Propuestas de ISSA Chile a la Política Nacional de Ciberseguridad (PNCS) 2016-2022

Technical Report · March 2016

DOI: 10.13140/RG.2.2.15314.45760

3 authors, including:

Juan Anabalon
MonkeysLab
9 PUBLICATIONS **4** CITATIONS

SEE PROFILE

Propuestas de ISSA Chile a la Política Nacional de Ciberseguridad (PNCS) 2016-2022

Juan Anabalón R.
jar@issachile.cl

Manuel Ramírez S.
manuel.ramirez@issachile.cl

Aldo Tobar E.
aldo.tobar@issachile.cl

Information Systems Security Association – ISSA Chile.

Introducción

La alta penetración de la Internet en el país ha cambiado la relación que se establece entre los ciudadanos y el estado de Chile y el acceso en línea a la información a permitido una sociedad más informada y empoderada[1] respecto de sus derechos y deberes como ciudadanos. Tal como sucede en el mundo real, las personas se reúnen en torno a ideas comunes a través de la red, sin embargo, la Internet también sirve para el desarrollo de comunidades con aficiones e intereses oscuros y algunos crímenes ahora son más fáciles de cometer: fraude electrónico, clonación de tarjetas bancarias, suplantación de identidad, violación de derechos de autor, robo de información confidencial, delitos sexuales y pedofilia[2] son realmente delitos triviales de realizar y el negocio en red es muy ágil.

ISSA Chile (*Information Systems Security Association – Chile*)[1], como asociación que agrupa a profesionales de la seguridad de la información, se siente en el deber cívico y republicano de presentar su visión respecto de la importancia de la seguridad de la información para el estado de Chile y aportar a la Propuesta de **Política Nacional de Ciberseguridad (PNCS) 2016-2022**[3] del **Comité Interministerial sobre Ciberseguridad**, y contribuir desde nuestra posición al desarrollo social y económico del país.

A continuación, exponemos algunas ideas que pueden ser desarrolladas como una política de Estado, que esperamos sean respaldadas y se le asigne el presupuesto necesario para su concreción.

Riesgos de las tecnologías de la información

La seguridad de la información es el conjunto de acciones preventivas y reactivas que permite resguardar y proteger la información en las organizaciones públicas como privadas, con el objetivo de mantener la disponibilidad, integridad y confidencialidad de la misma.

El actual desarrollo de la sociedad de la información y el conocimiento, tiene como tarea fundamental la custodia celosa de sus recursos de información y conocimiento debido a que estos son el motor fundamental de desarrollo, innovación y competitividad del país[4]. La adecuada administración y resguardo de la información y el conocimiento determina el desarrollo de la sociedad y esto se expresa en diferentes ámbitos del quehacer humano y tiene como principal instrumento de desarrollo las

[1] http://www.issachile.cl

tecnologías de la información cada vez más masivas y accesibles.

Por este motivo, para el estado de Chile le es indispensable plantearse una adecuada gestión de riesgos[5] [6] de la información concentrándose especialmente en la mitigación, la identificación y evaluación de impactos, y desarrollar un plan de mitigación de riesgos en los organismos de estado[7], involucrando activamente el sector privado en las áreas críticas de resguardo del país. Del mismo modo, el estado de Chile debe promover la seguridad de la información como un programa de evaluación continua de tal manera que se transforme en un proceso institucionalizado[8].

El objetivo de la realización de la gestión de riesgos[6] es permitir a las organizaciones del estado de chile a cumplir su misión asegurando los sistemas de almacenamiento, proceso y transmisión de información.

Propuestas

Agencia Nacional de Seguridad de la Información

En la actual sociedad de la información, en la economía y en la vida ciudadana hoy en día es fundamental que computadores, teléfonos, bancos, Internet e infraestructuras críticas funcionen de forma correcta y conjunta.

- La Agencia Nacional de Seguridad de la Información (ANSI) tendrá por misión garantizar el alto grado de seguridad de las redes y sistemas de información que Chile necesita, para lo cual:
    - Ofrecerá asesoramiento experto sobre seguridad en redes y sistemas de información[9] a las autoridades nacionales, ministerios, subsecretarías, intendencias, gobernaciones e instituciones estatales de importancia crítica.
    - Funcionará como agente de control y regulación para la implementación de buenas prácticas[10].
    - Facilita el contacto entre las instituciones estatales, autoridades nacionales y las empresas privadas de infraestructuras críticas.
    - La misión principal de la ANSI será la de apoyar a los organismos de estado a abordar, responder y, sobre todo, evitar problemas de seguridad de redes y sistemas de información.
    - La ANSI por su función de protección de los activos de información del Estado debe depender del ministerio del interior, que será el encargado de impulsar, coordinar y supervisar todas las actividades de seguridad de la información entre órganos de estado.

Desarrollo de planes de recuperación ante desastres (DRP) en las reparticiones públicas críticas

Es de público conocimiento que la geografía Chilena es muy variada y por lo mismo el país se ve afectado permanentemente a desastres naturales de gran envergadura. Es importante que todas las reparticiones públicas identificadas como críticas desarrollen un Plan

de Recuperación ante Desastres (DRP) que provea planes claros para la recuperación de los sistemas de información críticos, apoye la toma de decisiones oportuna y sirva para que las instituciones puedan desarrollar su función adecuadamente, aún en condiciones adversas.

Actualización de leyes sobre ciberdelitos

Actualmente en Chile no está regulada la figura de delito informático culposo. Los cuasidelitos generales de los arts. 490 y siguientes del Código Penal protegen a la persona física. Sin embargo, los cuasidelitos que se regulan en otros libros del Código, tienden a proteger bienes jurídicos distintos.

- Actualmente la Ley Nº 19.223 protege solamente la comisión de actos dolosos y no de los actos culposos y estos no son materia cuasidelitos civiles.

- Por lo tanto es importante incorporar una norma que permita hacer efectiva la responsabilidad penal de las personas en base de una imprudencia temeraria en materia de delitos informáticos.

- Adicional a esto, la Ley de 19.223 no cubre los distintos escenarios de ataque informático o la rápida evolución de las técnicas o métodos de hacking, por lo tanto, introducir continuos cambios en la legislación no es la mejor solución. Por lo tanto, para regular el hacking se debe promover su tipificación en una norma independiente para evitar confusiones y errores de interpretación.

Apoyo a Pymes en temas de seguridad de la información

En Chile las PYMES proporcionan el 80% de los puestos de trabajo a nivel nacional y son las empresas que tienen una mejor distribución a nivel nacional y no están concentradas en la región metropolitana. Los escasos recursos tecnológicos que una PYME puede tener, deben ser protegidos y resguardados debido a su fragilidad financiera, que haría desastrosa la perdida de los activos de información de las mismas, por lo tanto, se debe promover a través de distintos organismos de Estado, la seguridad de la información en la pequeña y mediana empresa y proporcionar incentivos para que estas incluyan buenas prácticas de seguridad de la información en sus actividades y asegurar su competitividad[11].

Incentivos a través de SENCE para capacitación en seguridad

La falta de personal calificado en materia de seguridad de la información hace que los emprendimientos y nuevos negocios iniciados en Chile estén en constante riesgo tecnológico, del mismo modo, la falta de personal calificado en instituciones del Estado hacen que áreas sensibles como Relaciones Exteriores e industrias productivas altamente automatizadas corran el riesgo de quedar inoperativas, parcial o permanentemente, ante la materialización de una amenaza tecnológica o un ataque informático real.

Por tal motivo, se hace necesario desarrollar el capital humano en las instituciones del Estado para lograr la excelencia operativa en distintas áreas estratégicas.

Promover el uso adecuado de redes sociales en colegios

Actualmente la alta penetración tecnológica en Chile hacen que cada vez más los chilenos estén más conectados y el uso de Smartphone es algo casi obligatorio en las nuevas generaciones.

Esto representa un riesgo, especialmente para los niños, debido a que a través de cualquier dispositivo se puede ver afectada la integridad personal mediante delitos como la pornografía, pedofilia, porno venganza entre otros riesgos.

Se hace necesario promover en el cuerpo docente una cultura de seguridad de la información que pueda ser transmitida y enseñada en las aulas de clase de todo el país.

Desarrollar e implementar un plan de Inteligencia Cibernética para todo el gobierno

Es necesario un plan de ciber inteligencia para todo el gobierno, con la finalidad de coordinar todas las actividades para detectar, disuadir y mitigar las amenazas de inteligencia extranjeras a sistemas de información de Chile y el sector privado clave. Para lograr estos objetivos, el plan debe establecer y ampliar una educación en contrainteligencia y programas de concientización y desarrollo de capital humano avanzado, para integrar todas las operaciones de análisis, sensibilización a empleados y aumentar la colaboración de inteligencia en el gobierno. El Plan de IC debe estar alineado con la Estrategia Nacional de Seguridad y Defensa (ENSYD)[12].

Definir y desarrollar programas y estrategias de disuasión permanente.

Las autoridades de gobierno deben pensar en las opciones estratégicas a largo plazo para Chile en un mundo que depende de asegurar el uso de las tecnologías de información y telecomunicaciones. Esta iniciativa pretende fundar una estrategia de Defensa Cibernética que evite interferencias y ataques a través de internet con el objetivo de desarrollar las capacidades de monitoreo y respuesta a ataques, articulando las funciones del sector privado y de los socios internacionales, que permitan llevar a cabo respuestas apropiadas para amenazas estatales y no estatales.

Tal estrategia debe estar definida en cinco objetivos fundamentales[13]:

1. Desarrollar y mantener listas fuerzas y capacidades para llevar a cabo operaciones de ciberespacio;
2. Defender la red de información de defensa, asegurar los datos y mitigar los riesgos para la misión del ministerio de defensa y sus ramas operativas.
3. Estar preparado para defender el territorio y los intereses vitales de ciberataques perjudiciales o destructivos de consecuencia significativa;
4. Desarrollar y mantener opciones cibernéticas viables y planear el uso de esas opciones para controlar la escalada del conflicto y dar forma a la situación de conflicto en todas las etapas;
5. Construir y mantener sólidas alianzas internacionales y asociaciones para disuadir las amenazas compartidas y aumentar la estabilidad y la seguridad internacionales.

Desarrollar un marco regulatorio para mejorar la ciberseguridad de infraestructuras críticas.

El buen funcionamiento del Estado depende de la seguridad cibernética de su infraestructura crítica. Las amenazas de ciberseguridad se han tornado de gran complejidad y representan un gran desafío para la seguridad pública, económica y del sistema de salud. El Marco Regulatorio para mejorar la ciberseguridad de infraestructuras críticas, deberá establecer una política de Estado para mejorar la seguridad y la resistencia de las

infraestructuras críticas de la nación, mantener un entorno cibernético que fomente la eficiencia, la innovación y la prosperidad económica promoviendo la confiabilidad, seguridad, confidencialidad comercial, la privacidad y las libertades civiles. Este marco de trabajo deberá ser fruto de la colaboración entre el gobierno y el sector privado, considerando las necesidades de cada negocio y permitiendo la flexibilidad necesaria para cada industria y tamaño corporativo. Este marco regulatorio debe ser de cumplimiento obligatorio para infraestructuras críticas de Estado y el sector privado cuyo objetivo principal será normar la identificación, protección, detección, respuesta y recuperación de incidentes de seguridad en importantes sectores industriales, civiles y de defensa.

Desarrollar un centro criptológico nacional

El Centro Criptológico nacional tendrá como objetivo desarrollar y promover el uso de mecanismos avanzados de seguridad, como la criptografía, y otras normas y estándares que permitan al país lograr la independencia tecnológica en cuanto al resguardo de información sensible y de seguridad de Estado.

Privacidad de la información

Promover el desarrollo de normas de privacidad de Información de Salud que contemplen sanciones civiles y penales respecto del incumplimiento de la normativa para el amplio espectro de prestadores de salud:

1. ISAPRE.
2. FONASA
3. Cajas de compensación y aseguradoras de salud.
4. Cínicas y Hospitales.

Desarrollar un marco de trabajo para la mejora de ciberseguridad de infraestructura crítica

La ANSI deberá desarrollar un marco de trabajo para la mejora de ciberseguridad de infraestructura crítica[14], basado en el riesgo la ciberseguridad y que apoye a las organizaciones a administrar los riesgos en sistemas de control industrial. El marco resultante estará basado en estándares internacionales y buenas prácticas de administración de sistemas de control industrial (SCADA). Debe ser creado mediante la colaboración entre el gobierno y el sector privado de la industria, minera, química, petrolera, electricidad, gas, puertos etc.

Preservar las libertades civiles

Todas las acciones de seguridad que se emprendan no deberán coartar las libertades civiles, incluyendo las libertades civiles en internet:

1. No se prohibirá ni limitará el acceso de los usuarios a las tecnologías de cifrado; o prohibir el uso de cifrado por grados o tipos;
2. No se deberá exigir el diseño o la implementación de "puertas traseras" (backdoors) o vulnerabilidades en herramientas, tecnologías o servicios;
3. No se requerirá que las herramientas, tecnologías o servicios sean diseñados o desarrollados para permitir el acceso de terceros a datos sin cifrar o a las claves de cifrado;
4. No se deberá tratar de debilitar o socavar los estándares de cifrado o influir intencionalmente en su desarrollo, a menos que sea para promover un mayor nivel de seguridad de la información.

5. No se debe exigir algoritmos, estándares, herramientas o tecnologías de cifrado inseguros. Tampoco debería, por acuerdo privado o público, obligar o presionar a entidades para que actúen de manera incompatible con los principios anteriores.

Referencias

[1] J. Heidemann, M. Klier, and F. Probst, "Online social networks: A survey of a global phenomenon," *Comput. Netw.*, vol. 56, no. 18, pp. 3866 – 3878, 2012.

[2] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Comput. Secur.*, vol. 24, no. 1, pp. 31–43, Feb. 2005.

[3] Comité Interministerial sobre Ciberseguridad (CICS), "Propuesta de Política Nacional de Ciberseguridad (PNCS) 2016-2022." .

[4] Instituto Español de Estudios Estratégicos, "Ciberseguridad. Retos y Amenazas a La Seguridad Nacional En El Ciberespacio." Imprenta del Ministerio de Defensa. España, Feb-2011.

[5] E. Paintsil, "Taxonomy of security risk assessment approaches for researchers.," in *CASoN*, 2012, pp. 257–262.

[6] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," *Nist Spec. Publ.*, vol. 800, no. 30, pp. 800–30, 2002.

[7] F. PUB, "Standards for Security Categorization of Federal Information and Information Systems," 2004.

[8] National Institute of Standards and Technology, "Building an Information Technology Security Awareness and Training Program." National Institute of Standards and Technology (NIST) U.S., Oct-2003.

[9] N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya, and J. K. Kalita, "Network attacks: Taxonomy, tools and systems," *J. Netw. Comput. Appl.*, vol. 40, no. 0, pp. 307–324, Apr. 2014.

[10] R. Ross, S. Katzke, A. Johnson, M. Swanson, G. Stoneburner, G. Rogers, and A. Lee, "Recommended security controls for federal information systems," *NIST Spec. Publ.*, vol. 800, p. 53, 2005.

[11] P. Weill and S. L. Woerner, "The Future of the CIO in a Digital Economy," *MIS Q. Exec.*, vol. 12, no. 2, Jun. 2013.

[12] "Estrategia Nacional de Seguridad y Defensa." .

[13] DoD, "The Department of Defense - Cyber Strategy." Apr-2015.

[14] B. Obama, "Executive Order 13636—Improving Critical Infrastructure Cybersecurity." U.S. National Archives and Records Administration, 12-Feb-2013.

Juan Anabalón R. es CISO en MonkeysLab e investigador independiente, Ingeniero de Ejecución en Informática y Licenciado en Ciencias de la Ingeniería (UDLA) y Magíster en Seguridad, Peritaje y Auditoría en Procesos Informáticos (USACH). Puede ser contactado a través de:
url: http://www.monkeyslab.cl
blog: http://deoxyt2.livejournal.com

Aldo Tobar E. es Ingeniero de Ejecución en Control de Gestión, UNAP, Diplomado en Control, Auditoría y Seguridad de la Información, USACH, Programador de Aplicaciones Comerciales, Instituto A.I.E.P. Puede ser contactado a través de:
url: http://www.issachile.cl

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: http://www.issachile.cl