Documento de política pública

Ciberseguridad en Chile: panorama normativo e institucional

DERECHOS DIGITALES
América Latina

Esta publicación fue creada por Derechos Digitales, una organización independiente sin fines de lucro, fundada en 2005, que tiene como misión la defensa, promoción y desarrollo de los derechos humanos en entornos digitales en América Latina.

Supervisión general: Michel Souza y J. Carlos Lara
Investigación y textos: Isidora Ruggeroni Romero
Edición: J. Carlos Lara
Diseño: Catalina Viera

Diciembre, 2023 / Noviembre, 2024.

Esta publicación fue posible gracias al apoyo de Global Partners Digital.

Índice

Resumen Ejecutivo

El presente informe examina la evolución normativa e institucional de la ciberseguridad en Chile, abordando las leyes vigentes, los procesos de reforma legislativa, las estrategias nacionales y la institucionalidad en la materia. Con un enfoque en derechos humanos, diversidad e inclusión, se analiza el marco legal y las políticas públicas que han definido el desarrollo de la ciberseguridad en el país.

Entre los avances normativos se destaca la consagración constitucional de la protección de datos personales y la promulgación de leyes específicas como la Ley de Delitos Informáticos y la Ley de Transformación Digital del Estado. Estas normativas han sido complementadas con estrategias nacionales como la Política Nacional de Ciberseguridad 2023-2028, que refuerza el compromiso de Chile con una infraestructura digital resiliente y segura.

El informe se presenta en el contexto del fin de la tramitación de la Ley Marco de Ciberseguridad, junto a otras reformas legislativas y políticas nacionales con implementación en curso. Estas iniciativas buscan adaptar la gobernanza digital del país a los estándares internacionales, promoviendo una cultura de ciberseguridad en todos los sectores.

Finalmente, se identifican desafíos clave, como la necesidad de mayor coordinación interinstitucional, la actualización de normativas en torno a la inteligencia artificial y el fortalecimiento de la participación ciudadana. Este análisis proporciona una visión integral del panorama actual y de las oportunidades para consolidar un entorno digital más seguro y equitativo.

1. Introducción

Siguiendo distintas declaraciones de organismos oficiales en Chile, la ciberseguridad se ha convertido en un componente esencial para garantizar derechos fundamentales en la era digital, que por tanto amerita medidas de política pública. En Chile, este ámbito ha experimentado un desarrollo significativo en los últimos años, reflejando una mayor preocupación por proteger tanto a los individuos como a las instituciones frente a las crecientes amenazas cibernéticas. Este informe busca proporcionar un análisis exhaustivo del marco normativo e institucional que sustenta la ciberseguridad en el país.

Desde la consagración constitucional de la protección de datos personales hasta la implementación de la Política Nacional de Ciberseguridad, Chile ha avanzado en la construcción de un ecosistema digital seguro. Sin embargo, estos logros están acompañados de desafíos que requieren atención, como la fragmentación de la gobernanza en ciberseguridad y la necesidad de integrar nuevos enfoques tecnológicos, como la inteligencia artificial, en las políticas públicas.

El enfoque de este documento se centra en la intersección entre derechos humanos y tecnología, destacando la importancia de una ciberseguridad inclusiva y participativa. Este enfoque no solo responde a los compromisos internacionales del país, sino también a la creciente demanda de la ciudadanía por políticas más transparentes y efectivas.

A través de este análisis, se espera contribuir al debate nacional e internacional sobre cómo fortalecer las capacidades en ciberseguridad, promoviendo la colaboración entre actores estatales, privados y de la sociedad civil. Este informe es, en esencia, una herramienta para comprender y abordar los retos que plantea la ciberseguridad en el contexto chileno.

2. Panorama normativo

Chile cuenta con un panorama normativo diverso en materia de ciberseguridad, compuesto por leyes, decretos supremos y resoluciones de órganos sectoriales. Entre las normativas vigentes destacan la Ley de Delitos Informáticos, que establece sanciones para los delitos en el entorno digital; la Ley de Transformación Digital del Estado, orientada a modernizar la administración pública mediante la digitalización; y la Ley Fintec, que promueve servicios financieros basados en tecnologías innovadoras. A ello se suman quizás los más importantes avances legislativos en la materia, ambos en 2024: la aprobación del proyecto de Ley de Protección de Datos Personales y la promulgación de la Ley Marco de Ciberseguridad, que buscan modernizar la normativa y fortalecer la gestión de riesgos en el ámbito digital.

En términos de estrategia y gobernanza, Chile ha diseñado políticas y planes que refuerzan su compromiso con la ciberseguridad. La Estrategia de Transformación Digital del Estado establece lineamientos para un Estado Digital eficiente, mientras que la Política Nacional de Ciberseguridad 2017-2022 y su actualización 2023-2028 articulan objetivos y líneas de acción específicas en esta materia. La institucionalidad en este campo se reparte entre órganos con competencias sectoriales como la Comisión para el Mercado Financiero (CMF) o el Servicio Nacional del Consumidor (SERNAC), así como también órganos viceministeriales como la Subsecretaría de Telecomunicaciones (SUBTEL) y la Subsecretaría del Interior.

2.1. Constitución Política

La Constitución Política de la República, promulgada en 1980 y objeto de sucesivas reformas en el tiempo,[1] es la norma fundamental que establece los derechos y deberes de los ciudadanos, así como las bases de la institucionalidad estatal. Es la Constitución donde se regulan las potestades estatales y sus límites, y como parte de estos últimos los derechos fundamentales de las personas. Entre ellos, la Constitución asegura la protección de la vida privada, la protección de los datos personales (artículo 19 Nº 4), la inviolabilidad de objetos y documentos y la inviolabilidad de comunicaciones privadas (artículo 19 Nº 5), especialmente importantes en razón de su posible afectación por ataques cibernéticos.

Con la publicación de la Ley Nº 21.096 (de 16 de junio de 2018), se reformó la Constitución para consagrar la protección de los datos personales como un derecho constitucional. Esta reforma atribuye a cada individuo la facultad de controlar, disponer y decidir sobre sus datos personales, estableciendo así un derecho de autodeterminación informativa que se suma al artículo 19, numeral 4, junto al respeto y protección de la vida privada y la honra aunque de forma no subordinada a ellos. De esta forma, la garantía

[1] El Decreto Nº 100 del Ministerio Secretaría General de la Presidencia, de 22 de septiembre de 2005, fijó el texto refundido de la Constitución después de una serie de reformas. A la fecha del cierre de este informe la última reforma data de enero de 2024.

de este derecho se puede ejercer frente a afectaciones, perturbaciones o amenazas mediante la acción de protección (artículo 20), además de los recursos legales como el habeas data (Ley N° 19.628).

2.2. Legislación

2.2.1. Ley Marco de Ciberseguridad

La Ley Marco de Ciberseguridad (LMC) fue presentada al Congreso en marzo de 2022 y aprobada en diciembre de 2023, publicada en abril de 2024 como Ley N° 21.663. Esta iniciativa crea un modelo de gobernanza en ciberseguridad, que promueve la gestión de riesgos y la implementación de estándares en los sectores público y privado, ampliando y fortaleciendo el trabajo preventivo. También propicia la formación de una cultura pública en materia de seguridad digital, enfrentando las contingencias en el aparato público y de la industria, resguardando la seguridad de las personas en el ciberespacio. Para la determinación de sus obligaciones, la Ley Marco incorpora los conceptos de "servicios esenciales" y "operadores de importancia vital", estableciendo un régimen de obligaciones de ciberseguridad y sanciones.

Para su puesta en práctica, la Ley Marco crea la Agencia Nacional de Ciberseguridad (ANCI) con facultades reguladoras, fiscalizadoras y sancionatorias para los organismos de la Administración del Estado y de las instituciones privadas en esta materia. El proyecto también crea el Consejo Multisectorial sobre Ciberseguridad, y un Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional).

2.2.2. Ley de protección de datos personales

La Ley N° 19.628 sobre "Protección de la Vida Privada" se publicó en el Diario Oficial de Chile el 28 de agosto de 1999. A pesar de ser una ley pionera en la región, sucesivos ajustes a su articulado intentaron adaptarla a las necesidades propias de una sociedad cada vez más digitalizada y conectada.

Las principales características de la Ley N° 19.628 incluyen la regulación del tratamiento de datos personales, aunque con deficiencias significativas como la ausencia de una institución autónoma para la supervisión de su cumplimiento y la falta de claridad en el manejo de flujos de información internacional. Además, no se alinea completamente con los estándares internacionales de protección de datos, lo cual se volvió crítico tras la incorporación de Chile a la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en 2010 y la elevación de la protección de datos personales a rango constitucional en 2018.

En 2024, se aprobó una reforma integral a la Ley N° 19.628, que busca modernizar su articulado para cumplir con los estándares internacionales de privacidad. Esta

reforma introduce nuevas bases legales para el tratamiento de datos, como el consentimiento explícito o las autorizaciones legales, y establece principios de transparencia, seguridad y calidad en el manejo de la información. También crea la Agencia de Protección de Datos Personales, autoridad de control encargada de vigilar el cumplimiento de estas normas, cuya ausencia fue un punto sensible durante 25 años de vigencia de la Ley Nº 19.628. Esta reforma entrará plenamente en vigor dos años después de su publicación en el Diario Oficial.

2.2.3. Ley de delitos informáticos

La Ley Nº 21.459, publicada el 20 de junio de 2022, actualizó la legislación chilena en materia de delitos informáticos, derogando y reemplazando a la antigua Ley Nº 19.223 sobre delitos informáticos, además de incluir una serie de otras modificaciones legales, todo con el objeto de adecuar la legislación al Convenio sobre la Ciberdelincuencia del Consejo de Europa, (el Convenio de Budapest) ratificado Chile es parte desde el 2017.

La Ley Nº 21.459 prevé delitos específicos, entre ellos: el ataque a la integridad de un sistema informático, acceso ilícito, interceptación ilícita, ataque a la integridad de los datos informáticos, falsificación informática, receptación de datos informáticos, fraude informático y el abuso de dispositivos. Adicionalmente, se incorporan circunstancias modificatorias de responsabilidad penal, en especial, como atenuante, la cooperación eficaz, y como agravantes, cometer el delito abusando de una posición de confianza en la administración del sistema informático. No obstante, esta Ley no establece obligación de comunicar riesgos de ciberseguridad o pérdida de información.

Durante su discusión legislativa aparecieron propuestas para introducir una exención de responsabilidad para investigadores en seguridad que actuaran de buena fe. La propuesta fue continuamente reducida durante la tramitación, culminando en la curiosa despenalización del acceso no autorizado, cuando existe autorización. La exención sería modificada por una más elaborada a través de la LMC, a favor de hipótesis muy específicas y reducidas de investigación sobre sistemas del Estado.

2.2.4. Procedimientos administrativos y transformación digital del Estado

El 11 de noviembre de 2019 se publicó la Ley Nº 21.180 sobre Transformación Digital del Estado. Su finalidad es dar inicio al proceso de digitalización y modernización de los procedimientos administrativos seguidos ante los órganos de la administración del Estado. De esta forma, se pretende digitalizar trámites ante servicios públicos, simplificar y eliminar trámites que las personas realizan ante el Estado. Además, se crea un Archivo Nacional digital que registrará de forma mucho más eficiente toda la información de los servicios públicos.

En concordancia con el objetivo que persigue la ley, esta introduce modificaciones en la Ley Nº 19.880, en su artículo 19, sobre el uso obligatorio de plataformas electrónicas, señalando que los organismos de la administración del Estado tienen la obligación de emplear y gestionar adecuadamente plataformas digitales para la administración de expedientes electrónicos, plataformas que "deberán cumplir con estándares de seguridad, interoperabilidad, interconexión y ciberseguridad". Esto condiciona en general la forma en que el Estado administrador debe proveer sus servicios por vías electrónicas.

2.2.5. Ley Fintec

El 4 de enero de 2023 se publicó la Ley Nº 21.521, "Promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros, Ley Fintec". La normativa procura lograr los objetivos en su título bajo condiciones de adecuada protección de los clientes, resguardo de los datos personales, medidas ciberseguridad, preservación de la integridad y estabilidad financiera, y prevención del lavado de activos y financiamiento del terrorismo. Asimismo, encarga a la Comisión para el Mercado Financiero (CMF), entre otros, la regulación y supervisión de las entidades que se inscriben en el Registro de Prestadores de Servicios Financieros (RPSF). La ley ordena a la CMF establecer, mediante norma de carácter general, los estándares de gobierno corporativo y gestión de riesgos, incluyendo aspectos de ciberseguridad y seguridad de información. Además crea obligaciones para sujetos obligados dentro del mercado financiero para "*adoptar las medidas necesarias para cumplir con los estándares mínimos de seguridad de información, ciberseguridad y políticas de gestión de riesgos y control interno*" establecidas por normas de la CMF, con el objeto de resguardar la confidencialidad, integridad y disponibilidad de los datos y de la información.

2.3. Decretos y reglamentos

— **Decreto Supremo N° 5.996, de 1999, del Ministerio del Interior:** Crea la Red Interna del Estado (Intranet) para mejorar la comunicación y colaboración entre las instituciones gubernamentales, detallando procedimientos para su implementación y asignando responsabilidades específicas al Ministerio del Interior.

— **Decreto Supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia:** Aprueba la "Norma Técnica sobre Seguridad y Confidencialidad del Documento Electrónico para los Órganos de la Administración del Estado", estableciendo características mínimas obligatorias de seguridad y confidencialidad para documentos electrónicos.

— **Decreto Supremo N° 1.299, de 2005, del Ministerio del Interior:** Regula la Red de Conectividad del Estado, estableciendo normas para la interconexión segura entre instituciones públicas, definiendo estándares de seguridad, interoperabilidad y acceso para el intercambio eficiente de información.

— **Decreto Supremo N° 93, de 2006, del Ministerio Secretaría General de la Presidencia:** Establece una norma técnica para combatir el spam en las casillas electrónicas de los órganos del Estado y de sus funcionarios, incluyendo disposiciones para la detección, filtrado y prevención del correo no deseado.

— **Decreto Supremo N° 14, de 2014, del Ministerio Secretaría General de la Presidencia:** Modifica el Decreto N° 181, de 2002, actualizando las disposiciones de la Ley 19.799 sobre documentos electrónicos y firma electrónica, adaptándolas a los avances tecnológicos para asegurar su validez jurídica en procesos digitales.

— **Decreto Supremo N° 533, de 2015, del Ministerio del Interior y Seguridad Pública:** Crea el Comité Interministerial sobre Ciberseguridad (CICS), una comisión asesora presidencial permanente encargada de elaborar la Política Nacional de Ciberseguridad 2017-2022 y sugerir alternativas para su seguimiento e implementación.

— **Decreto Supremo N° 1, de 2015, del Ministerio Secretaría General de la Presidencia:** Aprueba normas técnicas para los sistemas y sitios web de los órganos de la Administración del Estado, estableciendo estándares de accesibilidad, seguridad, diseño y usabilidad para garantizar una experiencia de usuario coherente y segura.

— **Decreto Supremo N° 83, de 2017, del Ministerio de Relaciones Exteriores:** Promulga el Convenio sobre la Ciberdelincuencia, conocido como Convenio de Budapest, que establece un marco internacional para la cooperación en la prevención, investigación y persecución de delitos informáticos, además de definir estándares para la recolección de pruebas electrónicas.

— **Instructivo Presidencial N° 8, de 2018:** Imparte instrucciones urgentes en materia de ciberseguridad a los órganos de la administración del Estado, incluyendo medidas como la designación de un encargado de ciberseguridad de alto nivel en cada servicio, actualización de normativa técnica, medidas internas de ciberseguridad, revisión de redes y plataformas críticas, vigilancia de la infraestructura tecnológica, reporte y respuesta a incidentes, y gobernanza transitoria de ciberseguridad.

— **Decreto Supremo N° 4, de 2020, del Ministerio Secretaría General de la Presidencia:** Regula el uso de medios electrónicos en los procedimientos administrativos, promoviendo la interoperabilidad entre los sistemas digitales de los órganos del Estado, la simplificación de trámites y la transparencia en la gestión pública, conforme a la Ley 21.180 sobre Transformación Digital del Estado.

— **Decreto Supremo N° 579, de 2020, del Ministerio del Interior y Seguridad Pública:** Modifica el Decreto Supremo N° 533/2015 y crea la Comisión Técnica Asesora del CICS, para apoyar y proponer el seguimiento y avance de la Política Nacional de Ciberseguridad 2017-2022, así como el cumplimiento de sus funciones.

— **Decreto N° 273, de 2022, del Ministerio del Interior y Seguridad Pública:** Establece la obligación de reportar incidentes de ciberseguridad. Los jefes de servicios y demás órganos de la administración del Estado deben informar al Ministerio del Interior y Seguridad Pública sobre los incidentes que les afecten, mediante notificación al CSIRT del Gobierno.

— **Decreto Supremo N° 7, de 2023, del Ministerio Secretaría General de la Presidencia:** Establece la "Norma Técnica de Seguridad de la Información y Ciberseguridad" conforme a la Ley N° 21.180, definiendo estándares y directrices técnicas que deben cumplir los órganos de la Administración del Estado para resguardar la confidencialidad, integridad y disponibilidad de la información, así como la infraestructura informática de las plataformas electrónicas que sustentan sus procedimientos administrativos.

— **Decreto Supremo N° 107, de 2023, del Ministerio del Interior y Seguridad Pública:** Modifica el Decreto Supremo N° 533, de 2015, incorporando a la Subsecretaría de Ciencia, Tecnología, Conocimiento e Innovación como integrante permanente del Comité Interministerial sobre Ciberseguridad, fortaleciendo la coordinación en materias de ciberseguridad.

— **Decreto Supremo N° 164, de 2023, del Ministerio del Interior y Seguridad Pública:** Aprueba la Política Nacional de Ciberseguridad 2023-2028, definiendo cinco pilares estratégicos: protección de la infraestructura crítica, gestión de riesgos, desarrollo de capacidades, colaboración internacional y educación en ciberseguridad, estableciendo un plan de acción para fortalecer la seguridad digital a nivel nacional.

2.4. Normativa sectorial

— **Norma Técnica sobre Fundamentos Generales de Ciberseguridad para el Diseño, Instalación y Operación de Redes y Sistemas Utilizados para la Prestación de Servicios de Telecomunicaciones (2020).**[2] Emitida por la Subsecretaría de Telecomunicaciones, esta norma establece los principios básicos de ciberseguridad que deben considerarse en el diseño, instalación y operación de redes y sistemas utilizados para la prestación de servicios de telecomunicaciones.

[2] Disponible en: https://www.subtel.gob.cl/wp-content/uploads/2020/08/ResEx1318_Aprueba_Norma_Tecnica_Ciberseguridad.pdf

— **Instructivo de Seguridad de la Información y Ciberseguridad para el Sector Salud (2021).**[3] Elaborado por la Subsecretaría de Redes Asistenciales, este instructivo define directrices específicas para proteger la información y los sistemas en el ámbito sanitario, garantizando la confidencialidad, integridad y disponibilidad de los datos relacionados con la atención en salud.

— **Circular N° 3.265 que Imparte Instrucciones Relativas a los Lineamientos de Ciberseguridad que Deben Observar las Sociedades Operadoras y las Sociedades Concesionarias de Casinos de Juego (2018).**[4] Emitida por la Superintendencia de Casinos y Juegos, esta circular establece lineamientos de ciberseguridad que deben seguir las sociedades operadoras y concesionarias de casinos de juego para proteger sus sistemas tecnológicos y datos sensibles.

— **Resolución Exenta N° 250, de 2023, que aprueba el Compendio de Normas que regulan a las Cajas de Compensación de Asignación Familiar.** Emitido por la Superintendencia de Seguridad Social, reúne en un cuerpo único, coordinado y sistematizado, las normas que rigen sobre las cajas de compensación conforme a la Ley Nº 18.833 que establece el estatuto general para las mismas. El Compendio de Normas contiene en su Libro VI (Gestión de Riesgos), Título I (Riesgo Operacional), la sección 6.1.12 sobre Ciberseguridad,[5] incluyendo medidas específicas para gestionar riesgos operacionales y proteger la información sensible.

— **Modelo de Gestión de Seguridad de la Información y Ciberseguridad (2019).**[6] Desarrollado por la Superintendencia de Pensiones, este modelo proporciona directrices para que las entidades bajo su supervisión implementen medidas de ciberseguridad sólidas, incluyendo la adopción de planes de gestión de riesgos, capacitación y procedimientos para la detección y respuesta ante incidentes, en el ámbito de la seguridad de la información relativa al sistema de pensiones.

— **Norma de Carácter General N° 454: Impone Normas sobre Gestión de Riesgo Operacional y Ciberseguridad para Entidades Aseguradoras y Reaseguradoras (2021).**[7] Emitida por la Comisión para el Mercado Financiero (CMF), esta norma establece directrices para la gestión del riesgo operacional y ciberseguridad, incluyendo la identificación, evaluación y mitigación de riesgos. Requiere la implementación de políticas, procedimientos y controles, así como la realización de autoevaluaciones periódicas para fortalecer la resiliencia operativa de las entidades aseguradoras y reaseguradoras.

---

3 Disponible en: https://www.minsal.cl/sites/default/files/files/Normativa%20del%20Sistema%20de%20Gesti%C3%B3n%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf

4 Disponible en: https://www.scj.gob.cl/sites/default/files/2021-01/Circular%20de%20Ciberseguridad%20SCJ.pdf

5 Disponible en: https://www.suseso.cl/620/w3-propertyvalue-600756.html

6 Disponible en: https://www.spensiones.cl/portal/compendio/596/w3-propertyvalue-10526.html

7 Disponible en: https://www.cmfchile.cl/normativa/ncg_454_2021.pdf

— Norma de Carácter General N° 502: regula a los prestadores de servicios financieros tecnológicos según la Ley Fintec (2024).[8] Emitida por la CMF en enero de 2024, establece requisitos de registro y autorización para los servicios de la Ley Fintec, incluyendo directrices específicas en ciberseguridad para garantizar la integridad y protección de los datos financieros. Los prestadores deben implementar medidas de gestión de riesgos operacionales y de seguridad de la información, con énfasis en la protección contra amenazas cibernéticas.

— Recopilación Actualizada de Normas que Contiene Disposiciones Basadas en Buenas Prácticas para la Gestión de la Seguridad de la Información y Ciberseguridad (2020), Capítulo 20-10.[9] Emitido por la CMF, este capítulo establece lineamientos mínimos que deben cumplir las entidades supervisadas para proteger sus sistemas y datos frente a amenazas cibernéticas. Desarrolla en detalle los elementos mínimos para la gestión de la seguridad de la información y la ciberseguridad. Incluye aspectos como la protección de activos críticos, la detección de amenazas y vulnerabilidades, y la capacidad de respuesta y recuperación ante incidentes. Requiere la adopción de buenas prácticas internacionales en ciberseguridad y controles robustos.

— Directiva N° 32 que Contiene Recomendaciones para la Contratación de Servicios en la Nube (2021).[10] Emitida por ChileCompra, esta directiva orienta a las entidades públicas en la adquisición de servicios en la nube de manera segura y conforme a las mejores prácticas de ciberseguridad, asegurando la protección de la información sensible almacenada y procesada en dichos entornos.

— Circular Interpretativa sobre Buenas Prácticas en el Comercio Electrónico (Resolución Exenta N° 184, 2019).[11] Emitida por el Servicio Nacional del Consumidor (SERNAC), esta circular establece que los proveedores de servicios y productos a través de medios electrónicos deben adoptar medidas técnicas necesarias para asegurar la seguridad, integridad y confidencialidad de las transacciones y de los datos personales de los consumidores, además de proteger a consumidores vulnerables, como menores de edad.

— Circular Interpretativa sobre Criterios de Equidad en Contratos de Adhesión Referentes a la Recolección y Tratamiento de Datos Personales de los Consumidores (Resolución Exenta Nº 174, 2022).[12] En esta circular, el SERNAC aborda las cláusulas abusivas que eximen de responsabilidad al proveedor en casos de acceso no autorizado, pérdidas, alteraciones o filtraciones de datos personales de los consumidores, estableciendo que los proveedores deben aplicar medidas de seguridad integrales para proteger la confidencialidad, integridad y disponibilidad de los datos personales.

8 Disponible en: https://www.cmfchile.cl/portal/principal/613/articles-77283_recurso_1.pdf

9 Disponible en: https://www.cmfchile.cl/portal/principal/613/articles-29310_doc_pdf.pdf

10 Disponible en: https://www.chilecompra.cl/wp-content/uploads/2018/12/619-B-Res.-Aprueba-directiva-de-contratacion-publica-32-recomendaciones-para-la-Contratacion-de-Servicios-en-la-nube.pdf

11 Disponible en: https://www.sernac.cl/portal/618/articles-9195_archivo_01.pdf

12 Disponible en: https://www.sernac.cl/portal/618/articles-65388_archivo_01.pdf

— **Circular Interpretativa sobre Protección de los Consumidores frente al Uso de Sistemas de Inteligencia Artificial (Resolución Exenta Nº 33, 2022).**[13] El SERNAC emitió esta circular para establecer principios que resguarden los derechos de los consumidores en el contexto del uso de herramientas de Inteligencia Artificial por parte de los proveedores, enfocándose en garantizar el acceso adecuado a la información, el tratamiento seguro de los datos personales y la prevención de manipulaciones que puedan perjudicar a los consumidores.

— **Guía para el Resguardo de los Datos Personales en el Desarrollo e Implementación de Plataformas de Datos Abiertos por Parte de los Órganos de la Administración del Estado (2020).**[14] Emitida por el Consejo para la Transparencia (CPLT), esta guía proporciona directrices para que las instituciones públicas protejan los datos personales al implementar plataformas de datos abiertos, asegurando el respeto a la privacidad y la seguridad de la información de los ciudadanos.

— **Recomendaciones sobre Protección de Datos Personales por Parte de los Órganos de la Administración del Estado (2020).**[15] Emitidas por el Consejo para la Transparencia (CPLT), estas recomendaciones orientan a las entidades públicas en el cumplimiento de la normativa vigente sobre protección de datos personales. Promueven prácticas que garanticen la integridad, confidencialidad y disponibilidad de la información, previniendo riesgos de alteración, filtración, o acceso no autorizado.

— **Reglamento sobre Acciones Relacionadas con Salud a Distancia (2022).**[16] Emitido por el Ministerio de Salud, este reglamento regula las actividades de salud realizadas a través de tecnologías digitales, tanto en el sector público como en el privado. Exige a los proveedores de servicios de salud la aplicación de mecanismos de transmisión segura de datos, gestión de riesgos de privacidad y el reporte de incidentes de ciberseguridad al Comité de Seguridad de la Información del Ministerio.

2.5. Estrategias nacionales relevantes

2.5.1. Política Nacional de Ciberseguridad 2017-2022

El programa de gobierno de Michelle Bachelet propuso el desarrollo de una estrategia de seguridad digital que protegiera tanto a usuarios privados como públicos. En cumplimiento de este compromiso, en julio de 2015 se emitió el Decreto Supremo Nº 533 del Ministerio del Interior y Seguridad Pública, que creó el Comité Interministerial sobre Ciberseguridad (CICS). Este comité, como comisión

13 Disponible en: https://www.sernac.cl/portal/618/articles-64740_archivo_01.pdf

14 Disponible en: https://www.consejotransparencia.cl/guia-datos-abiertos-cplt.pdf

15 Disponible en: https://www.consejotransparencia.cl/recomendaciones-proteccion-datos.pdf

16 Disponible en: https://www.minsal.cl/reglamento-salud-distancia.pdf

asesora presidencial de carácter permanente, tuvo entre sus principales misiones la elaboración de la Política Nacional de Ciberseguridad 2017-2022 (PNCS) y la propuesta de mecanismos para su implementación y seguimiento.

En abril de 2017, se publicó oficialmente la Política Nacional de Ciberseguridad 2017-2022, estableciendo lineamientos estratégicos en esta materia, con el objetivo de fortalecer las capacidades del país frente a las amenazas del ciberespacio. Esta política se organizó en torno a dos fases: medidas específicas para ser implementadas en el período 2017-2018 y objetivos de largo plazo orientados a 2022. La PNCS definió cinco objetivos estratégicos clave: contar con una infraestructura de información fuerte y resiliente, velar por los derechos de las personas en el ciberespacio, fortalecer la cooperación nacional e internacional, desarrollar capacidades y cultura de ciberseguridad, y promover la innovación y el desarrollo en el ámbito digital.

En cuanto a su relación con los derechos fundamentales, la PNCS introdujo un enfoque de género de forma expresa, destacando la importancia de considerar la equidad de género como parte integral de las estrategias de ciberseguridad. Este enfoque busca garantizar la inclusión y protección de los derechos de todas las personas en el ciberespacio, promoviendo la igualdad en el acceso y uso seguro de las tecnologías digitales. Chile ha sido el único país de la región que dispuso explícitamente la consideración de un enfoque de género en materia de ciberseguridad.[17]

2.5.2. Política Nacional de Ciberseguridad 2023-2028

En mayo de 2023, el Comité Interministerial sobre Ciberseguridad presentó la propuesta de la nueva Política Nacional de Ciberseguridad 2023-2028, destinada a actualizar y guiar las directrices en esta materia para el período mencionado. Esta política fue oficialmente aprobada y publicada en el Diario Oficial mediante el Decreto Supremo N° 164 del Ministerio del Interior y Seguridad Pública.

La nueva política se estructura en torno a cinco objetivos fundamentales: infraestructura resiliente, protección de los derechos de las personas, cultura de ciberseguridad, coordinación nacional e internacional, y fomento a la industria y la investigación científica. Estos objetivos reflejan una continuidad con los establecidos en la Política Nacional de Ciberseguridad 2017-2022. La nueva política a la vez innova agregando cuatro objetivos transversales, que deben abordarse en todas las medidas propuestas: paridad de género, protección a la infancia, protección del adulto mayor y protección al medio ambiente.

El proceso de elaboración de esta política incluyó dos consultas públicas que permitieron recoger las opiniones de más de 1.000 ciudadanos de distintas regiones

17 Herrera Carpintero, P. (2020). El enfoque de género en la Política Nacional de Ciberseguridad de Chile. Revista Chilena De Derecho Y Tecnología, 9(1), 5–32. https://doi.org/10.5354/0719-2584.2020.51577

del país, quienes participaron activamente aportando ideas sobre los lineamientos propuestos. Estas contribuciones ayudaron a ajustar y enriquecer el contenido del documento final.

La Política supone la publicación de un Plan de Acción para detallar las medidas específicas a corto plazo, con revisiones periódicas planificadas para garantizar su cumplimiento y efectividad a lo largo del período 2023-2028. Este plan es anunciado como un documento separado y complementario, permitiendo el monitoreo y la evaluación continua de los avances en ciberseguridad. A la fecha de cierre de este documento ese plan no se conoce.

2.5.3. Política Nacional de Ciberdefensa

La Política Nacional de Ciberdefensa, aprobada a fines de 2017 y publicada en 2018, complementa la PNCS 2017-2022 y la PNCS 2023-2028, abordando específicamente la protección de las capacidades de la Defensa Nacional frente a amenazas en el ciberespacio. Se estructura en seis capítulos que abarcan el contexto tecnológico, principios rectores, modificaciones institucionales, asignación de roles dentro del sector defensa, un glosario y disposiciones presupuestarias.

En el ámbito institucional, la política establece roles específicos para los actores del sector defensa, reconociendo al ciberespacio como una dimensión clave en las operaciones de defensa. Se enfatiza el respeto al marco jurídico nacional y a los tratados internacionales suscritos por Chile, asegurando que las acciones en ciberdefensa se alineen con el Derecho Internacional, incluyendo los Derechos Humanos y el Derecho Internacional Humanitario. Además, se promueve la cooperación internacional para prevenir actividades cibernéticas ilícitas que afecten al país, fortaleciendo la infraestructura de información para que sea robusta y resiliente ante incidentes de ciberseguridad.

La política también subraya la importancia de fomentar una cultura de ciberseguridad basada en la educación y las buenas prácticas, tanto en el sector defensa como en la sociedad en general. Al complementar la PNCS, la Política Nacional de Ciberdefensa busca asegurar un ciberespacio libre, abierto, seguro y resiliente, protegiendo la soberanía nacional y los derechos de las personas en el ámbito digital.

2.5.4. Estrategia de Transformación Digital del Estado

El 28 de enero de 2019, el Gobierno de Chile publicó la Estrategia de Transformación Digital del Estado, con el objetivo de establecer definiciones, lineamientos e iniciativas para avanzar hacia un Estado Digital que facilite instituciones públicas modernas y eficientes, enfocadas en satisfacer las necesidades de las personas.

Uno de los principios fundamentales de esta estrategia es la ciberseguridad, protección de datos y privacidad. Se subraya la importancia de garantizar la seguridad de las plataformas digitales y la protección de los datos personales, promoviendo la confianza de la ciudadanía en los servicios públicos digitales.

Entre las líneas de acción definidas en la estrategia, la quinta línea aborda las medidas de ciberseguridad necesarias para asegurar la continuidad operativa de los servicios ofrecidos por el Estado a través de plataformas y sistemas digitales. Este enfoque no solo garantiza la disponibilidad permanente de los servicios, sino también la protección de la integridad y confidencialidad de la información administrada, particularmente cuando involucra datos personales proporcionados por los ciudadanos.

En cuanto a las áreas de trabajo del Gobierno Digital, la ciberseguridad se encuentra entre las políticas y estándares prioritarios. La Estrategia establece que, en colaboración con el Ministerio del Interior y Seguridad Pública, se desarrollarán normativas, legislación y acciones concretas para definir los estándares mínimos de ciberseguridad que las instituciones públicas deberán cumplir. Estos estándares tienen como objetivo la protección de los datos y la privacidad de las personas que interactúan con los servicios estatales.

A fines del año 2019, se promulgó la Ley 21.180 que obliga a las instituciones del Estado a adoptar las medidas para avanzar en Transformación Digital en los próximos años.

2.5.5. Política Nacional de Inteligencia Artificial

El 28 de octubre de 2021, el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación de Chile publicó la Política Nacional de Inteligencia Artificial, junto con un Plan de Acción. La Política tiene tres áreas de enfoque, y en la primera (factores habilitantes) regula los datos. En ella fomenta y consolida una agenda de datos de interés público, que resulte tanto en certezas legales como en definiciones claras de responsabilidades al interior del Estado, y que impulse un ecosistema público-privado de generación y acceso a datos de calidad para el uso y desarrollo de IA y tecnologías afines.

Además, la Política en su eje 3 incorpora la IA en las estrategias de ciberseguridad y ciberdefensa, así como en proyectos de ley asociados a ellas. El objetivo es posicionar la IA como un componente relevante en estos ámbitos, promoviendo sistemas tecnológicos seguros. También fomenta el uso de sistemas de IA para reaccionar a los ataques informáticos en el Estado, promueve la capacitación en IA en las áreas asociadas a la ciberseguridad y llama a incorporar la IA en la institucionalidad pública de ciberseguridad.

3. Institucionalidad

3.1. Institucionalidad a nivel nacional

— **Agencia Nacional de Ciberseguridad (ANCI):** La promulgación de la Ley Marco de Ciberseguridad en abril de 2024 creó la ANCI como un organismo autónomo, encargado de regular, fiscalizar y sancionar a los órganos públicos y los organismos privados que prestan servicios esenciales. Entre sus principales atribuciones se encuentran asesorar al Presidente en la formulación de políticas, planes y programas de acción en ciberseguridad, y coordinar con otros organismos para fortalecer la seguridad del ciberespacio nacional. Tiene responsabilidades específicas, como elaborar e implementar planes y capacitaciones para promover una cultura de ciberseguridad entre los ciudadanos, supervisar al CSIRT Nacional y otros CSIRT sectoriales dentro de la Administración Pública, y coordinar con el CSIRT de la Defensa Nacional la definición de estándares y plazos para la comunicación de incidentes de ciberseguridad o vulnerabilidades. A la fecha de cierre del presente informe, no se ha hecho instalación de la ANCI.

— **Consejo Multisectorial sobre Ciberseguridad:** Órgano asesor de la Agencia Nacional de Ciberseguridad (ANCI), encargado de analizar y revisar periódicamente la situación de ciberseguridad del país. Está integrado por el Director Nacional de la ANCI, quien lo preside, y seis consejeros ad honorem de distintos sectores, designados por el Presidente de la República. Su función principal es formular recomendaciones para enfrentar amenazas actuales o potenciales en el ciberespacio. A la fecha de cierre del presente informe, no se ha hecho instalación de este Consejo.

— **Comité Interministerial de Ciberseguridad (CICS):** Con existencia formal desde 2015, el CICS tiene como objetivo coordinar las políticas y estrategias nacionales en materia de ciberseguridad. Está integrado por representantes de las subsecretarías de Interior, Defensa, Relaciones Exteriores, Justicia, General de la Presidencia, Telecomunicaciones, Economía, Hacienda, Minería, Energía y Ciencia, además de la Dirección Nacional de la Agencia Nacional de Inteligencia. Su objetivo es articular esfuerzos entre las distintas instituciones del Estado para fortalecer la protección de las infraestructuras críticas de información y garantizar la seguridad digital en el país.

— **Equipo de Respuesta ante Incidentes de Seguridad Informática:** el CSIRT Nacional. El CSIRT de Gobierno fue establecido en marzo de 2018 como una agencia gubernamental dependiente del Ministerio del Interior y Seguridad Pública, con el objetivo de fortalecer y promover buenas prácticas, políticas y estándares de ciberseguridad en los órganos de la administración del Estado y las infraestructuras críticas del país. Con la promulgación de la LMC, se creó el CSIRT Nacional, que asume funciones más amplias y específicas en la coordinación y respuesta a incidentes de ciberseguridad de efecto significativo en el país. Este nuevo marco legal establece una estructura más robusta para la ciberseguridad nacional, integrando al CSIRT Nacional en una estrategia coordinada bajo la supervisión de la Agencia Nacional de Ciberseguridad (ANCI), con el fin de mejorar la protección

de las infraestructuras críticas y la respuesta a amenazas cibernéticas. Tiene como función principal responder ante ciberataques o incidentes de ciberseguridad de efecto significativo, coordinando con otros CSIRT de la Administración del Estado y sirviendo como punto de enlace con equipos similares en el extranjero.

— **CSIRT de la Defensa Nacional:** Equipo de Respuesta a Incidentes de Seguridad Informática dependiente del Ministerio de Defensa Nacional y operado por el Estado Mayor Conjunto. Su misión es coordinar, proteger y asegurar las redes y sistemas del Ministerio, así como los servicios esenciales para la defensa nacional. Entre sus funciones se incluye conducir y asegurar la protección contra riesgos y amenazas en el ciberespacio, preservando la confidencialidad, integridad y disponibilidad de las redes de información críticas para la defensa del país.

— **Ministerio de Seguridad Pública:** Durante 2024 quedó aprobada la ley que crea el Ministerio de Seguridad Pública, nueva secretaría encargada de colaborar con el Presidente de la República en la promoción, mantenimiento y protección de la seguridad pública, el orden público y la prevención del delito. El Ministerio de Seguridad Pública tiene entre sus atribuciones en materia de ciberseguridad diseñar y aprobar políticas, planes y programas para prevenir, detectar y neutralizar amenazas en el espacio digital, especialmente en relación con servicios esenciales y operadores de importancia vital. Además, es responsable de coordinar la implementación de estas medidas con otros organismos competentes y garantizar la protección de la infraestructura crítica. Por su parte, la Subsecretaría de Seguridad Pública, como órgano de colaboración inmediata, supervisa la formulación y ejecución de estas políticas y asegura la coherencia en su aplicación. Además, diseña e implementa medidas específicas para gestionar los riesgos asociados al ámbito digital y promueve la interoperabilidad entre las instituciones públicas en esta materia. A la fecha de cierre del presente informe, la normativa está aprobada por el Congreso.

— **Agencia de Protección de Datos Personales:** Creada por la Ley de Protección de Datos Personales aprobada en 2024, es un organismo autónomo responsable de fiscalizar el cumplimiento de la normativa en materia de privacidad y aplicar sanciones por infracciones clasificadas como leves, graves o gravísimas. Sus funciones incluyen supervisar el tratamiento de datos personales, certificar medidas de seguridad, exigir notificaciones de vulnerabilidades, y garantizar la implementación de políticas de privacidad. Además, la Agencia promueve programas de cumplimiento voluntarios que, en caso de infracción, pueden atenuar las sanciones aplicables. A la fecha de cierre del presente informe, la Agencia no está instalada ni en operaciones.

3.2 Reguladores con competencias sectoriales

— **Subsecretaría de Telecomunicaciones de Chile (SUBTEL):** SUBTEL es la entidad gubernamental responsable de proponer y supervisar la implementación de políticas nacionales en materia de telecomunicaciones, asegurando el desarrollo y regulación del sector en el país. En cuanto a ciberseguridad, SUBTEL ha establecido normas técnicas que definen los fundamentos generales para el diseño, instalación y operación de redes y sistemas utilizados en la prestación de servicios de telecomunicaciones, con el fin de proteger la infraestructura crítica y la información que circula a través de estas redes.

— **Subsecretaría del Interior:** Esta entidad coordina y ejecuta políticas relacionadas con la seguridad interior y el orden público en Chile. A través de su División de Redes y Seguridad Informática, proporciona plataformas tecnológicas que apoyan la gestión del Ministerio del Interior, incluyendo conectividad, servicios TI y sistemas de información. Además, asiste en el desarrollo tecnológico gubernamental para mejorar la gestión y el acercamiento a la ciudadanía, incorporando medidas de ciberseguridad para proteger la información y los sistemas del Estado.

— **Ministerio de Salud (MINSAL):** El MINSAL es responsable de la formulación y ejecución de políticas públicas de salud en Chile. En el ámbito de la ciberseguridad, promueve la implementación de un Sistema de Seguridad de la Información para mitigar riesgos asociados a los activos de información. Cuenta con un instructivo de ciberseguridad para el sector salud, una política de protección de datos personales y una resolución que aprueba cláusulas de protección de datos, asegurando la confidencialidad y seguridad de la información sanitaria.

— **Consejo para la Transparencia (CPLT):** El CPLT es una corporación autónoma de derecho público encargada de velar por el cumplimiento de la Ley de Transparencia y el derecho de acceso a la información pública en Chile. En materia de ciberseguridad, supervisa que los órganos de la Administración del Estado cumplan con la Ley N° 19.628 sobre protección de datos personales. Ha emitido recomendaciones y guías para instituciones públicas, y ha establecido procedimientos para el tratamiento de solicitudes relacionadas con los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), promoviendo la adopción de medidas de seguridad para salvaguardar la integridad, confidencialidad y disponibilidad de los datos personales.

— **Servicio Nacional del Consumidor (SERNAC):** El SERNAC es la institución encargada de proteger y promover los derechos de los consumidores en Chile. Tras la promulgación de la Ley Nº 21.398 (Ley Pro Consumidor), asumió funciones transitorias en la supervisión de la protección de datos personales en relaciones de consumo, hasta que se establezca un organismo especializado. Sus facultades incluyen presentar demandas colectivas por violaciones de datos personales, supervisar el cumplimiento de las normativas, realizar mediaciones, solicitar informes y emitir circulares interpretativas relacionadas con la seguridad de la información y ciberseguridad, aplicables a sus funcionarios, con el objetivo de garantizar la protección de los datos de los consumidores.

— **Comisión para el Mercado Financiero (CMF):** La CMF es un servicio público técnico encargado de supervisar y regular las actividades y entidades que participan en los mercados financieros de Chile, incluyendo valores, seguros y bancos, con el objetivo de asegurar su correcto funcionamiento, desarrollo y estabilidad. En el ámbito de la ciberseguridad, la CMF ha emitido normativas que obligan a las instituciones financieras a reportar incidentes de seguridad y a implementar medidas de gestión de riesgos operacionales y ciberseguridad, garantizando la integridad y confiabilidad del sistema financiero.

4. Análisis

El marco normativo e institucional en materia de ciberseguridad en Chile ha evolucionado en los últimos años con hitos clave como la promulgación de la Ley Marco de Ciberseguridad (2024) y la Ley de Protección de Datos Personales. Estos avances han establecido una base legal para abordar las crecientes amenazas digitales, destacando la creación de la Agencia Nacional de Ciberseguridad (ANCI) como eje central de la gobernanza en este ámbito. No obstante, debido a lo reciente de estos cambios normativos, aparecen desafíos importantes, particularmente en la puesta en operación de las nuevas instituciones, como la ANCI y la Agencia Nacional de Protección de Datos Personales, cuya instalación efectiva aún está pendiente. Esta brecha afecta la capacidad del Estado para responder a los riesgos cibernéticos emergentes.

La trayectoria de estas reformas muestra un progreso significativo, pero también revela áreas críticas de mejora en la implementación. La Política Nacional de Ciberseguridad 2023-2028, por ejemplo, incorpora objetivos innovadores y transversales, pero su efectividad dependerá del desarrollo del Plan de Acción y de la mencionada operación de las nuevas instituciones. Ello es relevante no solo para sus propias funciones, sino también para el cumplimiento de labores de coordinación entre organismos del Estado.

Finalmente, el éxito de esta transición normativa e institucional radica en garantizar el delicado equilibrio entre esta multiplicidad de instituciones y sus diferencias de objetivos y capacidades. Esto requiere una asignación adecuada de recursos, un seguimiento riguroso de los planes propuestos y una coordinación efectiva entre los organismos responsables. La capacidad del Estado para consolidar una gobernanza cibernética resiliente dependerá de cómo se aborden estos desafíos estructurales en el corto y mediano plazo.


DERECHOS
DIGITALES
América Latina