misiones, el coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, y coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl

5. Que, el artículo 48 de la ley Nº 21.663, determinó la creación del Comité Interministerial sobre Ciberseguridad, cuyo objeto es asesorar al Presidente de la República en materias de ciberseguridad relevantes para el funcionamiento del país. En tal contexto, la citada ley dispone que el Comité deberá, en el ejercicio de sus funciones, coordinar la implementación de la Política Nacional de Ciberseguridad.

6. Que, de acuerdo con lo establecido en los artículos 49 y 50 de la ley Nº 21.663, corresponde al Director Nacional de la Agencia Nacional de Ciberseguridad presidir el referido Comité, e implementar los acuerdos que este adopte.

7. Que, en virtud de lo establecido por el artículo 52 de la ley Nº 21.663, por medio del decreto supremo Nº 275, de 2024, del Ministerio del Interior y Seguridad Pública, se aprobó el Reglamento de Funcionamiento del Comité Interministerial sobre Ciberseguridad y, asimismo, se derogó el decreto supremo Nº 533, de 2015, del Ministerio del Interior y Seguridad Pública, que creó el Comité Interministerial de Ciberseguridad.

8. Que, de acuerdo con lo establecido en el artículo 3º de la ley 19.880, las decisiones de los órganos administrativos pluripersonales se denominan acuerdos y se llevan a efecto por medio de resoluciones de la autoridad ejecutiva de la entidad correspondiente.

9. Que, con fecha 27 de marzo de 2025, se llevó a cabo la primera sesión del Comité Interministerial sobre Ciberseguridad, a la que concurrieron sus integrantes, los representantes de la Subsecretaría del Interior, de la Subsecretaría Secretaría General de la Presidencia, de la Subsecretaría de Defensa, de la Subsecretaría de Relaciones Exteriores, de la Subsecretaría de Hacienda, de la Subsecretaría de Telecomunicaciones, de la Subsecretaría de Ciencia, Tecnología, Conocimiento e Innovación, de la Agencia Nacional de Inteligencia y de la Agencia Nacional de Ciberseguridad.

10. Que, en tal instancia, los integrantes del Comité aprobaron por unanimidad el Plan de Acción de la Política Nacional de Ciberseguridad 2023-2028, en cuya elaboración se continuó con el trabajo realizado por el ahora derogado Comité Interministerial de Ciberseguridad.

11. Que, teniendo en cuenta lo anteriormente señalado.

Resuelvo:

Artículo único: Impleméntase el Acuerdo del Comité Interministerial sobre Ciberseguridad, que aprueba el Plan de Acción de la Política Nacional de Ciberseguridad 2023-2028, cuyo texto se entiende parte integrante de la presente resolución.

Plan de Acción
Política Nacional de Ciberseguridad 2023-2028

Este documento ha sido creado en base a un trabajo realizado por el Comité Interministerial sobre Ciberseguridad, durante el período de 2022 a 2024. Se han analizado 76 medidas, de las cuales han sido seleccionadas 15 para ser incorporadas en el plan de acción, en base al criterio de viabilidad en su implementación. Adicionalmente, se ha realizado un análisis de estas 15 medidas en cuanto a su aplicabilidad en los 4 ejes transversales que considera la Política Nacional de Ciberseguridad 2023-2028.

A continuación, se presentan en la tabla las medidas consideradas para el plan de acción:

N°	Nombre medida	Descripción medida	Responsable	Objetivo central	Objetivo transversal
1	Generación de Guías e Instructivos de apoyo a los Organismos de la Administración del Estado (OAEs)	Las guías tienen el objetivo de orientar a los OAEs en materias de ciberseguridad, facilitando el entendimiento en la materia y seguridad de la información. Se partirá con la publicación de una guía técnica de apoyo a la Norma Técnica de Ciberseguridad y Seguridad de la Información de la Ley de Transformación Digital y continuará con guías de apoyo a la actualización del Decreto N°83 del 2005 (Norma técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos). **Transversal:** Estos documentos serán revisadas por la Secretaría de Gobierno Digital (SGD), en coordinación con la Red de Mujeres de Transformación Digital del Estado y la Agencia Nacional de Ciberseguridad para fomentar una cultura de evaluación y gestión del riesgo desde una perspectiva de género, de protección de la infancia y de protección a los adultos mayores en los servicios digitales del Estado.	1. Subsecretaría de Hacienda. Secretaría de Gobierno Digital.	• Coordinación nacional e internacional • Cultura de la ciberseguridad	▪ Equidad de género ▪ Protección de la infancia ▪ Protección adultos mayores

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl

N°	Nombre medida	Descripción medida	Responsable	Objetivo central	Objetivo transversal
2	Informe diagnóstico en I+D+i sobre ciberseguridad	Elaborar el segundo informe sobre I+D+i en materias de ciberseguridad en Chile, que tenga por objeto determinar las áreas clave de investigación en ciberseguridad que Chile debe priorizar para fortalecer la protección de su infraestructura crítica, datos sensibles y responder a amenazas emergentes **Transversal:** De este informe, se debe trabajar en colaboración entre los responsables de esta medida, en incentivos concretos para que los investigadores locales con experiencia en las dimensiones transversales de equidad de género, protección de la infancia y adulto mayores, además de áreas como alfabetización digital, comunicaciones digitales y diseño digital, diseñen investigaciones en aspectos de la ciberseguridad y educación ya identificados en el informe.	1. Ministerio de Ciencia, Tecnología, Conocimiento e Innovación 2. Agencia Nacional de Investigación y Desarrollo	• Cultura ciberseguridad • Fomento a la industria y la investigación científica	▪ Equidad de género ▪ Protección de la infancia ▪ Protección adultos mayores
3	Focalización de becas en materias de ciberseguridad	Entregar un máximo de 15 becas para la formación de talentos en materia de ciberseguridad, a través de procesos de focalización en áreas prioritarias. **Transversal:** Debido a las brechas de mujeres en ciberseguridad, estas becas son una oportunidad de introducir una cuota de género que permita la equidad en el acceso a ellas. Asimismo, tanto el área transversal de equidad de género, como protección de la infancia y protección adultos mayores, será incluida como parte de la evaluación de los proyectos de investigación, sobre todo en el área prioritaria de Educación.	1. Ministerio de Ciencia, Tecnología, Conocimiento e Innovación 2. Agencia Nacional de Investigación y Desarrollo	• Cultura ciberseguridad • Fomento a la industria y la investigación científica	▪ Equidad de género ▪ Protección de la infancia ▪ Protección adultos mayores
4	Norma Técnica Ciberseguridad Sector Eléctrico	El desarrollo de la Norma Técnica tendrá por objeto principal establecer el marco regulatorio que incluya los fundamentos generales de Ciberseguridad, los que deben ser considerados como lineamientos mínimos a cumplir por las empresas eléctricas para la gestión de Ciberseguridad y Seguridad de la información. **Transversal:** En la elaboración del documento se deberá especificar cómo este documento contribuye, desde la ciberseguridad, a la consecución de la Agenda 2030, en particular, el Objetivo de Desarrollo Sostenible (ODS) número 7: Energía asequible y no contaminante. Es decir, a prevenir y mitigar los ciberataques a la infraestructura de energía; seguridad digital a las instalaciones de energía renovable, privacidad de datos en el uso energético, protección de infraestructura crítica, etc.	1. Ministerio de Energía 2. Comisión Nacional de Energía 3. Coordinador Eléctrico Nacional	• Infraestructura resiliente • Coordinación Nacional e Internacional	▪ Protección medioambiente
5	Metodología de evaluación de riesgos de ciberseguridad	Elaboración de una metodología de evaluación de riesgos de ciberseguridad que pueda ser puesta a disposición a todas las organizaciones del país, basada en modelos internacionales, pero adaptados a la realidad nacional. **Transversal:** 2025: La ANCI revisa la metodología y la complementa respecto a la evaluación de riesgos y el impacto del riesgo en las dimensiones transversales de protección a la infancia, protección adultos mayores y equidad de género y elabora una metodología para aquello.	1. Agencia Nacional de Ciberseguridad	• Infraestructura resiliente • Cultura ciberseguridad	▪ Equidad de género ▪ Protección de la infancia ▪ Protección adultos mayores
6	Fomentar ejercicios de ciberseguridad en alianza con instituciones públicas y privadas	Fomentar instancias de ejercicios de ciberseguridad para instituciones públicas, en colaboración con instituciones nacionales o internacionales que colaboren con el conocimiento, recursos	1. Agencia Nacional de Ciberseguridad	• Infraestructura resiliente • Fomento de la industria y la investigación científica	▪ Equidad de género

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl

N°	Nombre medida	Descripción medida	Responsable	Objetivo central	Objetivo transversal
		tecnológicos o recursos de infraestructura para la ejecución de dichas instancias. Además, generar un set de materiales para que las organizaciones puedas realizar sus propios ejercicios internos. **Transversal:** Organizar al menos un ejercicio, durante el periodo del plan de acción, en las instituciones públicas y que sean espacios de mujeres en la ciberseguridad.			
7	Elaboración de Manual de protocolos de comunicación ante incidentes de ciberseguridad	Establecer lineamientos base para la comunicación tanto interna como externa en una situación de incidente de ciberseguridad, que permita a las instituciones públicas tener un correcto manejo comunicacional en caso de afectación. **Transversal:** En la definición de los lineamientos de comunicación, se deben establecer acciones en caso de que un incidente de ciberseguridad afecte real o potencialmente los derechos de las mujeres, la infancia y los adultos mayores.	1. Agencia Nacional de Ciberseguridad 2. Ministerio de Secretaría de Gobierno/ SECOM	• Coordinación Nacional e Internacional • Derecho de las personas	▪ Equidad de género ▪ Protección de la infancia ▪ Protección adultos mayores
8	Agenda compartida de compromisos internacionales en ciberseguridad	Generación de una agenda compartida y consensuada entre el Ministerio de Relaciones Exteriores y la Agencia Nacional, donde se plasmen todas las iniciativas sobre ciberseguridad que se están llevando a cabo con coordinación o cooperación con instituciones internacionales. **Transversal:** Incluir en esta agenda todas las iniciativas y compromisos ya adquiridos que tengan relación con género y ciberseguridad y también protección del medioambiente y ciberseguridad.	1. Ministerio de Relaciones Exteriores 2. Agencia Nacional de Ciberseguridad	• Coordinación Nacional e Internacional	▪ Equidad de género ▪ Protección del medioambiente
9	Generación de reporte anual nacional de ciberseguridad	Elaborar un reporte anual que dé cuenta de la realidad nacional en ciberseguridad, de las amenazas, vulnerabilidades de los sistemas públicos, etc,.	1. Agencia Nacional de Ciberseguridad	• Infraestructura resiliente • Coordinación Nacional e Internacional	▪ Equidad de género ▪ Protección infancia ▪ Protección adulto mayor
		Este reporte debe ser complementado con las estadísticas de vulnerabilidades y amenazas generadas por la Agencia, el cual permita, en caso de aplicar, adecuar el Plan de Acción y/o tomar las medidas que estime conveniente la Agencia. Este reporte debe tener como énfasis proponer medidas accionables y recomendaciones que puedan tomar en cuenta los Organismos de la Administración del Estado. **Transversal:** Incluir en este informe, la situación anual sobre iniciativas o acciones implementadas que apunten a cubrir los ejes transversales de esta medida en materia de ciberseguridad.			
10	Ferias estudiantiles de ciberseguridad	Realizar alianzas con universidades e institutos técnicos para realizar ferias donde se muestren y concienticen las carreras de ciberseguridad. Estas ferias deben considerar las múltiples opciones de carreras directamente o vinculadas a la ciberseguridad, planes de carrera y certificaciones que se pueden obtener en los perfiles de cada carrera. **Transversal:** En la ejecución de estas ferias se debe considerar diferentes acciones que apunten a cubrir la brecha de género que existen en la industria de ciberseguridad.	1. Ministerio de Ciencia, Tecnología, Conocimiento e Innovación 2. Agencia Nacional de Ciberseguridad 3. Ministerio de Educación	• Cultura de ciberseguridad • Fomento de la industria y la investigación científica	▪ Equidad de género

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl

N°	Nombre medida	Descripción medida	Responsable	Objetivo central	Objetivo transversal
11	Propuesta de nueva carrera o especialidad técnica de nivel medio en ciberseguridad para EMTP	Creación de propuesta de piloto de carrera Técnico de Nivel Medio, para la Educación Media Técnico-Profesional (EMTP). Esto tiene por objetivo disminuir la brecha de falta de profesionales en ciberseguridad y comenzar a formar desde la etapa educacional temprana. **Transversal:** La medida debe considerar acciones que incorporen a mujeres en el plan piloto.	1. Agencia Nacional de Ciberseguridad 2. Ministerio de Hacienda 3. Ministerio de Educación	• Cultura de ciberseguridad • Fomento de la industria y la investigación científica	▪ Equidad de género
12	Desarrollo de documento sobre líneas de investigación en ciberseguridad	Elaboración de un documento conjunto entre el Estado y el sector privado, con una descripción de áreas de investigación en ciberseguridad que podrían beneficiar al país dentro de los próximos años. **Transversal:** El documento debe considerar las prioridades de investigación científica aplicada para fortalecer los derechos de las personas en el ciberespacio desde el enfoque de la ciberseguridad, en el contexto de las problemáticas y vacíos que hoy se tienen en Chile sobre: Género, Infancia, Adulto mayor y Medio ambiente.	1. Agencia Nacional de Investigación y Desarrollo de Chile (ANID) 2. Agencia Nacional de Ciberseguridad	• Fomento de la industria y la investigación científica • Infraestructura resiliente • Derecho de las personas	▪ Equidad de género ▪ Protección a la infancia ▪ Protección adultos mayores ▪ Medio ambiente
13	Ampliación del programa Plan Nacional de Tutorías a materias de educación digital	Desarrollar tutorías que consideren materia sobre educación y autocuidado digital para personas con mayores necesidades de apoyo en el aprendizaje de estas materias. **Transversal:** Las tutorías deben considerar como público objetivo aquellos considerados en los ejes transversales, implementando acciones dirigidas a ellos.	1. Ministerio de Ciencia, Tecnología, Conocimiento e Innovación 2. Agencia Nacional de Ciberseguridad *3. Ministerio de Educación*	• Derecho de las personas • Cultura de ciberseguridad	▪ Equidad de género ▪ Protección infancia ▪ Protección adulto mayor
14	Actualización de la Política de Ciberdefensa 2024 - 2028	Actualizar la Política de Ciberdefensa, publicada el año 2018, la que presentaba objetivos para ser cumplidos hasta el 2022. Para lo anterior, se efectuará un diagnóstico para medir el nivel de cumplimiento, para posteriormente fijar los nuevos objetivos alineados con la Política Nacional de Ciberseguridad 2023-2028, Ley Marco de Ciberseguridad y futuros desafíos de la Defensa Nacional. **Transversal:** Perspectiva de género en el proceso de actualización de la política de ciberdefensa.	1. Ministerio de Defensa 2. Subsecretaría de Defensa	• Infraestructura resiliente	▪ Equidad de género
15	Exigencias de ciberseguridad en concursos públicos de espectro radioeléctrico	Establecer exigencias de cumplimiento de la Resolución exenta N° 1318 de 2020 norma técnica sobre fundamentos generales de ciberseguridad para el diseño, instalación y operación de redes y sistemas utilizados para la oferta y explotación de servicios de telecomunicaciones.	1. Subsecretaría de Telecomunicaciones	• Infraestructura resiliente • Cultura de ciberseguridad • Fomento de la industria y la investigación científica	▪ No aplica.

Anótese y publíquese.- Daniel Álvarez Valenzuela, Director Nacional, Agencia Nacional de Ciberseguridad.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N°19.799 e incluye sellado de tiempo y firma electrónica avanzada. Para verificar la autenticidad de una representación impresa del mismo, ingrese este código en el sitio web www.diariooficial.cl