Information Systems Security Association (ISSA)
Chile
Desarrollando y Conectando los Líderes de Ciberseguridad Globalmente
http://www.issa.org
05 de octubre de 2018

Propuestas de ISSA Chile a Normativa de Incidentes de Ciberseguridad de la Superintendencia de Bancos e Instituciones Financieras (SBIF)

Autores
Juan Anabalón Riquelme
Cristian Bobadilla Cepeda
Pedro Novoa Johnson
Marcos Soto Briones
Marcos Vildoso Flores

Autoría

Este documento ha sido desarrollado por el *Information Systems Security Association (ISSA)* capítulo chileno, fundado el año 2006, en cumplimiento de su misión de ser la voz de la seguridad de la información en Chile a través de la participación de cada uno de sus miembros y la comunidad de profesionales de la ciberseguridad a nivel nacional.

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.

Este documento ha sido preparado para su uso por parte de la *Superintendencia de Bancos e Instituciones Financieras (SBIF)*. Puede ser utilizado por otras organizaciones interesadas en la respuesta a incidentes o en ciberseguridad general.

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

Introducción

La Superintendencia de Bancos e Instituciones Financieras (SBIF) ha anunciado el comienzo de un proceso de consulta para dar lugar a una nueva normativa de incidentes de ciberseguridad para las instituciones por Ella reguladas, el que debería ser la oportunidad para que la ciudadanía exprese directamente sus propuestas fundamentales acerca de la materia, siempre orientada al bien común y al mejoramiento material y social de la nación.

En *ISSA Chile*, consideramos de capital importancia la participación activa de los profesionales de ciberseguridad en este tipo de iniciativas como reconocimiento a que estas actividades son un eficaz medio para influir en la correcta materialización de políticas, normas e instructivos de seguridad de alcance nacional, para lo cual, ISSA, ha convocado a distinguidos profesionales del área a colaborar con sus conocimientos y experiencia práctica en la mejora participativa de la norma propuesta por la SBIF.

Propósito

Este documento proporciona comentarios de mejora a la normativa de Incidentes de Ciberseguridad en trámite que ha sido liberada para consultas[1]. Por parte de la Superintendencia de Bancos e Instituciones Financieras (SBIF). El documento incluye observaciones sobre como es que la SBIF a de enfrentar los desafíos de coordinar o supervisar las acciones de ciberseguridad en su ámbito de acción y como aportar a la mejora continua de la ciberseguridad del sistema financiero nacional.

[1] Incidentes de Ciberseguridad https://www.sbif.cl/sbifweb/internet/archivos/norma_tramite_12220_4.pdf

Audiencia

Estos comentarios pretenden ser útiles para varias audiencias clave en una organización, incluidos, entre otros: el CEO, CIO, CFO, CMO, CISO y el equipo de ciberseguridad corporativo, los gerentes (incluidos los propietarios de sistemas y aplicaciones) y sus contratistas, y los coordinadores de respuesta a incidentes.

Documento SBIF

La Superintendencia de Bancos e Instituciones Financieras, en concordancia con lo dispuesto por la Ley 20.500 sobre participación ciudadana en la gestión pública, realiza consultas públicas periódicas acerca de la normativa que emite.

En particular la normativa sobre incidentes de seguridad código I1X ha sido sometida a consulta pública. ISSA Chile en cumplimiento de su misión se ha dispuesto a reunir a destacados profesionales de ciberseguridad de distintas áreas e industrias con el objetivo de contribuir a la mejora de la práctica de ciberseguridad a nivel nacional y promover el sano ejercicio de contribuir en la construcción de una nación prospera para todos.

En particular, el documento indicado anteriormente parte por establecer que las diversas instituciones de su sector deberán informar de los incidentes de seguridad mensualmente con un plazo de 10 día hábiles; propone una estructura de registro con 21 campos, que además incluyen código IFI, código de banco, código de archivo y la identificación de un periodo reportado. Esta estructura debe tener una extensión en bytes específica y una codificación definida para los distintos tipos de vulnerabilidades, amenazas y activos de información, además de identificar los tipos de canales, productos o servicios involucrados en un incidente de seguridad, y la individualización de clientes y proveedores afectados. Dicho documento además solicita costos de incidentes, mitigación y reparación, como además, las instituciones deberán informar el porcentaje de recuperación luego de las acciones de mitigación y el estado de un incidente, como también exige informar el nivel de criticidad de un incidente de acuerdo a una métrica cualitativa de 3 niveles. Para finalizar, con la cuadratura de carátula que debe ser entregada.

Comentarios a normativa

ISSA Chile reconoce que una normativa efectiva es total y absolutamente necesaria y positiva para apoyar el proceso de avanzar en temas de ciberseguridad a nivel nacional, sin embargo, este tipo de iniciativas deben ser pensadas, diseñadas e implementadas con el firme objetivo de ser ágiles y efectivas en su implementación. Al respecto, los profesionales por ISSA Chile reunidos en sucesivas jornadas de trabajo y debate, con motivo de aportar a la normativa, proponen ciertos aspectos que deben ser mejorados y que detallaremos a continuación:

1. De acuerdo con lo señalado en el sitio web de SBIF el “mandato que le impone la Ley General de Bancos a la Superintendencia de Bancos e Instituciones Financieras (SBIF), es supervisar las empresas bancarias y otras instituciones financieras, en resguardo de los depositantes u otros acreedores y del interés público”. En este sentido, no se visualiza una alineación de la normativa aquí comentada con el deber mandatado a la SBIF ni se establece el objetivo general o específico que se persigue con la normativa propuesta.
2. Al no definir expresamente el objetivo de la nueva normativa el objetivo de la norma qué se promueve es difuso, ya que no se explica el objetivo del registro de incidentes propuesto ni las acciones que se tomarán posterior al registro señalado.
3. Recomendamos adherir a una norma o estándar internacional que permita alinear las definiciones que serán utilizadas en los documentos sucesivos derivados de esta normativa. Con el objetivo de resguardar la triada de disponibilidad, confidencialidad e integridad de la información.

4. La SBIF solicita informar si los incidentes de seguridad fueron materializados o no. Es aquí, donde el punto tres anterior cobra importancia, debido a que mal entiende la definición de incidente. Debido a que no existen incidentes no materializado.
5. Se establece que se debe informar los incidentes en un plazo de 10 días hábiles. Un plazo tan extendido como el señalado entorpece el actuar sinérgico de la banca y reduce la posibilidad de minimizar los impactos en el resto de las instituciones.
6. Se recomienda establecer anualmente uno o dos días para el desarrollo de mesas de conversación o seminarios respecto de incidentes y lecciones aprendidas por las diversas instituciones reguladas por la SBIF.
7. El documento confunde la diferencia entre amenazas, incidentes, riesgos, eventos, mitigación y reparación lo que afecta gravemente la forma de estructurar la colaboración entre instituciones.
8. No considera informar cuando un incidente de seguridad pasa a un siguiente nivel de severidad y se hace necesaria la activación de un plan de recuperación ante desastres (DRP), esta información es muy valiosa para que puedan tomar los resguardos necesarios los otros actores del sector.
9. La normativa no establece los canales formales de comunicación o un plan de manejo de crisis, eficiente y claro al que adhieran las instituciones.
10. No incluye la coordinación con un *Computer Emergency Response Team* (CERT) establecido.
11. La normativa propuesta es una iniciativa de importante valor para el sector, sin embargo, no está clara la alineación de esta normativa con el cumplimiento de la Política Nacional de Ciberseguridad.
12. Cuando se establece la estructura de registro se indica que "*En caso de no existir información, completar el campo con nueves*". Esta ambigüedad abre la puerta para que todos los reportes sean entregados con esa información, de esta manera, elimina la obligatoriedad de informar y evita el real cumplimiento del registro de incidentes que se intenta establecer.
13. La normativa propuesta solicita informar sobre los "montos recuperados" respecto delos incidentes informados, sin embargo, este registro es muy probable que no se consiga pues pueden existir acciones legales que puede entorpecer el cumplimiento de este punto de la norma, al respecto, recomendamos que este requerimiento sea revisado anualmente según lo indicado en el punto seis (6) anterior.

Conclusiones

La implementación de normas de ciberseguridad para el sector financiero es un trabajo en curso en el que todos los actores de la industria tienen el deber de participar y los profesionales de ciberseguridad tienen una oportunidad única de influir positivamente en la agenda nacional para la construcción colectiva de mejores servicios, cuidando necesariamente la disponibilidad, integridad y confidencialidad de la información. La aplicación de diversas actividades de control financiero y de Tecnologías de la Información y ciberseguridad en particular, conduce necesariamente a una mayor reglamentación y peso administrativo para las instituciones reguladas, sin embargo, se presenta una oportunidad extraordinaria para la mejora de la postura de ciberseguridad corporativa, evitar ineficiencias derivadas de perdida de servicios y lograr mejoras productivas valiosas de una manera rentable.

ISSA Chile pone a disposición de la Superintendencia de Valores y Seguros una serie de recomendaciones que creemos, firmemente, contribuyen a la mejora sustancial de los procesos de ciberseguridad del sistema financiero nacional y contribuyen a mejorar la prestación de servicios para el sector y la ciudadanía en general.

Juan Anabalón Riquelme. Es especialista en temas de seguridad de la información, informática forense, privacidad, vigilancia, censura y cuestiones políticas y sociales de Ciberseguridad. Cofundador y presidente del *Information Systems Security Asociation – ISSA Chile*, consultor en ciberseguridad en *MonkeysLab*. Juan es Magíster en Seguridad, Peritaje y Auditoría en Procesos Informáticos (USACH); Ingeniero de Ejecución en Informática y Licenciado en Ciencias de la Ingeniería (UDLA). Puede ser contactado en http://monkeyslab.cl/jar/

Cristian Bobadilla Cepeda, CISSP. Es Oficial de Seguridad y consultor especialista en ciberseguridad para la industria de Financiera, Retail y Minería. Es Licenciado en Ciencias de la Ingeniería con mención Computación e Ingeniero en Computación de la Universidad de Chile. Actualmente se desempeña como consultor principal para una compañía internacional en ciberseguridad. Puede ser contactado en https://www.linkedin.com/in/cbobadil/

Marcos Soto Briones. Oficial de Seguridad de la Información. Es Ingeniero en Computación e Informática y Licenciado en Ingeniería de la Universidad Andrés Bello. Diplomado de Gerencia de Seguridad de la Información en la Universidad Adolfo Ibáñez. Socio & Delegado Directorio ISACA capítulo Santiago de Chile, miembro de Fundación Educacional de Ciberseguridad WHILOLAB, miembro de OWASP capítulo Chile, miembro del Internet Society capítulo Cybersecurity SIG. Puede ser encontrado en https://www.linkedin.com/in/sotobrionesmarcos/

Pedro Novoa Johnson Es Jefe de Riesgo Tecnológico en Aguas Andinas 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/

Marcos Vildoso Flores. Ingeniero Civil Industrial, Magíster en Finanzas y Magíster en Educación Superior, con más 10 años de experiencia profesional, en planificación estratégica de negocios dirección general, operativa, administrativa y comercial. Asesor corporativo de diversas empresas nacionales e internacionales. académico en ciencias de la ingeniería, gestión de proyectos, gestión por procesos, sistemática y cibernética organizacional, Innovación, emprendimiento, procesos industriales, entre otras.