ECIJA OTERO
Av. Apoquindo 3669, Piso 13,
Las Condes, Santiago - Chile
Tel: +562 2361 8900
www.ecija.com

# Norma técnica sobre fundamentos generales de ciberseguridad

El pasado 14 de agosto fue publicada en el Diario Oficial la **Resolución Exenta número 1.318** del Ministerio de Transportes y Telecomunicaciones, que aprueba la **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**.

La norma aprobada tiene por objeto prevenir o reducir las posibilidades de que los servicios de telecomunicaciones sean interrumpidos o afectados por incidentes de seguridad informática, contribuir a prevenir los ataques de que puedan ser objeto los usuarios durante su desenvolvimiento en el ciberespacio y facilitar la posterior investigación de tales hechos.

Se busca evitar toda afectación o interrupción importante de los servicios de telecomunicaciones que pueda generar graves perjuicios al bienestar, la salud y la seguridad de la población, así como a la integridad de las instituciones públicas e, inclusive, a la seguridad nacional.

Dentro de los **aspectos principales** de esta norma, cabe destacar los siguientes:

I. Establece un marco regulatorio que comprende los fundamentos generales de ciberseguridad en base a los cuales deben ser diseñadas, instaladas y operadas de manera segura las redes y sistemas utilizados para la prestación de servicios de telecomunicaciones regulados por la Ley General de Telecomunicaciones (ley N°18.168).

II. Norma los reportes sobre ciberincidencias que los concesionarios y permisionarios de servicios de telecomunicaciones deben enviar a la Subsecretaría de Telecomunicaciones o Subtel.

III. Dispone que todo operador de servicios públicos de transmisión de datos, indistintamente de si es o no relevante, deberá implementar medidas técnicas y de organización para gestionar los riesgos de ciberseguridad de las redes y sistemas que utiliza para la prestación de servicios de telecomunicaciones a sus usuarios, indistintamente de si tal gestión estuviere o no externalizada.

IV. Define al Operador Relevante como todo proveedor de servicio público, intermedio o limitado de telecomunicaciones que haya sido declarado como relevante por la Subtel mediante resolución fundada para los efectos de la misma norma, así como todas aquellas entidades que operen sistemas de

telecomunicaciones que hayan sido declarados como infraestructura crítica de Nivel 1 o Nivel 2 conforme el reglamento pertinente. Asimismo, serán considerados operadores relevantes los ISP Relevantes Móviles y los ISP Relevantes Fijos.

V. Como **medidas de prevención y mitigación,** establece que los operadores deberán tomar las medidas adecuadas para prevenir y reducir al mínimo los efectos de las ciberincidencias que afecten la seguridad de las redes y sistemas utilizados para la prestación de los servicios, con el objeto de garantizar su continuidad operativa. En todos los casos, se deberá diseñar, implementar, practicar y evaluar un plan de respuesta que otorgue adecuada cobertura a sus redes y sistemas en conformidad con estándares internacionales o nacionales, y deberán aplicar criterios orientados a minimizar los riesgos de ciberincidencias y a facilitar una adecuada gestión de éstas durante su operación, mantención y optimización.

VI. Conforme a ella, los operadores deberán contar con **planes de gestión de riesgos** de ciberseguridad formulados con arreglo a principios, estándares y directrices que guarden la debida coherencia con las características de las redes y sistemas a los cuales se aplican. Los planes de gestión deberán estar permanentemente actualizados.

VII. Establece que todo operador relevante deberá contar con un equipo de respuesta para la adecuada gestión de la ciberseguridad. Además, deberá contar permanentemente con una **unidad de ciberseguridad** integrada por, a lo menos, un titular y un suplente. Por su parte, los operadores no relevantes deberán contar permanentemente con, al menos, un encargado titular de ciberseguridad en funciones y un suplente.

VIII. Establece como **obligación de los operadores reportar todas las ciberincidencias** que detecten en sus redes y sistemas y que alcancen los Niveles de peligrosidad e impacto establecidos en esta normativa. Los reportes deberán comunicarse a la Subsecretaría de Telecomunicaciones, al CSIRT de referencia o al órgano que designe para dichos fines.

IX. Dispone que los reportes de ciberincidencias **deberán omitir todo dato de carácter personal o información personal de carácter sensible**, así como toda otra información a partir de la cual sea posible inferirlos. Asimismo, en los casos en que la autoridad competente instruya al operador para que envíe a un tercero una copia de un reporte, deberá eliminar todos los datos personales o que permitan deducir la identidad de la persona aludida.

X. Respecto a su **fiscalización**, será la Subsecretaría de Telecomunicaciones la encargada de fiscalizar el cumplimiento de la norma aprobada, pudiendo para ello recurrir a las sanciones establecidas en la Ley General de Telecomunicaciones.

Javier Sabido.: jsabido@ecija.com