Ciberseguridad Estratégica aplicada al Sector Eléctrico

PNCS _ Infraestructuras Críticas de la Información

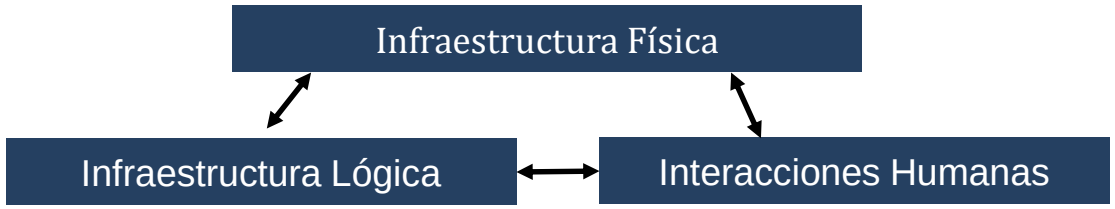
Política Nacional de Ciberseguridad (PNCS)

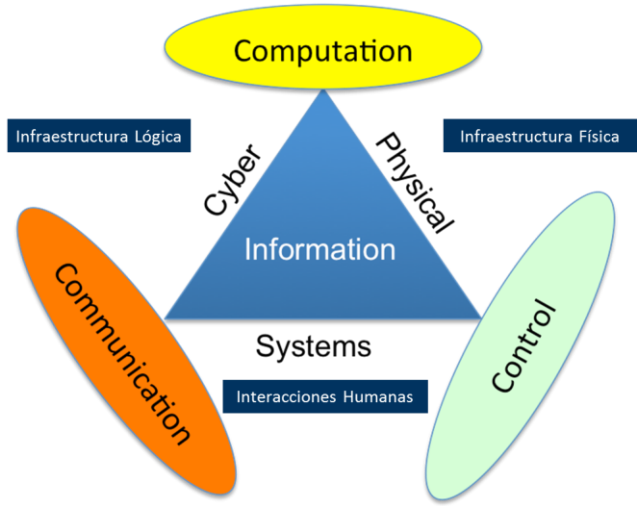
A. El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos

> 3. Identificación y jerarquización de las infraestructuras críticas de la información

Los sectores que componen la clasificación de ICI son muy similares y se repiten en varias clasificaciones a nivel internacional. En el caso chileno, mientras se adopta una política específica para infraestructuras críticas, la infraestructura de la información de los siguientes sectores será considerada como crítica: **energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa**, entre otras.

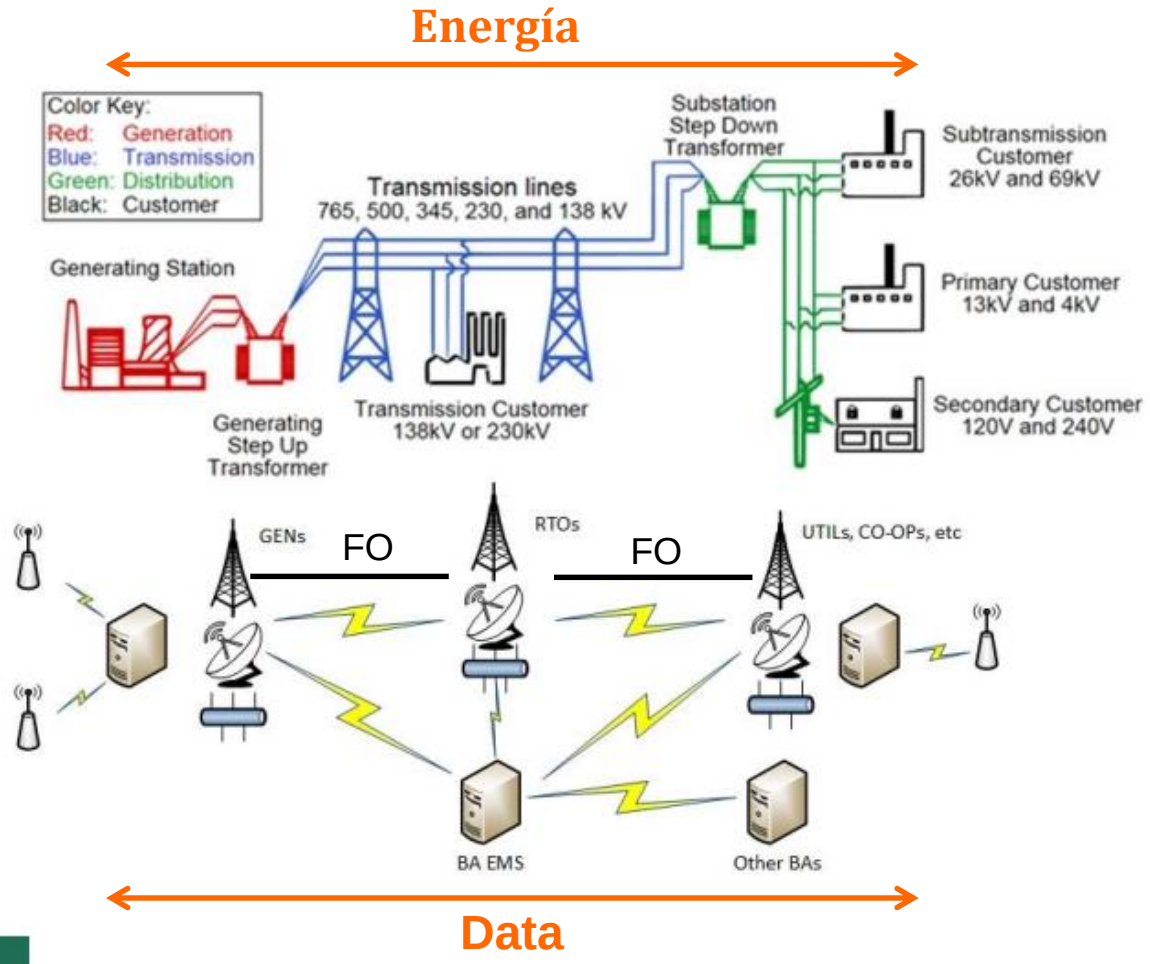
CIBERESPACIO





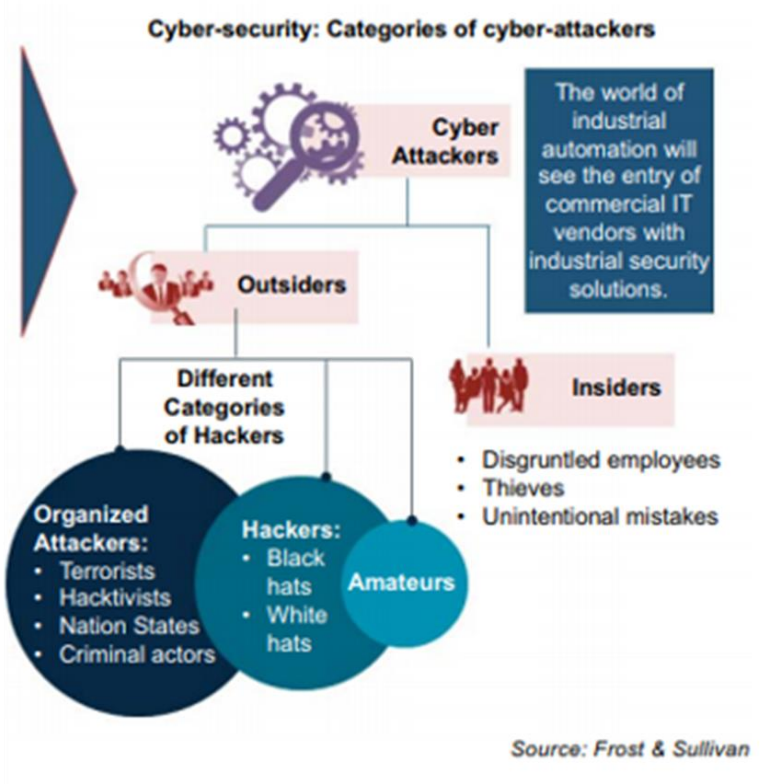
"Los Sistemas de Control Industrial Tradicionales evolucionan a un Cyber Physical System (CPS)"

Activos Críticos del Sector Eléctrico _ Energía + Data



Causa Raíz de Ciberataques

	DINERO	PODER	SUBVERSIÓN
Ej:	Cyber *Espionaje Industrial*	*Sabotaje Informático*	*Hacktivismo – CyberTerrrorrismo*



Desafío _ Redes Inteligentes Seguras

Los sistemas de control industrial fueron desarrollados sin pensar en la seguridad

Ciberseguridad Embebida por Diseño

Grid Modernization

Electric Vehicles

Advanced Metering

Distributed Generation

Distribution Automation

NIST

NIST 800-82 (Industrial)

EPRI ELECTRIC POWER RESEARCH INSTITUTE

NIST Inter-Agency Report (NISTIR) 7628 (Smart Grid)

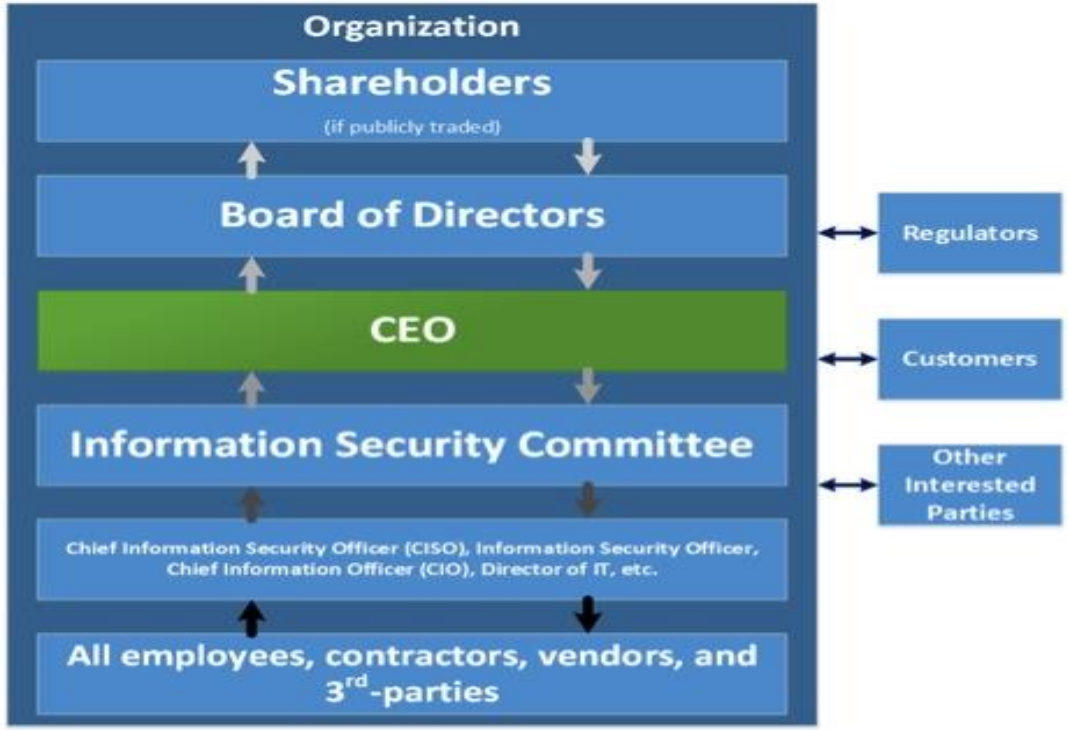
SANS INSTITUTE

ISO

NERC CIP NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

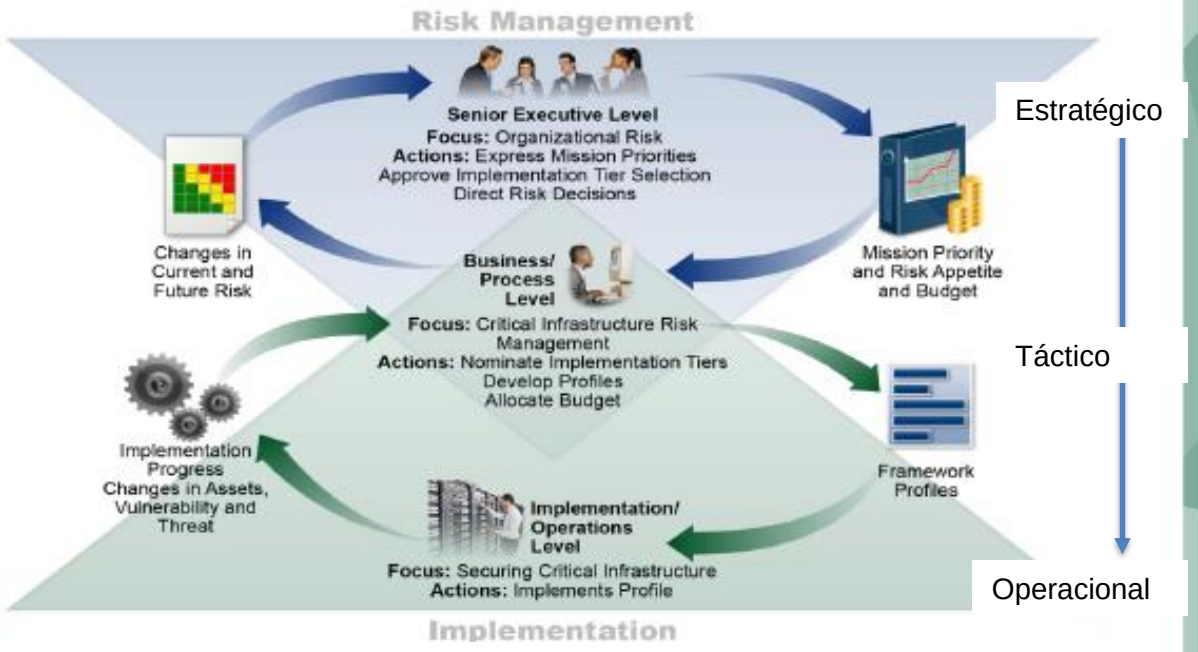
ISA/IEC 62443

Ciberseguridad _ Visión Estratégica en 360°



Ciberseguridad Estratégica

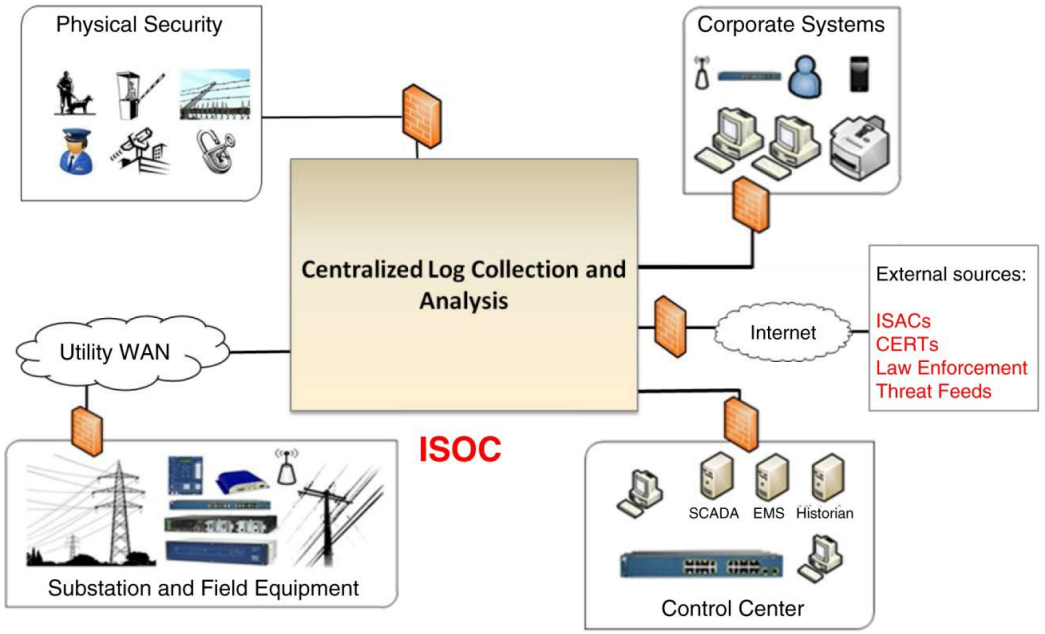
Legal – Normativo – Política interna – Organizacional – Management – Tecnológico – Partners – Procesos – Personas



Evolución _ Centros de Operaciones de Seguridad Integrados

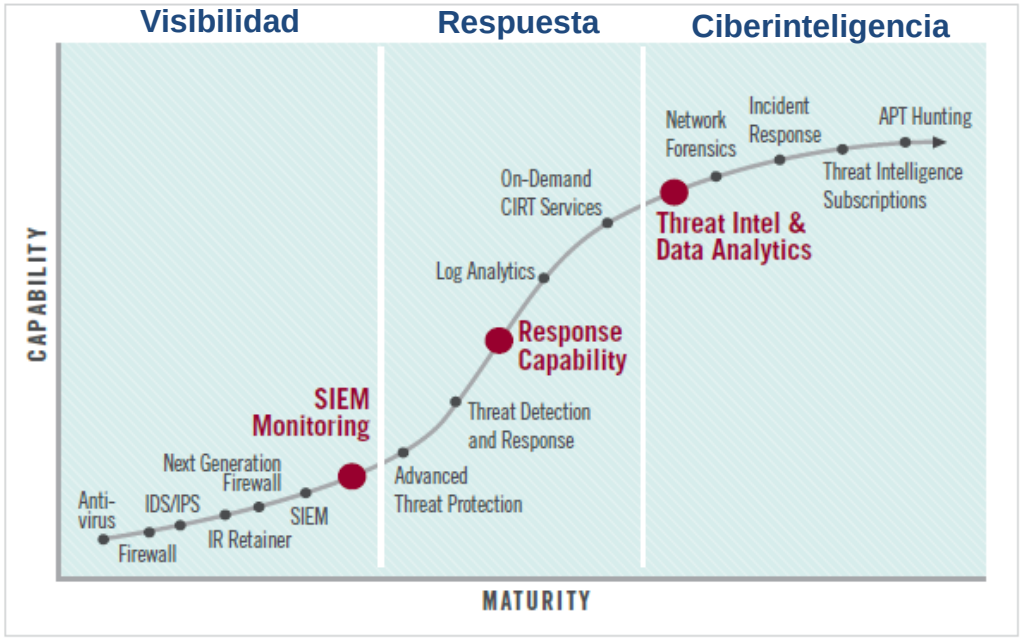
Guidelines for Planning an Integrated Security Operations Center

EPRI ELECTRIC POWER RESEARCH INSTITUTE

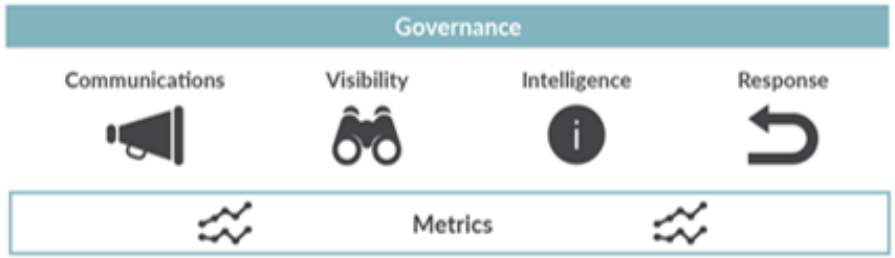


ISOC integra la supervisión de seguridad de múltiples dominios dentro de una Utility, incluidos sistemas de TI corporativos, sistemas de entrega de energía, sistemas de generación y seguridad física. El ISOC también incluye información de vulnerabilidad y amenazas de fuentes externas, tales como: Information Sharing and Analysis Centers (ISAC), Computer Emergency Readiness Teams (CERT) y organismos encargados de hacer cumplir la ley.

Cyber Defense Program Development Model



Six Core Capabilities to Attack the Security Gap™



Eduardo Morales Cabello
ecmorales@entel.cl

Santiago, Chile
Agosto 2018