ISSA Chile
Juan Anabalón R.
Presidente ISSA Chile Chapter
CISO MonkeysLab
15 de noviembre de 2018

Inscripción: https://welcu.com/bsidescl/bsidescl-latam

Política de ciberseguridad para infraestructuras de agua y electricidad

Fotografía: Central Hidroeléctrica Queltehues https://flic.kr/p/d2GSTS

En esta charla examinará las diversas políticas de infraestructuras de agua potable y de electricidad que se han desarrollado en EE.UU. para ayudar a guiar y fortalecer sus programas de seguridad cibernética. Estas infraestructuras son dos de los catorce subsectores que comprende lo que se conoce como infraestructura de “lifeline".

El Plan Nacional de protección de infraestructura del año 2013 identifica cuatro sectores de infraestructura de lifeline: 1) agua, 2) energía, 3) transporte y 4) comunicaciones. Estos sectores se señalan como "lifeline" porque de ellos dependen muchas otras infraestructuras. Ambos subsectores son supervisadas por el Department of Homeland Security National Protection and Programs Directorate que gestiona el programa de protección de infraestructura nacional del DHS. El NIPP emplea un Framework de administración de riesgos de mejora continua de cinco pasos, que es supervisado por organismos sectoriales (Sector Specific Agency - SSA) designados por el DHS. Las agencias sectoriales trabajan en cooperación voluntaria con representantes de la industria para aplicar los resultados de marco de gestión de riesgo en los correspondientes planes sectoriales.

En febrero de 2013, el Presidente Obama emitió la EO13636 dirigida al National Institute of Standards and Technology para desarrollar un conjunto de recomendaciones, de adhesión voluntaria, para el fortalecimiento de las medidas de ciberseguridad de infraestructura. La Agencia de Protección del Medio Ambiente, que es a la vez la SSA y la autoridad reguladora para el subsector de agua potable recomienda la aplicación voluntaria del Marco Ciberseguridad NIST. El Departamento de Energía, que es a la vez la SSA y la autoridad reguladora para el subsector eléctrico respondió que ya estaba implementando el Modelo de Madurez de capacidad de ciberseguridad en el subsector Electricidad, basado en el NIST Cybersecurity Framework. El Departamento de energía, sin embargo, recomienda la aplicación voluntaria de la ES-C2M2.

¿Cuales son las diferencias de ambos modelos?, ¿Es aplicable esta metodología en Chile?, ¿Compete esta regulación a la nueva Agencia de Ciberseguridad del Gobierno?.

Relator:

Juan Anabalón R. Es especialista en seguridad de la información, informática forense, privacidad, vigilancia, censura y cuestiones políticas y sociales de Ciberseguridad. Entre otras cosas es Profesor en Universidad Autónoma de Chile, Co-fundador y Presidente del *Information Systems Security Association – ISSA Chile*, capítulo chileno de ISSA International; es fundador y consultor en ciberseguridad en MonkeysLab y tiene amplia experiencia en dirección de sistemas de gestión de seguridad de la información, Ethical Hacking y auditoría informática. Ha sido expositor en diferentes conferencias de seguridad. Puede ser ubicado en:
http://monkeyslab.cl/jar/
https://deoxyt2.livejournal.com