Una Contribución de ISSA Chile a la Nueva Normativa de Ciberseguridad de la Subsecretaría de Telecomunicaciones

Juan Anabalón R., Cristian Bobadilla C., Aldo Tobar E., Manuel Ramírez S., Víctor Villar J.[1]

INFORMACIÓN ARTÍCULO

Disponible en línea 14 de junio de 2020

Palabras clave:
information security,
risk assessment,
threat,
CSIRT,
Governance
Public-Interest
Technology

RESUMEN

Este artículo proporciona una revisión por parte de un panel de expertos adscritos a ISSA Chile convocados para comentar la nueva normativa de ciberseguridad (20 de mayo de 2020) de la Subsecretaría de Telecomunicaciones (SUBTEL) sujeta a consulta pública. Los resultados de esta revisión sugieren que dicha normativa debe avanzar en la ampliación de las áreas de interés respecto de la ciberseguridad de la SUBTEL, redefinir los SLA propuestos para la respuesta a incidentes, estandarizar términos y definiciones con estándares internacionales y no innovar respecto de lineamientos que ya fueron entregados en la Política Nacional de Ciberseguridad.

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 colaborar y participar en la consulta ciudadana de la Subsecretaría de Telecomunicaciones (SUBTEL) sobre fundamentos generales de Ciberseguridad para el diseño, instalación y operación de redes y sistemas utilizados en la prestación de servicios de telecomunicaciones.

[1] Information Systems Security Association - ISSA Chile http://issa.org

Nada en este documento debe tomarse para contradecir las normas y directrices que la propia Subsecretaría promueve o de la Política Nacional de Ciberseguridad que le precede o establecer estos comentarios como obligatorios y vinculantes. Tampoco se debe interpretar que estas pautas alteran o sustituyen a las autoridades existentes.

Introducción

La Subsecretaría de Telecomunicaciones (SUBTEL) ha solicitado la participación ciudadana para establecer los fundamentos generales de Ciberseguridad para el diseño, instalación y operación de redes y sistemas utilizados en la prestación de servicios de telecomunicaciones, este proceso de consulta es la forma principal que tienen los ciudadanos y colegios de profesionales para colaborar en la construcción de estas normativas, siempre orientada al bien común y al mejoramiento material y social de la nación.
ISSA Chile, considera de capital importancia la participación activa de sus profesionales asociados 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 Chile, ha convocado a distinguidos profesionales del área, en todos sus niveles, a colaborar con sus conocimientos y experiencia práctica en la mejora participativa de la norma propuesta por la SUBTEL.

Propósito

Este documento proporciona comentarios de mejora a la Normativa de Ciberseguridad (20 de mayo de 2020)[1] que ha sido liberada para consultas. Por parte de la Subsecretaría de Telecomunicaciones de Chile. El documento incluye observaciones sobre cómo es que la SUBTEL ha de enfrentar los desafíos de coordinar o supervisar las acciones de ciberseguridad en su ámbito de acción y como aportar a la mejora en el diseño, instalación y operación de redes y sistemas utilizados en la prestación de servicios de telecomunicaciones.

Audiencia

Estos comentarios pretenden ser útiles para varias audiencias clave en una organización, incluidos, entre otros: el CEO, CIO, 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 SUBTEL

La Subsecretaría de Telecomunicaciones ha realizado una consulta pública acerca de la normativa de mejora en el diseño, instalación y operación de redes y sistemas utilizados en la prestación de servicios de telecomunicaciones.
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 “PROPUESTA NORMATIVA SOBRE FUNDAMENTOS GENERALES DE CIBERSEGURIDAD PARA EL DISEÑO, INSTALACIÓN Y OPERACIÓN DE REDES Y SISTEMAS UTILIZADOS EN LA PRESTACIÓN DE SERVICIOS DE TELECOMUNICACIONES” [1] comienza señalando los objetivos de la norma técnica para definir un marco regulatorio que comprenda los fundamentos generales de ciberseguridad en base a los cuales deben diseñarse, instalarse y operarse las redes y sistemas utilizados para la prestación de servicios de telecomunicaciones por parte de aquellos titulares de concesión o permiso que hayan sido

declarados como operadores relevantes por parte de la Subsecretaría, precisa las definiciones necesarias para delimitar la arquitectura de la nueva normativa, define los ámbitos de aplicación y los criterios de relevancia para incluir un titular de servicios de telecomunicaciones como operador relevante mediante resolución fundada; continúa con establecer obligaciones generales de seguridad, el nombramiento de encargados de ciberseguridad en cada una de las empresas reguladas y la obligatoriedad de reportar ciberincidencias junto con sus respectivos desarrollo de reportes y vislumbrar el contenido de los reportes y su tratamiento, regula además el intercambio de información a terceros, la obligación de la resolución de ciberincidencias, el tratamiento de datos personales, establece periodicidad de reportes, establece cuales son los reportes no obligatorios por parte de los operadores que no sean considerados relevantes, y finaliza esclareciendo la necesidad de mantener la supervisión de la gestión de seguridad y las fiscalizaciones y sanciones.

Comentarios a la normativa

Tal como lo han hecho otros países, Chile tiene la necesidad inevitable de promover y consolidar una estrategia de seguridad cibernética unificada que permita alzarse como un país sólido y eficiente en materia de ciberseguridad en infraestructura crítica.
Con motivo de proponer ideas para la implementación de este tipo de normativas en la Subsecretaría de Telecomunicaciones ISSA Chile propone algunos aspectos de sugiere deben ser revisados e incorporados:

1. Artículo 2°. Definiciones: Las definiciones entregadas en el documento emitido por la SUBTEL debieran ser revisadas en algunos aspectos que son de particular interés:
    a. ciberincidencia: Las normativas, frameworks y estándares internacionales hablan y se refieren a los incidentes cibernéticos solamente como "*incidentes*" [2] es importante homologar las definiciones[3] para contextualizar un alcance más exacto respecto del espíritu de la norma propuesta. Debe señalar además que una incidencia "Es toda acción que comprometa o *pueda comprometer* la disponibilidad..." de tal manera que, si se detectan amenazas que son de real importancia y aún no han materializado su impacto real sean tratadas como la celeridad e importancia adecuada.
    b. Ciberseguridad: Tal definición debe estar alineada con la definición de ciberseguridad indicada en la política nacional de ciberseguridad pagina 16, punto 6.
    c. Equipo de Respuesta ante Incidentes de Seguridad Informática, en adelante "CSIRT": Debe estar alineada con la Política Nacional de Ciberseguridad[4] y no debe restringir las atribuciones dadas en ella. Punto 4 página 17. Respecto de las atribuciones que tendrá el CSIRT se debe señalar que "es el órgano encargado de recibir y analizar reportes de ciberincidencias, con el fin de analizarlos, monitorear el desarrollo de éstas, emitir alertas y proponer medidas tanto de mitigación como de prevención, *y tendrá la autoridad necesaria para coordinar la respuesta técnica frente a incidentes que comprometan la seguridad del país*"
    d. Gestión de incidentes: Además de señalar que son los procedimientos para la detección, análisis, contención, erradicación y recuperación de una incidencia de ciberseguridad, debe considerar la preparación toda vez que el proceso debe entenderse como una acción planificada y proactiva y no puramente reactiva, considerando además las lecciones aprendidas (pos incidente) para la mejora continua.
    e. Incidente: el alcance debe ser establecido en "*seguridad de las redes y sistemas de información*" sin agregar el término "*de telecomunicaciones*" debido a que pueden existir incidentes que no están relacionados con los sistemas de información de

telecomunicaciones pero que igualmente pueden afectar gravemente la infraestructura crítica.

f. Infraestructura crítica de telecomunicaciones: Tal definición debe considerar la integridad como un elemento de interés para la normativa: "…generaría un serio impacto en la seguridad, privacidad, *integridad* o disponibilidad de servicio de la población afectada".
g. Riesgo: No es necesario describir ejemplos en el párrafo de definiciones, de lo contrario se debe ejemplificar en todas las definiciones dadas en el documento. Por otra parte, la matriz riesgo x impacto no es la única manera de medir el riesgo existiendo otras metodologías que podrían quedar inmediatamente descartadas si es que se ejemplifica en la norma técnica. Adicionalmente, Se debe definir "*impacto en la ciberseguridad*" para ser consistentes con el contenido de la norma en general.

2. Artículo 3°. Ámbito de aplicación: Se debe considerar los equipos adyacentes a los activos de información del alcance pues, en un ataque cibernético existe la posibilidad de realizar movimientos laterales que podrían afectar las redes y sistemas críticos para la compañía. Por lo tanto, proponemos: *"…y todos los activos de información que pudieran afectar a la seguridad de las redes y sistemas del alcance de esta normativa*."
3. Artículo 4°. Criterios de relevancia: SUBTEL debe definir una periodicidad de revisión de los actores relevantes para mantener la idoneidad de tal categoría asignada a cada empresa.
4. Artículo 5°. Obligaciones generales de seguridad: La lista propuesta no considera otros aspectos importantes de la ciberseguridad tales como: Gobierno de seguridad, seguridad operaciones, administración de seguridad, seguridad de personal y entrenamiento, ciberinteligencia, gestión de identidades y acceso, gestión de configuraciones de seguridad, aspectos de desarrollo seguro etc. Además, la norma habla de "*de las redes, sistemas e instalaciones*" términos que no fueron definidos en el alcance, el documento debe ser consistente con el alcance determinado. Por otra parte, en el mismo artículo se establece que "*Tanto el diseño de las redes y sistemas como la elaboración de los planes de gestión de riesgos serán de responsabilidad exclusiva del respectivo operador relevante*" sin embargo, continua indicando que "*en todos los casos, deberá tener en consideración, a lo menos, las recomendaciones de esta Subsecretaría*", a tal afirmación se hace necesario señalar que deben considerar las recomendaciones y "*mandatos*" de esta manera la labor de la SUBTEL no termina solo en las recomendaciones sino que ejerce disposiciones que deben cumplirse. Debe agregar además que "La documentación y demás antecedentes que den cuenta del detalle de los planes de *gestión de riesgo, gestión de seguridad y repuesta a incidentes* deberá estar permanentemente disponible en caso de inspecciones a realizar por Subtel" y que "los operadores relevantes deberán considerar en sus planes el estado de la técnica, *tácticas y procedimientos* y la tecnología disponible en los ámbitos de seguridad de sistemas" para finalizar con que "determinados operadores relevantes deban adoptar los estándares y *acciones* que la autoridad le indique"
5. Artículo 6°. Encargados de ciberseguridad: Debe señalar que "Todo operador relevante deberá contar permanentemente con, a lo menos, un encargado titular de ciberseguridad en funciones y un suplente, quienes deberán poseer las *competencias, habilidades, conocimiento y experiencia suficientes* para identificar los riesgos de afectación de los servicios de telecomunicaciones por causa de ciberincidencias".
6. Artículo 7°. Obligación de reportar ciberincidencias: Si se establece claramente lo señalado en el Punto 4. Artículo 5 se debe indicar que los operadores relevantes deberán reportar "las ciberincidencias que detecte en sus redes, sistemas *e instalaciones* y que alcance los umbrales de gravedad establecidos en las instrucciones pertinentes emitidas por Subtel". Por otra parte, La matriz de Acuerdo de Niveles de Servicio (SLA) debe preferentemente utilizar la misma

tabla de impacto de incidentes que utilice el CSIRT Chile dependiente del ministerio del interior de esta manera homologar la respuesta entre los distintos actores; donde dice "Alcance ciberincidencia" debe decir "impacto" y se propone que los SLA impacto Alto: 15 minutos, Media: 24 horas, baja: 5 días. Además, el plazo de reportar una incidencia no puede depender de un acuse de recibo de la SUBTEL, por lo tanto, se debiera mejorar la redacción del párrafo en cuestión para reflejar el correcto espíritu de la letra.

7. Artículo 8°. Desarrollo de los reportes: De acuerdo a la definición de ciberincidencia indicada en esta propuesta este artículo debe comenzar con: "En caso de ciberincidencias con un *inminente impacto alto, o bien, ciberincidentes ya materializados de alto impacto* que se extiendan por un período de tiempo que exceda de treinta minutos,…".
8. Artículo 9°. Contenido de los reportes: Respecto de lo dispuesto en el Punto d), se debe avanzar en proporcionar información de infraestructura crítica potencialmente impactada más allá de la infraestructura crítica de la compañía de telecomunicaciones afectada. Principalmente porque muchas otras infraestructuras críticas dependen de Internet y los servicios de telecomunicaciones. Es importante además agregar puntos como *Responsable del sistema* y *Persona que detectó el incidente* de esta manera se agilizan los procesos de comunicación y se registra la responsabilidad al momento de resguardar información que no debe ser divulgada. Respecto del registro de la evolución de la incidencia, el registro debe extenderse hasta la completa resolución *de la causa raíz* del incidente. En el caso particular de ciberincidencias que afecten o puedan afectar infraestructuras críticas el operador afectado deberá conservar por, a lo menos, *Un año* desde el cierre de la ciberincidencia.
9. Artículo 10°. Tratamiento de los reportes: Es importante mantener un registro de los informantes y receptores de la información de tal modo que, si hay información o incidentes que deban mantenerse de forma confidencial, tal registro actúe de forma disuasiva en la revelación de información, se debe considerar además la obligatoriedad de comunicación de información por canales seguros o con sistemas de cifrado de extremo a extremo para mantener la confidencialidad de los datos considerando para esto los planes de instrucción adecuados.
10. Artículo 11. Información a terceros e intercambio de información: Se debe mantener concordancia en la norma técnica, ajustando la narrativa a seguridad física o seguridad de instalaciones según corresponda.
11. Artículo 12. Obligación de resolución de ciberincidencias: La última disposición del artículo doce debe especificar la resolución de vulnerabilidades y *fallos*, debido a que podrían existir amenazas de ciberseguridad que deriven de fallos operación, diseño o arquitecturas y no sean una vulnerabilidad propiamente tal.
12. Artículo 13. Tratamiento de datos personales: Para el tratamiento de información de carácter personal, se propone que la norma técnica indique que: "En caso de que se deban incorporar datos personales de carácter sensible en un informe de ciberincidencia en razón de ser indispensables para la adecuada comprensión del mismo, *se debe privilegiar el uso de enmascaramiento de datos en la entrega de estos informes*,…"
13. Artículo 14. Reportes trimestrales: Tal disposición finaliza indicando que "El período de los reportes será aquel que Subtel indique en las instrucciones pertinentes", sin embargo, en el título del Artículo ya se señala que los reportes son trimestrales.
14. Artículo 16. Supervisión de seguridad: Esta norma técnica de tener a fortalecer en el mayor grado posible la ciberseguridad de las empresas reguladas, por tal motivo, en el según párrafo del artículo debe indicar que "*los operadores relevantes deberán someter a pruebas de seguridad a lo menos semestralmente sus redes y sistemas de telecomunicaciones identificados como críticas en el análisis de riesgos*". Asimismo, al finalizar el artículo se señala que SUBTEL podría requerir "los resultados de las pruebas de seguridad y, en general,

todo otro tipo de antecedentes relacionados con *políticas* de seguridad de sus redes y sistemas", creemos importante retirar la referencia a las políticas e indicar que se podría requerir "los resultados de las pruebas de seguridad y, en general, todo otro tipo de antecedentes relacionados con *la* seguridad de sus redes y sistemas".

15. Artículo 17. Fiscalización: Esta normativa señala que la "Subsecretaría *podrá* fiscalizar en cualquier momento el cumplimiento de las obligaciones contenidas en esta normativa", sin embargo, la normativa debiera establecer que la Subsecretaría "*Deberá*" fiscalizar a lo menos anualmente y en cualquier momento el cumplimiento de esta normativa.
16. Artículo 19: Es importante considerar un artículo extra en la presente normativa en el que se señale que esta norma técnica deberá ser revisada a lo menos anualmente por SUBTEL, en forma directa o a través del órgano que ésta designe para dicho fin. El objetivo de esta cláusula es asegurar la actualización permanente de la normativa y sus particularidades.

Análisis

Los servicios de telecomunicaciones son, hoy en día, una de las principales herramientas de las empresas, instituciones y la sociedad civil para efectuar diversas actividades de la vida cotidiana, por lo tanto, el acceso a los servicios que se pueden obtener mediante este tipo de infraestructura cobra mayor relevancia conforme se extiende su uso en el territorio.

Si revisamos la experiencia internacional, En diciembre de 2003 el presidente de los Estados Unidos George W. Bush, por ejemplo, emitió el Homeland Security Presidential Directive 7 (HSPD-7) [5] actualizando la política nacional de protección de infraestructura crítica siguiendo un patrón similar al establecido en PDD-63 de mayo de 1998 [6], después del atentado del 11 de septiembre de 2002 en el que se logró subvertir infraestructura crítica en un ataque físico HSPD-7 dio mayor énfasis a la protección física en comparación con el énfasis de ciberseguridad de PDD-63. En febrero de 2013 el presidente Barack Obama emitió la Presidential Policy Directive 21 (PDD-21) [7] que actualizó la política nacional de protección de infraestructura crítica restaurando el énfasis en ciberseguridad e introduciendo el concepto de resiliencia. Mismo ejemplo han seguido otros países como China, Israel, UK, Rusia entre otros.

Tal como las infraestructuras de agua, electricidad y la aviación, internet debiera ser considerada una de las infraestructuras críticas dentro de cualquier normativa, desde su creación en la década de 1960, Internet ha experimentado una rápida evolución que puede resumirse en tres hitos principales: 1) la creación y expansión de ARPANET para la investigación relacionada con el gobierno de EE.UU. entre 1969 a 1981. 2) La introducción del Protocolo TCP/IP y la transición a NSFNET dieron como resultado una rápida proliferación entre las universidades entre 1982 y 1995 y 3) tuvo un crecimiento explosivo desde 1995 hasta la actualidad, después de su liberación por parte del gobierno de EE.UU. y la introducción del protocolo HTML que provocó la expansión de la web a nivel mundial. Actualmente, hay voces que se aventuran en decir que la próxima epopeya estará caracterizada por la internet de las cosas (IoT por sus siglas en inglés) debido a que se proyecta que la comunicación entre personas será ampliamente superada por las comunicaciones entre dispositivos y aparatos.

Sin embargo, a pesar de la rápida evolución de Internet, esta sigue siendo colección de enlaces, routers y protocolos muy simple que proporcionan un medio común para la comunicación entre distintos computadores y dispositivos, si bien es cierto, nadie es dueño de Internet, la gran mayoría de los enlaces y routers son propiedad de un pequeño número de proveedores de servicios de Internet corporativos de nivel 1 y estos ISP a su vez se interconectan entre sí y con otros ISP más pequeños que, muchas veces, se dedican proveedor conectividad de última milla.

Uno de los principales componentes para facilitar el intercambio global de datos es el esquema de direccionamiento de protocolos de Internet. Las direcciones IP son controladas por el Internet

Corporation for Assigned Names and Numbers, ICANN[2]. Un departamento dentro de la ICANN, llamado Internet Assigned Numbers Authority, IANA[3], administra varios cientos de servidores de nombres de dominio distribuidos geográficamente. Los servidores de nombres de dominio IANA, que en nuestro país es representado por NIC Chile[4], proporcionan a los routers ISP traducciones de direcciones IP que son esenciales para entregar paquetes de comunicación entre origen y destino. Aunque hay cientos de servidores de nombres de dominio, IANA mantiene listas de direcciones IP maestras solo en 13 servidores raíz[5]. Esto tiene como consecuencia que Internet tenga al menos dos puntos de vulnerabilidad. 1) Los Internet eXchange Point (IXP) y 2), los servidores raíz. Un ataque de denegación de servicio es aquel que intenta inundar las comunicaciones de un computador saturándolo con solicitudes maliciosas. Un ataque masivo de denegación de servicio bien coordinado podría derribar cualquier número de IXP y dejar fuera partes significativas de Internet. Sin embargo, un destino más probable son los servidores de enrutamiento DNS. De hecho, en diciembre de 2015 un ataque coordinado de denegación de servicio de muchas fuentes logró neutralizar 3 de los 13 servidores de rutas IANA[6].

Estados Unidos, clasifica internet como parte de la infraestructura de tecnología de la información en PPD-21 pero también constituye el soporte subyacente para la mayor parte de la infraestructura de comunicaciones. La Oficina de Ciberseguridad y Comunicaciones del Departamento de Seguridad Nacional, bajo la Dirección Nacional de Protección y Programas, es la agencia específica del sector designada para Internet. El DHS no tiene autoridad reguladora a través de Internet, pero trabaja con los ISP y la ICANN de forma voluntaria[8]. En la normativa propuesta por SUBTEL se hace necesario ampliar el alcance no solo a las compañías de telecomunicaciones calificadas como de relevancia, sino que definir Internet como objetivo estratégico y acordar planes para evaluar, priorizar y gestionar el riesgo de la infraestructura cibernética con todos los actores proporcionando una imagen de los riesgos sectoriales para diferentes categorías de infraestructura crítica.

Conclusiones

La implementación de normas de ciberseguridad para preservar la disponibilidad, confidencialidad e integridad de los sistemas de información de las empresas de telecomunicaciones es de vital importancia para el bienestar general de la sociedad y, tales sistemas, deben ser considerados como infraestructura crítica de la nación, por lo tanto, es imperativo resguardar la seguridad de los sistemas de información que soportan la entrega de los servicios del alcance.

La normativa propuesta cumple con algunos aspectos de la seguridad de sistemas de información, sin embargo, es importante aclarar cuál es el objetivo principal de su promulgación, entendiendo que, regulará no solo la respuesta a incidentes como se declara en el cuerpo de la normativa, por otra parte, se necesita avanzar en otros aspectos relacionados de ciberseguridad que sostengan las diversas situaciones de riesgo a los que se puedan ver enfrentados cada uno de los operadores de telecomunicaciones, entendiendo que la respuesta a incidentes es necesaria, pero debe considerar el gobierno, gestión de riesgos, gestión de operaciones y otros aspectos relacionados que no están declarados en la normativa; asimismo, es necesario involucrar una mirada mucho más amplia en la gestión de riesgos que incluya la arquitectura general de la Internet nacional e involucrar otros actores importante en esta evaluación de riesgos.

---

[2] Internet Corporation for Assigned Names and Numbers https://www.icann.org/
[3] Internet Assigned Numbers Authority https://www.iana.org/
[4] NIC Chile https://www.nic.cl/
[5] https://www.iana.org/domains/root/servers
[6] Root DNS servers DDoS'ed: was it a show-off? https://threatpost.com/internet-root-name-servers-survive-unusual-ddos-attack/115614/

Referencias

[1] T. Subsecretaría, «Normativa de Ciberseguridad (20 de mayo de 2020)». [En línea]. Disponible en: https://www.subtel.gob.cl/participacion-ciudadana/consultas-ciudadanas/.

[2] P. Cichonski (NIST), T. Millar (DHS), T. Grance (NIST), y K. Scarfone (Scarfone Cybersecurity), «Computer Security Incident Handling Guide». ago. 2012, [En línea]. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final.

[3] C. Paulsen y R. Byers, «Glossary of Key Information Security Terms». National Institute of Standards and Technology. Computer Security Division Information Technology Laboratory, jul. 2019, [En línea]. Disponible en: https://csrc.nist.gov/publications/detail/nistir/7298/rev-3/final.

[4] Comité Interministerial sobre Ciberseguridad, «Política Nacional de Ciberseguridad». Gobierno de Chile, 2017, [En línea]. Disponible en: https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf.

[5] G. W. Bush, «Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection». feb. 12, 2013, [En línea]. Disponible en: https://www.da.usda.gov/physicalsecurity/hspresidential.pdf.

[6] National Security Council and National Security Council Records Management Office, «PDD-63 - Critical Infrastructure Protection, 5/20/1998». Clinton Digital Library, jun. 07, 2020, [En línea]. Disponible en: https://clinton.presidentiallibraries.us/items/show/12762.

[7] B. Obama, «Presidential Policy Directive 21 -- Critical Infrastructure Security and Resilience». feb. 12, 2013, [En línea]. Disponible en: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[8] R. White, «Towards a Unified Homeland Security Strategy: An Asset Vulnerability Model», *Homel. Secur. Aff.*, vol. 10, 2014, [En línea]. Disponible en: http://www.hsaj.org.

Autores

Juan Anabalón Riquelme. Docente, consultor, fundador de MonkeysLab, presidente del Information Systems Security Association – ISSA Chile. Es especialista en la aplicación de los frameworks de seguridad cibernética NIST CSF, ES-C2M2, Transportation Roadmap y CARMA para proteger la infraestructura de líneas de vida en los sectores de Agua, Electricidad, Aviación e Internet. Juan es Magíster en Seguridad, Peritaje y Auditoría en Procesos Informáticos (USACH); Ingeniero de Ejecución en Informática, Licenciado en Ciencias de la Ingeniería (UDLA) y Certificado en Homeland Security and Cybersecurity por University of Colorado. Escribe regularmente sobre ciberseguridad en http://deoxyt2.livejournal.com. 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/

Manuel Ramírez S. es Ingeniero en Informática y Licenciado en Ciencias de la Ingeniería (UFRO), Diplomado en Seguridad Informática (UChile) y Diplomado en "La Función Inteligencia en el Estado Contemporáneo" (ANEPE). Ha sido expositor en 8.8 Cyber Security Conference. Actualmente, se desempeña como Líder de Proyectos de Seguridad en Cencosud y como Comunnity Manager de ISSA Chile. Puede ser contactado a través de: url: https://www.linkedin.com/in/manuel-ramírez-53968410/

Aldo Tobar E. Es Líder de Seguridad y Calidad, consultor especialista en gestión de seguridad de la información y calidad. Magíster en control y gestión de riesgo corporativo de la Universidad Central de Chile. Diplomado en Control, Auditoría y Seguridad de la Información, Docente del Diplomado de Ciberseguridad CORFO-USACH 2019, Certificado Ciberseguridad SAP ERP, Ingeniero en Control de Gestión, UNAP, Programador de Aciones Comerciales, Instituto A.I.E.P.
Puede ser contactado en https://www.linkedin.com/in/aldotobarespinoza/

Víctor Villar J., Suboficial especialista Nivel Superior en Telecomunicaciones Navales en la Armada de Chile con 26 años de experiencia, Diplomado en Redes CCNA (Inacap - Concepción), está capacitado en la Configuración avanzada Servidores Linux (UFSM - Viña del Mar), actualmente cursa la carrera Técnico Nivel Superior en Ciberseguridad (IACC), puede ser contactado en www.linkedin.com/in/loadmasther