Aportes de ISSA Chile a Consulta Pública sobre Reglamentos Ley Marco de Ciberseguridad

Juan Anabalón R.
ISSA Chile
MonkeysLab
jar@monkeyslab.cl

Aldo Tobar E
ISSA Chile
aldo.tobar@gmail.com

Pedro Novoa J.
ISSA Chile
pedro.novoa@gmail.com

Felipe Moreno C.
ISSA Chile
fmcerda@gmail.com

Daniel González B.
ISSA Chile
dgonzalezb@gmail.com

Carlos Hoffmann E.
ISSA Chile
choffmane@gmail.com

***Resumen*—Este documento presenta un análisis exhaustivo de las Consulta Pública sobre Reglamentos Ley Marco de Ciberseguridad, en lo que respecta a los Reglamento sobre Calificación de Operadores de Importancia Vital (OIV) y Reglamento sobre Reportes de Incidentes de Ciberseguridad. Se destaca la importancia de la participación pública en el desarrollo de normativas de ciberseguridad y privacidad, subrayando cómo esta colaboración contribuye a la creación de estándares robustos y relevantes. La metodología utilizada se centra en una consulta estructurada a expertos en seguridad informática asociados a ISSA Chile, quienes aportan su conocimiento técnico y perspectiva estratégica para evaluar y comentar sobre los borradores propuestos. Los objetivos del análisis son dobles: proporcionar retroalimentación constructiva para mejorar las regulaciones y fortalecer la alineación entre las prácticas de la industria y las directrices del Coordinador Nacional de Ciberseguridad. Este trabajo resume las recomendaciones clave y enfatiza la necesidad de un enfoque proactivo y colaborativo para la seguridad cibernética entre las instituciones públicas y privadas, y que no solo responde a las amenazas actuales, sino que también anticipe desafíos futuros. Este trabajo refleja el compromiso de ISSA Chile con la excelencia con la gobernanza de la seguridad de la información y la protección de la privacidad.**

Palabras clave – Cybersecurity, National Security, Legislation, key information infrastructure

I. INFORMATION SYSTEMS SECURITY ASSOCIATION (ISSA)

El Information Systems Security Association (ISSA)® es una organización internacional sin fines de lucro de profesionales y técnicos de seguridad de la información. Proporciona foros educativos, publicaciones y oportunidades de interacción entre pares para mejorar el conocimiento, las habilidades y el crecimiento profesional de sus miembros. Con la participación activa de capítulos en todo el mundo, ISSA es la asociación internacional sin ánimo de lucro más grande para profesionales de la seguridad. Los miembros incluyen profesionales en todos los niveles del campo de la seguridad en una amplia gama de industrias, como comunicaciones, educación, salud, manufactura, finanzas y gobierno.

El objetivo principal de la ISSA es promover prácticas de gestión que garanticen la confidencialidad, la integridad y la disponibilidad de los recursos de información. ISSA facilita la interacción y la educación para crear el más exitoso entorno de seguridad de sistemas de información y para los profesionales involucrados globalmente.

Nada en este documento debe interpretarse para contradecir las normas y directrices que la propia institucionalidad de ciberseguridad de Chile establece como obligatorias y vinculantes. Tampoco se debe interpretar que estas pautas alteran o sustituyen a las autoridades existentes.

II. INTRODUCCIÓN

Desde el ciberataque al Banco de Chile[1] en el año 2018 este ha sido el mejor de los tiempos para la legislación y la política de ciberseguridad de Chile. La Política Nacional de Ciberseguridad del 2017–2022 [2], a la que ISSA Chile aportó sus recomendaciones [3], significó un gran reconocimiento gubernamental de la

importancia de la ciberseguridad, lo que motivó el desarrollo de diversas iniciativas sectoriales [4], [5] en las que ISSA Chile también aportó su visión. Posteriormente la Ley N°21.459/2022 que Establece normas sobre delitos informáticos[6], deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest; la Política Nacional de Ciberseguridad 2023-2028 [7]; la creación de una nueva estructura administrativa como el CSIRT Nacional; y la Ley N°21.663/2024 [8] que tiene por objetivo regular la normativa general aplicable a las acciones de ciberseguridad de los organismos del Estado, y sus relaciones con entidades privadas y establece los requisitos mínimos para enfrentar incidentes de ciberseguridad, entre otras materias; garantizan y amplían la estructura de ciberseguridad del Estado e impulsa nuevos desafíos y oportunidades.

Recientemente, el Estado de Chile ha abierto la consulta pública[9] virtual sobre los reglamentos que deben dictarse para la puesta en marcha de la futura Agencia Nacional de Ciberseguridad, conforme a lo dispuesto en la Ley N°21.663, marco sobre ciberseguridad. Esta consulta pública es un proceso participativo abierto a todas las personas, incluyendo representantes de organizaciones gremiales, de la sociedad civil, de la academia y particulares. ISSA Chile, como lo ha hecho desde su fundación en 2006, considera vital la participación de profesionales de ciberseguridad en estas iniciativas, para lo que, ha convocado a profesionales de ciberseguridad a participar en una jornada de reflexión para buscar puntos en común que permitan un aporte a la definición de estos nuevos reglamentos.

III. COMENTARIOS A REGLAMENTOS

El Coordinador Nacional de Ciberseguridad ha iniciado la Consulta Pública sobre Reglamentos de Ley Marco de Ciberseguridad. Estas publicaciones en fase de borrador buscan “recoger opiniones, sugerencias y propuestas de mejora sobre la regulación propuesta” que a continuación se indican:

1. Reglamento sobre Calificación de Operadores de Importancia Vital
2. Reglamento sobre Reportes de Incidentes de Ciberseguridad

Los profesionales de ISSA Chile reunidos en una jornada de trabajo y debate, para aportar a la normativa, proponen algunas ideas que tienen por objetivo enriquecer el debate conjunto y se detallan a continuación:

IV. REGLAMENTO SOBRE CALIFICACIÓN DE OPERADORES DE IMPORTANCIA VITAL (OIV)

El Reglamento sobre Calificación de Operadores de Importancia Vital (OIV)[10] tiene por objeto regular el procedimiento de calificación de los operadores de importancia vital de la ley N° 21.663, marco de Ciberseguridad, entendiendo como servicio vital a: aquellos provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional; los prestados bajo concesión de servicio público, y los proveídos por instituciones privadas que realicen las siguientes actividades: generación, transmisión o distribución eléctrica; transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento; telecomunicaciones; infraestructura digital; servicios digitales y servicios de tecnología de la información gestionados por terceros; transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de su infraestructura respectiva; banca, servicios financieros y medios de pago; administración de prestaciones de seguridad social; servicios postales y de mensajería; prestación institucional de salud por entidades tales como hospitales, clínicas, consultorios y centros médicos, y la producción y/o investigación de productos farmacéuticos; así como también aquellos otros servicios que sean calificados por la Agencia como esenciales, mediante resolución fundada de su Director o Directora Nacional, conforme lo dispuesto en el inciso tercero, del artículo 4° de la Ley.

En el Título III de este reglamento, que trata sobre la Consulta pública y nómina final de calificación, en el Art. 12 del proceso de apertura se indica que se dará inicio al proceso de consulta mediante la resolución respectiva, y se dará un periodo de difusión y promoción que no podrá ser inferior a 10 días corridos. Si observamos la experiencia internacional, el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos generalmente permite un período de 30 a 45 días para que el público comente sobre los borradores de sus publicaciones. La consulta y apertura propuesta en este reglamento, al señalar 10 días como mínimo periodo, nos parece completamente adecuado, sin embargo, para otros procesos similares y dependiendo de la naturaleza del documento y la urgencia del tema tratado es necesario fijar un periodo

máximo de consulta, de tal manera que no sea posible ejecutar una consulta en un periodo indeterminado, y que por lo tanto, pueda resultar en una dilación innecesaria en los importantes temas que deban deliberarse.

V. REGLAMENTO SOBRE REPORTES DE INCIDENTES DE CIBERSEGURIDAD

El Reglamento sobre Reportes de Incidentes de Ciberseguridad[11] instruye respecto del deber de reportar los diferentes incidentes de seguridad en "las instituciones públicas y privadas que presten servicios esenciales y aquellas que hubieren sido calificadas como operadores de importancia vital de conformidad a la Ley y su Reglamento, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos".

Esta obligación parece pertinente y acertada, pero queda en la indefinición, o no está explícito, cuando se deberá reportar además al correspondiente CSIRT sectorial, si lo hubiere, para que las partes involucradas manejen la misma información en todo momento.

Art 4. sobre Incidente de ciberseguridad con efecto significativo. En este artículo se define que se considerará un incidente significativo al que es capaz de producir:

a) Interrumpir la continuidad de un servicio esencial. En dicho caso deberá considerarse, tanto los servicios entregados por proveedores, como la cadena de suministro, de una institución que preste servicios esenciales o de un operador de importancia vital.
b) Afectar la integridad física o la salud de las personas; o
c) Afectar sistemas informáticos que contengan datos personales.

En este artículo es importante cuidar el punto a), ya que en la industria se pueden manejar elementos que eviten una regulación si no se define claramente el servicio esencial y su alcance al interior de cada organización, considerando la cadena de suministro interna de la empresa o institución, dejando fuera de control elementos importantes para la correcta prestación de los servicios digitales.

Art. 6 de las mantenciones regulares. En este artículo propone la obligatoriedad de notificar a la Agencia sobre la programación de las mantenciones regulares, pero no se dan los criterios respecto de, con qué anticipación se informará de las mantenciones regulares, de esta manera evitar o reducir avisos urgentes que son correcciones de incidentes de seguridad no reportados. Por otra parte, el artículo no da instrucciones de cómo informar la actualización de los planes previamente informados. Además, no se propone un método de notificación de mantenciones ni una taxonomía para tal fin.

Artículo 7° sobre plataforma de reporte de incidentes. Se dicta respecto de la obligatoriedad de reportar los incidentes de seguridad en una plataforma especialmente dispuesta, sin embargo, es deseable que la misma plataforma pueda ser utilizada para reportar las mantenciones regulares del Artículo 6 anterior.

Art. 10. sobre Alerta Temprana "Una vez que la institución obligada a reportar hubiere tomado conocimiento de la ocurrencia de un ciberataque o incidente". Las alertas tempranas en ciberseguridad son cruciales para la protección proactiva de los sistemas informáticos ay que permiten identificar y mitigar amenazas antes de que causen daños significativos. La implementación de estas alertas puede reducir considerablemente el impacto económico y de reputación asociado a las brechas de seguridad. Sin embargo, este reglamento, no establece nada respecto de la necesidad de mantener o no un monitoreo 24x7 en los servicios de ciberseguridad, para poder cumplir efectivamente con los plazos propuestos.

Art. 14. sobre el Informe parcial de incidente de ocurrencia prolongada. La necesidad de reportar cada 15 días es un tiempo razonable, sin embargo, en OIV que tengan directa relación con el riesgo de vida de las personas, como agua o electricidad se debiera mantener una obligatoriedad de 7 días para informar.

Art. 16 sobre la necesidad de informar las vulnerabilidades e incidentes que puedan afectar a las redes y sistemas informáticos de los organismos del Estado. La gestión de vulnerabilidades es un problema axial en la gestión de riesgos cibernéticos y es muy complejo informar y mantener actualizadas las bases de datos de vulnerabilidades presentes en las diferentes instituciones del alcance y los OIV identificados. En su lugar, proponemos promover directivas que obliguen a las empresas e instituciones a no mantener vulnerabilidades por más de 30 días de antigüedad o

bien, por ejemplo, 72 horas para las vulnerabilidades críticas. Un tema adicional muy importante que debiera estar explícito en la normativa es que no se debe permitir tecnología deprecada u obsoleta en los servicios tecnológicos, incluyendo la infraestructura base más allá de los meros servicios contratados, de esta manera se evita que exista infraestructura de base o que servicios de seguridad administrados, sean proveídos con tecnología sin licenciamiento o sin soporte de marca, como las tecnologías de virtualización que soportan servicios contratados. Normalmente las empresas que pasarán a obsolescencia su tecnología informan con anticipación el fin de soporte de sus líneas de producto, por lo tanto, se recomienda normar que las plataformas que sean identificadas en proceso de obsolescencia deban ser actualizadas hasta con un año de anticipación del plazo End of Life (EoL) definido por la marca, de esta manera se ajustan los planes de mantenimiento al periodo de planificación presupuestaria adecuado.

Art. 18. Declara que los CSIRT sectoriales tendrán la obligación de apoyar el restablecimiento del servicio afectado. Esta directiva obliga a cada CSIRT sectorial a trabajar coordinadamente con el CSIRT nacional, sin embargo, es importante agregar en este artículo, o agregar un nuevo numeral que indique, que si existe un incidente de ciberseguridad que afecta a un servicio en una zona remota de importancia y no tenga la capacidad técnica de reaccionar en esa zona, pueda ser atendido o soportado por capacidades de CSIRT de un servicio o institución de Estado distinto, así poder disponer de mejor manera los recursos necesarios y fomentar el trabajo colaborativo entre distintos servicios.

VI. CONCLUSIONES

La apertura de un proceso de consulta pública para proponer y comentar nuevos reglamentos para cumplir con la Ley Marco de Ciberseguridad refleja un ejercicio democrático ejemplar, donde el trabajo colaborativo y de dialogo fraterno han sido fundamentales. La participación activa de diversos sectores de la sociedad en la propuesta de reglamentos no solo enriquece el marco normativo, sino que también fortalece el tejido social y la gobernanza de nuestra nación. Este proceso ha demostrado que, al unir esfuerzos y compartir conocimientos, podemos construir propuestas robustas que resguardan el interés nacional y promueven un ciberespacio más seguro para todos. Es imperativo continuar fomentando estos espacios de diálogo y colaboración, pues son el pilar de una república que se adapta y evoluciona ante los desafíos del futuro digital.

VII. REFERENCIAS

[1] D. Financiero, «El origen del hackeo al Banco de Chile que le significó el robo de US$ 10 millones | Diario Financiero». Accedido: 10 de agosto de 2024. [En línea]. Disponible en: https://www.df.cl/empresas/banca-instituciones-financieras/el-origen-del-hackeo-al-banco-de-chile-que-le-significo-el-robo-de-us

[2] C. Comité Interministerial sobre Ciberseguridad, «PNCS 2017-2022 - Coordinación Nacional de Ciberseguridad». Accedido: 10 de agosto de 2024. [En línea]. Disponible en: http://ciberseguridad.gob.cl/pncs-2017-2022/

[3] J. Anabalon, M. Ramírez, y A. Tobar, «Propuestas de ISSA Chile a la Política Nacional de Ciberseguridad (PNCS) 2016-2022». 1 de marzo de 2016. doi: 10.13140/RG.2.2.15314.45760.

[4] J. Anabalón, C. Bobadilla, A. Tobar, M. Ramírez, y V. Villar, «Una Contribución de ISSA Chile a la Nueva Normativa de Ciberseguridad de la Subsecretaría de Telecomunicaciones». Accedido: 10 de agosto de 2024. [En línea]. Disponible en: https://www.researchgate.net/publication/342159180_ISSA_CHILE_WORKING_PAPER_1_Una_Contribucion_de_ISSA_Chile_a_la_Nueva_Normativa_de_Ciberseguridad_de_la_Subsecretaria_de_Telecomunicaciones

[5] J. Anabalón, C. Bobadilla, M. Soto, M. Vildoso, y P. Novoa, «Propuestas de ISSA Chile a Normativa de Incidentes de Ciberseguridad de la Superintendencia de Bancos e Instituciones Financieras (SBIF)». Accedido: 10 de agosto de 2024. [En línea]. Disponible en: https://www.researchgate.net/publication/328172656_Propuestas_de_ISSA_Chile_a_Normativa_de_Incidentes_de_Ciberseguridad_de_la_Superintendencia_de_Bancos_e_Instituciones_Financieras_SBIF

[6] C. Biblioteca del Congreso Nacional, *LEY 21459 Establece Normas Sobre Delitos Informáticos, Deroga La Ley N° 19.223 y Modifica Otros Cuerpos Legales con el Objeto de Adecuarlos al Convenio de Budapest*. 2022. Accedido: 11 de agosto de 2024. [En línea]. Disponible en: https://www.bcn.cl/leychile

[7] C. Comité Interministerial sobre Ciberseguridad, «Política Nacional de Ciberseguridad 2023-2028 - Coordinación Nacional de Ciberseguridad». Accedido: 11 de agosto de 2024. [En línea]. Disponible en: https://ciberseguridad.gob.cl/pncs-2023-2028/

[8] C. Biblioteca del Congreso, *LEY 21663 Ley Marco de Ciberseguridad*. 2024. Accedido: 11 de agosto de 2024. [En línea]. Disponible en: https://www.bcn.cl/leychile

[9] C. Coordinador Nacional de Ciberseguridad, «Consulta Pública sobre Reglamentos Ley Marco de Ciberseguridad - Coordinación Nacional de Ciberseguridad». Accedido: 11 de agosto de 2024. [En línea]. Disponible en: http://ciberseguridad.gob.cl/consulta-publica/

[10] C. Coordinador Nacional, *Reglamento de Calificación de Operadores de Importancia Vital*. Accedido: 11 de agosto de 2024. [En línea]. Disponible en: https://formularios.csirt.gob.cl/index.php/335666?lang=es-CL

[11] C. Coordinador Nacional, *Reglamento de Reportes de Incidentes de Ciberseguridad*. Accedido: 11 de agosto de 2024. [En línea]. Disponible en: https://formularios.csirt.gob.cl/index.php/228242?lang=es-CL

Agradecimientos:

Los autores desean expresar su agradecimiento a Patricia Tremont de Universidad San Sebastián por facilitar los recursos logísticos necesarios para la actividad de debate y reflexión durante el desarrollo de estas propuestas.

VIII. AUTORES:

Juan Anabalón R. Es CISO, investigador y consultor en ciberseguridad en monkeyslab.cl, también ha sido docente Universidad San Sebastián, Universidad de Santiago de Chile, Universidad Autónoma. Juan es Ingeniero en Informática (UDLA) y tiene un Magíster en Seguridad, Peritaje y Auditoría en Procesos Informáticos (USACH). Puede ser contactado en: https://www.linkedin.com/in/janabalon/.

Aldo Tobar E. Ingeniero con más de 20 años de experiencia en empresas nacionales y multinacionales.
Aldo cuenta con el curso de certificación Cybersecurity Technology Application And Policy por el Massachusetts Institute of Technology, el curso LA ISO 27001.
Es Magíster en Control y Gestión de Riesgo Corporativo por la Universidad Central de Chile; Diplomado en Control, Seguridad y Auditoría Informática. Universidad de Santiago de Chile e Ingeniero en control de Gestión en Universidad Arturo Prat. Puede ser contactado en https://www.linkedin.com/in/aldotobarespinoza/

Pedro Novoa J. Es Oficial de seguridad de la información con sólida experiencia en el área de Seguridad de la Información, Seguridad OT ICS/SCADA en empresas nacionales y multinacionales. Pedro es Ingeniero en Computación e Informática (UNAB), Diplomado en ciberseguridad (Uchile). Cofundador Information Systems Security Asociation – ISSA Chile. Puede ser contactado en https://www.linkedin.com/in/pnovoaj/

Felipe Moreno C. es Ingeniero en Ciberseguridad y Auditoría Informática en la Universidad San Sebastián (USS). Ha sido responsable de ciberseguridad para los Juegos Panamericanos y Parapanamericanos de Santiago 2023. Con una trayectoria de 15 años en informática en el sector bancario. Puede ser contactado en https://www.linkedin.com/in/felipe-moreno-cerda-32519960/

Daniel González B. es Ingeniero en Ciberseguridad y Auditoría Informática por la Universidad San Sebastián (USS), se desempeña como ingeniero en seguridad de la información en Caja de Compensación los Andes en el Área de Gobierno desde 2023. Con una trayectoria de 15 años en Telecomunicaciones y Microinformática. Puede ser contactado en https://www.linkedin.com/in/daniel-alejandro-gonzalez-burgos-407a8577/.

Carlos Hoffman E. Es ingeniero en ciberseguridad y desarrollador de software con más de 10 años de experiencia en la industria tecnológica. Su trabajo se centra en el diseño, implementación y mantenimiento de sistemas de seguridad informática, así como en el desarrollo de soluciones de software robustas y seguras. Puede ser contactado en https://www.linkedin.com/in/carlos-hoffmann-079b5a4/