FCI Ltda..

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 5.	Teniendo en consideración que tanto las redes y sistemas utilizados para la prestación de servicios de telecomunicaciones, como la infraestructura crítica podrían ser victimas de ciberataques o ciberdelitos, es que se hace imprescindible que los operadores cuenten con todos los medios para realizar una investigación forense adecuadamente y un correcto tratamiento de la evidencia digital, para tener la certeza que puedan presentar evidencia con alto valor probatorio en procesos judiciales y así perseguir eficientemente responsabilidades de los cibercriminales. Se propone que las etapas mencionadas se alinean con las utilizadas internacionalmente, en normas técnica tales como: • ISO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processes • ISO/IEC 27042:2015 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence • ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

	Como también con las normas técnicas nacionales publicadas por el Instituto Nacional de Normalización, tales como: • NCh-ISO27037:2015 Tecnología de la información - Técnicas de seguridad - Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital • NCh-ISO IEC 27042:2019 Tecnología de la información - Técnicas de seguridad - Directrices para el análisis e interpretación de evidencia digital • NCh-ISO IEC 27043:2018 Tecnología de la información - Técnicas de seguridad - Principios y procesos de investigación de incidentes Por lo tanto, se propone la incorporación del siguiente párrafo "El operador realiza un proceso de investigación forense para las ciberincidencias relevantes, ciberataques y ciberdelitos, efectuados tanto por personal interno como también desde el exterior. Que considere al menos las etapas de identificación, recopilación, adquisición, examen y análisis de evidencias digitales, junto con la generación de documentación e informes de la investigación forense, interpretación de evidencia digital y las conclusiones del trabajo realizado; además de cumplir los requerimientos necesarios para preservar y realizar adecuadamente la

	cadena de custodia de las evidencias digitales obtenidas y generadas. Este proceso de investigación forense debe ser realizado exclusivamente por personal con competencias comprobables, como también con absoluta independencia e imparcialidad, para asegurarse que sus análisis, interpretaciones y conclusiones sean libres de sesgos, como también de eventuales presiones indebidas”.
Artículo 9.	Se propone aumentar el nivel de exigencia para la preservación de la evidencia digital de un ciberataque, por medio de las modificaciones incorporadas al siguiente párrafo. "Asimismo, el operador afectado deberá conservar por, a lo menos, seis meses desde el cierre de la ciberincidencia, todos los logs, registros y cualquier evidencia digital que hubieren podido registrar efectos y actividades relacionadas con el posible ataque, asegurando y preservando su integridad y autenticidad por todos los medios tecnológicos y procedimientos que sean necesarios, así como las medidas de gestión y resolución adoptadas."