H · D
LEGAL

HDGROUP.CL

# Alerta Legal

**Compliance - Fintech**

**Febrero 2025**

## CIBERSEGURIDAD

**DECRETOS QUE APRUEBAN EL FUNCIONAMIENTO DEL COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD (DECRETO N°275) Y DEL CONSEJO MULTISECTORIAL SOBRE CIBERSEGURIDAD (DECRETO N°276) Y RESOLUCIÓN QUE AUTORIZA LA PUBLICIDAD DE ALERTAS TEMPRANAS, AVISOS E INFORMACIÓN SOBRE RIESGOS E INCIDENTES DE CIBERSEGURIDAD POR PARTE DE LA CSIRT NACIONAL (RESOLUCIÓN EX. N°2).**

+56 2 2405 3200
AV. VITACURA 2939 – 8TH FLOOR
LAS CONDES, SANTIAGO, CHILE

El 12 de febrero de 2025 se publicó en el Diario Oficial en materia de Ciberseguridad, lo siguiente:

i. Decreto N°275 del Ministerio del Interior y Seguridad Pública, Subsecretaría del Interior, que aprueba el Reglamento de Funcionamiento del Comité Interministerial sobre Ciberseguridad.

ii. Decreto N°276 del Ministerio del Interior y Seguridad Pública, Subsecretaría del Interior, que aprueba el Reglamento que establece normas para el funcionamiento del Consejo Multisectorial sobre Ciberseguridad.

iii. Resolución Exenta N°2 del 15 de enero de 2025, del Ministerio del Interior y Seguridad Pública, Agencia Nacional de Ciberseguridad, en adelante, "ANCI", que autoriza la publicidad de alertas tempranas, avisos e información sobre riesgos e incidentes de ciberseguridad.

A continuación, desglosaremos los aspectos principales de dichas publicaciones.

**i. Decreto N°275 del Ministerio del Interior y Seguridad Pública, Subsecretaría del Interior, que aprueba el Reglamento de Funcionamiento del Comité Interministerial sobre Ciberseguridad.**

El objeto del presente reglamento consiste en regular el funcionamiento del Comité Interministerial sobre Ciberseguridad, en adelante, el "Comité", que fue creado en virtud del artículo 48 de la Ley

N°21.663, Ley Marco de Ciberseguridad, en adelante, "Ley". Dicho Comité tiene como propósito asesorar al Presidente de la República, en adelante, "PdR", en materias de ciberseguridad relevantes para el funcionamiento del país.

El presente Reglamento regula especialmente lo siguiente:

i. Objetivos y funciones del Comité.

Por ejemplo, se establece que el Comité deberá:

- Asesorar al PdR en el análisis y definición de la Política Nacional sobre Ciberseguridad;
- Proponer al PdR cambios a la normativa constitucional, legal o reglamentaria vigente en materias de ciberseguridad;
- Coordinar la implementación de la Política Nacional de Ciberseguridad;
- Apoyar las funciones de la ANCI.
- Revisar y considerar las recomendaciones del Consejo Multisectorial sobre Ciberseguridad.

ii. Colaboración con otros órganos de la Administración del Estado.

El Comité podrá solicitar a los órganos de la Administración del Estado, toda la colaboración necesaria para el cumplimiento de su cometido, dentro de sus competencias y atribuciones, especialmente, respecto de aquellas materias objeto de la Ley.

Las personas y entidades del sector privado podrán colaborar voluntariamente con el Comité.

iii. Integración del Comité.

El Comité se integrará por miembros permanentes que pertenecen a la Subsecretaría del Interior, de Defensa, Relaciones Exteriores, General de la Presidencia, Telecomunicaciones, Hacienda, Ciencia, Tecnología, Conocimiento e Innovación, además, por el Director Nacional de la Agencia Nacional de Inteligencia, y, por el Director Nacional de la Agencia Nacional de Ciberseguridad, quien lo presidirá y actuará de conformidad a la Ley.

iv. Funcionamiento del Comité.

Se regula el funcionamiento del Comité, entre los cuales, se encuentran las sesiones del Comité, quorum, citaciones, acuerdos, etc.

**ii. Decreto N°276 del Ministerio del Interior y Seguridad Pública, Subsecretaría del Interior, que aprueba el Reglamento que establece normas para el funcionamiento del Consejo Multisectorial sobre Ciberseguridad.**

El objeto del presente reglamento tiene por objeto regular el funcionamiento del Consejo Multisectorial sobre Ciberseguridad, en adelante, el "Consejo", creado en virtud del artículo 20 de la Ley.

Dicho Consejo tiene como propósito ser un órgano de carácter consultivo y su función consistirá en asesorar y formular recomendaciones a la ANCI, respecto de lo siguiente:

- Análisis y revisión periódica de la situación de ciberseguridad del país;
- En el estudio de las amenazas existentes y potenciales en el ámbito de ciberseguridad; y,
- Proponer medidas para abordar dichas amenazas.

i. Integración del Consejo.

El Consejo será integrado por las siguientes personas:

- Director Nacional de la ANCI.
- Dos personas provenientes del sector industrial o comercial.
- Dos personas del ámbito académico.
- Dos personas de las organizaciones de la sociedad civil, cuyo objeto o razón social se refiera a materias de la Ley.

ii. Funcionamiento del Consejo.

Se regula el funcionamiento del Comité, entre los cuales, se encuentran las sesiones del Comité, quorum, citaciones, acuerdos, etc.

El Consejo para su adecuado funcionamiento contará con el apoyo técnico y administrativo de la ANCI.

iii. **Resolución Exenta N°2 del 15 de enero de 2025, del Ministerio del Interior y Seguridad Pública, Agencia Nacional de Ciberseguridad, que autoriza la publicidad de alertas tempranas, avisos e información sobre riesgos e incidentes de ciberseguridad.**

La presente resolución autoriza al Equipo Nacional de Respuesta a Incidentes de Seguridad Informática, en adelante, "CSIRT Nacional", para difundir alertas tempranas, avisos e información sobre riesgos e incidentes para la comunidad.

Dicha autorización comprende las alertas de ciberseguridad, los avisos y los informes técnicos sobre vulnerabilidades de ciberseguridad que divulgue el CSIRT Nacional.

A continuación, desglosaremos su contenido:

Alerta de Seguridad: Consiste en aquella comunicación que tiene por objeto informar sobre una amenaza o vulnerabilidad específica y sobre las medidas que se deben adoptar para proteger la infraestructura de redes y sistemas informáticos.

Existen al menos, las siguientes categorías de alertas:

i. Alertas de falsificación: información sobre sitios que se hacen pasar por otros, y que podrían intentar capturar credenciales u otra información sensible de personas.

ii. Alertas de incidentes: información urgente sobre una vulnerabilidad que está siendo explotada activamente.

iii. Indicadores de compromiso: información urgente que permite identificar con un alto grado de probabilidad cuando un sistema ha sido comprometido. Se incluye en esta categoría información sobre malware, phishing, vishing, smishing y otros.

iv. Alertas de vulnerabilidad: información sobre vulnerabilidades en software y aplicaciones utilizadas en los activos informáticos en las organizaciones.

En cuanto a los avisos e informes técnicos, se incluye el siguiente listado:

i. Manuales: documentos que pueden servir de ayuda principalmente a los encargados de ciberseguridad para entender un tema específico.

ii. Guías: documentos que pueden servir al público general para entender aspectos técnicos sobre ciberseguridad.

iii. Informes: mensuales o anuales sobre información estadística que pueden ser de interés del público general sobre ciberseguridad.

iv. Otro tipo de información técnica de difusión.

Los canales de difusión serán aquellos medios de comunicación manuales o automáticos que utilice la ANCI, disponibles en la página web oficial de la ANCI https://anci.gob.cl/ y del CSIRT Nacional https://csirt.gob.cl/, o aquellas que las reemplacen, además de las cuentas institucionales de redes sociales que utilice.

**Para más información, contactar a:**


| | |
|---|---|
| **Matías Langevin**<br>**Socio Fintech**<br>**mlangevin@hdgroup.cl** | **Rebeca Zamora**<br>**Socia Compliance**<br>**rzamora@hdgroup.cl** |
| **Fernanda Aillach**<br>**Asociada Fintech**<br>**faillach@hdgroup.cl** | **Camilo Sanhueza**<br>**Asociado Compliance**<br>**csanhueza@hdgroup.cl** |