



**Charla Nro. 1**

**Jueves 29 de marzo de 2018**

**10:30-11:15**

**Sala 1**

**Ciberseguridad industrial en  
la distribución de energía  
eléctrica**

Licencia Creative Commons  
Atribución – No Comercial –  
Compartir Igual (by-nc-sa)  
Attribution-NonCommercial-  
ShareAlike 4.0 International



Fuerza Aérea Argentina

UNDEF – Instituto Universitario Aeronáutico – Facultad de Ingeniería  
Carrera de Posgrado “Especialización en Seguridad Informática”

## **Ciberseguridad industrial en la distribución de energía eléctrica**

Autor: Walter Ernesto Heffel

Tutor: Samuel Linares. Director de la Especialización: Eduardo Casanovas

**Presentación adaptada y actualizada a marzo 2018**

# Propuesta de Trabajo Final Integrador (TFI)

## **Objetivos:**

Definir la CSI, describir particularidades en la Distribución, establecer relaciones, analizar el estado del arte, identificar debilidades, proponer recomendaciones, reflexionar, concluir. Realidad argentina. Fuentes públicas

## **Alcances:**

Infraestructuras críticas, SCI/SCADA, medidores inteligentes. Abordaje holístico, multifactorial y multidisciplinario. Referencias extranjeras

## **Metodología:**

Descriptiva. Recopilación y ordenamiento, elaboración, conclusiones

## **Destinatarios:**

Auditorio amplio y general. Documento de posición, análisis y difusión

# Introducción

## Revoluciones industriales:

- **Primera:** Uso del vapor de agua y aplicaciones de la presión
- **Segunda:** Combustible líquido derivado del petróleo
- **Tercera:** Mecánica, electrificación masiva. Sociedad del conocimiento: inteligencia, ciencia y tecnología. Controlador Lógico Programable (1969) Modicon 084
- **Cuarta:** Sistemas ciberfísicos. Industria 4.0

Rol de la electricidad en la vida moderna. Generación y Transporte

Luz, calor, magnetismo. Distribución. Servicio Público. Dependencias

Innovación, automatización. Nuevos riesgos, inseguridad, ataques

# 1. Definiciones. Ciber. Seguridad

## Prefijo **CIBER**:

- Griego: *kibernes, kibernetikós, kibernetiké*. Inglés: *cybernetics*
- Francés: *cybernétique*. Español: cibernético
- Libro: “*Cibernética o el control y comunicación en animales y máquinas*” Wiener, 1948

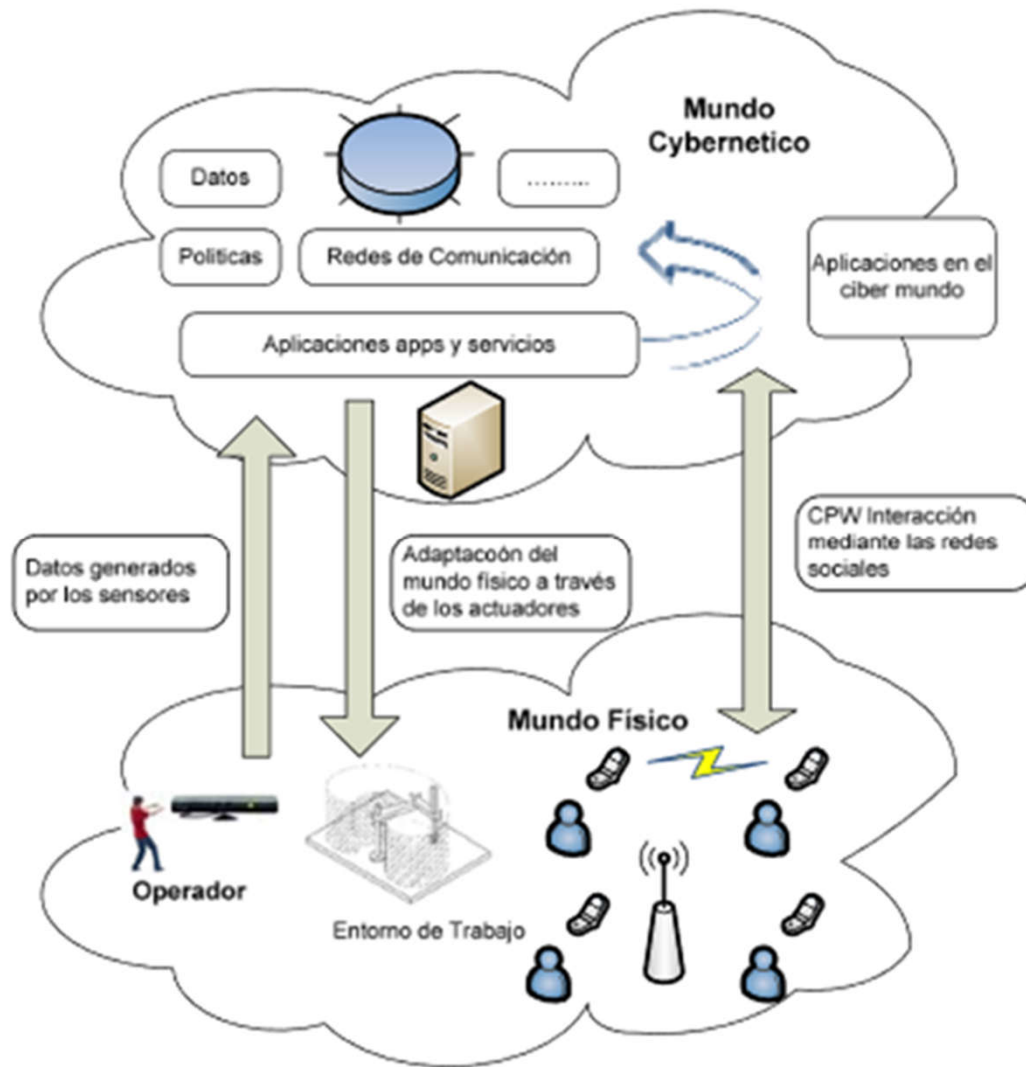
## **Seguridad**: significado, dimensiones, ambigüedades y traducciones

- Seguridad multidimensional (Organización de Estados Americanos)
- *Safety* : aspectos relacionados con integridad física y salud de una persona
- *Security* : prevención de ataques, sabotajes, daños o robos perpetrados sobre equipamiento

## **Ciber + seguridad**. Significado según ITU, CARI y ETH

**Industria**. Particularidades. Maquifectura. Automatización. Interfaces Hombre – Máquina / Máquina – Máquina

# 1. Definiciones

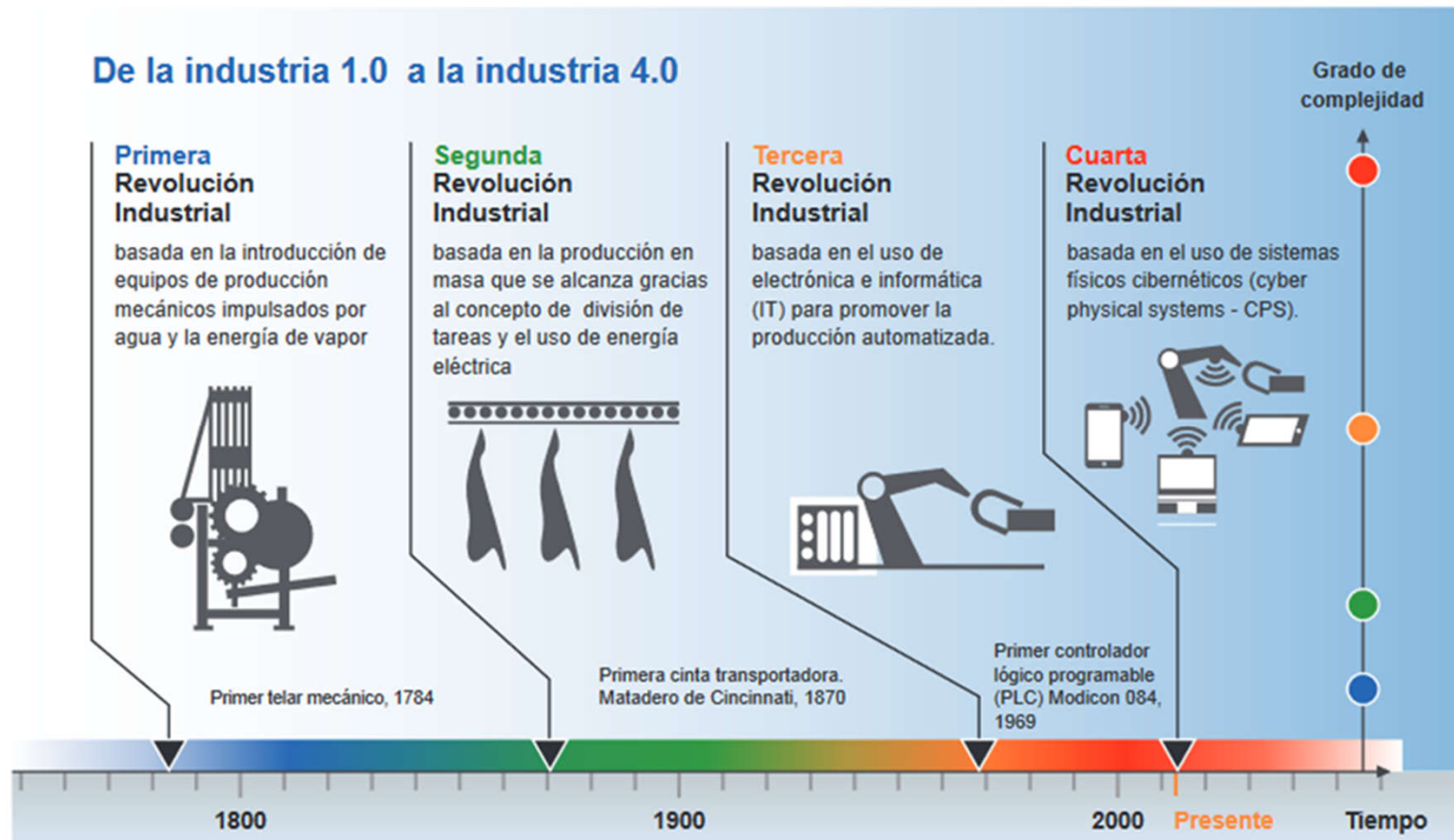


Relación entre lo  
ciber y lo físico,  
convergencia  
genérica

# 1. Definiciones. Convergencia ciber-física



# 1. Definiciones. Evolución de la Industria





# 1. Definiciones. Ciberseguridad Industrial

**CCI:** Conjunto de prácticas, procesos y tecnologías, diseñados para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales, utilizando las perspectivas de personas, procesos y tecnologías.

**WisePlant:** Se ocupa de analizar los riesgos y vulnerabilidades que integran los entornos industriales y de manufactura, y determinar acciones que se van a implementar para mitigar estos riesgos. Los SC están basados en computadoras para controlar y supervisar procesos sensibles y funciones físicas. El término Sistema de Control se refiere en forma genérica al conjunto de hardware, firmware, comunicaciones y software encargado de supervisar y controlar las funciones vitales de las infraestructuras físicas.

## 2. Infraestructuras Críticas. Definiciones

Raíces de “Infraestructura”: Infra (debajo) + Structura (viga, base).

Es aquello situado en la capa más baja posible.

Conjunto de estructuras de ingeniería e instalaciones, generalmente de larga vida útil, que constituyen la base sobre la cual se produce la prestación de servicios considerados necesarios para el desarrollo de fines productivos, personales, políticos y sociales.

España: Las infraestructuras estratégicas (es decir, aquellas que proporcionan servicios esenciales) cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. (Centro Nacional de Protección para I.C.).

## 2. Infraestructuras Críticas. Rol del Estado

“La salud, riqueza y seguridad de la Nación dependen de la producción y distribución de determinados bienes y servicios. El conjunto de los activos físicos, funciones y sistemas a través del cual se mueven estos bienes y servicios se denominan infraestructuras críticas”. (John D. Moteff)

Argentina: En 2011 se creó el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) que introduce la noción de Infraestructura Crítica, aunque no define explícitamente a la Ciberseguridad. “Solamente el Estado está en condiciones de tener un enfoque global que tome en cuenta las interdependencias y las externalidades de seguridad”. (Eduardo A. Thill)

**Decreto 577 (28/07/2017). Creación del Comité de Ciberseguridad. Ministerios de Defensa, Seguridad y Modernización**

## 2. Infraestructuras Críticas. Enumeración

Según CNPIC, de España, agrupa a 12 sectores:

Administración

Agua

Alimentación

**Energía**

Espacio

Industria Química

Industria Nuclear

Instalaciones de Investigación

Salud

Sistema Financiero y Tributario


Tecnologías de la Información y las Comunicaciones (TIC)

Transporte

## 2. Infraestructuras Críticas

**Lista de 12 sectores y 35 productos y servicios. (2004). Holanda.**

**Sistemas electorales (EEUU – 2016)**

Sector	Producto o servicio
I Energía 	1 Electricidad
	2 Gas Natural
	3 Petróleo
II Telecomunicaciones	4 Provisión de infraestructura fija
	5 Provisión de infraestructura móvil
	6 Comunicación y navegación por radio
	7 Comunicaciones satelitales
	8 Radiodifusión (broadcasting)
	9 Acceso a Internet
	10 Servicios postales y de mensajería
III Agua potable	11 Provisión de agua potable

## 2. Infraestructuras Críticas. Protección

**Los acueductos romanos y una hipótesis sobre la caída del Imperio**

**Escenarios:** Tierra, agua, aire, espacio, **ciberespacio “el quinto dominio”**

### **Objetivos de la protección:**

- Garantizar la continuidad del servicio prestado
- Implementar medidas para la prevención de fallas y ataques
- Ante un incidente, dar respuesta para lograr la rápida restitución del servicio

### **Vulnerabilidades:**

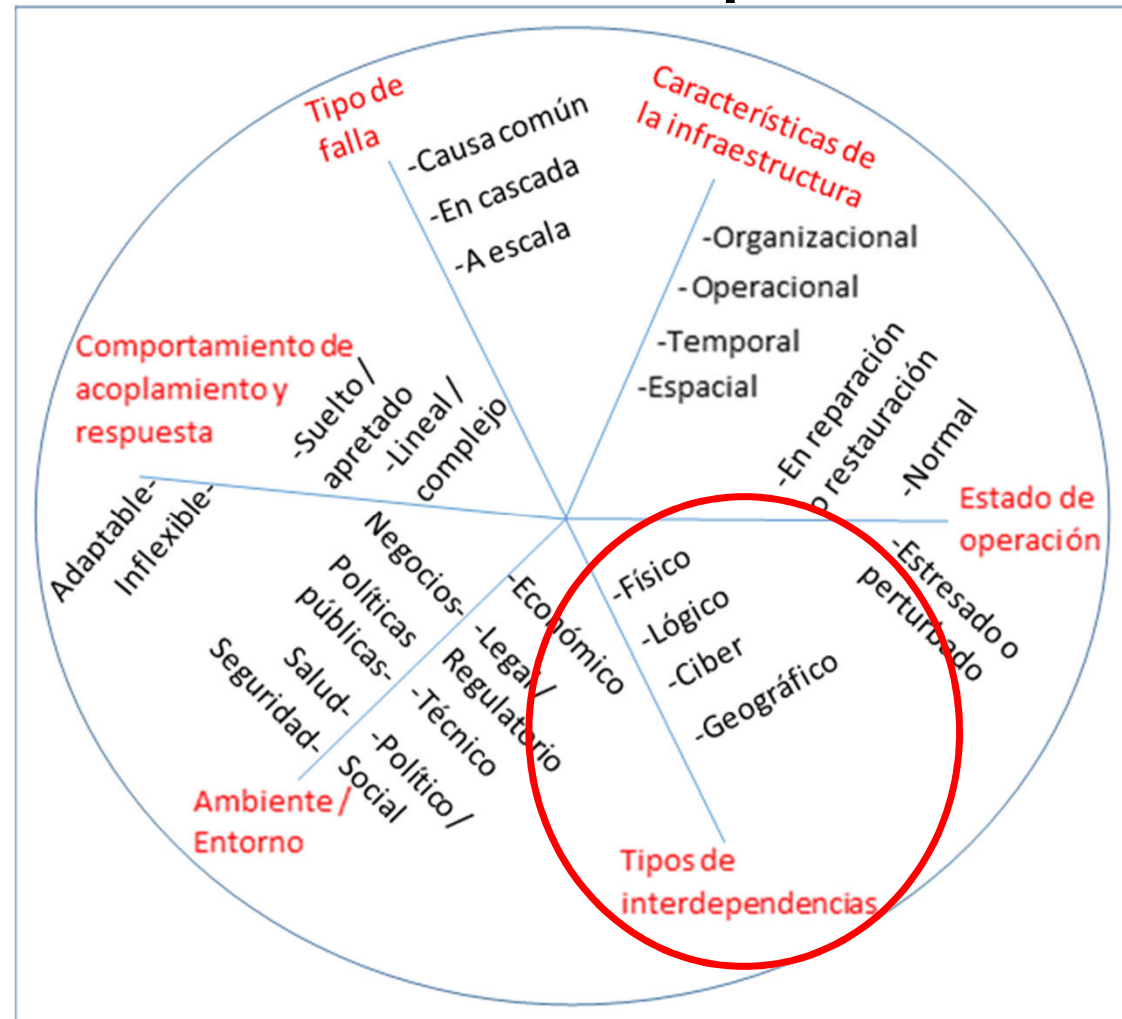
Toda infraestructura crítica es una entidad susceptible de ser golpeada, rota, deteriorada, aislada, quemada, inundada o afectada de cualquier forma para que no cumpla su función principal

### **Interdependencias:**

- Son las relaciones de dependencia recíproca entre dos personas o cosas

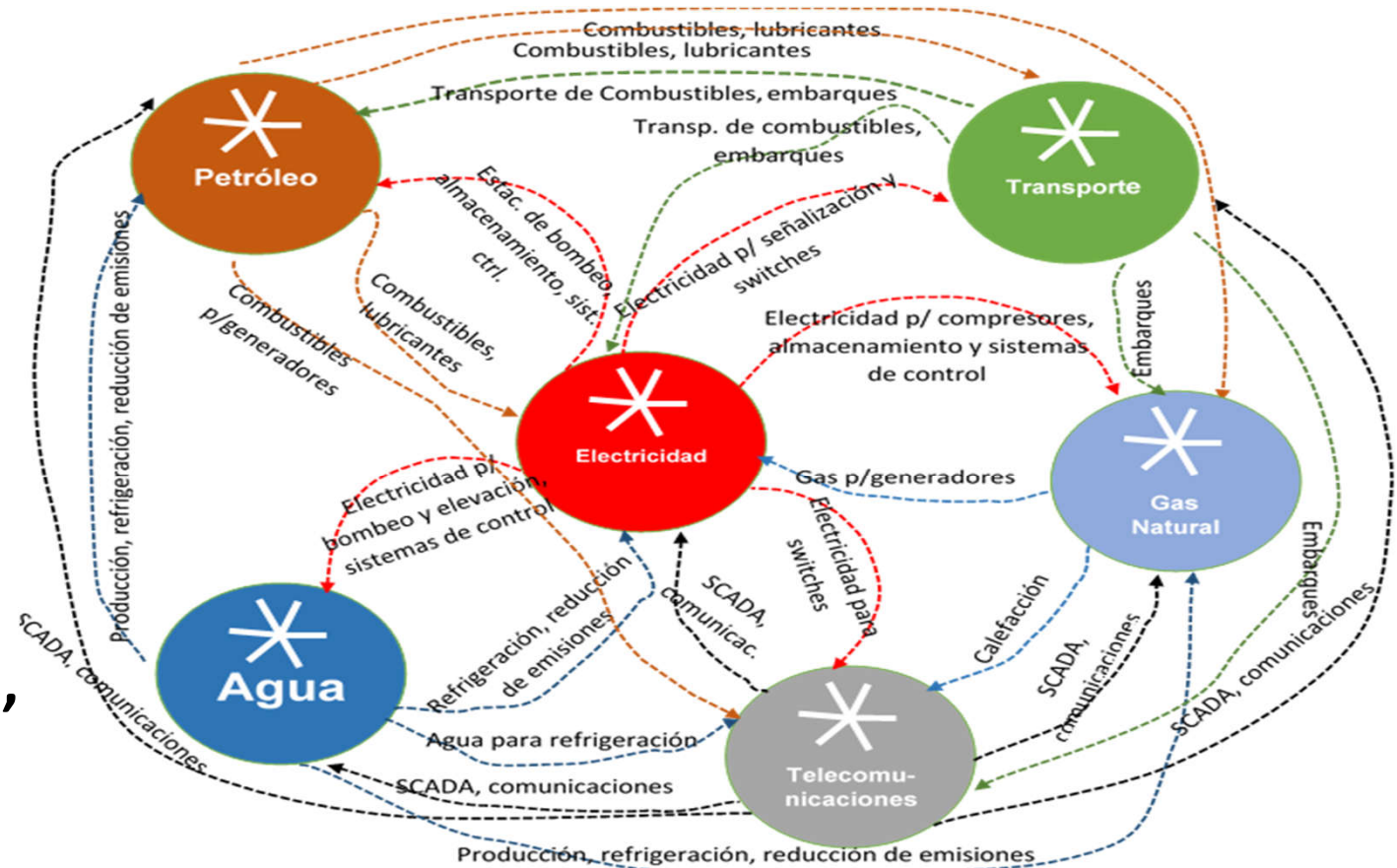
## 2. Infraestructuras Críticas. Interdependencias

**Seis dimensiones para describir interdependencias entre infraestructuras.**  
**El foco está puesto en los Tipos.**



## 2. Infraestructuras Críticas. Interdependencias

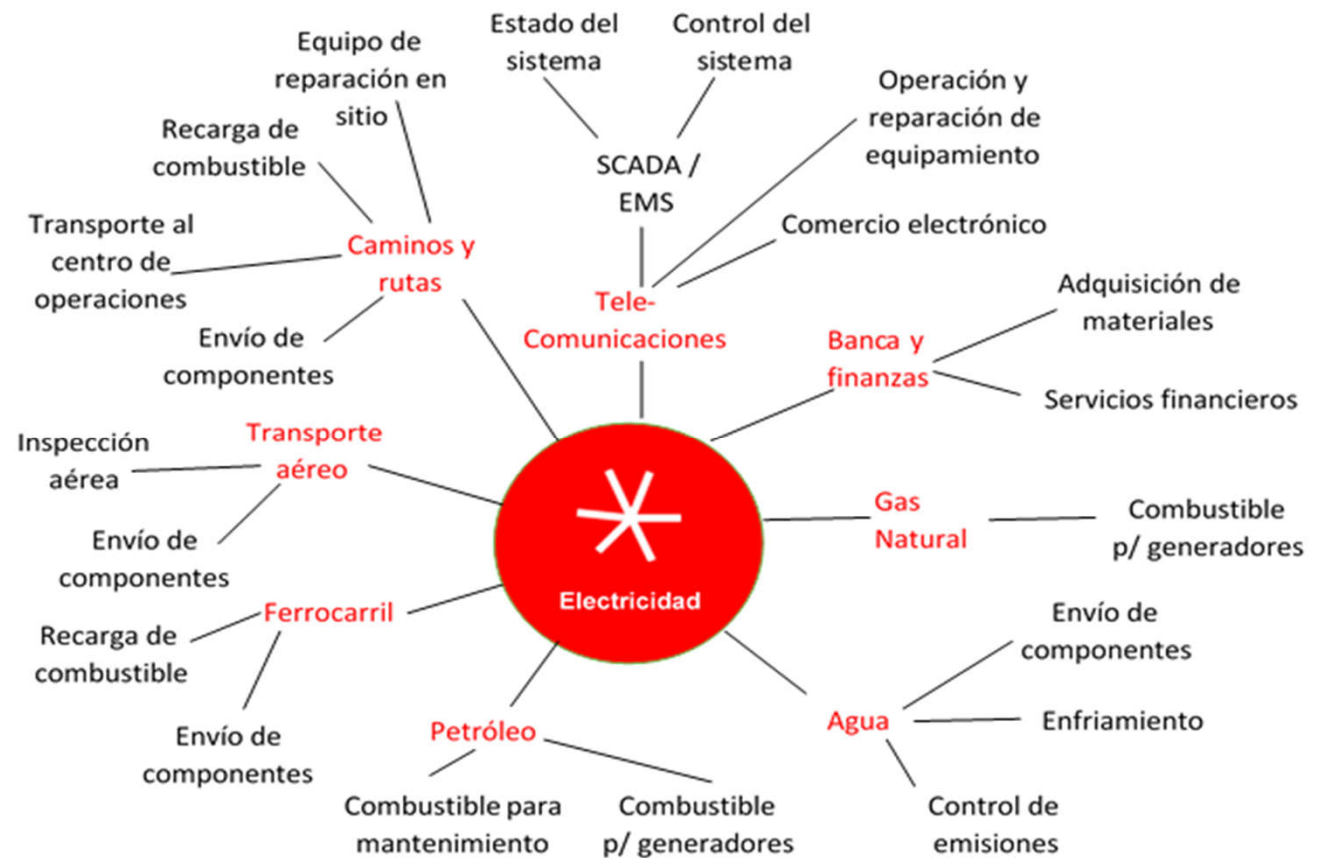
Ejemplos de interdependencias, centradas en la electricidad





## 2. Infraestructuras Críticas. Interdependencias

**Ejemplos de infraestructuras que dependen del servicio eléctrico**



# 3. Sistema Eléctrico en Argentina

Electricidad: *eléktron*, ámbar, estática

Primeras aplicaciones: Iluminación de calles y casas (Siglo XIX)

**Modelo argentino, breve historia reciente:**

- Régimen de energía eléctrica, 1960. Deficiencias:
  - Fallas en el planeamiento estratégico
  - Politización de la gestión empresarial
  - Inexistencia de mínimos mantenimientos
  - Crisis de abastecimiento 1988/89
  - Ausencia del concepto costo - precio
- Privatizaciones, 1990. Separación de actividades: GENERAC., TRANSP. y DISTRIB.
- Libre competencia en GENERACION. Monopolios regulados en TRANSP. y DISTRIB.
- Entes Reguladores autárquicos, algunos intervenidos políticamente
- Algunas re-estatizaciones a partir de 2005

### 3. Sistema Eléctrico en Argentina. Actores

**Actores principales  
del sistema  
eléctrico argentino**



# 3. Sistema Eléctrico en Argentina. Actores

## **Generadoras:**

- Transforman energía térmica, solar, hidráulica, eólica, etc. en electricidad
- Es una actividad de interés público, sujeta a competencia
- Hay 46 instalaciones fijas en el territorio. Ninguna puede superar el 15 % de la capacidad total del sistema (unos 33 000 MW a diciembre de 2015)

## **Transportistas:**

- Trasladan el fluido por cables, desde la fuente de generación hasta redes locales
- Hay dos sistemas: Extra alta tensión (500 kV.) y Troncal (132/220/330 kV.)
- El 95 % de las líneas son (28 000 Kms.) son operadas por la firma Transener

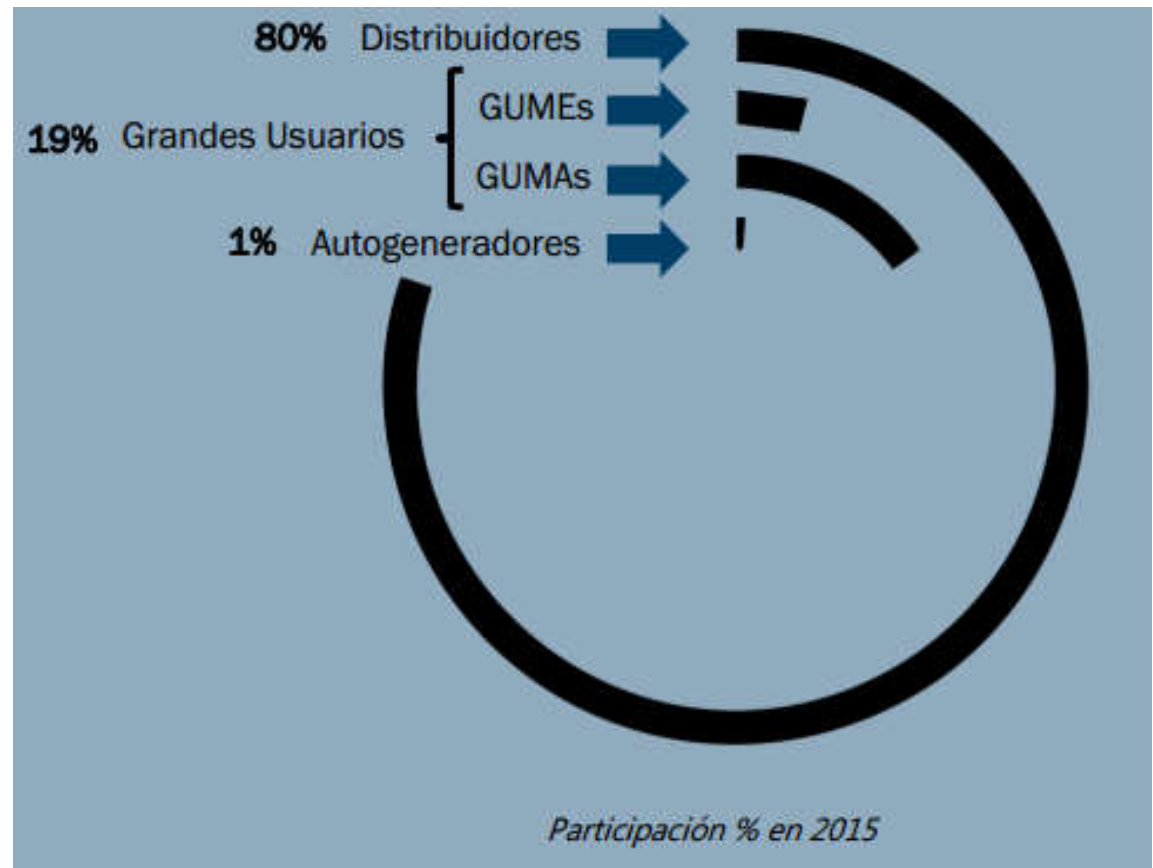
## **Distribuidoras:**

- Entregan la electricidad en el punto final de la cadena, el usuario-cliente
- A diciembre de 2012 se estimaban 16.500.000 acometidas y 36.000.000 de personas
- Hay 47 empresas en el territorio nacional, agrupadas en ADEERA

### 3. Sistema Eléctrico en Argentina. Actores

**Grandes usuarios  
(Mayores y Menores). Son  
industrias que demandan  
grandes volúmenes y  
pueden contratar  
suministro sin pasar por  
una Distribuidora. Son 69  
empresas**

Composición de la demanda anual  
2015 por tipo de agente MEM



# 3. Sistema Eléctrico en Argentina. Actores

**Consumidores residenciales. CAMMESA los agrupa en 4 categorías**

**Otros actores:**

- CFEE. Consejo Federal de la Energía Eléctrica
- Fundelec. Fundación para el Desarrollo Eléctrico
- FACE. Federación Argentina de Cooperativas Eléctricas
- Insituto Argentino de la Energía “General Mosconi”
- CACIER. Comité Argentino de la Comisión de Integración Energética Regional
- AEA. Asociación Electrotécnica Argentina

**Pasado, presente y futuro de la electricidad como servicio**

## 4. Tecnologías de Información y de Operación

**TI:** Refiere a almacenar, proteger, recuperar y procesar datos electrónicamente, usando computadoras y equipos de telecomunicaciones, generalmente asociadas a negocios y empresas, aunque sin ser exclusivas

**TO:** Representan a las Tecnologías de Operación propias del ámbito industrial, y pueden definirse desde dos perspectivas complementarias:

- Tradicional: Integran información, interoperabilidad y conectividad como principales características para operar sobre el mundo físico
- **Inteligente o *smart*: Cuando son aplicadas a la automatización, al control y a la operación de los procesos productivos característicos del ambiente industrial**

## 4. Tecnologías de Información y de Operación

### Comparación entre factores de TI y TO

	Tecnologías de la Información	Tecnologías de Operación
<b>Duración de los ciclos de cambio</b>	Entre 3 y 5 años	Entre 10 y 20 años
<b>Madurez</b>	Alta. Conocimiento extendido y consolidado	Baja. Escasa conciencia de las necesidades
<b>Arquitecturas y protocolos</b>	Estandarizados	Ad hoc, a medida, sin estandarizar Sistemas heredados ( <i>legacy</i> )
<b>Prioridades en Seguridad de la Información</b>	1° Confidencialidad 2° Integridad 3° Disponibilidad	1° Disponibilidad 2° Integridad 3° Confidencialidad



# 4. Tecnologías de Información y de Operación

## **Fuentes de desacoples entre TI y TO:**

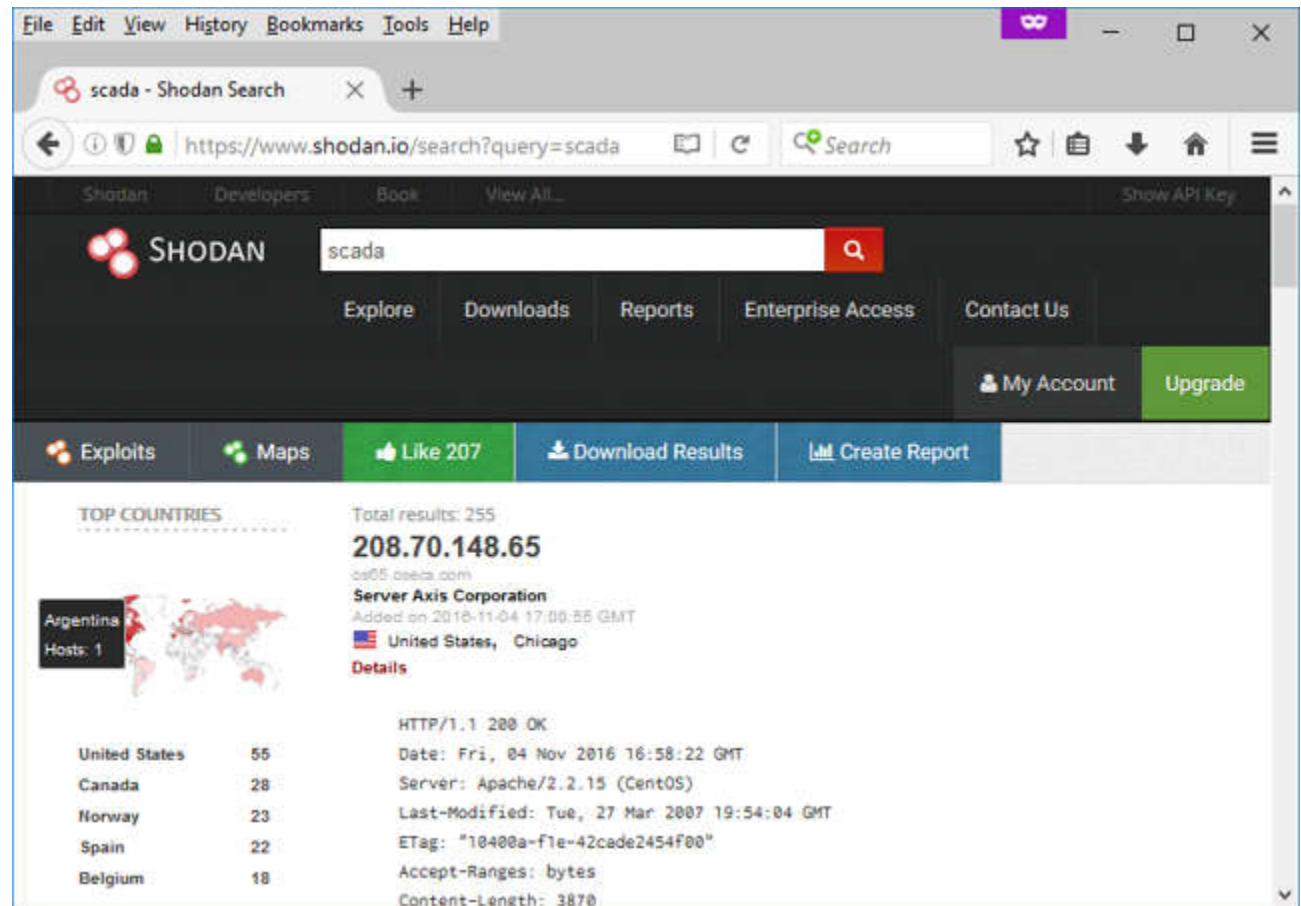
- Administración de ambos terrenos como si fueran compartimentos estancos
- Falta de atención hacia los canales de comunicación entre uno y otro dominio
- Asunción de que los puntos donde los SCI y los sistemas corporativos se contactan son, literalmente, tierra de nadie. Esto da lugar a la teoría de los “agujeros o brechas de aire” (*airgaps*)

## **Estado de situación actual:**

- Incremento de ataques dirigidos a sistemas corporativos y basados en malware
- Creciente nivel de interconexión entre a) sistemas de control y automatización industrial y b) redes corporativas
- Existencia de herramientas para búsqueda en línea. Protagonismo del factor H

# 4. Tecnologías de Información y de Operación

Shodan en acción, búsqueda de la palabra “scada”



The screenshot shows the Shodan search engine interface in a web browser. The search query is 'scada', and the results show a total of 255 results. The top result is for the IP address 208.70.148.65, which is associated with the domain os65.osaca.com and the server Axis Corporation. The server was added on 2016-11-04 17:00:55 GMT and is located in the United States, Chicago. The interface also displays a 'TOP COUNTRIES' section with a world map and a table of results by country.

Country	Count
United States	55
Canada	28
Norway	23
Spain	22
Belgium	18

Additional details for the top result include: HTTP/1.1 200 OK, Date: Fri, 04 Nov 2016 16:58:22 GMT, Server: Apache/2.2.15 (CentOS), Last-Modified: Tue, 27 Mar 2007 19:54:04 GMT, ETag: "10400a-f1e-42cade2454f00", Accept-Ranges: bytes, and Content-Length: 3870.

# 4. Tecnologías de Información y de Operación

## Jugadores importantes:

- **Fabricantes** de dispositivos industriales y sistemas de control
- **Integradores.** Consultoras de ingeniería especializadas en diseño, construcción, implementación y mantenimiento de las instalaciones
- **EPCs** (*Engineering, Procurement and Construction companies*), encargadas de todo el diseño de infraestructuras y procesos, compra y construcción
- **Empresas que producen hardware y software dedicado para seguridad.** Firewalls, sistemas de prevención de intrusiones, mecanismos de autenticación, etc.
- **Asociaciones de profesionales.** Organismos que aglutinan a expertos de diversas áreas
- **Entes de normalización y estandarización.** Las normas y estándares definen técnicas de manera detallada, destinadas a usos comunes y repetidos
- **Usuarios finales.** Tendría poco sentido pergeñar infraestructuras, sistemas o programas informáticos sin el factor humano que los maneje
- **El Estado.** Su influencia alcanza sobre todo a los servicios públicos e infraestructuras críticas, tanto por acción como por omisión

## 4. Buenas prácticas, Normas y Estándares

Se consideran las 4 más relevantes para las temáticas de este Trabajo:

- **ISA 99 (Devenida ISA/IEC-62443 a partir de 2010)**
- **ISO/IEC 27001 y 27002**
- **Serie 800 de NIST**
- **NERC**

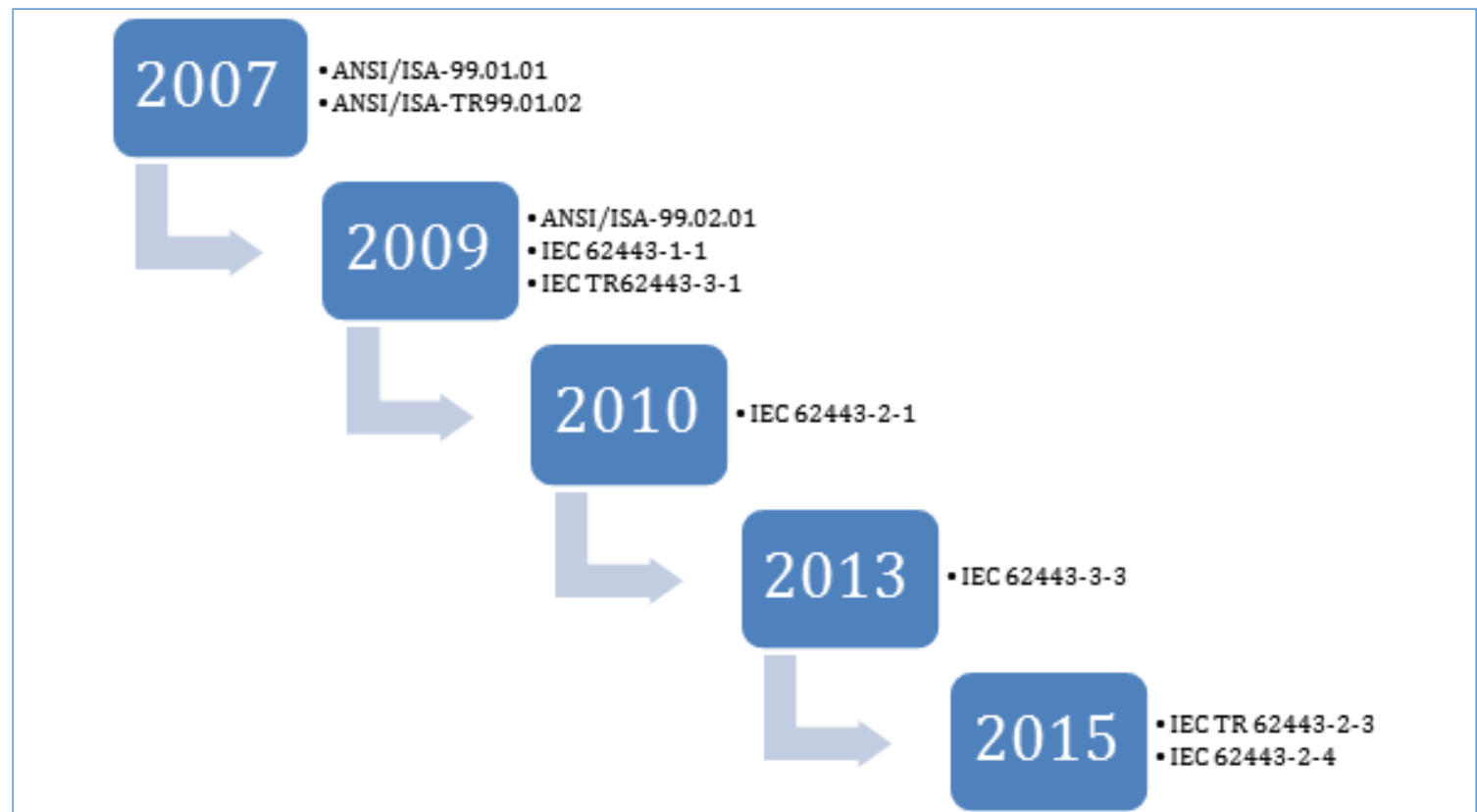
**ISA 99:** Consta de 5 partes o categorías bien diferenciadas, 1. General, 2. Políticas y Procedimientos, 3. Sistemas, 4. Componentes. 5. Informe Técnico, mas 1 informe técnico

Se basa en dos ideas principales: Zonas de seguridad y Conductos

**IEC-62443:** Se compone de 13 cuerpos (8 documentos + 5 informes)

## 4. Buenas prácticas, Normas y Estándares

**Publicaciones  
ISA 99 e IEC  
62443**

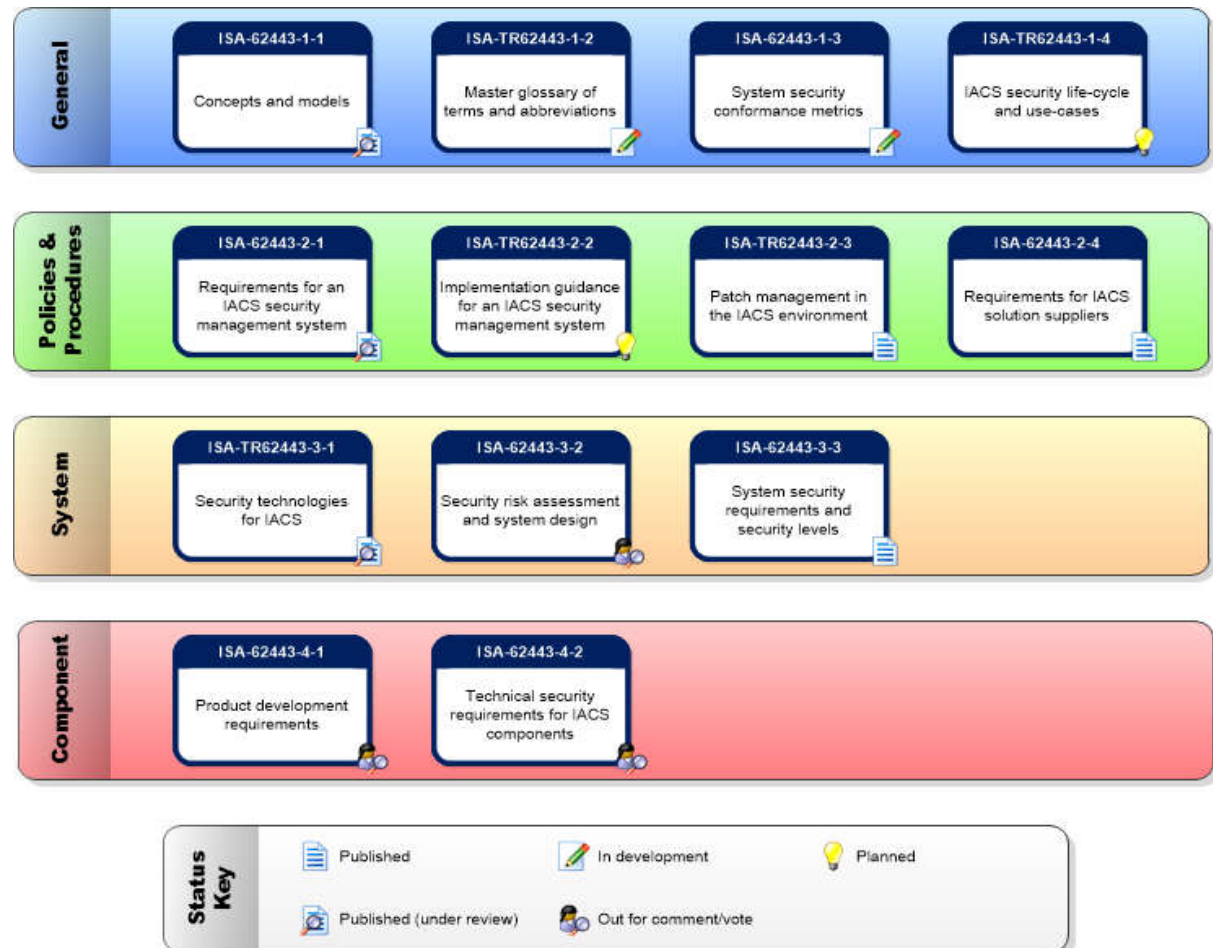


# 4. Buenas prácticas, Normas y Estándares

Estado de las publicaciones IEC 62443 a setiembre de 2015

El 15/01/2018 se publicó IEC 62443-4-1:2018. *Secure Development Life-cycle (SDL)*

[+ 2000 págs.]



# 4. Buenas prácticas, Normas y Estándares

## **ISO/IEC 27001 y 27002, Seguridad de la Información al auxilio de los SCI**

- Basadas en el ciclo de Deming, PDCA. 27001: SGSI, certificable. 27002: Código de práctica
- La organización documental abarca 5 capítulos introductorios, 14 dominios, 35 objetivos de control y 114 controles
- Capítulos preliminares: 0. Introducción, 1. Alcance, 2. Referencias normativas, 3. Términos y definiciones, 4. Estructura del estándar
- Dominios: 5. Políticas de seguridad de la información, 6. Organización de la seguridad de la información, 7. Seguridad de los recursos humanos, 8. Gestión de los activos, 9. Control de acceso, 10. Controles criptográficos, 11. Seguridad física y ambiental, 12. Seguridad de las operaciones, 13. Seguridad de las Comunicaciones, 14. Adquisición de sistemas, desarrollo y mantenimiento, 15. Relaciones con los Proveedores, 16. Gestión de Incidencias que afectan a la Seguridad de la Información, 17. Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio, 18. Conformidad con requisitos legales y contractuales

## 4. Buenas prácticas, Normas y Estándares

### Serie 800 de NIST

- *NIST Special Publication **800-53** Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.* Febrero 2014. La original contiene 17 familias de controles. *Revision 5 (Agosto 2017).*
- *NIST Special Publication **800-82** Revision 2, Guide to Industrial Control Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC).* Mayo 2015



## 4. Buenas prácticas, Normas y Estándares

### NERC CIP

- La North American Electric Reliability Corporation es una entidad con autoridad reguladora internacional sin fines de lucro cuya misión es asegurar la confiabilidad del sistema de energía a granel o mayorista en Norteamérica
- Sus 4 pilares son:
  - **Fiabilidad**, para abordar eventos y riesgos identificables
  - **Aseguramiento**, con el fin de proporcionar seguridad al público, la industria y el gobierno. para el desempeño confiable del sistema de energía
  - **Aprendizaje**, como forma de promover la mejora continua de las operaciones y adaptarse a las lecciones aprendidas del sistema de potencia
  - **Enfoque basado en el riesgo**, concentra la atención, los recursos y las acciones en los asuntos prioritarios de la operación del sistema

# 4. Buenas prácticas, Normas y Estándares

**Estándares de  
ciberseguridad  
NERC CIP  
vigentes a  
noviembre  
2016**

Reliability Standards	
Critical Infrastructure Protection	
Standard Number	Title
Subject to Enforcement (11)	
CIP-002-5.1	Cyber Security - BES Cyber System Categorization
CIP-003-6	Cyber Security - Security Management Controls
CIP-004-6	Cyber Security - Personnel & Training
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems
CIP-007-6	Cyber Security - System Security Management
CIP-008-5	Cyber Security - Incident Reporting and Response Planning
CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems
CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments
CIP-011-2	Cyber Security - Information Protection
CIP-014-2	Physical Security
Pending Regulatory Filing (1)	
CIP-002-5.1a	Cyber Security — BES Cyber System Categorization

# 5. El universo SCADA. Definiciones y partes

## Supervisory Control and Data Acquisition

### Definiciones:

- Es un mecanismo basado en computadoras que permite supervisar y controlar a distancia una instalación, proceso o sistema de características variadas
- Este tipo de sistemas permite la gestión y control de cualquier sistema local o remoto gracias a una interface gráfica que comunica al usuario con el sistema. Es el *software* que brinda acceso a datos remotos de un proceso y controla el mismo mediante las herramientas de comunicación necesarias

### Módulos componentes:

- a) Mecanismos de captación de datos y b) Herramientas de análisis. Estas últimas contienen: b1) interfaces hombre-máquina, b2) una unidad central, b3) unidades remotas y b4) un sistema de comunicaciones
- Lo más importante: operadores humanos

## 5. El universo SCADA. Controles y *hardware*

- **Noción de lazo abierto y lazo cerrado.**
- **Controladores lógicos programables (PLC)**, computadoras de propósito específico con capacidad de gestionar señales de entrada y salida, en tiempo real
- **Unidades terminales remotas (RTU)**, dispositivos basados en microprocesadores. Permiten obtener señales independientes de los procesos y enviar la información a un sitio remoto
- **Computadoras industriales**, su rendimiento es similar a equipos industriales pesados. En algunos casos pueden asumir funciones de un PLC
- **Controladores automáticos programables (PAC)**, incorporan tecnología industrial orientada al control automatizado avanzado y medición de magnitudes analógicas
- **Dispositivos electrónicos inteligentes (IED)**: Su singularidad reside en que cuentan con propiedades de decisión propia

## 5. El universo SCADA

**Comparación  
entre  
características  
de PLC, PC  
estándar y PAC**

Características	PLC	PC Estándar	PAC
Soporta shocks eléctricos y vibración	Si	No	Si
Seguridad y estabilidad	Si	No	Si
Rangos de temperatura industriales	Si	No	Si
Trabajo en tiempo real	Si	No	Si
Fuentes de poder redundantes	Si	No	Si
Procesador de punto flotante	No	Si	Si
Memoria no volátil	No	Si	Si
Conectividad Ethernet	No	Si	Si
Capacidad para administrar recursos	No	Si	Si
Capacidad ilimitada de lazos de control	No	Si	Si

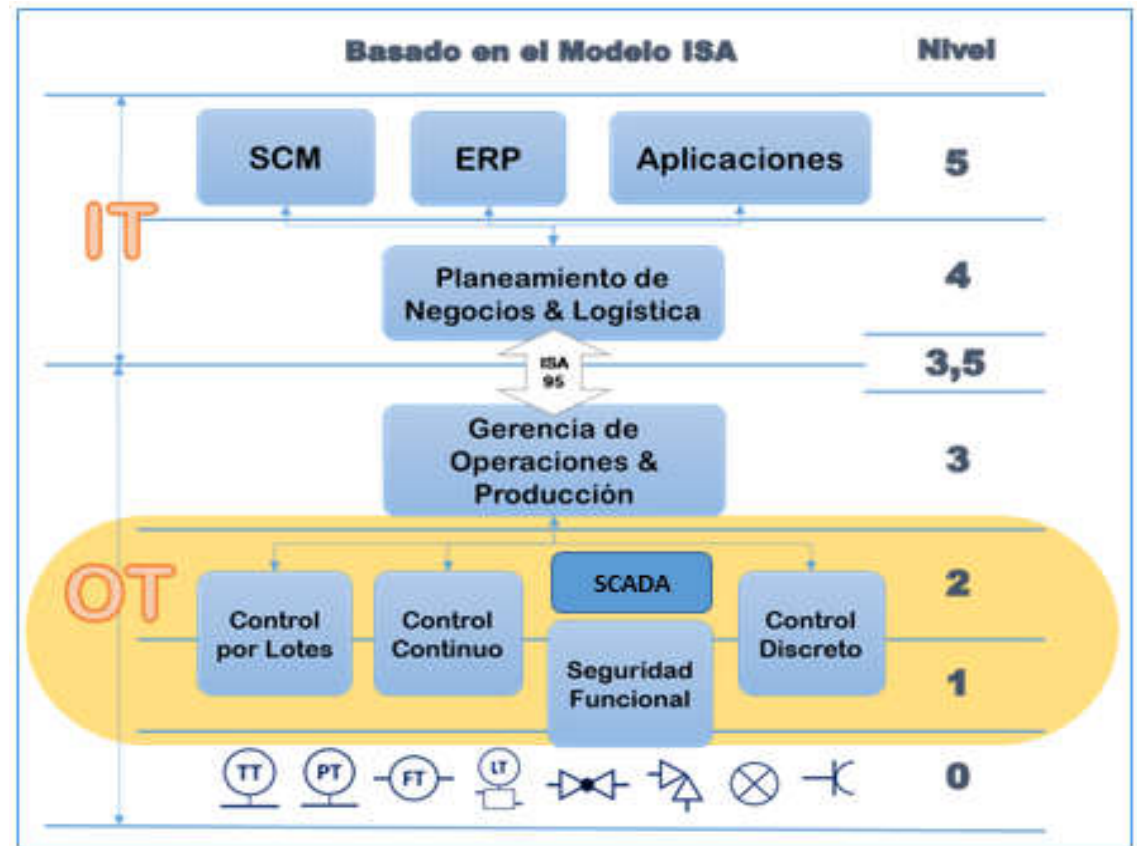
## 5. El universo SCADA. Los DCS vs. SCADA

Sistemas de Control Distribuido, el lazo se cierra automáticamente.  
En los SCADA se requiere la intervención de un operador humano

### Comparación entre SCADAs y DCSs

Características	SCADA	DCS
Modelo de control	Centralizado	Distribuido
Orientación	Adquisición de datos	Procesos
Impulso principal	Evento	Estado del proceso
Dispersión geográfica de los elementos	Alta	Baja
Estado de las estaciones de trabajo	Prescindibles ante fallas	Siempre conectadas
Cierre de lazo	Manual	Automático
Nivel de injerencia del operador humano	Alto	Bajo

## 5. El universo SCADA. Contexto organizacional



Jerarquía de los sistemas industriales

# 5. El universo SCADA. Distribución eléctrica

## Funciones de un SCADA para distribución de electricidad

1. Aplicaciones de tiempo real y tiempo de respuesta crítico:
  - a. Gestión de eventos en tiempo real
  - b. Procesos en aplicaciones específicas de tiempo crítico
  - c. Soporte y aplicaciones en bases de datos de tiempo real
  - d. Procesos específicos de la aplicación, no críticos en cuanto al tiempo
  - e. Procesos y aplicaciones de la seguridad del sistema
2. Aplicaciones de la interface del operador:
  - a. Aplicaciones propiamente dichas
  - b. Interface del operador
  - c. Soporte a la interface
  - d. Registro de eventos cronológicos
3. Almacenamiento de datos históricos:
  - a. Captura de datos históricos
  - b. Bases de datos históricos
  - c. Procesos de manipulación de datos históricos (aplicaciones específicas)



## 5. El universo SCADA. Interfaces

- **SCADA** con arquitectura de n niveles, componentes distribuidos y modulares, conexiones vía bus de datos lógico (*middleware*)
- **GIS** (*Geographic Information System*). Ofrece una serie de funciones integradas por capas, tales como cartografía, identificación de los elementos que conforman la red eléctrica, discriminación de los elementos pertenecientes a Alta, Media y Baja tensión, etc.
- **DMS** (*Distribution Management System*). Dentro de sus capacidades se halla la adquisición y el procesamiento de datos sobre la carga de los equipos del sistema de distribución
- Módulo de informes. Los principales destinatarios son los entes reguladores
- **OMS** (*Outages Management System*). Se encarga de gestionar el circuito de incidencias (fallas, interrupciones, trabajos programados, manejo de las cuadrillas de operarios que atienden reclamos y efectúan maniobras, etc.)
- **EAM** (*Enterprise Asset Management*). El sistema de gestión de activos corporativos organiza la información en una plataforma, sigue los flujos de trabajo asociados con su gestión en todas las instancias del ciclo de vida
- **Herramientas de administración**. Posibilitan la modificación de los parámetros en el SCADA

# 5. El universo SCADA. Riesgos. Referencias

**Potenciales atacantes:** *hackers, crackers e insiders*

**Principales riesgos y tipos de ataques contra una distribuidora:**

- Interrupción del servicio. Imposibilidad de restablecer el mismo
- Ataques físicos (vandalismo, sabotaje) y ciber (denegación de servicio)

## **IEC 61850**

Norma específica sobre automatización de subestaciones eléctricas, organizada en 10 capítulos. **A fines de 2017 se publicó IEC 61850-6 Ed. 2.1.**

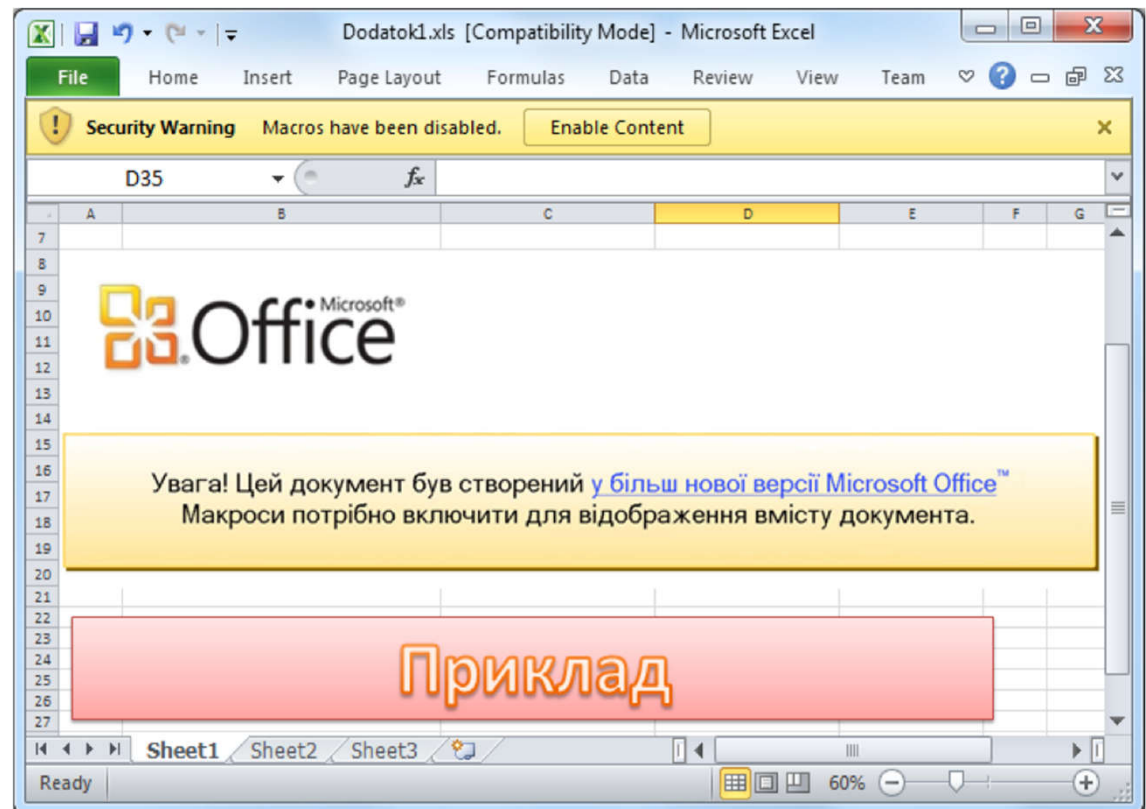
## **C37.240-2014**

Es una especificación que lleva el título *IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems*

## 5. El universo SCADA. Ciberataques

- El caso **BlackEnergy**

Captura pantalla de  
archivo Excel con  
macros, vector de  
infección de  
BlackEnergy (2015)



# 5. El universo SCADA. Protección

## Programa de Ciberseguridad Industrial, partes:

1. Políticas
2. Riesgos
3. Análisis
4. Prioridades
5. Tecnología
6. Vulnerabilidades
7. Detección
8. Mitigación
9. Protección

Abordaje en una distribuidora eléctrica. Aproximación a **ES-C2M2**  
(*Electricity Subsector Cybersecurity Capability Maturity Model*)

## 5. El universo SCADA. Dominios de ES-C2M2

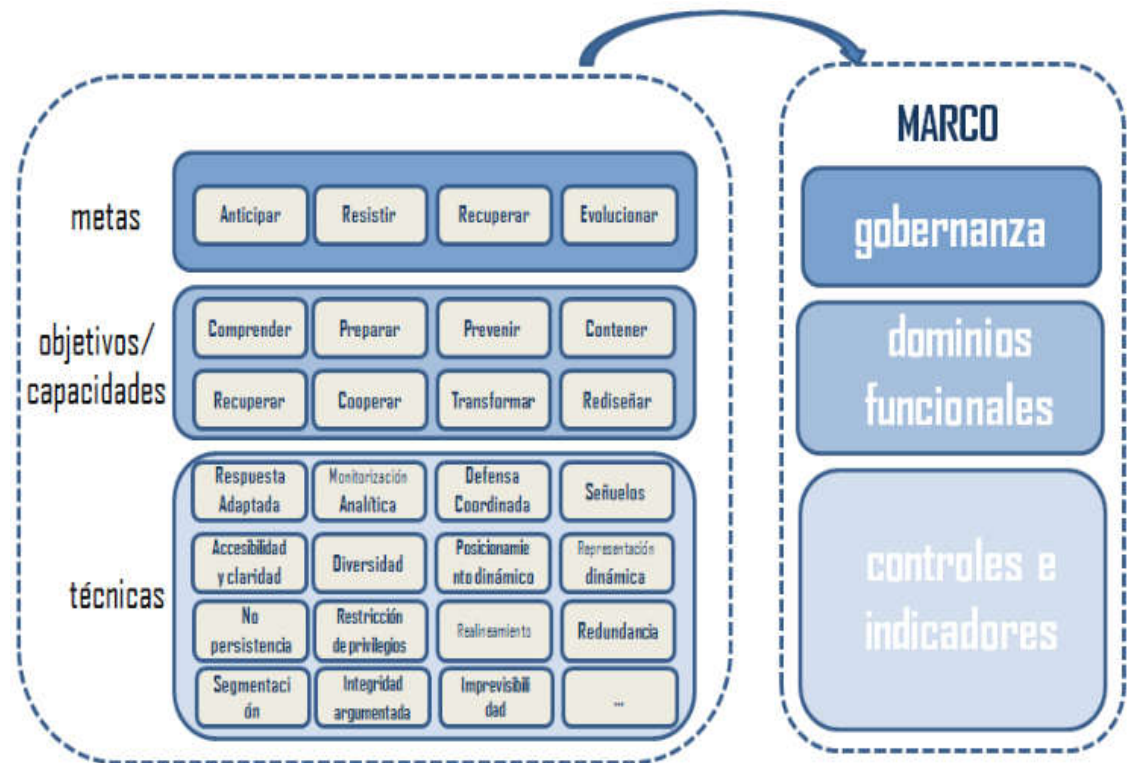
1. Gestión de riesgos
2. Gestión de Activos, Cambios y Configuración
3. Gestión de Identidad y Acceso
4. Gestión de amenazas y vulnerabilidades
5. Conciencia Situacional
6. Intercambio de Información y Comunicaciones
7. Respuesta ante Eventos e Incidentes, Continuidad de Operaciones
8. Gestión de la Cadena de Suministro y Dependencias Externas
9. Administración de personal
10. Gestión del Programa de Ciberseguridad

## 5. El universo SCADA. Ciber-resiliencia

“Cuando un sistema es capaz de soportar todo tipo de presiones sin cambiar su comportamiento, entonces es robusto.

Cuando no es capaz de soportar más presiones, pero puede integrar cambios para disminuirlas y puede seguir adelante, entonces es ciber-resiliente”.

Bruce Schneier.



Ciber-resiliencia, aproximación de la propuesta con base en el Framework del MITRE

## 6. Medidores inteligentes. Conceptos. Bases

**Prosumidor: Productor + Consumidor**

La evolución de la infraestructura: ***Smart Grid***:

- **Generación distribuida**
- **Seguridad informática y de la información**
- **Gestión de la información**
- **Privacidad**

**NISTIR 7628 Rev. 1:** Ciberseguridad para Smart Grid. El informe 7628 fue publicado en 2010, revisado y aumentado en 2014, consta de tres volúmenes y se titula *Guidelines for Smart Grid Cyber Security* o Directrices para la Ciberseguridad en la Red Inteligente

## 6. Medidores inteligentes. Migración hacia SG

**Red tradicional + comunicaciones + tecnología. Transición gradual:**

- 1. Tele-medición.** Se utiliza software y comunicaciones de dos vías para administrar remotamente los equipos emplazados en las instalaciones de los usuarios – clientes y en lugares estratégicos de la red
- 2. Tele-supervisión.** Es la recolección continua y remota de datos mediante sensores colocados en puntos sensibles de la red eléctrica
- 3. Tele-control o tele-gestión.** Está soportado por el seguimiento y comando a distancia de diversos equipos para obtener agilidad en la operación
- 4. Sistema Integrado de Gestión.** Estructura que posibilita agregar y recopilar datos, ordenar y compartir información



# 6. Medidores inteligentes. Migración hacia SG.

## Niveles de Tele-Medición

### **Medición Inteligente (Smart Metering)**

Posee capacidad de informar parámetros sobre calidad de producto y servicio, programación y actualización remotas desde un Centro de Gestión. Interacción con dispositivos eléctricos inteligentes del usuario-cliente.

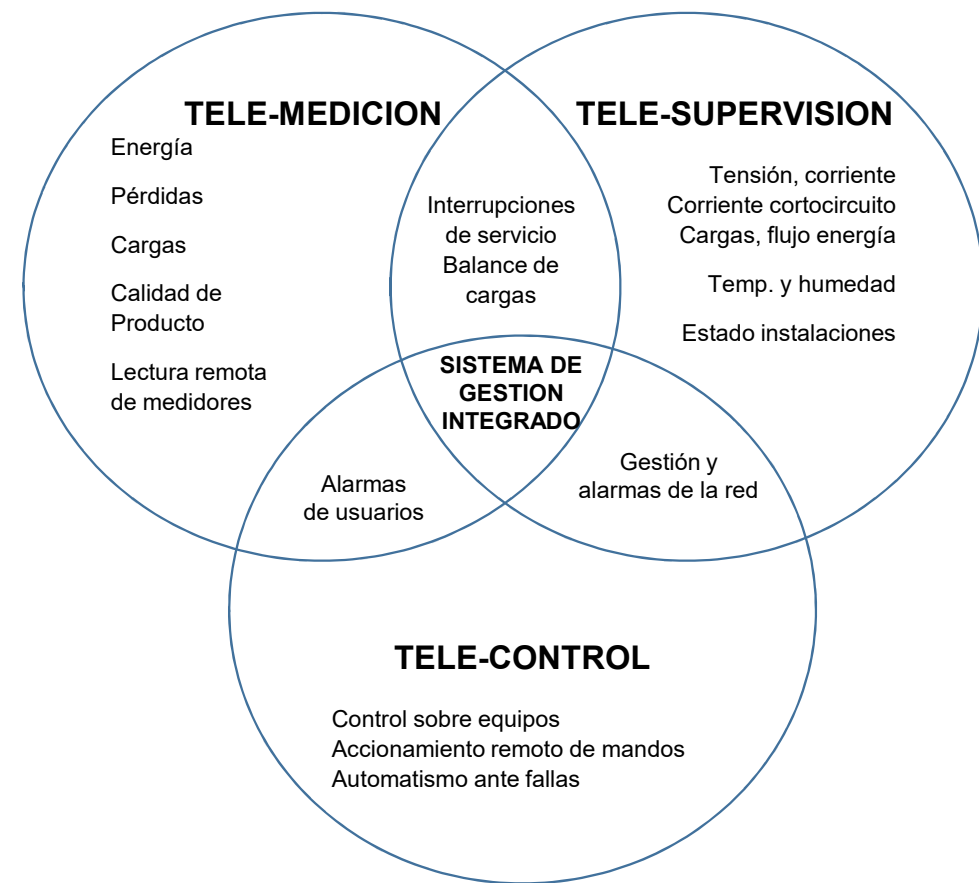
### **Infraestructura de Medición Avanzada (AMI – Advanced Metering Infrastructure)**

Agrega comunicación bidireccional para solicitar información y lecturas bajo demanda. Posibilita el control de carga mediante conexión y desconexión del suministro. Provee herramientas para detectar anomalías y fraudes.

### **Lectura Automática de Medidores (AMR – Automatic Meter Reading)**

Abarca la comunicación unidireccional entre los medidores y un servidor de datos. Registra la medición de energía y potencia durante intervalos de tiempo predefinidos.

# 6. Medidores inteligentes. Migración hacia SG



**Sistema de  
Gestión Integrado**

# 6. Medidores inteligentes

**Tecnologías de comunicación aplicables a *Smart Grid*:**

1. *Telefonía fija*
2. *Móviles*
3. *RF de corto alcance*
4. *Onda portadora*
5. *WiFi*
6. *Enlaces RF*
7. *Fibra óptica*
8. *Satelital*

Tipo	Tecnología	Tasa de transferencia	Alcance
Telefonía fija (cableada)	Par telefónico	Hasta 56,6 kbps	Nacional
Móviles (inalámbricas)	GSM (2G)	Hasta 14,4 kbps	Nacional, s/ cobertura
	GPRS / EDGE (2.5G)	Hasta 40 kbps y 384 kbps	Nacional, s/ cobertura
	UMTS (3G)	Hasta 2 mbps	Nacional, s/ cobertura
	WIMAX (4G)	Hasta 70 mbps	Hasta 50 Kmts a la vista
	LTE (4G)	Hasta 75 mbps	Nacional, s/ cobertura
Radio frecuencia de corto alcance (2.4 GHz) (inalámbrica)	6LoWPAN	Entre 250 kbps y 2 mbps	Entre 10 y 100 metros
	ZigBee	Entre 250 kbps y 2 mbps	Entre 10 y 100 metros
	Bluetooth	Entre 250 kbps y 2 mbps	Entre 10 y 100 metros
	Propietarias	Entre 250 kbps y 2 mbps	Entre 10 y 100 metros
Onda portadora (cableada)	PLC (banda angosta)	Hasta 100 kbps	Desde mts. a pocos kms.
	BPL (banda ancha)	Hasta 200 kbps	Desde mts. a pocos kms.
WiFi (inalámbrica)	WiFi	Entre 2 mbps y 300 mbps	Hasta 150 mts.
Enlaces de RF (radiofrecuencia)	Soluciones propietarias	Entre 9,6 kbps y 2 mbps	Hasta 70 kms.
Fibra óptica (cableada)	Multimodo	Entre 0,1 y 10 mbps	Entre 300 mts y 2 kms
	Monomodo	Hasta 10 mbps	Entre 50 y cientos de km
Satelital (inalámbrica)	Órbita baja (LEO)	Hasta 10 kbps	Entre 3000 y 4000 kms
	Geoestacionario	Hasta 500 mbps	1/3 de la superf. terrestre

## 6. Medidores inteligentes. Migración hacia SG

### Tipos de medidores:

- **Electromecánicos:** Poseen un disco de aluminio que gira como consecuencia del paso de corriente y tensión producidos por bobinados. Cada vuelta completada mueve agujas en un cuadrante, acumulando valores que son leídos periódicamente con el fin de facturar el consumo resultante.
- **Electrónicos:** Miden el consumo a través de convertidores con capacidad de traducir magnitudes analógicas en digitales. Cuando son telemedidos es posible conocer el consumo en tiempo real. De no haber infraestructura de comunicaciones la lectura es manual y periódica.
- **Inteligentes:** Los *Smart Meters* agregan funcionalidades al uso convencional, las cuales dependen en gran medida de la comunicación bidireccional altamente disponible contra un centro de gestión.

## 6. Medidores inteligentes. Migración hacia SG

**Comparación entre  
una red eléctrica  
tradicional y una  
inteligente**

Características	Red actual	<i>Smart Grid</i>
Tipo	Electromecánica	Digital
Comunicaciones	De una vía	De dos vías
Generación	Centralizada	Distribuida
Sensores y actuadores	Escasos	Numerosos
Monitoreo	Manual	Automático
Restauración	Manual	Automática
Respuestas ante incidentes físicos	Fallas e interrupciones	Adaptable y en islas
Alcance del control	Limitado	Generalizado
Opciones para los usuarios–clientes	Pocas	Muchas
Grado de automatización	Bajo – Medio	Alto

## 6. Medidores inteligentes. Riesgos

**Deben diferenciarse los riesgos desde tres puntos de vista:**

- Los **usuarios–clientes**. Reclaman privacidad y un tratamiento adecuado de sus datos personales. Aquí entra a jugar fuerte el rol del Estado mediante legislación y regulación, arbitrando los medios para hacer cumplir las mismas
- Los **prosumidores**. También solicitan privacidad y cuidado de sus datos propios, además de una correcta calibración de los Smart Meters con el objeto de reflejar fielmente el balance energético. En un futuro ideal los prosumidores reemplazarán por completo a los usuarios–clientes
- Las **distribuidoras**. Necesitan garantizar, entre otras cosas, la exactitud y fidelidad de los valores correspondientes a las lecturas, por lo que combaten el fraude y el robo de electricidad. Existe la posibilidad de que personas malintencionadas manipulen los contadores para intentar reflejar menores consumos a los reales, o mostrar de manera ficticia mayor nivel de electricidad generada distribuida

## 6. Medidores inteligentes. Protección

**Las medidas de protección apuntan a garantizar aspectos tales como:**

- **No repudio.** De modo que ninguna de las partes puede rechazar la transmisión de datos. Debe existir un conocimiento y consentimiento pleno de todos y cada uno de los actores involucrados
- **Autorización.** Es necesaria antes de poder iniciar una acción de control remoto. A modo de ejemplo, una conexión entre el medidor y el centro de gestión puede autenticar mutuamente ambos extremos implementando protocolo TLS
- **Privacidad.** Tanto de las estadísticas de consumo como de la información personal. Es factible usar cifrado como una herramienta válida, siempre que el protocolo elegido cumpla con estándares y no penalice el rendimiento del hardware o introduzca retardos o latencia en las comunicaciones

## 6. Medidores inteligentes

**Termineter:** ¿Malware o herramienta para pruebas?

**Vulnerabilidades.** Exposición a factores climáticos, incorrecto montaje e instalación y configuraciones inadecuadas o por defecto. Hacking

**Legislación y regulaciones.** Poco desarrollo y regulación. Hay 6 provincias con Normativa. 3 casos concretos: Santa Fe, Mendoza y Neuquén, con foco en Generación Distribuida y medidores inteligentes

**Industrial Internet Consortium y su visión de la seguridad en Smart Meters.** Marco de seguridad: IISF (*Industrial Internet of Things, Volume G4: Security Framework*), capítulo 8 dedicado a seguridad en endpoints, entre los cuales se hallan los *Smart Meters*. Seguridad física

**Entre Ríos: Decreto 4315. Diciembre 2016. Pequeños generadores**



## 7. Conclusiones y Reflexiones

La **Ciberseguridad Industrial** es un asunto complejo, con muchas aristas, que involucra a diversos sectores y protagonistas

El experto Claudio Caracciolo aporta 3 aspectos clave para la puesta en marcha de una estrategia exitosa: cooperación internacional, planes de acción concretos, respaldo político-económico

Retos: integración de disciplinas, incorporación de metodologías relativas al análisis de riesgos, desarrollo de estrategias sobre defensa en profundidad y mecanismos predictivos ante amenazas

## 7. Conclusiones y Reflexiones

**Infraestructuras Críticas.** Algunos hablan del inicio de la Cuarta Revolución Industrial, caracterizada por la fusión de tecnologías que difuminan las fronteras entre lo físico, digital y biológico. La realidad argentina atrasa, mostrando situaciones entre inexplicables e increíbles, al punto de que a la fecha actual ningún funcionario público con competencia en la materia sabe a ciencia cierta si el relevamiento de infraestructuras críticas lanzado en 2011 ha sido completado

El caso de la supuesta venta de los planos correspondientes a 3 plantas potabilizadoras en Bernal, Tigre y Capital Federal

Obligación de reportar las brechas de seguridad. Hora Oficial

# 7. Conclusiones y Reflexiones

## Sistema eléctrico en Argentina

Hacia 2009 se conjugaban 3 factores:

- El sector ha mostrado dificultades en ampliar la oferta de nueva generación.
- El funcionamiento del sistema se vuelve crítico ante temperaturas extremas.
- La visión es cortoplacista; con erogaciones retrasadas y equipos al límite

Es difícil lograr inversiones en el ámbito de la ciberseguridad industrial aplicada al sistema eléctrico en Argentina cuando durante más de 12 años el valor de la tarifa no ha remunerado siquiera los costos correspondientes a operación y mantenimiento del mismo

# 7. Conclusiones y Reflexiones

## **TI, TO, buenas prácticas, Normas y Estándares**

Uno de los dogmas sagrados en TO es el mito de la disponibilidad: “mientras la maquinaria continúe operando, lo demás pasa a segundo plano”. Coincido en parte con Eric Byres: la integridad debe estar garantizada previamente

Resultaría beneficioso un mayor nivel de apertura desde TO hacia el resto de las áreas que componen una distribuidora, especialmente TI

Del lado de TI, sería deseable que el grado de madurez en ciertas prácticas de gestión se refleje en un interés creciente por entender los requerimientos de TO

Las buenas prácticas, Normas y Estándares constituyen una hoja de ruta de gran valor, aunque seguirlas al pie de la letra no es suficiente. Deben ser adoptadas y adaptadas a cada necesidad

# 7. Conclusiones y Reflexiones

## SCADAs

Las lecciones aprendidas del incidente BlackEnergy resultan útiles:

- Los atacantes tuvieron entre 6 y 9 meses para prepararse
- Las conexiones remotas a SCADAS exigen 2 factores de autenticación
- Las fuentes de alimentación y las UPS son críticas y blanco de ataques
- Las actualizaciones de *firmware* son vectores de ataque
- Se requiere un sistema de detección y protección comprensiva (holístico)
- Es imperioso identificar vulnerabilidades y evaluar riesgos en ciberseguridad
- Cualquier recurso que describa el funcionamiento de la red eléctrica y la arquitectura de los sistemas de control, debe ser asegurado

Estadísticas del US-CERT. Ciber-Resiliencia

# 7. Conclusiones y Reflexiones

## Medidores inteligentes

Oleada de cortes en 2013. Propuesta de las empresas. Respuesta del gobierno de turno

Experiencias piloto en Santa Fe, Mendoza y Neuquén

Mientras no haya tarifa diferenciada en base a bandas horarias no se logrará masificar el uso de medidores inteligentes

Ciberseguridad, Internet de las Cosas, Internet de las Cosas Industrial

*Cualquier dispositivo IoT ó IIoT que tenga una dirección IP es susceptible a hacking*

Generación distribuida, fuentes renovables. Ley 27424 . Dec. 1075/2017.

Entre Ríos: Decreto 4315 del 29/12/2016

¡ Muchas gracias por su atención !

Contacto: **wheffell** *[at]* **gmail** *[dot]* **com**

Descarga del Material completo (126 páginas):

<http://www.segu-info.com.ar/terceros/?autor=heffel>