Política de ciberseguridad para infraestructuras de agua y electricidad

Juan Anabalón
MonkeysLab - ISSA Chile

Juan Anabalon
http://www.monkeyslab.cl/jar

- Especialista ciberseguridad e infraestructura crítica, informática forense, privacidad, vigilancia, censura y cuestiones políticas y sociales de Ciberseguridad. Cuenta con certificaciones para 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 subsectores de Agua, Electricidad, Aviación e Internet.
Profesor en Universidad Autónoma de Chile e Instituto Profesional Santo Tomás, 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.

ISSA Chile

- 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.

Agenda

- Introducción
- Seguridad nacional
- Ciberseguridad
- Infraestrutura crítica de Agua
- NIST CSF
- Infraestrutura crítica de Setor Eléctrico
- ES-C2M2
- Diferencias en ambos modelos
- Conclusiones

Seguridad nacional y ciberseguridad

- Seguridad nacional tiene por objetivo salvaguardar a una nación de la destrucción catastrófica interna.

Todo comenzó

- Ataques del metro de Tokio 1995.
- Demostró la capacidad de los actores no estatales de emplear armas de destrucción masiva.

Luego 9/11

- Mientras que 9/11 demostró la capacidad de actores no estatales para lograr efectos de armas de destrucción masiva al **subvertir infraestructura crítica**.

ciberseguridad

- Es un componente integral de la protección de la infraestructura crítica

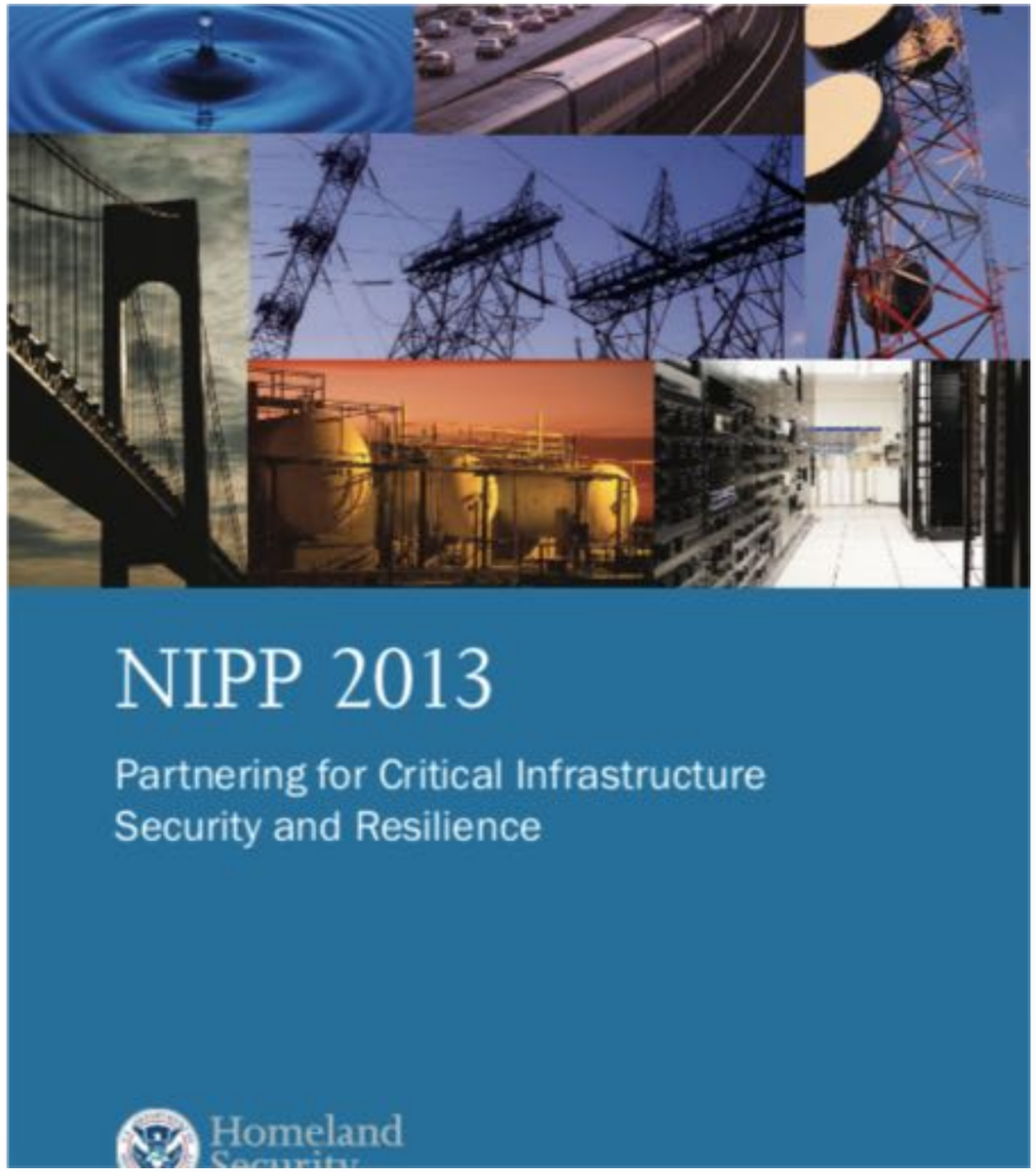
¿Por qué?

BSides Latam Chile 2018

- El ciberespacio proporciona una vía para atacar la infraestructura crítica de cualquier parte del mundo.
- Los componentes cibernéticos hacen a las infraestructuras críticas susceptibles de subversión, interrupción o destrucción.
- Y el ciberespacio es una infraestructura crítica, en la que dependen muchas otras infraestructuras críticas.

EE.UU.

- PPD-21 de la administración Obama identifica 16 sectores de infraestructura diferentes.
- De estos sectores, el 2013 El Plan Nacional de protección de infraestructuras designa a cuatro infraestructura de Lifeline.



NIPP 2013

01	02	03	04
Agua	Energía	Transporte	Comunicaciones

BSides Latam Chile 2018

NIPP 2013

Estos cuatro sectores de Lifeline engloban 14 subsectores más

#	Sector	Subsector	System Asset	Concerning Party
1	Water/Wastewater	Water	Water Treatment & Distribution Utility	Utility Owner/Operator
2		Wastewater	Sewer Treatment & Collection Utility	Utility Owner/Operator
3	Energy	Electricity	Electrical Utility	Utility Owner/Operator
4		Natural Gas	Gas Utility	Utility Owner/Operator
5		Oil	Oil Refinery	Refinery Owner/Operator
6	Transportation	Aviation	Passenger/Cargo Jet	Air Service Owner/Operato
7		Highway	Major Transportation Bridge	State DOT
8		Rail Freight	Rail Freight Service	Rail Owner/Operator
9		Mass Transit	Major Transportation Corridor	Route Owner/Operator
10		Pipeline	Oil Pipeline	Pipeline Owner/Operator
11		Maritime	Shipping Port	Port Owner/Operator
12		Maritime	Cruise Ship	Cruise Line Owner/Operato
13	Information	Internet	Internet Exchange Point	Internet Service Provider
14		Internet	Domain Name Servers	Root Server Administrator

NIST Cybersecurity Framework

NIST CSF

BSides Latam Chile 2018

Infraestructura de Agua

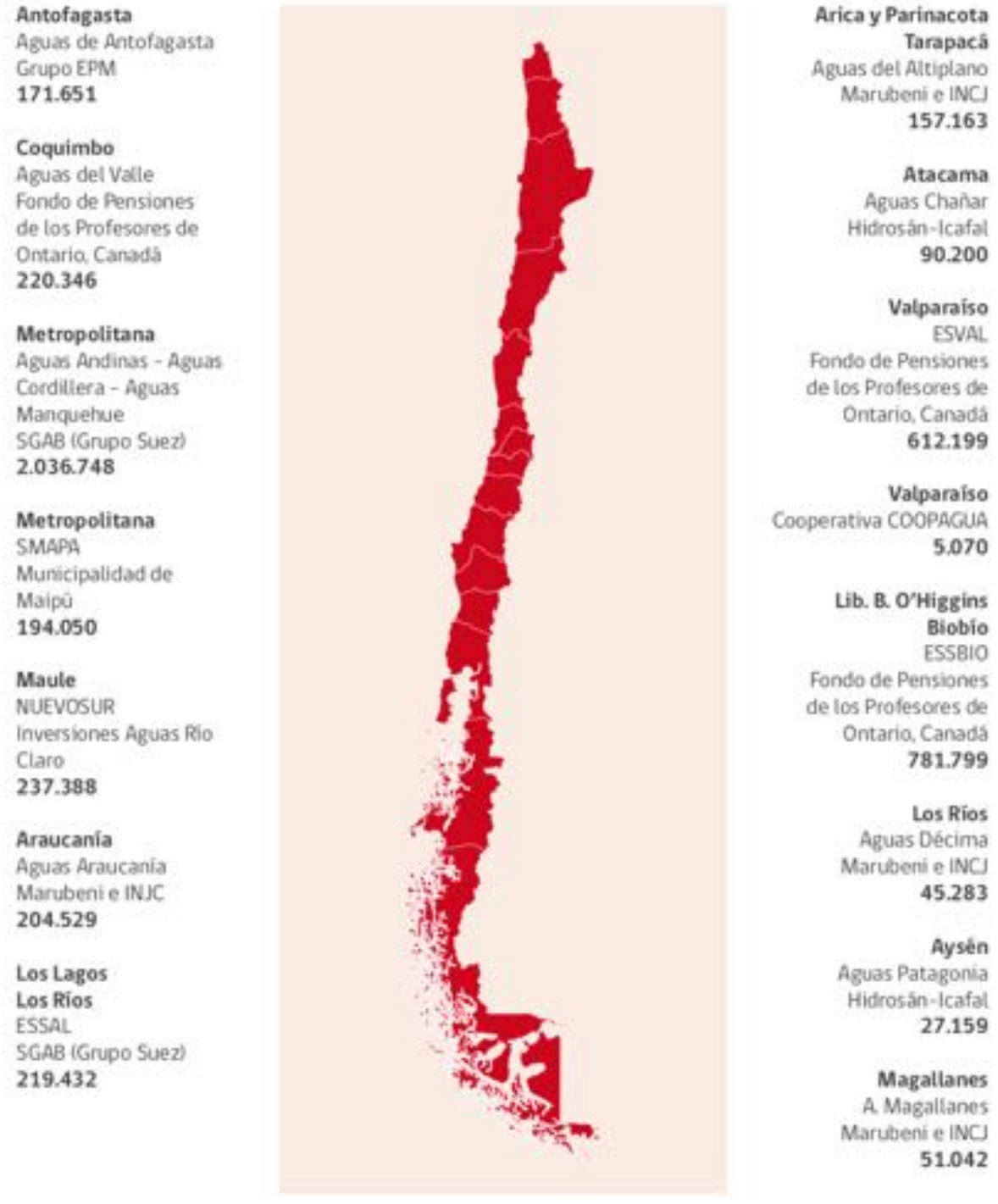
- La infraestructura de agua incluye agua potable y servicios de aguas residuales.
- A diciembre de 2016, la cobertura de agua potable en los territorios urbanos y concesionados a nivel nacional es de 99,92% y la de alcantarillado, de 96,83%; mientras que la cobertura de tratamiento de las aguas servidas recolectadas mediante sistemas de alcantarillado, es de 99,93%.
- El ataque cibernético podría interrumpir servicios de agua durante un período prolongado, causando fallas físicas en equipos de control y bombeo.
- Las utilidades del agua se diseñan para resistir la tormentas y vandalismo, pero no ataque concertado.
- Bajo la nueva normativa de gobierno, ¿cual será la institución responsable de coordinar las medidas de seguridad del sector con la industria.
- ¿Se exigirá cumplir con una norma como NIST CSF u otro marco de ciberseguridad para protección de la infraestructura crítica?.

99,59% zonas urbanas

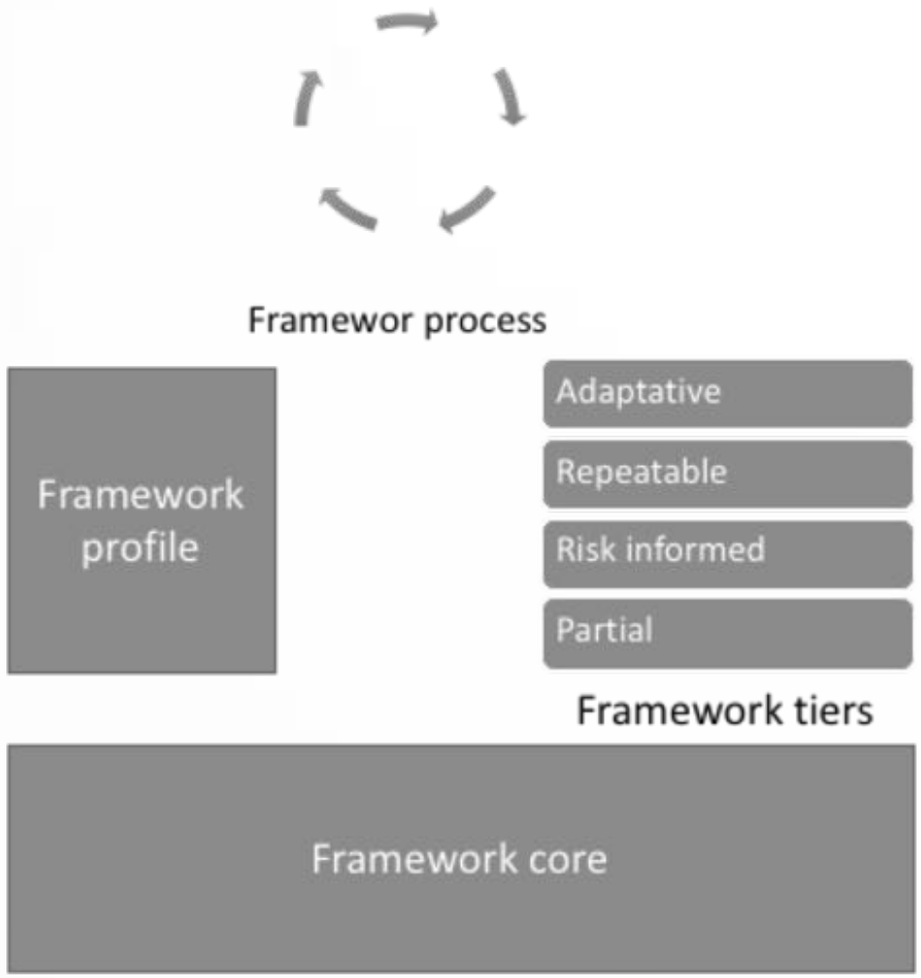
94,06% clientes residenciales

4,76% clientes comerciales y

1,18% a industriales y otros.



NIST CSF



*Original figure made by Richard White

- Compuesto de cuatro partes:
  - Framework Core
  - Framework Tiers
  - Framework Profiles
  - Framewok proces

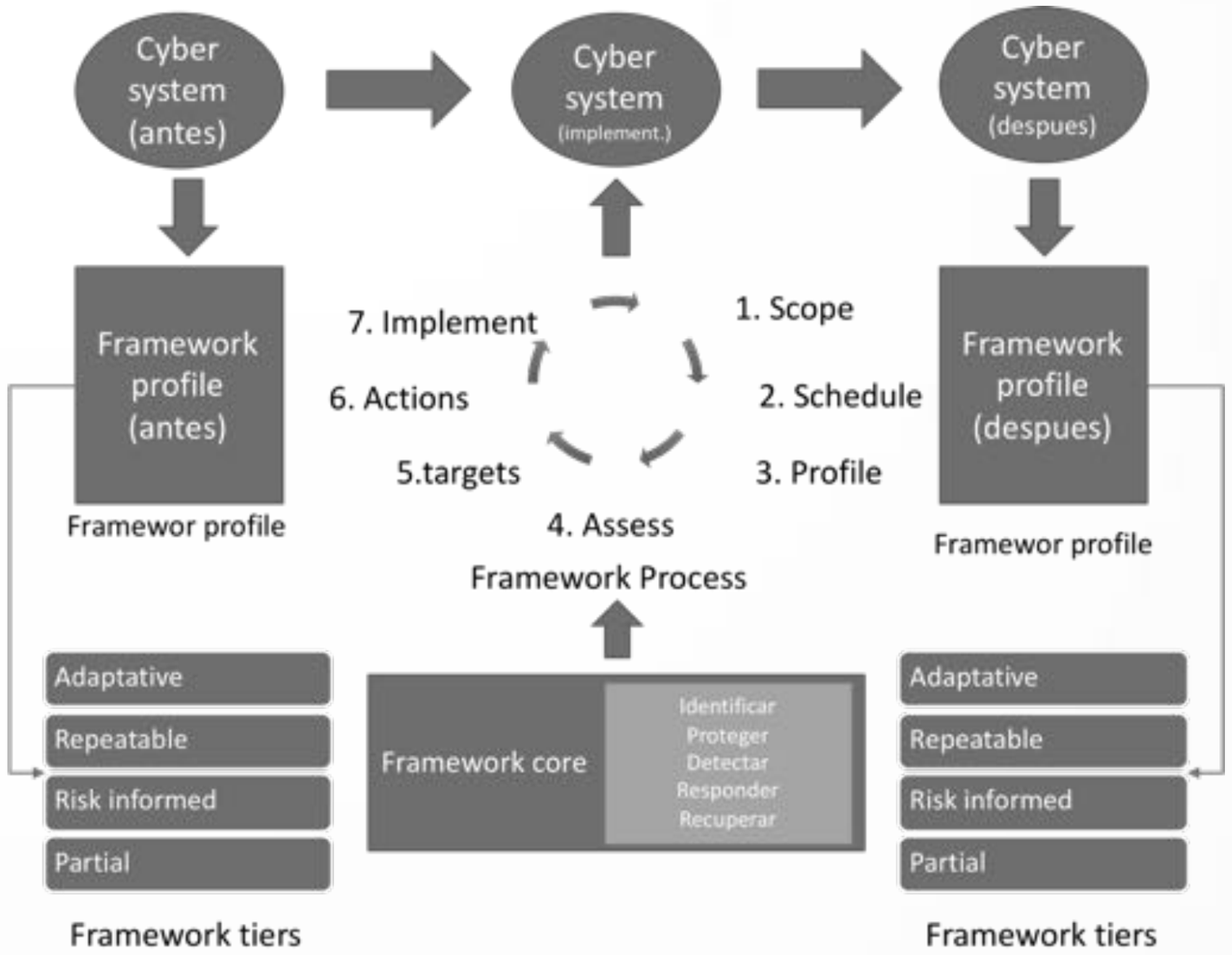
NIST CSF

- El núcleo es un conjunto de actividades de ciberseguridad, los resultados deseados y las referencias aplicables que son comunes en los sectores de la infraestructura.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness & Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies & Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST SCF

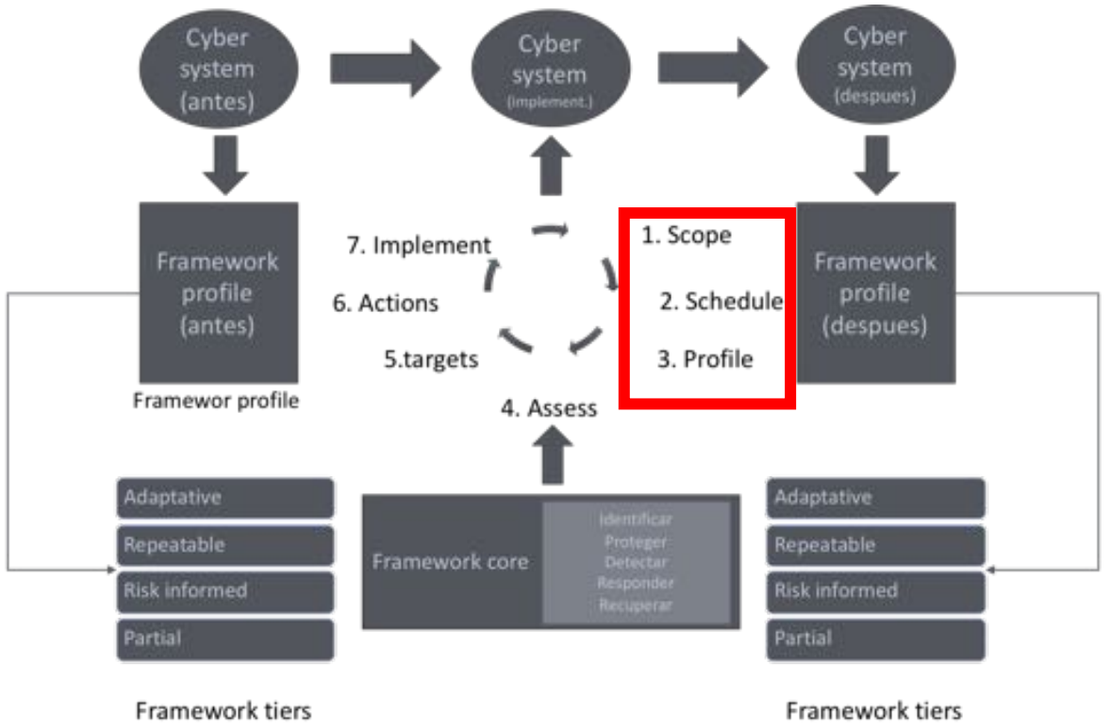
- El NIST CyberSecurity Framework es un proceso de mejora continua para reducir el riesgo.
- El NIST CyberSecurity Framework se basa en un marco basado en un conjunto de normas relacionadas con la identificación, detección y protección contra las amenazas, respuesta y recuperación ante un ataque cibernético.
- El NIST Cybersecurity Framework define un conjunto de cuatro niveles que representan un aumento de los niveles de protección.
- Es un esfuerzo colaborativo entre la operación del sistema y la Gestión empresarial.
- El Framework de ciberseguridad del NIST es un proceso de 1) asignación de un Perfil actual 2) Desarrollar un perfil de objetivo. 3) Identificar y priorizar las acciones básicas necesarias para alcanzar el perfil objetivo. 4) Implementar las acciones identificadas del Framework Core.
- NIST Cybersecurity Framework requiere un esfuerzo significativo en tiempo y recursos.
- El NIST Cybersecurity Framework facilita una estrategia planificada de reducción de riesgos.



*Original figure made by Richard White

Aplicación NIST CSF

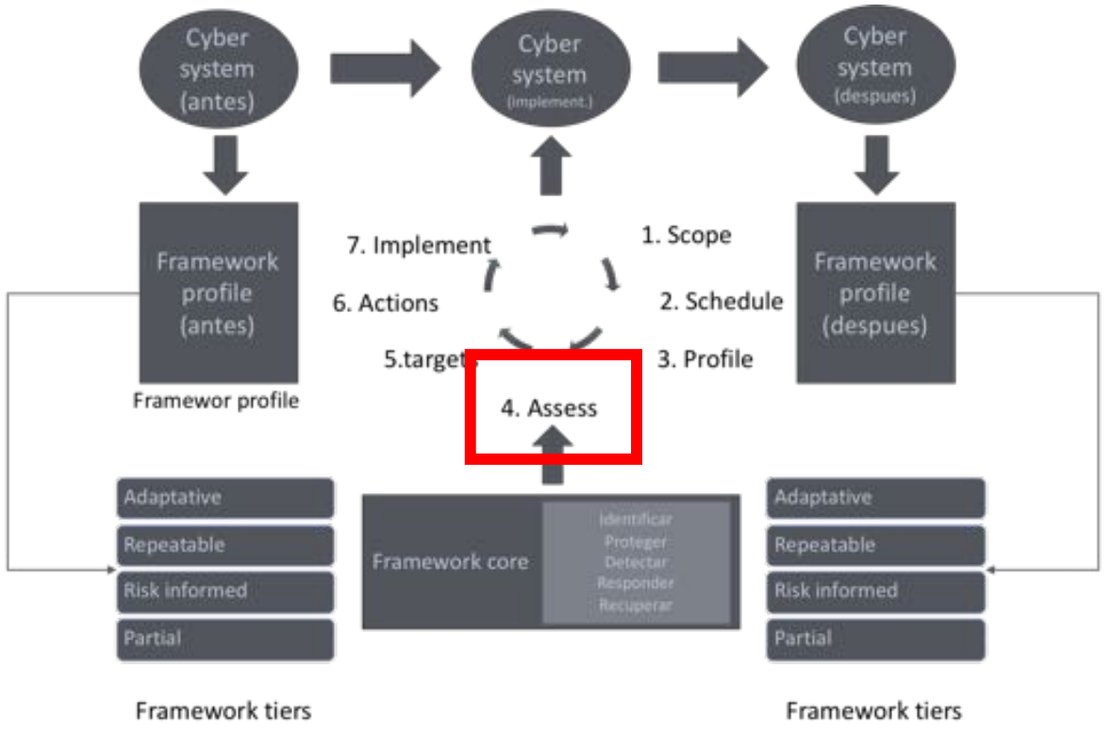
- Ud es CISO de una compañía de agua potable.
- Proporciona 90% de suministros a una ciudad mediana (Chillan, Linares)
- Primer intento de implementación de NIST CSF.
- Se ha desarrollado un Profile:
  - Nivel 1: Parcial.
  - No hay proceso formal
  - No hay organización de gestión de riesgo.
  - No incluye proveedores.



*Original figure made by Richard White

Aplicación NIST CSF

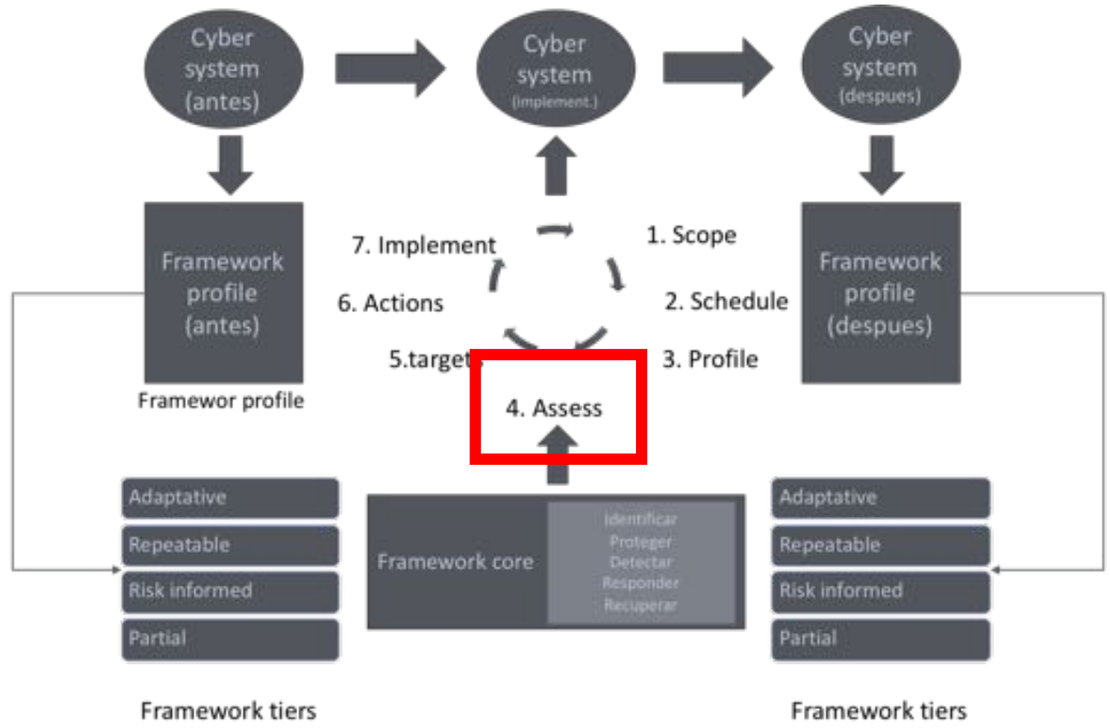
- Paso 4: análisis de riesgo:
- Hay una muy baja probabilidad de ataques cibernéticos maliciosos que podrían interrumpir el 100% de el servicio de utilidad hasta por una semana.
- ¿El perfil actual de seguridad es suficiente, o debemos avanzar al siguiente paso y intentar alcanzar el nivel dos?



*Original figure made by Richard White

Aplicación NIST CSF

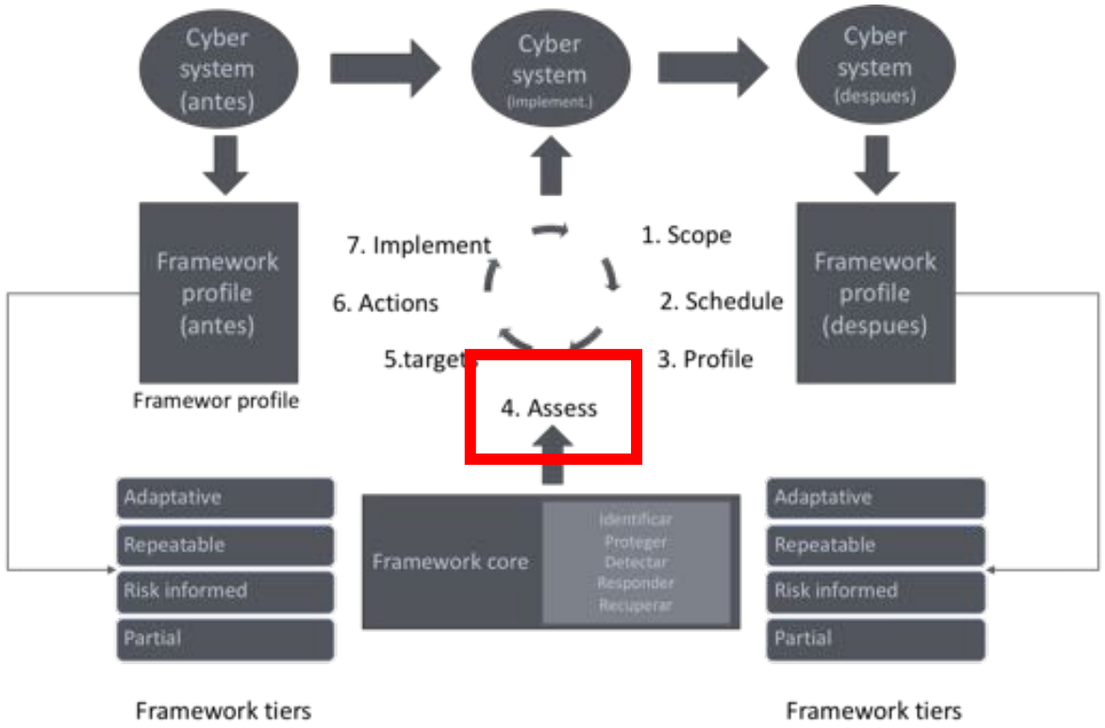
- ¿Nos mantenemos en el nivel 1 - Parcial?
- ¿Avanzamos a Nivel 2 – Riesgo informádo?
- Avanzamos



*Original figure made by Richard White

Consideraciones de análisis

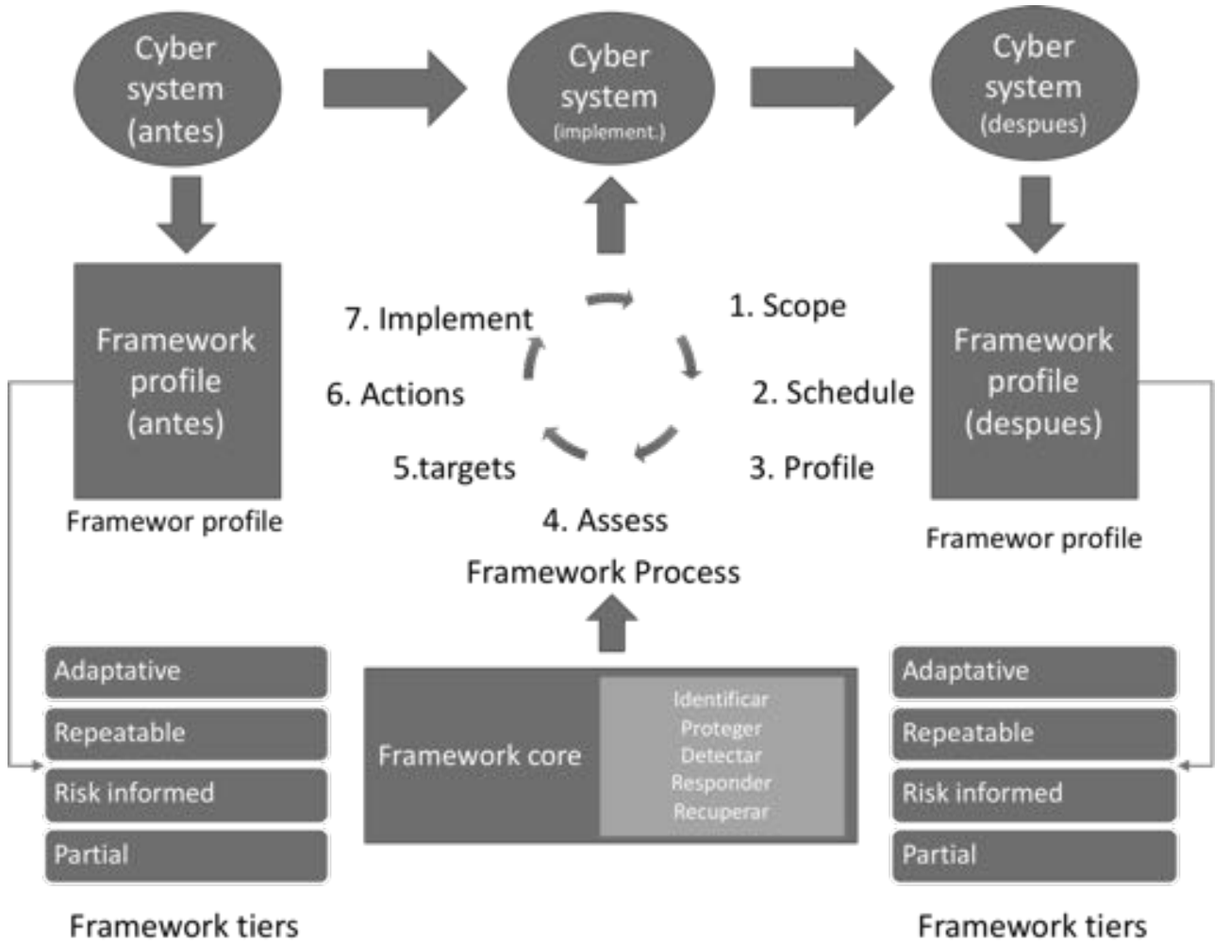
- Puede perder más que solo el suministro de agua potable.
- Puede perder presión para combatir incendios.
- Gobierno, empresas y las escuelas podrían tener que cerrar.



*Original figure made by Richard White

Cambiemos el escenario

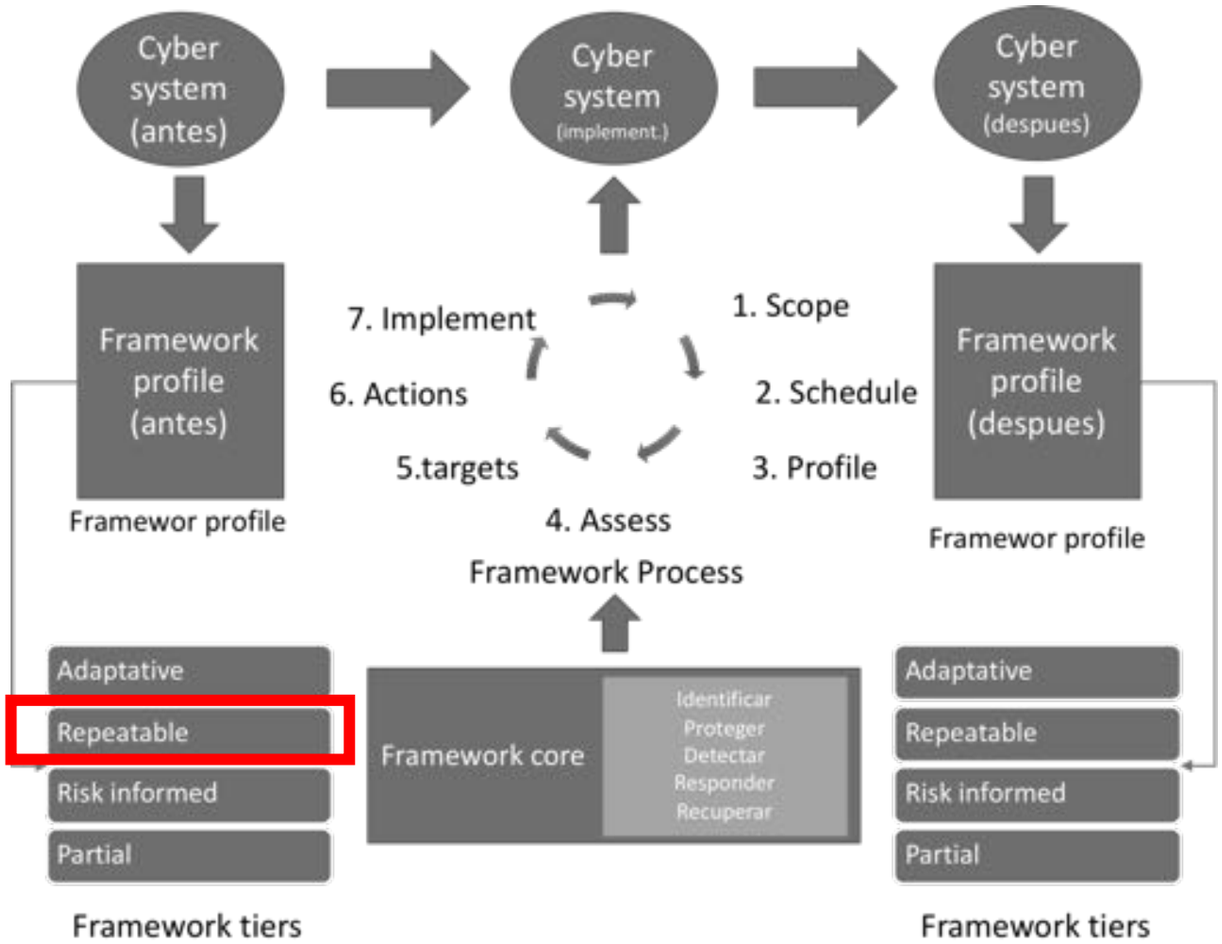
- Ud. Es CISO en una planta de agua potable en una ciudad grande (Santiago).
- Opera dos plantas independientes.
- Ambas reciben agua de fuentes separadas.
- Sistemas propios de distribución.
- Una es backup de la otra.



*Original figure made by Richard White

Cambiemos el escenario

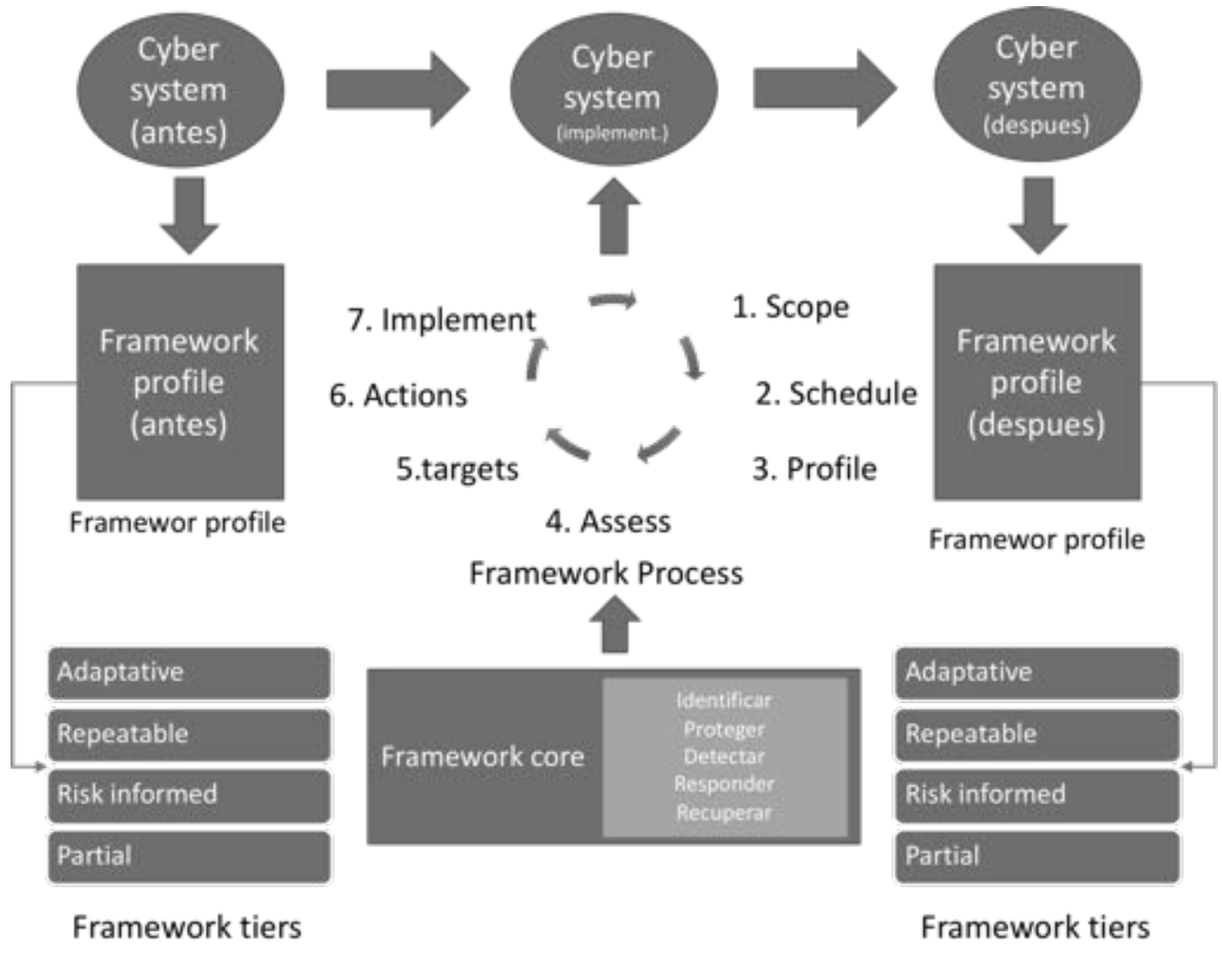
- NIST CSF 3 años.
- Perfil en el nivel tres repetible.
- En revisión anual: ¿Cuál es tu objetivo para el próximo año?
- ¿Avazamos a Nivel 4 – Adaptativo?
- Para avanzar requeriría la contratación de personal adicional, lo que exige al menos un 20% más de presupuesto.
- ¿Cuál es el propósito?
- Según su estimación, las ganancias de seguridad serían marginales.



*Original figure made by Richard White

Cambiemos el escenario

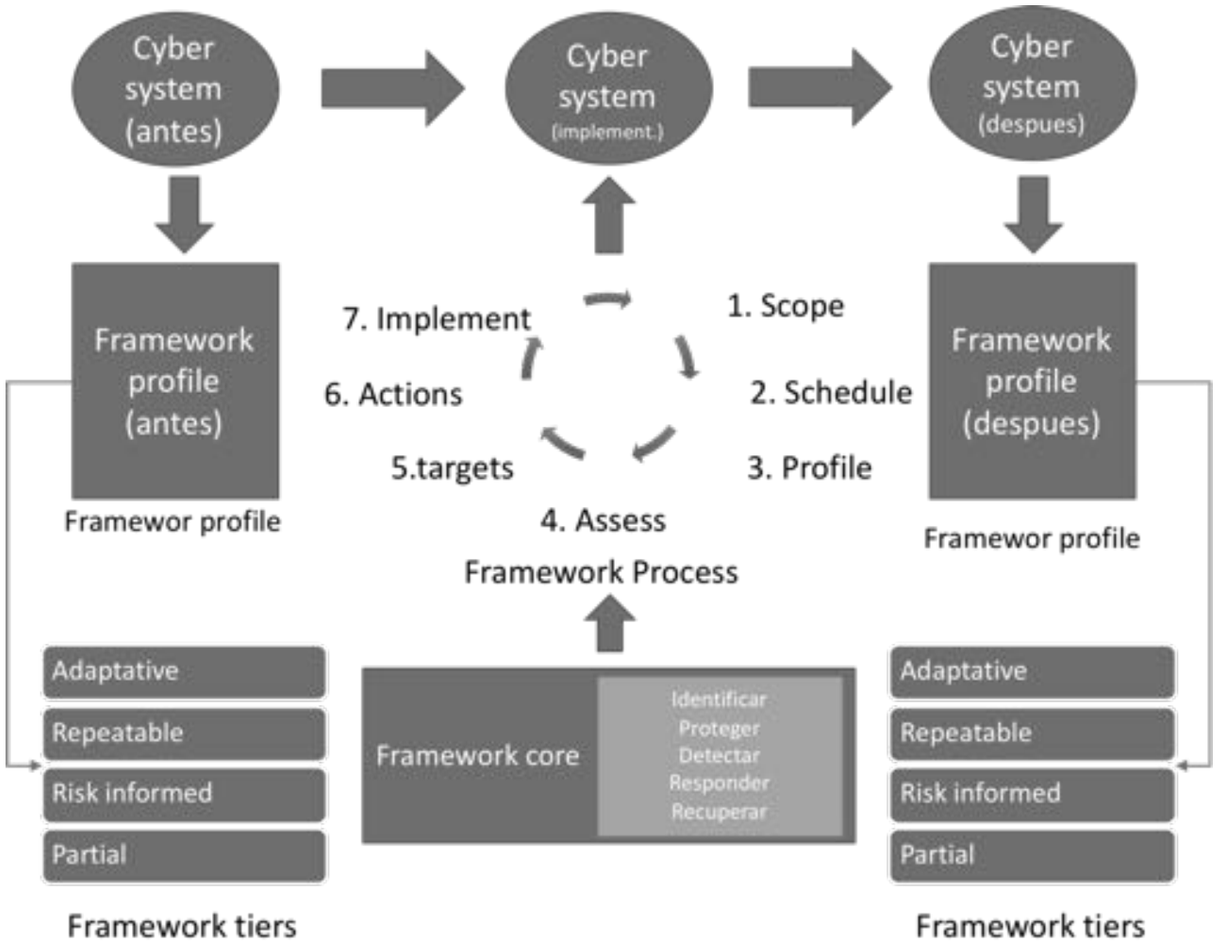
- Pero el CIO quiere lo mejor en seguridad ☺
- Aún existe riesgo de ciberataques.
- ¿Avanzamos a nivel 4?



*Original figure made by Richard White

Cambiemos el escenario

- Bajo estas circunstancias es mejor mantener nivel 3 - Repetible.
- Toda la ciberseguridad se trata de la gestión del riesgo.
- No existe una seguridad absoluta.
- Por lo tanto se debe utilizar una metodología de análisis costo-beneficio.
- Gana menos protección a un costo más alto.



*Original figure made by Richard White

Electricity Subsector Cyber Capability Maturity Model

BSides Latam Chile 2018


latercera.com

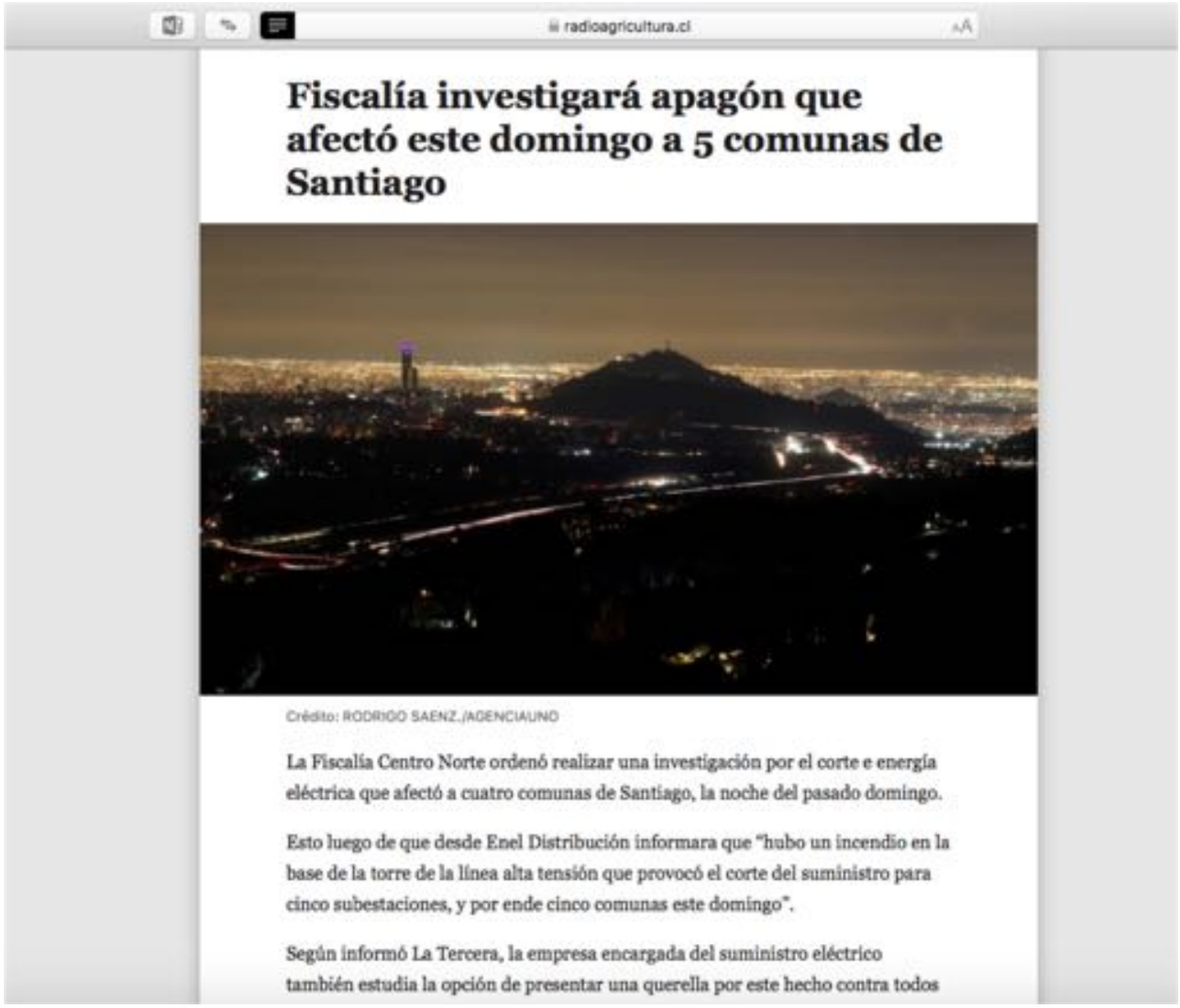
Apagón en zona oriente afectó a más de 247 mil clientes

Corte de suministro eléctrico se generó por la falla en una línea de transmisión. Investigan las causas.

Cuando faltaban cinco minutos para las 19.00, las comunas de Las Condes, Vitacura, Providencia y Lo Barnechea quedaron abruptamente a oscuras, producto de un corte masivo de suministro eléctrico que afectó a 247 mil clientes de la empresa Enel, según informó la Superintendencia de Electricidad y Combustibles (SEC), y que provocó la alerta de autoridades y alcaldes.

Importancia

En Chile



radioagricultura.cl

Fiscalía investigará apagón que afectó este domingo a 5 comunas de Santiago

Crédito: RODRIGO SAENZ./AGENCIAUNO

La Fiscalía Centro Norte ordenó realizar una investigación por el corte e energía eléctrica que afectó a cuatro comunas de Santiago, la noche del pasado domingo.

Esto luego de que desde Enel Distribución informara que "hubo un incendio en la base de la torre de la línea alta tensión que provocó el corte del suministro para cinco subestaciones, y por ende cinco comunas este domingo".

Según informó La Tercera, la empresa encargada del suministro eléctrico también estudia la opción de presentar una querella por este hecho contra todos

Importancia

En Chile

En USA

En agosto de 2003, un corte de energía afectó a 50 millones personas en el noreste de los Estados Unidos durante casi una semana. La causa fue accidental.

$4 a $10 mil millones en pérdidas económicas se atribuyen al apagón.

al igual que una caída del 0,7% en el PIB de Canadá.

Un estudio de John Hopkins determinó que 90 personas en la ciudad de Nueva York murieron como resultado directo de la interrupción del suministro eléctrico.

Proyecto Aurora

- En 2006 el DHS junto con el Departamento de energía, llevó a cabo un conjunto experimento llamado Proyecto Aurora.
- Demostrando cómo un generador de electricidad podría ser controlado remotamente por Internet para autodestruirse.
- PPD-21 asigna el Departamento de Energía como organismo sectorial específico responsable del sector energético, incluyendo electricidad.
- Los funcionarios federales se preocupan de que un ataque cibernético coordinado podría cerrar la red norteamericana por meses, si no años.

https://youtu.be/u0fouxPO3uo

Sector eléctrico (USA)

El Departamento de energía trabaja con el Consejo de coordinación del sector eléctrico para aplicar las disposiciones del Plan de protección de infraestructuras, y actualizar su plan sectorial específico.

La política energética de 2005 crea la Federal Energy Regulatory Commission. Una agencia del DoE con autoridad regulatoria sobre el sector eléctrico, incluida la autoridad para aplicar normas de ciberseguridad.

FERC trabaja con el North American Electric Reliability Corporation para mantener la supervisión de la fiabilidad de la red norteamericana.

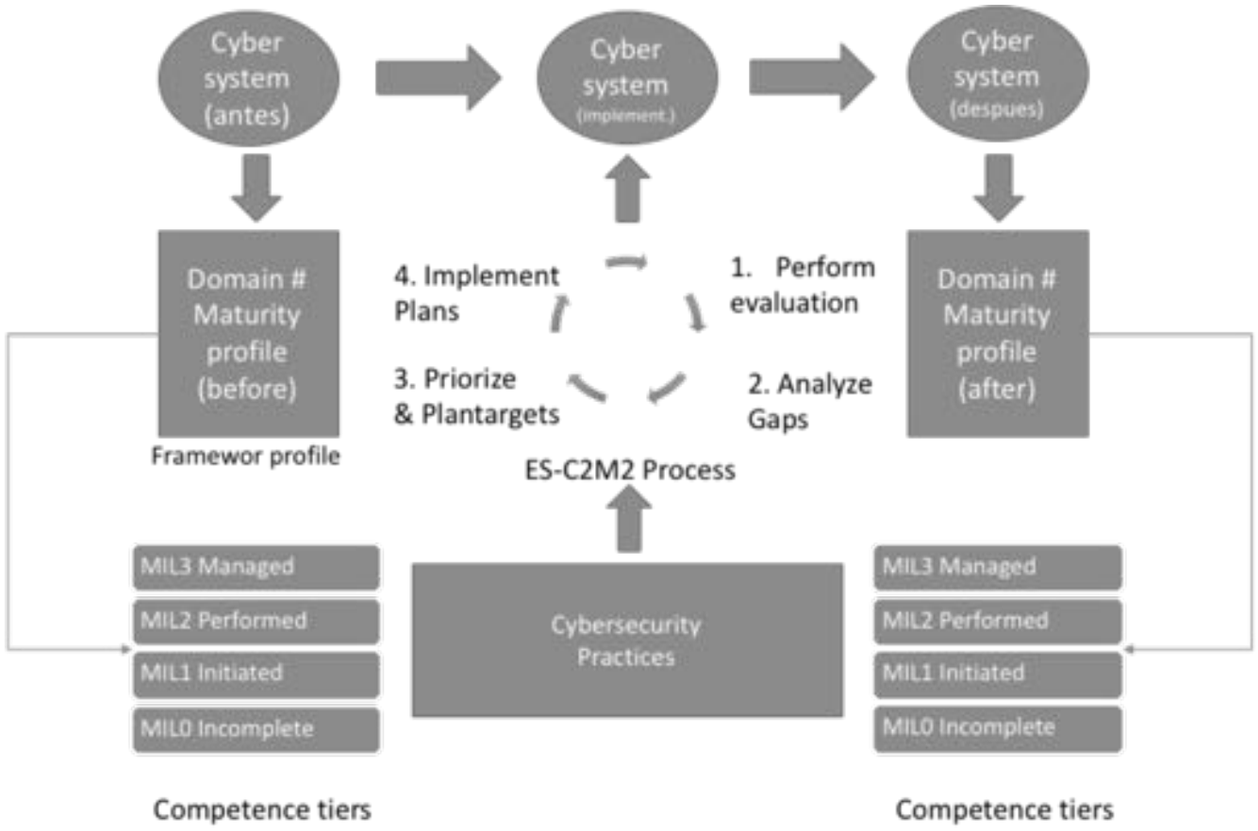
FERC desarrolló un conjunto de normas de ciberseguridad para el sector eléctrico.

FERC también ayudó al NIST a desarrollar el marco de ciberseguridad 2014.

El NIST Cybersecurity Framework se asemeja estrechamente al Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).

Electricity Subsector Cyber Capability Maturity Model (ES-C2M2)

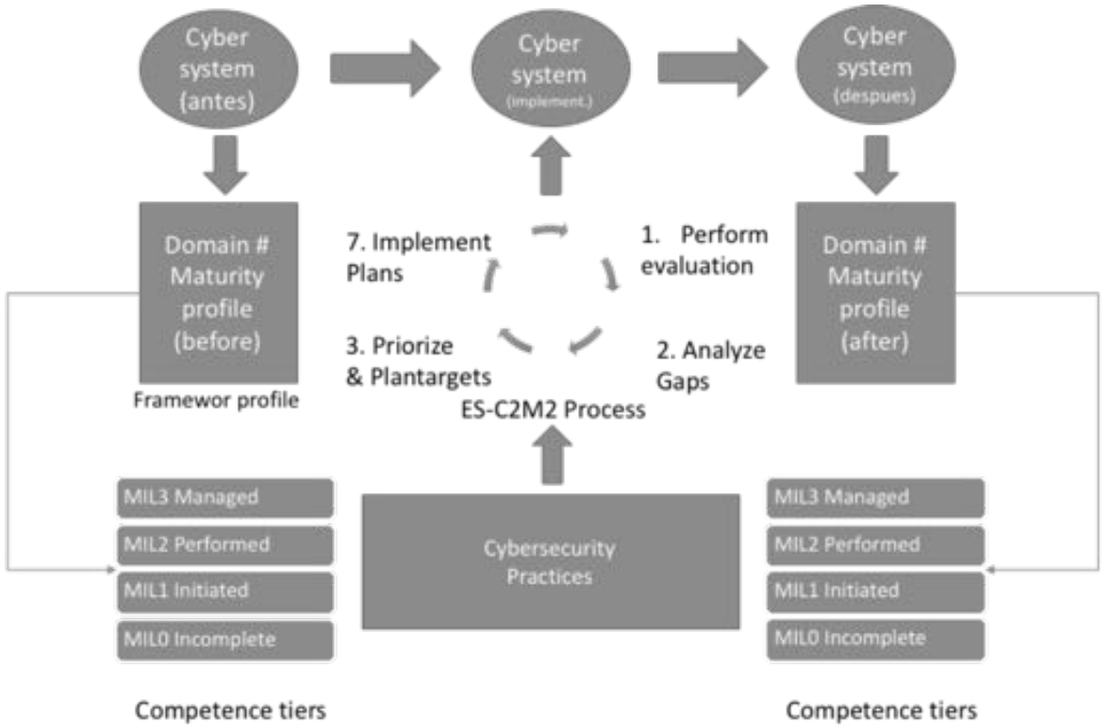
- ES-C2M2 se construye sobre un conjunto de prácticas de ciberseguridad que incorporen las normas existentes, pautas y mejores prácticas.
- Las prácticas de ciberseguridad de ES-C2M2 se organizan en diez dominios.
- Los dominios de ES-C2M2 pueden evaluarse en uno de los cuatro niveles de madurez diferentes: cero, uno, dos o tres.
- Las métricas de dominio ES-C2M2 ya están asignadas a su nivel de madurez correspondiente.
- El proceso de ES-C2M2 consta de cuatro pasos. 1) realizar la evaluación. 2) analizar brechas identificadas. 3) priorizar y planificar. Y 4) implementar planes.
- ES-C2M2 es un proceso de mejoramiento continuo.
- Es-C2M2 no se aplica a las centrales nucleares que están reguladas por separado por la Comisión reguladora nuclear.



*Original figure made by Richard White

Aplicación ES-C2M2

- Realizar la evaluación. Hemos evaluado en nivel madurez de dominio 2.
- Existe un diagrama de todos los componentes de las plantas generadoras y cómo están interconectados.
- ¿cómo evaluar el nivel de madurez de la planta con respecto al objetivo 2,1 del dominio?



*Original figure made by Richard White

Aplicación ES-C2M2

- ¿cómo evaluar el nivel de madurez de la planta con respecto al objetivo 2,1 del dominio?.

  Recuerde:
  Existe un diagrama de todos los componentes de las plantas generadoras y cómo están interconectados.
  Respuesta: Nivel 0

  Recuerde: debe satisfacer todas las criterios dentro de un dominio con el fin de ser evaluados a ese nivel de madurez.

Domain-Specific Objectives and Practices

1. Manage Asset Inventory

MIL1	a.	There is an inventory of OT and IT assets that are important to the delivery of the function
	b.	There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, historian, state estimations)
MIL2	c.	Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, Service Level Agreements and conformance of assets to relevant industry standards)
	d.	Inventoried assets are prioritized based on their importance to the delivery of the function
MIL3	e.	The asset inventory is current (as defined by the organization) for assets of defined categories
	f.	There is an inventory for all connected OT and IT assets related to the delivery of the function

2. Manage Asset Configuration

MIL1	a.	Configuration baselines are established for inventoried assets where it is desirable to ensure that multiple assets are configured similarly
	b.	Configuration baselines are used to configure assets at deployment
MIL2	c.	The design of configuration baselines includes cybersecurity objectives
MIL3	d.	Configuration of assets are monitored for consistency with baselines throughout the assets' lifecycle
	e.	Configuration baselines are routinely reviewed and updated

Aplicación ES-C2M2

- Dominio 2,2, Administrar la configuración de activos

Domain-Specific Objectives and Practices

1. Manage Asset Inventory

MIL1	a.	There is an inventory of OT and IT assets that are important to the delivery of the function
	b.	There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, historian, state estimations)
MIL2	c.	Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, Service Level Agreements and conformance of assets to relevant industry standards)
	d.	Inventoried assets are prioritized based on their importance to the delivery of the function
MIL3	e.	The asset inventory is current (as defined by the organization) for assets of defined categories
	f.	There is an inventory for all connected OT and IT assets related to the delivery of the function

2. Manage Asset Configuration

MIL1	a.	Configuration baselines are established for inventoried assets where it is desirable to ensure that multiple assets are configured similarly
	b.	Configuration baselines are used to configure assets at deployment
MIL2	c.	The design of configuration baselines includes cybersecurity objectives
MIL3	d.	Configuration of assets are monitored for consistency with baselines throughout the assets' lifecycle
	e.	Configuration baselines are routinely reviewed and updated

Aplicación ES-C2M2

- Dominio 2,2, Administrar la configuración de activo.
- Su taller de mantenimiento de Planta mantiene una base de datos de configuración de cada pieza de equipo operacional. Esta base de datos es consultada cada vez que se mantiene o reemplaza una parte de equipos.
- ¿Cómo evaluar el nivel de madurez de las plantas con respecto al objetivo 2,2 del dominio?

2. Manage Asset Configuration

MIL1	a.	Configuration baselines are established for inventoried assets where it is desirable to ensure that multiple assets are configured similarly
	b.	Configuration baselines are used to configure assets at deployment
MIL2	c.	The design of configuration baselines includes cybersecurity objectives
MIL3	d.	Configuration of assets are monitored for consistency with baselines throughout the assets' lifecycle
	e.	Configuration baselines are routinely reviewed and updated

Diferencias ambos modelos

Principal diferencia

- El marco de ciberseguridad del NIST puede considerarse más flexible, puede aplicarse a cualquier infraestructura, mientras que ES-C2M2 puede considerarse más fácil de usar, sus niveles de capacidad están predefinidos.

Niveles de madurez

Cybersecurity Framework Tiers	ES-C2M2 Maturity Indicator Levels (MILs)
	0 – Incomplete
1 – Partial	1 – Initiated
2 – Risk Informed	2 – Performed
3 – Repeatable	3 – Managed
4 – Adaptive	

https://ciprock.wordpress.com/comparing-the-nist-cyber-security-framework-and-es-c2m2/

Niveles de madurez

- NIST CSF puede ser más preciso al ser comparado con los niveles de madurez en el ES-C2M2.
- NIST CSF es mucho menos formal y sólo incluye una discusión general en la sección 2.2, no tiene el nivel de detalle que se encuentra en ES-C2M2.

Cybersecurity Framework Tiers	ES-C2M2 Maturity Indicator Levels (MILs)
	0 – Incomplete
1 – Partial	1 – Initiated
2 – Risk Informed	2 – Performed
3 – Repeatable	3 – Managed
4 – Adaptive	

https://ciprock.wordpress.com/comparing-the-nist-cyber-security-framework-and-es-c2m2/

Funciones y categorías

- En NIST CSF cada categoría es un conjunto de subcategorías que representan los resultados esperados específicos.
- Esto puede hacer que NIST CSF puede sea más complejo comparado con el diseño ES- C2M2.

Cybersecurity Framework Tiers	ES-C2M2
Function	Domain
Category	Objectives
Subcategory	Practices

https://ciprock.wordpress.com/comparing-the-nist-cyber-security-framework-and-es-c2m2/

Conclusiones

- NIST CSF es más flexible, pero no desprecie otras metodologías.
- No hay seguridad absoluta, toda la seguridad conlleva riesgo.
- La gestión de riesgo es parte integral de los dos modelos de ciberseguridad.
- La gestión del riesgo es el proceso de selección y priorización de las contramedidas basado en el análisis costo-beneficio.

Conclusiones

- ¿Cuál será el plan de infraestructura crítica que implementará el gobierno?
- ¿Lo someterán a consulta pública?.
- ¿Cuáles serán las áreas prioritarias?
- El Department of Homeland Security (DHS) tiene la responsabilidad de proteger el ciberespacio de Estados Unidos, pero el DoD está dispuesto a prestar apoyo cuando lo indique el Presidente.
- ¿Cómo operarán los CSIRT sectoriales?
- ¿Las infraestructiras críticas responderán a un CSIRT sectorial civil o militar?

Enlaces

- NIST CyberSecurity Framework https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf
- Presidential Policy Directive – 21 https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Política de ciberseguridad para infraestructuras de agua y electricidad

¡Gracias!

Juan Anabalón R.

http://www.monkeyslab.cl/jar

http://deoxyt2.livejournal.com

MonkeysLab - ISSA Chile