Seguridad de la Información

POLITICA NACIONAL DE CIBERSEGURIDAD Y LEY 21,663

Antecedentes generales 2025

IMPORTANCIA DE LA CIBERSEGURIDAD

Los ataques a EMCO, Ejército, INDAP, Poder Judicial, ChileCompras, GTD y a varias empresas, establecieron la urgencia e importancia de legislar, con un sentido de Estado.

POLITICA NACIONAL DE CIBERSEGURIDAD

Diciembre de 2023,

Se publicó en el Diario Oficial la nueva Política Nacional de Ciberseguridad que comprende el período 2023-2028.

Esta política se basa en las recomendaciones de la Guía para desarrollar una estrategia nacional de Ciberseguridad de la Unión Internacional de Telecomunicaciones, y que se observó la experiencia de países con un nivel similar al de Chile en la materia, como Argentina, Uruguay y República Dominicana, y de otros más avanzados, como Israel, Reino Unido y Estados Unidos.

Se menciona que el Comité Interministerial sobre Ciberseguridad (CIC) sugerirá alternativas de seguimiento e implementación de la Política, y asesorará el cumplimiento de sus medidas para conseguir los objetivos de política pública contenidos en este documento.

DIARIO OFICIAL
DE LA REPUBLICA DE CHILE
Ministerio del Interior y Seguridad Pública

I SECCIÓN

LEYES, REGLAMENTOS, DECRETOS Y RESOLUCIONES DE ORDEN GENERAL

Núm. 43.717 | Lunes 4 de Diciembre de 2023 | Página 1 de 12

Normas Generales

CVE 2415658

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA

Subsecretaría del Interior

APRUEBA POLÍTICA NACIONAL DE CIBERSEGURIDAD 2023-2028

Núm. 164.- Santiago, 16 de junio de 2023.

Vistos:

Lo dispuesto en los artículos 24, 32 Nº 6 y 35 del decreto supremo Nº 100, de 2005, del Ministerio Secretaría General de Presidencia, que fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile; 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; 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 la ley Nº 20.502, que crea el Ministerio del Interior y Seguridad Pública y el Servicio Nacional para la Prevención y Rehabilitación del Consumo de Drogas y Alcohol, y modifica diversos cuerpos legales; en el decreto supremo Nº 533, de 2015, del Ministerio del Interior y Seguridad Pública, que crea el Comité Interministerial sobre Ciberseguridad y su modificación mediante el decreto supremo Nº 579, de 2020, de la misma cartera de Estado; en el instructivo presidencial Nº 1, de 27 de abril de 2017, que Instruye Implementación de la Política Nacional sobre Ciberseguridad; en el acuerdo del Comité Interministerial sobre Ciberseguridad, tomado en sesión de fecha 25 de mayo de 2023, que aprueba la propuesta de Política Nacional de Ciberseguridad para el período

OBJETIVOS ESTRATÉGICOS

1.- Infraestructura resiliente
2.- Derecho de las personas
3.- Cultura de Ciberseguridad
4.- Coordinación nacional e internacional
5.- Fomento a la industria y la investigación científica

LEY MARCO SOBRE CIBERSEGURIDAD

- Aprobada en Diciembre 2023
- Promulgada por el Presidente Sr. Gabriel Boric en Marzo 2024
- 8 de abril 2024 se publicó en el Diario Oficial de Chile, Ley N°21.663

LEY CIBERSEGURIDAD : OBLIGACIONES E INFRACCIONES

1.- Implementar un Sistema de Gestión de Seguridad de la Información: Establecemos sistemas robustos para identificar y mitigar riesgos, garantizando la seguridad continua de las redes y sistemas informáticos.

2.- Establecimiento y cumplimiento de Planes de Continuidad Operacional y Ciberseguridad: Desarrollar e implementar planes estratégicos que aseguran la resiliencia operativa de la organización frente a incidentes de Ciberseguridad.

3.- Notificación de Incidentes: Implementar protocolos para la rápida identificación y notificación de ciberataques o incidentes de seguridad, asegurando una comunicación efectiva con los afectados y las autoridades pertinentes, en este caso CSIRT.

Infracciones establecidas por la Ley

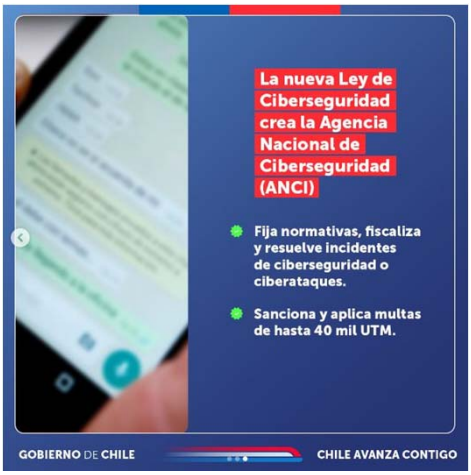
La falta de cumplimiento con la nueva ley puede resultar en severas sanciones, que varían según la gravedad de la infracción:

- Infracciones Leves: Pueden resultar en multas de hasta 5.000 Unidades Tributarias Mensuales (UTM).
- Infracciones Graves: Pueden acarrear multas de hasta 10.000 UTM.
- Infracciones Gravísimas: Estas infracciones pueden conllevar multas de hasta 20.000 UTM, y el doble para Operadores de Importancia Vital, llegando hasta 40.000 UTM.

CIBSERSEGURIDAD

La nueva normativa crea una legislación marco de Ciberseguridad con la instauración de la Agencia Nacional de Ciberseguridad (ANCI)

- ANCI se establece como un organismo público rector de la Ciberseguridad, fijará la normativa técnica, fiscalizará y podrá aplicar multas de hasta 40 mil UTM.
- Dictará protocolos y estándares para prevenir, reportar y resolver incidentes de Ciberseguridad o ciberataque
- Podrá calificar a servicios públicos como esenciales mediante resolución.
- Contará con autorización judicial si la Agencia requiere acceder a una red o sistema informático
- Regulará el funcionamiento de los Servicios Esenciales (SE) y los Operadores de importancia Vital (OIV), que son los prestadores de servicios esenciales.



CIBERSEGURIDAD

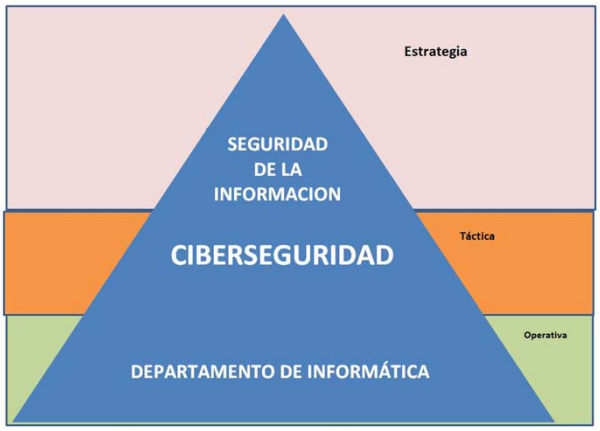
Servicios Esenciales (SE)

- Transporte terrestre, ferroviario o marítimo
- Banca, servicios financieros y medios de pago
- Administración de prestaciones de Seguridad social
- Servicios postales y de mensajería
- Prestación institucional de servicios de salud
- Producción y/o investigación de productos farmacéutico

Criterios

- Que la provisión de dicho servicio dependa de las redes y servicios informáticos.
- Que la afectación, interrupción o destrucción de sus servicios tenga un impacto significativo en la seguridad y orden público, en la provisión continua y regular de servicios esenciales, en el cumplimiento de las funciones del Estado o de los servicios que éste debe proveer o garantizar

LO QUE DEBIERA SER



Seguridad de la Información:

Establece políticas, procedimientos y manuales que dicen relación con la aplicación de estándares ISO 27001 – 27002 NIST, entre otros.

Ciberseguridad

Aplica procedimientos indicados por Seguridad de la Información, además, realiza configuración segura (hardening), técnicas de protección (Firewall, antivirus, IDS) realiza auditorias de eventos

Informática:

Gestiona AD, aplica controles establecidos por SI, configuración computadores – Importante actualizar sistemas operativos, cambio pcs antiguos.

SITUACION ACTUAL: CIBERSEGURIDAD

La operación de Informática debe estar balanceada con seguridad, y es difícil efectuarlo si ambas están "mezcladas", porque ya sabemos qué sucede cuando hay una urgencia operativa: TI está por encima de seguridad.

Las actividades de Informática –como administrar servidores, configurar telecomunicaciones, desarrollar, etc.– deben estar separadas de seguridad.

No se puede ser juez y parte a la misma vez.