Ciberseguridad en Chile: Retos Actuales y Proyecciones Futuras

Catalina Mendoza Schmitz[1]

La (ciber)seguridad se ha convertido en un pilar fundamental en la era digital. Se entenderá por Ciberseguridad en Chile, como "la preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad. La resiliencia en ciberseguridad es la capacidad de una entidad para prevenir y resistir los incidentes de seguridad informática y para recuperarse de ellos" (BCN, 2024)[2].

Con la digitalización acelerada en todos los sectores, desde el comercio hasta la administración pública, la protección de datos y la prevención de ataques cibernéticos son prioridades estratégicas para los países. Chile no es la excepción. Por lo tanto, una ley que abarcara estos problemas de ciberseguridad era notoriamente necesaria en el país. En este contexto, la reciente "Ley Marco de Ciberseguridad y Protección de Infraestructura Crítica" (ley 21.663) representa un paso importante hacia la modernización del marco regulatorio en Chile, estableciendo nuevas normas y mecanismos que buscan garantizar un entorno digital más seguro para individuos, empresas e instituciones.

Ahora bien, una ley no quita el peligro que puede representar la realidad digital. Si bien Chile con el pasar de los años se ha posicionado como un país en que la tecnología es usada altamente por los ciudadanos y los negocios[3] había un vacío legal en cuanto a la regulación y el cuidado[4] de la ciberseguridad. Al respecto,

---

[1] Cientista Política – Universidad Alberto Hurtado. Master in "Politics and Governance in the Digital Age" University of Tartu, Estonia.

[2] "Ciberseguridad de los organismos del Estado e infraestructura crítica de la información". Ley Fácil. Biblioteca del Congreso de Chile. Mayo, 2024. Visto en: https://www.bcn.cl/portal/leyfacil/recurso/ciberseguridad-de-los-organismos-del-estado-e-infraestructura-critica-de-la-informacion

[3] Hay diversos estudios que mencionan esto. Mas, es interesante mencionar lo resaltado por la revista Forbes: "Chile es el país más avanzado en el desarrollo de IA en América Latina" (2024). Cuando hablamos de Inteligencia artificial (IA), el uso de la tecnología es mayor y más compleja, por lo tanto, que Chile sea considerado dentro de esto, es bastante interesante. Más información en https://forbes.cl/tecnologia/2024-09-24/liderazgo-tecnologico-chile-es-el-pais-mas-avanzado-en-el-desarrollo-de-ia-en-america-latina-segun-estudio

[4] Si bien en septiembre del 2018 se promulgó la Ley 21.113 que declaraba octubre como el Mes Nacional de Ciberseguridad, la cual tenía como fin concientizar sobre la ciberseguridad durante el mes de octubre. El mes de ciberseguridad fue lanzado por la Alianza Nacional de Ciberseguridad, del dpto. de Seguridad Nacional de USA. Más información en: https://staysafeonline.org/es/programs/cybersecurity-awareness-

con la publicación de la ley "Marco de Ciberseguridad", se establecen bases para la gestión de riesgos cibernéticos y define responsabilidades de distintos actores en la protección de infraestructura crítica (y los "Operadores de importancia vital"). Eso sí, se podría mencionar que uno de los mayores aportes de ésta es que "se posiciona *como el modelo de gobernanza* en materia de seguridad digital para todas y todos los ciudadanos y un paso que pone a Chile en la vanguardia a nivel latinoamericano" (FCFM, 2024)[5]. Si bien esta ley no representa un cambio mayor a nivel individual, sí pone énfasis en empresas que pueden tener un impacto en la sociedad. Por lo tanto, hay un mayor cuidado en ese sentido. Ya que la ciberseguridad no es una materia que se acote solo a una persona, el error o descuido de un individuo, puede afectar a miles. Los ataques de ciberseguridad en Chile son cada vez mayores[6] y de diferentes tipos; ransomware y phishing, los llamados DDoS (en palabras muy sencillas y burdas es cuando hay un ciber ataque que hace que un servidor se vea saturado, haciendo que los usuarios no puedan acceder a los servicios), así como la brecha de datos (y el peligro al robo de datos personales) y tantos otros. Es interesante señalar sólo algunos ataques al Estado de Chile, por ejemplo, el hackeo al poder judicial en septiembre del 2022, un malware en Sernac en agosto de ese mismo año, al Ministerio de Defensa el año 2023, etc. El Estado está bajo constante problemas de ciberseguridad, sus ciudadanos también. Según cifras internacionales, "Chile fue el cuarto país de Latinoamérica más afectados por ciberataques" (txsplus.com, 2024)[7]. En otras palabras "Chile recibió 6.000 millones de intentos de ciberataques en 2023" (Pezoa, 2024)[8]

¿Qué es la infraestructura crítica que se trata de proteger?

Son sistemas, activos esenciales, empresas, etc.; que otorgan especial énfasis al funcionamiento de la sociedad, como el transporte, la energía, comunicaciones, servicios financieros, entre otros. En fin, son

---

month/#:~:text=Acerca%20del%20Mes%20de%20Concientizaci%C3%B3n,Unidos%20en%20octubre%20de%202004. Se cree que la Agencia tendrá mayor énfasis a la concientización de los peligros y ventajas que tiene el uso del internet. Habrá que esperar para ver los resultados.

[5] "A un mes de la Ley Marco de Ciberseguridad: un paso clave para la protección digital ciudadana y Chile como referente latinoamericano". Facultad de Ciencias Físicas y Matemáticas (FCFM) - Universidad de Chile. (Mayo, 2024.)

[6] Según un estudio de la compañía de ciberseguridad Kaspersky, Chile recibió entre agosto del 2022 y agosto 2023, "27 ataques digitales por minuto" (Castillo, 2024).
Más información en: https://www.gerencia.cl/security/ciberseguridad-chile-estadisticas-desafios-tecnologias/#:~:text=Seg%C3%BAn%20el%20National%20Cyber%20Security,27%20ataques%20digitales%20por%20minuto.

[7] Visto en TXS Plus, "Chile subió al cuarto lugar entre los países de Latinoamérica con más ciberataques durante 2023". Marzo, 2014. Visto en: https://txsplus.com/2024/03/chile-cuarto-ciberataques-2023/#:~:text=Chile%20subi%C3%B3%20al%20cuarto%20lugar,ciberataques%20durante%202023%20%2D%20TXS%20Plus

[8] Ciberseguridad. Bárbara Pezoa. La Tercera. Abril 2024. Visto en: https://www.latercera.com/pulso/noticia/juan-pablo-arias-experto-en-ciberseguridad-chile-recibio-6000-millones-de-intentos-de-ciberataques-en-2023/HO5ZRNDTHBHJBOVZLV3AAWICMI/

importantes porque representan elementos esenciales para la continuación de funciones vitales, seguridad nacional, economía o del bienestar de la población. La ley[9] genera obligaciones con aquellos que manejan infraestructura crítica, así también mínimos de seguridad que deben cumplir. Uno de los puntos más importantes es la creación y el rol que se dio a la Agencia Nacional de Ciberseguridad (ANCI). Ésta regulará y supervisará el cumplimiento de la ley. Deberá coordinar respuestas a incidentes de ciberseguridad a mediana y gran escala, así como promover la investigación y el desarrollo de la ciberseguridad. Otro punto importante es la creación de un equipo de Respuesta ante Incidentes de Seguridad Informática de la Defensa Nacional (CSIRT), organismo que se encargará "de coordinar, proteger y asegurar redes y sistemas al Ministerio de Defensa Nacional". Además, crea los llamados CSIRT sectoriales. También hace mención en su art. 23 sobre la "Red de conectividad segura del Estado", la importancia de ésta radica en la interconexión y la conectividad de internet a diversos organismos (administrativos) del Estado. Por otro lado, en su artículo 20, crea el Consejo multisectorial, el cuál asesorará y hará recomendaciones a la Agencia, facilitando presencia y cooperación desde distintas áreas del conocimiento. Además de otros elementos importantes que se tuvieron en consideración. En fin, establece una nueva institucionalidad. Y una nueva gobernanza, pero primeramente habrá que esperar a la creación y el funcionamiento de esta Agencia tan esperada. Sólo entonces podrá establecerse una mejor y mayor opinión de ésta y de la ley, más allá de lo escrito en el papel.

En conclusión, la Ley "Marco de Ciberseguridad y Protección de Infraestructura Crítica" marca un hito en el fortalecimiento de la seguridad digital -ciberseguridad- en Chile y establece una estructura regulatoria que promete un entorno más seguro y resiliente. Sin embargo, el verdadero impacto de esta normativa dependerá de su implementación efectiva, la adaptabilidad de los sectores involucrados y la capacidad del país para enfrentar amenazas que evolucionan constantemente. La pregunta que queda abierta es: ¿Logrará Chile adaptarse de manera continua y ágil a estos nuevos desafíos y convertirse en un referente en ciberseguridad en la región?"

[9] Más información en el Diario Oficial de Chile:
https://www.diariooficial.interior.gob.cl/publicaciones/2024/04/08/43820/01/2475674.pdf