
**Fuerza Aérea Argentina**
**Instituto Universitario Aeronáutico**
**Facultad de Ingeniería**
**Carrera de Posgrado. Especialización en Seguridad Informática**

**Trabajo Final Integrador**

# Ciberseguridad industrial en la distribución de energía eléctrica

**Autor: Walter Ernesto Heffel**
**Tutor: Samuel Linares**
**Director de la Especialización: Eduardo Casanovas**

**Diciembre de 2016**

# Ciberseguridad industrial en la distribución de energía eléctrica

# Índice General

## PARTE 2: TECNOLOGÍA DE LA INFORMACIÓN Y TECNOLOGIA DE OPERACIÓN. BUENAS PRACTICAS, NORMAS Y ESTÁNDARES. EL UNIVERSO SCADA.

### CAPÍTULO IV. TECNOLOGÍA DE LA INFORMACIÓN Y TECNOLOGÍA DE OPERACIÓN. BUENAS PRÁCTICAS, NORMAS Y ESTÁNDARES



### CAPÍTULO V. EL UNIVERSO SCADA



## PARTE 3: MEDIDORES INTELIGENTES. CONCLUSIONES Y REFLEXIONES.

### CAPÍTULO VI. MEDIDORES INTELIGENTES

# Índice de Figuras y Tablas

## FIGURAS



## TABLAS

# Ciberseguridad industrial en la distribución de energía eléctrica

## Licenciamiento



## Referencias a fuentes

Las citas bibliográficas y a recursos disponibles en Internet se presentan mayormente en formato APA (Asociación Psicológica Americana), respetando el siguiente orden y según corresponda cada ítem:

a) Autor y/o autores (Apellido, Nombre) u Organización (Denominación)
b) Título de la Obra (libro, revista, *paper*, artículo, etc.)
c) Número de página, orden de párrafo, capítulo, etc.
d) Fecha de publicación de la Obra
e) Editorial o Institución que publica la obra
f) Para material disponible en línea: Leyenda "Obtenido el dd/mm/aaaa, desde el sitio web http://www.url.com"

Ejemplo: a) Muñoz-Organero, M., Valera-Pintor, F., Vidal-Fernández, I. b) *Coding Techniques -2010*. c) Capítulo I, pág. 18. d) (12/03/2010). e) Universidad Carlos III. f) Obtenido el 30/03/2015, desde el sitio Web de OCW - UC3M: http://ocw.uc3m.es/ingenieria-telematica/coding-techniques.

No obstante, las referencias se realizan en cada página, al pie, de modo que el lector pueda rápidamente acceder a las mismas; evitando la interrupción al tener que desplazarse a la sección Bibliografía / Fuentes. Las expresiones en inglés o extranjero van en *letra cursiva*.

**Citas:**

***"si la buscas como a la plata,***

***como a un tesoro escondido […]***

***la sabiduría vendrá a tu corazón,***

***y el conocimiento te endulzará la vida.***

***La discreción te cuidará,***

***la inteligencia te protegerá."***

Proverbios 2:4,10-11

Texto tomado de la Santa Biblia, Nueva Versión Internacional, © 1999, por la Sociedad Bíblica Internacional

***"Todos somos muy ignorantes.***

***Lo que ocurre es que no todos ignoramos las mismas cosas."***

Albert Einstein (Ulm, 14/03/1879 – Princeton, 18/04/1955)

**Agradecimientos:**

A Dios. Tan grande es su amor por los que le temen como alto es el cielo sobre la tierra.

Ile: Tus desafíos son el combustible que me moviliza. San: Es maravilloso ver cómo creces y aprendes cada día. Feli: Tu llegada es un bálsamo para nuestras vidas. Juan: Descansa en paz, cumpliste con creces. Rita: Es tiempo de cosecha y disfrute.

A Alfredo Muzachiodi por la confianza. Gustavo Rodríguez y Gonzalo Dieser, por bancarme.

**Reconocimientos:**

Aldo D. Sigura. El primero en creer que esto de la seguridad podía ir conmigo.
Daniel A. Vázquez. Es difícil sacarse el sombrero de Auditor y ponerse el de Gerente.
Eduardo W. Ettlin: ¿Tiene sentido la disponibilidad sin confidencialidad e integridad? ☺

Omar M. Ramos: En efecto, muchas veces la peor enfermedad es creer que no se puede.
Eduardo Casanovas y Samuel Linares, amigos entrañables, admiro vuestra paciencia.
Esteban D. Bastanzo, por las revisiones, correcciones y sugerencias.

## Propuesta de Trabajo Final Integrador (TFI)

### Objetivos

Definir la Ciberseguridad industrial, describir particularidades inherentes al campo en el que se desarrolla la distribución de energía eléctrica, establecer relaciones entre ambos mundos, analizar la situación actual y el estado del arte en la materia, identificar debilidades o carencias, proponer recomendaciones, reflexionar y obtener algunas conclusiones. Interesa en especial la realidad de la Argentina, preferentemente desde fuentes de datos públicas.

### Alcances y exclusiones

El contexto que impone la temática eléctrica en su rol de servicio público esencial y la consideración en el marco de las llamadas Infraestructuras Críticas ayudan a delinear el alcance del texto. El desarrollo deriva a los dos temas centrales del presente texto, representados por las funciones y la operación de los sistemas industriales para Supervisión del Control y la Adquisición de Datos –conocidos como *SCI/SCADA*– y los medidores de consumo eléctrico inteligentes –o *Smart Meters*– en el ámbito de la Red Eléctrica Inteligente –o *Smart Grid*–; siempre desde la óptica de la Ciberseguridad Industrial. Dado el grado de desarrollo y madurez, algunas referencias se toman de países europeos o Estados Unidos.

Aunque la seguridad informática y de la información aparecen explícitas y latentes en este trabajo, no es intención avanzar con desarrollos tradicionales asociados a la gestión de la seguridad desde el punto de vista administrativo o el típico de la gobernanza relacionada con los sistemas informáticos, o a la mera aplicación de medidas técnicas para protección.

Se trata de realizar una mirada amplia, en donde se hace necesario un abordaje holístico, multifactorial y multidisciplinario.

### Metodología

La modalidad del trabajo es de tipo descriptivo y pretende recopilar información, junto con la elaboración y algunas conclusiones para ser presentadas a un tribunal examinador.

### Destinatarios

El público al que apunta el texto no abarca a expertos en Ciberseguridad Industrial, Automatización o Distribución de Energía Eléctrica, sino que intenta ser un documento de posición, análisis y difusión del estado actual; destinado a un auditorio amplio y general.

## Introducción

Para algunos la Tercera Revolución Industrial inició en 1969, cuando apareció el primer controlador lógico programable. En 2006 el Parlamento Europeo la declaró como tal, tomando las ideas impulsadas por Jeremy Rifkin. Así como la Primera nació a partir del uso del vapor de agua y la Segunda surgió desde el combustible líquido derivado del petróleo, en la Tercera se funden estratégicamente tres elementos: inteligencia, ciencia y tecnología. La mecánica dio paso a la electrificación masiva, mientras que los cambios culturales y sociales impulsados por las transformaciones abrieron el camino a la Sociedad del Conocimiento. El uso de sistemas ciberfísicos está pariendo una Cuarta Revolución: la “Industria 4.0”.

¿Habrán imaginado los pioneros de la electricidad que ésta tendría un rol preponderante en la existencia de las próximas generaciones?, ¿Podemos pensar hoy en un mundo sin energía eléctrica? El simple resumen de una jornada típica en la vida de una persona implica enumerar algunos ejemplos disímiles: agua caliente, afeitadora, teléfono móvil, computadora portátil, electrodomésticos, alumbrado público, carteles luminosos en la vía pública, edificios inteligentes, autos eléctricos… la lista podría ser tan larga y detallada como para ocupar varias páginas; lo cierto es que en un planeta urbanizado y globalizado la electricidad es el fundamento que hace posible el acceso al desarrollo, las comodidades y aplicaciones que dependen de los “electrones” para funcionar. Cualquiera de los efectos producidos, sea luminoso, térmico o magnético forma parte del cotidiano trajín humano en el siglo XXI. Carecer de ellos supondría poco menos que retroceder a la época de las cavernas.

Independientemente de la forma en que se produce y transporta el fluido eléctrico, su distribución constituye una etapa extremadamente sensible para la infraestructura que alimenta desde gigantescas fábricas hasta un pequeño nebulizador. Los avances tecnológicos no son ajenos a los servicios públicos. Debe resaltarse que el acceso al agua potable, el gas y el transporte es altamente dependiente de la red eléctrica para funcionar. Esto sitúa a la misma en la capa más baja del circuito, por lo que es clave su disponibilidad.

Resulta paradójico: los mismos avances tecnológicos que nutren un teórico círculo virtuoso de innovación, automatización y evolución constantes, sitúan a la distribución eléctrica ante riesgos que a primera vista aparecen como puramente técnicos y exclusivos de los dominios de las telecomunicaciones o la informática. Canales inseguros por definición, protocolos obsoletos, ausencia de controles, carencia de sentido común, accesos no autorizados, etc. son algunos de los temas que dan sustento a este escrito, particularmente en relación a los ambientes SCI / SCADA y la progresiva masificación de los medidores inteligentes. Ambas aplicaciones constituyen casos representativos para describir, aprender y obtener conclusiones desde el cristal de la Ciberseguridad Industrial.

# PARTE 1

## Definiciones. Infraestructuras críticas. Sistema eléctrico en Argentina

# Capítulo I

## Definiciones

*"El único sistema verdaderamente seguro*

*es aquel que se encuentra apagado,*

*encerrado en una caja fuerte de titanio,*

*enterrado en un bloque de hormigón,*

*sellado en una habitación revestida de plomo*

*y vigilado por guardias armados muy bien remunerados …*

*y aun así tengo mis dudas".*

**Eugene Spafford, "Computer Recreations of Worms, Viruses and Code War",**

**Scientific American (A.K. Dewndey), Marzo 1998, Página 110**

*"Dos grandes falacias respecto a la ciberseguridad:*

*<No tenemos nada que merezca la pena ser atacado> y*

*<No hemos sido comprometidos>"*

**Richard Stiennon (@cyberwar)**

**en el Congreso #CClCon3, 2014**

## El concepto “ciber”: del idioma griego a su uso actual

Dada la universalización de las nuevas tecnologías es común toparnos a diario con palabras que asumimos como naturales en nuestro lenguaje; mas no siempre tenemos en claro su raíz o el contexto en el que las usamos. Así, por ejemplo, incorporamos sin reparo términos tales como ciberespacio, cibercafé, ciberguerra, ciberjuegos, ciberterrorismo, ciberdelincuencia, etc. Pareciera que todo aquello en apariencia relacionado con lo virtual o con Internet debe ser citado con una palabra que agregue el prefijo en cuestión.

Pero, ¿de dónde surge esta asociación? Pues bien, deben mencionarse un par de cuestiones. En primer lugar la contracción **ciber**, a secas, refiere a la traducción del término en inglés ***cyber***; y en ambos casos resultan apócopes de **cibernética** y ***cybernetics***, respectivamente; es por ello que tal reducción puede hallarse con la letra < i > en español o con la < *y* > en idioma inglés, según corresponda. Por seguir, la etimología nos devela que su origen se remonta al vocablo griego ***kibernetiké*,** usado para significar “el arte de gobernar una nave”. En forma análoga, la palabra ***kibernetikós*** alude a la función del ***kibernes*** (timonel) a bordo de los barcos hace más de 2500 años atrás. Hacia 1830 en Francia el término ***cibernétique*** fue acuñado para referirse a “el arte de gobernar”. Dejando de lado los asuntos navales, aparentemente fue el matemático estadounidense Norbert Wiener quien reformuló la palabra otorgándole un nuevo sentido a partir de 1948, año en que se publicó el libro *Cybernetics: Or Control and Communication in the Animal and the Machine* (*Cibernética o el control y comunicación en animales y máquinas)*. Veamos un par de definiciones:

> **cibernética**[1]
> (Del francés *cybernétique*; este del inglés *cybernetics*, y este del griego *κυβερνητική*, arte de gobernar una nave).
> 1. f. Estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas; y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología.
>
> **cibernético, ca**
> 1. adj. Perteneciente o relativo a la cibernética.
> 2. adj. Dicho de una persona: Que cultiva la cibernética. U. t. c. s.

Una enmienda de la propia Real Academia Española (RAE) en el avance de la 23° edición (año 2014) agrega dos acepciones:

> 3. adj. Creado y regulado mediante computadora u ordenador. Ej.: “Arte cibernético”
> 4. adj. Perteneciente o relativo a la realidad virtual. Ej.: “Viaje cibernético”

[1] Real Academia Española, Diccionario de la lengua española, 22° edición. 2012. Obtenido el 28/01/15 desde el sitio web http://lema.rae.es/drae/?val=cibernética

Los aportes más cercanos se remontan a principios de los '80s. En 1981, a partir del cuento *Johnny Mnemonic* escrito por William Gibson. Y 1984, cuando aparece la novela futurista de ciencia ficción titulada *Neuromancer* (traducida al español como *Neuromante*) del mismo autor, siendo ésta la primera parte de una trilogía dedicada a temas de inteligencia artificial. En ambas obras se introdujeron vocablos tales como *cyberculture, cyberspace* y *cyberpunk* [2].

Lo cierto es que un rápido repaso histórico nos ayuda a atar algunos cabos y extrapolar definiciones. El término griego explica en cierta forma una idea actualmente adoptada, la del navegante como persona que hace uso de herramientas informáticas para transitar a través del océano virtual representado por la Internet pública o bien de los mares y ríos, en sentido figurado, que conectan a las redes de dispositivos (computadoras, tabletas, teléfonos inteligentes, etc.). La acepción en francés es tal vez la menos lógica de acuerdo a los cánones vigentes, sin embargo puede servir para referir a la noción del *browser* o navegador, ya que originalmente esta función es ejercida por una aplicación de computación que de alguna manera se encarga de guiar la experiencia del internauta. Los aportes conceptuales de Wiener y Gibson resultan, a los efectos del presente trabajo, los más significativos; ya que el primero plantea la semejanza entre las estructuras de los seres vivos y las máquinas; mientras que el segundo le dio forma a nuevas palabras que anteponen la etiqueta "ciber". Por citar un ejemplo, la idea de ciberespacio aparece hoy como algo intangible, aunque su significado saltó desde la literatura fantástica al despliegue de una inteligencia colectiva en red que permite relacionar personas con máquinas vinculándolas a través de múltiples dispositivos, todos ellos electrónicos.

## Seguridad: significado, dimensiones, ambigüedades y traducciones

La palabra que mayor cantidad de veces aparece en este trabajo tiene una definición extremadamente breve para su principal uso:

**seguridad** [3]

(Del lat. *securĭtas, -ātis*).

**1.** f. Cualidad de seguro.

Y no por escueta deja de ser menos explícita. Existen muchas otras significaciones que abarcan disciplinas que van desde lo jurídico a lo social, pasando por asuntos de Estado,

[2] Rouse, Margaret. Cyber. Sin indicación de fecha de publicación. Obtenido el 30/01/15 del sitio web http://searchsoa.techtarget.com/definition/cyber

[3] Real Academia Española. Diccionario de la lengua española, 22° edición. 2012. Obtenido el 26/03/15 del sitio web http://lema.rae.es/drae/?val=seguridad

salud pública, vialidad, alimentación, etc. La lista sería realmente larga si pretendiera enumerar todas y cada una de las temáticas con las que la seguridad puede ir apareada. Cabe entonces la pregunta: ¿a qué nos referimos cuando hablamos de algo "seguro"? Echando mano una última vez aquí de nuestro aliado tesauro en línea transcribo la primera parte:

**seguro, ra**[4]

(Del lat. *secūrus*).

**1.** adj. Libre y exento de todo peligro, daño o riesgo.

**2.** adj. Cierto, indubitable y en cierta manera infalible.

**3.** adj. Firme, constante y que no está en peligro de faltar o caerse.

**4.** adj. No sospechoso.

**5.** m. Seguridad, certeza, confianza.

**6.** m. Lugar o sitio libre de todo peligro.

**7.** m. Salvoconducto, licencia o permiso que se concede para ejecutar lo que sin él no se pudiera.

**8.** m. Mecanismo que impide el funcionamiento indeseado de un aparato, utensilio, máquina o arma, o que aumenta la firmeza de un cierre.

**9.** m. coloq. Asociación médica privada, que se ocupa de la prevención y remedio de las enfermedades de las personas que abonan las primas correspondientes.

**10.** m. coloq. seguridad social**.**

**11.** m. *Der.* Contrato por el que alguien se obliga mediante el cobro de una prima a indemnizar el daño producido a otra persona, o a satisfacerle un capital, una renta u otras prestaciones convenidas.

El detalle incluye dos variantes más y gran cantidad de construcciones gramaticales que incluyen el término en cuestión. Quedan fuera del alcance por razones de espacio.

El contexto aplicable en este trabajo cita a lo seguro como sinónimo de certeza o confianza, dejando en claro que es utópico pensar en la existencia de ámbitos "ciento por ciento seguros". La frase "todo es relativo, nada es absoluto" sintetiza con crudeza el panorama al que debe enfrentarse cualquier ente, producto o servicio que pretenda incorporar

[4] Real Academia Española, Diccionario de la lengua española, 22° edición. 2012. Obtenido el 26/03/15 del sitio web http://lema.rae.es/drae/?val=seguro

seguridad o ser percibido como seguro. Por otro lado las nociones de peligro, daño, amenaza o riesgo le dan sentido y razón de ser a los conceptos que intento explicar.

Analizando la cantidad de tópicos que involucran estos vocablos y sus derivados, surge un prototipo abarcador: la idea de seguridad multidimensional, la cual no es nueva. La Asamblea General de la Organización de Estados Americanos (OEA) adoptó en Bridgetown, en 2002, un enfoque multidimensional. Esto implicó la expansión de la definición tradicional, que involucraba exclusivamente amenazas de tipo militares externas, para incorporar una combinación de problemáticas políticas, económicas, medioambientales y de seguridad humana[5].

A modo de desambiguación se hace necesario profundizar los significados cada vez que se utiliza la palabra seguridad, ya que su uso aislado y a secas no siempre alcanza para transmitir de manera efectiva una idea. Algunas frases son ejemplificadoras:

- “el cinturón de seguridad salva vidas”,
- “para evitar pérdidas de datos se deben efectuar copias de seguridad periódicamente”,
- “ciertos países no poseen doctrina de seguridad nacional”,
- “determinadas empresas dependen de la seguridad por oscuridad en cuestiones tecnológicas”,
- “la seguridad social otorga bienestar a la comunidad”,
- “la seguridad alimentaria es un desafío mundial”,
- “dos inversores se retiraron por falta de seguridad jurídica”,
- “las estadísticas en materia de seguridad vial son alarmantes”,
- “el servidor estuvo fuera de servicio durante 3 horas debido a un agujero de seguridad”,
- “la seguridad industrial gestiona los riesgos físicos, laborales y medioambientales en la planta de producción”,
- “el Consejo de Seguridad de Naciones Unidas tuvo que reunirse de urgencia”.

Al ser tan vasto el universo de aplicación de la palabra debe ponerse especial énfasis al momento de emplearla, aun teniendo la ayuda del prefijo “ciber” para encausar su propósito en el marco del presente trabajo.

Otro tema que merece especial atención es la correcta traducción desde el idioma inglés al español, pues *security* no es lo mismo que *safety*, más allá de la ubicación contextual. Si bien estas diferencias deben ser explicadas y desarrolladas en detalle, debe quedar claro

[5] Stein, Abraham. El concepto de Seguridad multidimensional. Pág. 31. Sin indicación de fecha de publicación. Obtenido el 26/03/2015 del sitio web http://www.fundacionpreciado.org.mx/biencomun/bc176-177/A_Stein.pdf

que *safety* aplica a los aspectos relacionados con integridad física y salud de una persona, mientras que *security* refiere a medidas para prevenir ataques, sabotajes o robos perpetrados sobre equipamiento. A modo de introducción será suficiente mencionar la breve y magistral definición esbozada por Samuel Linares para separar las aguas: "*safety* es cuidar a las personas de las máquinas; mientras que *security* es preservar a las máquinas de las personas"[6] (sic). Esta última idea, la de *security*, es la que mejor describe y abarca a la "seguridad" contenida en "ciberseguridad".

**Ciberseguridad, un concepto amplio**

"El todo es más que la suma de las partes" sintetiza la idea atribuida a Aristóteles y es aplicable a lo que deseo transmitir. La comprensión del término Ciberseguridad exige analizar su significación como un "todo" cuyas propiedades y características no se encuentran en cada una de sus partes al considerarlas aisladamente. Dos nociones ayudan al respecto: la holística y la sinergia.

La holística es la forma de observar las cosas enteras, completas, en su totalidad, en su conjunto, en su complejidad, ya que de esta manera es posible distinguir interacciones, procesos y particularidades que por lo general no se perciben si se estudian separadamente los aspectos integrantes del todo.

La sinergia, bajo el cristal de la ingeniería de sistemas, estudia al todo como un producto o servicio que no se halla dentro de sus partes, sino en función de los resultados o efectos generados por la interrelación de sus componentes.

Con estos desafíos en mente, trataré de exponer algunas definiciones de Ciberseguridad, tan complejas o sencillas en función de su trama.

Para la Unión Internacional de Telecomunicaciones (*ITU International Telecommunication Union*, por su sigla en inglés) la ciberseguridad es "el conjunto de herramientas, políticas, estrategias, salvaguardas, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedia, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la

[6] Linares, Samuel. Presentación titulada "Implementando la Ciberseguridad desde la realidad: Perspectiva desde Europa, América y Medio Oriente". Pág 5. Junio 2015. Programa del evento obtenido el 01/06/2015 del sitio web https://www.cci-es.org/documents/10694/0/IV+Congreso+Iberoamericano+de+Ciberseguridad+ESP/cbfc6f0d-9210-417d-bdcf-60692ad77c4c

organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad, integridad (que puede agregar autenticidad o autenticación, y no-repudio) y confidencialidad" [7].

Según el Consejo Argentino de Relaciones Internacionales (CARI) desde la visión de su Instituto de Seguridad Internacional y Asuntos Estratégicos, la Ciberseguridad es el "conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propias y negarlo a terceros" [8].

Una tercer acepción, también concisa y propuesta por la Red de Crisis y Riesgo del Centro para estudios sobre Seguridad (Instituto Federal Suizo de Tecnología – ETH), refiere a la Ciberseguridad como "la ausencia de amenazas realizadas por medio de, o dirigidas a, las tecnologías de la comunicación y de la información, y a sus redes" [9].

Queda claro entonces que Ciberseguridad abarca componentes y elementos que giran alrededor de tecnología, informática, telecomunicaciones, información, amenazas, activos o bienes, aseguramiento en el tratamiento de datos, seguridad de la información, y lo más valioso: las personas.

**El ambiente industrial**

Desde su raíz en el latín *industruo* (*indu*, en el interior; y *struo*, organizar o fabricar) sumado al sufijo *ia* (cualidad) la palabra industria tiene variados usos. El más elemental sugiere: aplicación, laboriosidad, elaboración y en paralelo: ingenio, sutileza. Una perspectiva más utilitaria refiere a un grupo de procesos y actividades cuyo objetivo es cambiar materias primas en productos.

Actualmente también puede considerarse industria a ciertos proveedores de servicios, ya que si bien no ofrecen productos sus prestaciones surgen de combinar procesos y actividades, tal el caso del turismo, una verdadera "industria sin chimeneas".

Volviendo a la visión clásica, las materias primas por sí solas no son el único componente. Los eslabones que completan la cadena son la maquinaria y los recursos humanos; todo estructurado bajo la forma de una organización o empresa.

[7] International Telecommunication Union (ITU). Decisiones destacadas de Guadalajara, Ciberseguridad, Resolución 181. Noviembre 2010. Obtenido el 27/05/2015 del sitio web https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx
[8] Consejo Argentino de Relaciones Internacionales (CARI). Ciberdefensa: los riesgos que plantea. Pág. 2. Noviembre 2013. Obtenido el 27/05/2015 del sitio web http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf
[9] Brunner, Elgin, et al. Focal Report 3, Critical Infrastructure Protection, Cibersecurity – Recent Strategies and Policies: An Analysis. Pág 6. Agosto 2009. International Relations and Security Network (ISN). Obtenido el 11/06/2015 del sitio web http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=108743

Pueden hacerse muchas categorizaciones e interpretaciones. A los efectos del presente trabajo alcanza con establecer ciertos aspectos relevantes, a saber:

- Existe industria pesada y liviana. La pesada procesa inmensos volúmenes de recursos, en su mayoría naturales, y los transforma para convertirlos en productos semielaborados o bienes intermedios, utilizables a su vez en otras industrias. V.g.: Industria metalúrgica, petrolera, química, petroquímica, etc. La industria liviana apunta como destinatario al mercado minorista, generando bienes de uso y consumo masivos. V.g.: industria textil y alimenticia.
- La industrialización de una actividad implica pasar de la elaboración artesanal y manual a la fabricación en serie, a partir del uso de maquinaria cuyo funcionamiento depende de fuentes de energía. Algunos autores hablan de un salto desde la manufactura a la "maquifactura". Esto tiene un impacto enorme en términos de escala, a partir del aumento exponencial en la productividad.
- El fenómeno de la automatización en la industria transforma constantemente las formas de producir. Desde que en 1745 se inventó una máquina para tejer guiada mediante tarjetas perforadas o en 1784 un telar mecánico, las innovaciones en automatismo no se han detenido hasta la actualidad. Puede definirse a la automatización industrial como el empleo de sistemas y elementos basados en computación y electromecánica con el fin de controlar máquinas y procesos. No deben soslayarse los beneficios en tareas repetitivas, pesadas y peligrosas; y el desarrollo de interfaces hombre – máquina, referenciados como HMI (*Human Machine Interface*) o MMI (*Man Machine Interface*).

**Relación entre lo "ciber" y lo físico**

En el mundo ciber convergen acciones y datos producidos en el universo físico que pueden modificar contextos personales o sociales; y viceversa[10].

Los llamados sistemas ciberfísicos poseen capacidad para integrar funciones de cómputo y comunicación con seguimiento y control de entidades físicas. Abarcan un conjunto de agentes en red incluyendo sensores, actuadores, dispositivos de comunicaciones y unidades de procesamiento, tal como se muestra en la figura 1. El factor temporal resulta clave, ya que el período requerido para realizar una tarea es del orden de décimas o centésimas de segundo. De ahí la importancia en el adecuado manejo del tiempo real y la

[10] Pillajo, C. Sierra, J. Importancia del estudio del control para los sistemas cyber-físicos. Pág. 1. Diciembre 2014. Obtenido el 27/10/2015. URL: http://carlospillajo.info/wp-content/uploads/sites/1369/2014/12/Importancia-del-estudio-de-control-para-los-CPS_RevCP.pdf

gestión determinística, por ejemplo para corregir sobre la marcha el funcionamiento de un módulo.

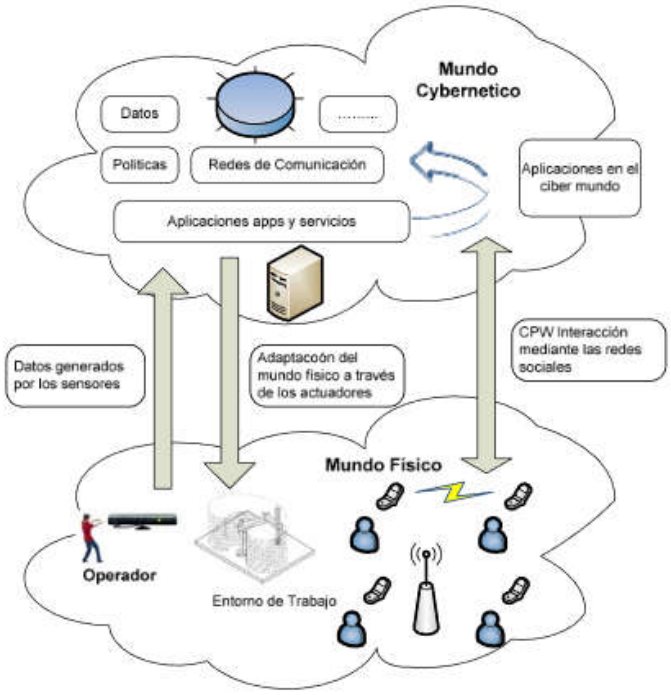


**Figura 1: Convergencia genérica entre los mundos ciber y físico.**[11]

Los procesos físicos son colecciones de eventos ocurriendo en el mismo instante, a diferencia de los procesos de *software*, que tradicionalmente se desarrollan forma secuencial. Mediante el seguimiento de los programas informáticos y el control de los procesos físicos, los sistemas ciberfísicos se encargan de operar y monitorear actividades como el transporte y la distribución eléctrica. Tienden a ser híbridos y distribuidos, compuestos por dominios de computación en red y dominios físicos distribuidos. Debe tenerse en cuenta no sólo la forma de diseñar lo discreto y digital (programas de computación) sino también lo continuo y analógico (entidades físicas), para lograr combinarlos de manera eficaz, eficiente y segura.

La figura 2 grafica la relación ciber – físico, extrapolada a dos entornos de una misma empresa, por un lado el corporativo y por el otro el industrial. En el primero se consideran consecuencias intangibles: el portal web no está disponible, el correo electrónico dejó de funcionar, etc. En el segundo se enumeran resultados tangibles: pérdida de producción, daños al medioambiente y a la salud pública, disminución del valor de la Compañía.

[11] Pillajo, C. Sierra, J. Importancia del estudio del control para los sistemas cyber-físicos. Pág. 2. Diciembre 2014. Obtenido el 27/10/2015. URL: http://carlospillajo.info/wp-content/uploads/sites/1369/2014/12/Importancia-del-estudio-de-control-para-los-CPS_RevCP.pdf

La alta cohesión hace que cualquier desequilibrio o compromiso en la seguridad impacte no solo sobre recursos cibernéticos sino también en activos físicos y vidas humanas.

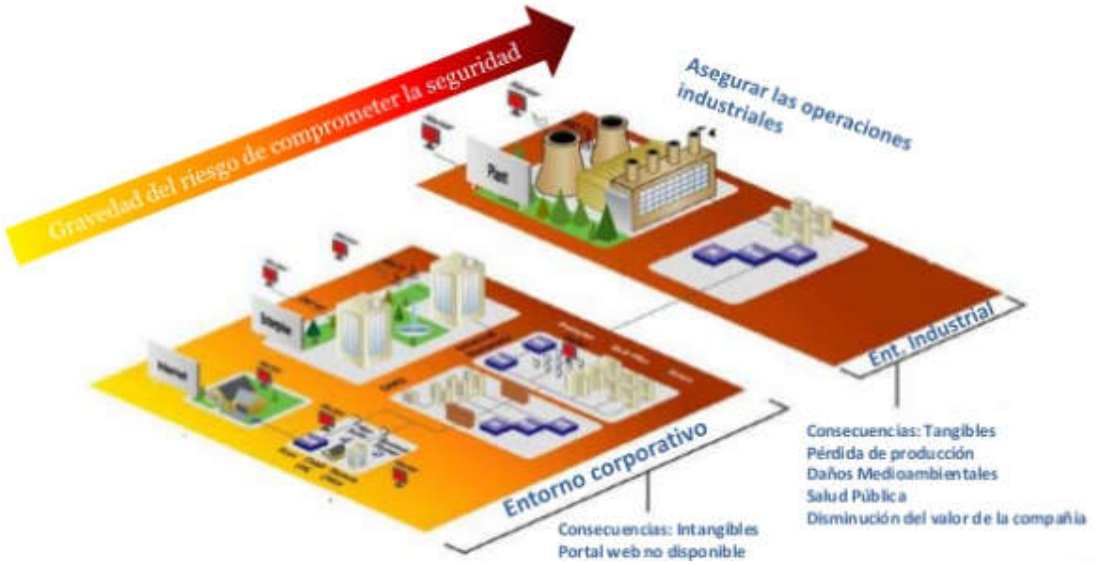


**Figura 2: Convergencia específica entre los mundos ciber y físico.** [12]

## Referencias a cibersistemas y automatización

El Centro de Análisis e Intercambio de Información sobre Sistemas de Control Industrial, ICS-ISAC (*Industrial Control System Information Sharing and Analysis Center*) apunta a la cuestión mediante un enfoque basado en la conciencia situacional: "La sociedad moderna está apoyada por una infraestructura interdependiente que soporta las funciones necesarias de los servicios. Los sistemas que proveen energía, comida, agua, bienes, servicios, transporte, comunicación, etc., dependen a su vez de la disponibilidad de otros servicios. Cada uno de estos segmentos de infraestructura está cada vez más controlado por cibersistemas que mejoran su efectividad funcional y económica. Dichos cibersistemas traen aparejados cambios en los riesgos que enfrentan los operadores de infraestructura y aquellos que dependen de ellos. Abordar estos riesgos requiere habilidades individuales y de la infraestructura global de la cual forman parte para mejorar la capacidad de mantener conciencia del entorno" [13].

[12] Paredes, Ignacio. Tsunami: ¿Vas a quedarte mirando la ola? Panorama actual de ciberseguridad industrial. Slide 7. Sin fecha de publicación. Obtenido el 27/10/2016. URL: http://es.slideshare.net/NextelSA/tsunami-vas-a-quedarte-mirando-la-ola-panorama-actual-de-ciberseguridad-industrial . Autor de la presentación original: Linares, Samuel.
[13] Industrial Control Systems Information Sharing and Analysis Center. About ICS-ISAC, párrafo 3. Sin indicación de fecha de publicación. Obtenido el 12/06/2015 del sitio web http://ics-isac.org/blog/home/about/. (adaptado al castellano).

La Sociedad Internacional para la Automatización, mundialmente conocida como ISA (*International Society of Automation*) separa claramente dos campos de actuación para *Cybersecurity*. "La Ciberseguridad para la empresa industrial es muy diferente de la Ciberseguridad para otras áreas. En seguridad de la empresa, ya sea para una oficina o incluso para un Banco o un emisor de tarjetas de crédito, los factores confidencialidad, integridad y disponibilidad (CIA) (la "A" corresponde a *Availability*) son preponderantes en ese orden; la protección de los datos en los servidores es la primera prioridad. En la seguridad de operaciones o de control industrial, el acrónimo está formado por las mismas letras con un orden diferente: AIC. La primera prioridad en una situación de fabricación es mantener la planta en funcionamiento (disponibilidad) con integridad y confidencialidad, si es posible"[14].

ISA es una entidad sin fines de lucro fundada en 1945 que, entre otras actividades, publicó en 2000 la Norma ISA-95, la cual evolucionó para dar paso en 2007 a ANSI/ISA-99 y en 2013 comenzó a convertirse en un estándar de alcance mundial al transformarse en ISA/IEC-62443. ANSI es la sigla de *American National Standards Institute*, IEC corresponde a *International Electrotechnical Commision*. El contenido de ISA/IEC-62443 es fundamental y ocupa un papel central en Ciberseguridad industrial, por lo que se le dedicará una sección a su análisis, junto con Normas y buenas prácticas específicas aplicables a la gestión integral y manejo de la electricidad.

**Industria 4.0**

La evolución de las prácticas y procesos industriales a partir de la incorporación de tecnología ha sido constante, al punto que ciertos sucesos establecen el nacimiento (y a veces la muerte) de las "revoluciones" o "eras" industriales. Si bien no pueden establecerse fechas taxativas de principio y fin, determinados hitos ayudan a delimitar los períodos; asumiendo lapsos de tiempo solapados, a modo de transición. También es verdad que muchos autores no se ponen de acuerdo en cuestiones puntuales, por lo que la línea temporal difiere un poco según el punto de vista. La figura 3 ilustra la evolución de las 4 etapas.

El término "Industria 4.0" es sinónimo de ciberindustria o industria inteligente. Fue acuñado en 2012 por la Academia Alemana de Ciencias para dar nombre a una iniciativa de la Comisión Europea tendiente a aumentar la participación de la manufactura en el PIB Europeo desde el 15% en 2010 al 20% en 2020. En 2013 se creó la plataforma tecnológica y en 2014 aparecieron los primeros *smart services*.

[14] International Society of Automation. Cybersecurity. Home / Technical Topics / Cybersecurity. Sin indicación de fecha de publicación. Obtenido el 12/06/2015 del sitio web https://www.isa.org/technical-topics/cybersecurity/. (adaptado al castellano).

Los principales componentes de esta Cuarta Revolución son: Internet de las cosas, *Big Data*, Computación en la Nube, cultura "hágalo usted mismo, fabricación aditiva, impresión en tres dimensiones (3D), robótica colaborativa. No se trata de una realidad consolidada, sino un dominio cambiante y disruptivo.

Sintetizando: Industria 4.0 se asocia a sistemas ciberfísicos o físicos cibernéticos, entendidos como tecnologías informáticas y de la comunicación embebidas en todo tipo de dispositivos, dotándolos de "inteligencia" y autonomía para lograr mayor eficiencia. Se localizarán en los sistemas de transporte, automóviles, fábricas, procesos industriales, hospitales, oficinas, hogares, ciudades y dispositivos personales, configurando una nueva generación de elementos interconectados[15].

Los avances en implementaciones de RFID (*Radio Frequency IDentification*) en complejos fabriles, el software de simulación para analizar elementos de la cadena productiva o evaluar vulnerabilidades e incidentes de seguridad imposibles de reproducir de otro modo y la IIoT (*Industrial Internet of Things*) son ejemplos concretos.

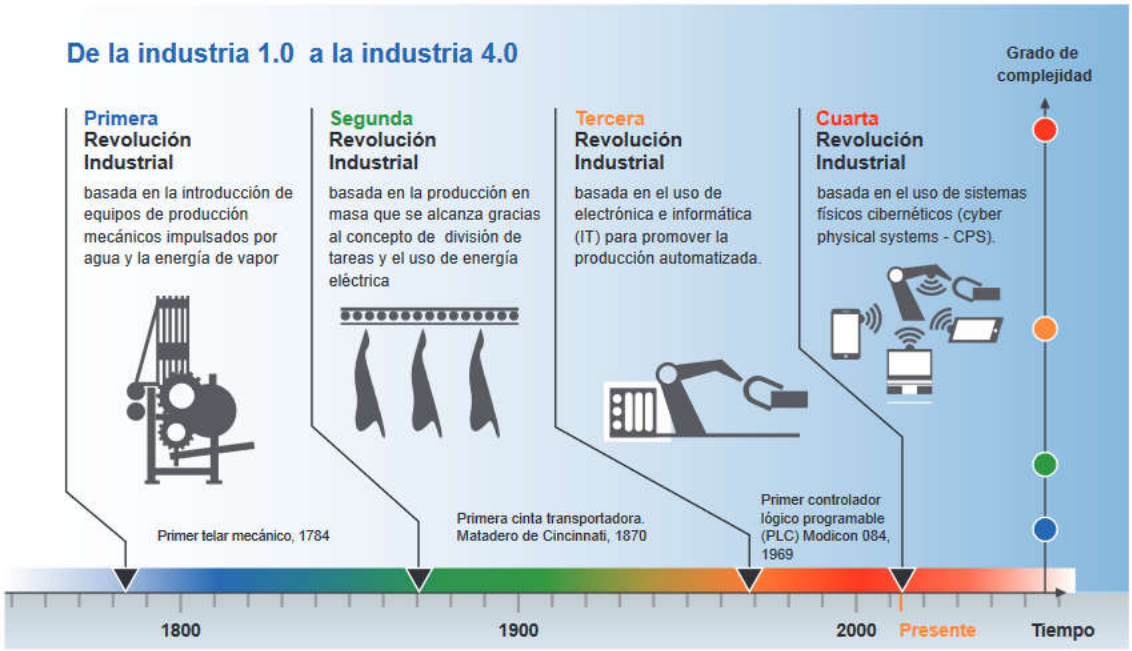


**Figura 3: De la industria 1.0 a la industria 4.0.** [16]

[15] Ministerio de Ciencia y Tecnología. Industria 4.0: Escencarios e impactos para la formulación de Políticas Tecnológicas en los umbrales de la Cuarta Revolución Industrial. Fecha publicación: Febrero 2015. Obtenido el 07/11/2016 del sitio web: http://www.mincyt.gob.ar/adjuntos/archivos/000/038/0000038319.pdf .
[16] Ministerio de Ciencia y Tecnología. Ibid.Traducido, fuente original: http://www.engineersjournal.ie

### Infraestructuras Críticas y Ciberseguridad en Argentina

A nivel nacional se creó en julio de 2011 el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (conocido como ICIC), el cual "tiene como objetivo la elaboración de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas de las entidades y jurisdicciones definidas en el artículo 8º de la Ley Nº 24.156 y sus modificatorios (Sector Público Nacional), los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado que así lo requieran, así como al fomento de la cooperación y colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías" [17]. Sin embargo, no se define explícitamente a la Ciberseguridad. Se introduce la noción de Infraestructura Crítica, la cual será desarrollada en el Capítulo 2 del presente trabajo.

### Armando el rompecabezas: ¿qué es la Ciberseguridad industrial?

Habiendo realizado esbozos de los conceptos ciber, seguridad e industrial, además de analizar las relaciones entre lo ciber y lo físico, junto con referencias a infraestructuras críticas, cibersistemas, automatización y realidad local, resta ahora intentar darle sentido al conjunto.

No resulta sencillo encontrar definiciones taxativas y completas, menos aún en idioma español. La mayor parte de lo que existe son acercamientos referidos a Ciberseguridad que no incluyen propiamente al ámbito industrial, o bien es material en idioma inglés que debe ser traducido, interpretado y adaptado para que sea de utilidad.

Según el Centro de Ciberseguridad Industrial, con sede en España, Ciberseguridad Industrial es **"el 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"**[18].

El CCI y en particular Samuel Linares, uno de sus fundadores, han sido pioneros en el mundo de habla hispana al acuñar conceptualmente la idea de "Ciberseguridad Industrial", logrando hacia 2012 condensar en esta expresión varios términos, asunciones, siglas, frases o traducciones que por sí solos y en forma aislada no reflejaban completa y adecuadamente

[17] Jefatura de Gabinete de Ministros. Resolución 580/2011, Art. 2°. Julio de 2011. Obtenido el 12/06/2015 del sitio web http://www.infoleg.gov.ar/infolegInternet/anexos/185000-189999/185055/norma.htm.
[18] Centro de Ciberseguridad Industrial. Portal CCI, El Centro. Sin indicación de fecha de publicación. Obtenido el 27/01/2015 del sitio web https://www.cci-es.org/el-centro

el campo de acción de esta disciplina. Algunos ejemplos de ello, considerando como referencia temporal el período anterior a 2012:

- No existía documentación en español al respecto, solo contenidos en inglés sobre *SCADA Security*, *Industrial Control System Security*, etc. Las traducciones literales no clarificaban el significado.
- El enfoque meramente tecnológico resultaba insuficiente. Hablar de "Seguridad en los Sistemas de Control" implicaba referirse a un subconjunto, sistema o agrupamiento de sistemas desde una única óptica, dejando de lado los planos correspondientes a las personas y los procesos.
- Inicialmente la Ciberseguridad, a secas, apuntaba solo a la seguridad lógica, aunque sin abarcar al mundo industrial.
- Pensar en Seguridad Industrial para designar esta disciplina supondría agregar ambigüedad, además ésta lleva años ocupándose de los riesgos físicos, laborales y medioambientales.
- En la cultura anglosajona este inconveniente no existe, ya que se diferencian las palabras *safety* y *security*, cuyos alcances ya se detallaron.

Otra de las pocas explicaciones que pueden hallarse corresponde a la firma WisePlant, para la cual la disciplina que estoy analizando en este capítulo **"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 sistemas de control están basados en computadoras que se utilizan para controlar y supervisar procesos sensibles y funciones físicas. En este caso, 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"**[19].

### Evolución conceptual

Debe señalarse como un hito la metamorfosis conceptual que se ha forjado desde hace unos años a la actualidad, que implicó pasar de ideas tales como "Seguridad en sistemas SCADA" o "Seguridad de los sistemas de control industrial" hacia una visión específica e identidad propia como es la Ciberseguridad Industrial; con un alcance de mayor amplitud y más abarcador.

[19] WisePlant. Servicios para la Ciberseguridad Industrial, Pág. 3. Fecha de publicación: junio 2014. Obtenido el 27/10/2015 del sitio web http://docplayer.es/1228551-Servicios-para-la-ciberseguridad-industrial-ics.html

# Capítulo II

# Infraestructuras Críticas

*Ciberespacio: Dominio global dentro del entorno de la información,*

*constituido por redes interdependientes de infraestructuras informáticas*

*y los datos que en ellas se albergan.*

*Incluye Internet, redes de telecomunicaciones,*

*sistemas informáticos, procesadores y controladores embebidos.*

**Manual de la Ley de Guerra Sección 16.1.2 (Edición junio de 2015)**

**Departamento de Defensa de los EEUU**

*"No comprenderemos nuestra dependencia de las Tecnologías de la Información*

*hasta que haya un desastre.*

*Es como tener sangre sin oxígeno".*

**Khalid Al Falih, 2013**

**CEO de Saudi Aramco (@Saudi_Aramco)**

**Relación entre Infraestructuras Críticas y servicios esenciales. El rol del Estado**

Etimológicamente hablando, infraestructura es la suma de dos palabras latinas: *infra* (debajo) y *structura* (esqueleto, viga, base, cimiento o fundación que soporta y sostiene una construcción o edificio). Podemos imaginar entonces que se trata de aquello situado en la capa más baja posible.

En general se trata de la agrupación de elementos considerados como imprescindibles para que una organización pueda funcionar o que una actividad se desarrolle eficazmente. Desde otro punto de vista la componen los factores de producción: recursos naturales, medios técnicos y fuerzas laborales, los cuales unidos conforman las corrientes productivas.

Del material y las fuentes evaluadas, la visión más atinada aquí es "el 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" [20].

Tales servicios brindados se consideran esenciales o estratégicos, con lo cual cobra relevancia la función de las infraestructuras críticas. Quizá por una cuestión de significado desde el lenguaje, el término "crítica" suene más impactante que "esencial". El tratamiento especial abarca instalaciones, redes y procesos de trabajo que se combinan para que la función se convierta en algo real y concreto.

Según el especialista norteamericano John D. Moteff "la salud, la riqueza y la 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 (por ejemplo, la electricidad: las centrales que la generan y la red eléctrica que la distribuye)" [21]. Esta tesis pone el foco en el alto grado de subordinación que tiene la población de Estados Unidos, sus recursos naturales y hasta la seguridad nacional respecto a estas infraestructuras, aunque la opinión pública o la prensa no tengan una real dimensión del asunto. No en vano se habla de CNI (*Critical National Infrastructure*) como sigla para referirse al tema en EE.UU. Siendo esta nación una potencia mundial, su realidad es representativa y constituye un modelo a seguir para buena parte del mundo occidental.

En sentido amplio y de acuerdo a Eduardo A. Thill "La acción del Estado es imprescindible por dos razones: una es cumplir el rol de articulador en la hipótesis de crisis que afecten a dichas infraestructuras, la otra, es el único actor que tiene una mirada

[20] Definición ABC. Definición de infraestructura. Sin indicación de fecha de publicación. Obtenido el 16/06/2015 del sitio web http://www.definicionabc.com/general/infraestructura.php
[21] Moteff, John D. Critical Infrastructures: Background, Policy, and Implementation. Pág. 2. Obtenido el 10/06/2015 del sitio web https://www.fas.org/sgp/crs/homesec/RL30153.pdf (adaptado al castellano).

omnicomprensiva y dispone de la información, los resortes regulatorios y el poder de policía para poder hacer cumplir las normas y garantizar la continuidad de los servicios. Solamente el Estado está en condiciones de tener un enfoque global que tenga en cuenta las interdependencias y las externalidades de seguridad" [22].

### La referencia de España

La legislación española las define explícitamente: "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" [23].

El Centro Nacional para la Protección de Infraestructuras Críticas menciona doce sectores estratégicos, a saber:

- 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

Aparece la energía como uno de los ítems.

### Categorización de las Infraestructuras Críticas. Agrupamientos

Para lograr una comprensión cabal del carácter subyacente que presentan, la tabla 1 detalla una de las primeras aproximaciones en la materia por parte de investigadores

[22] Thil, Eduardo A. Infraestructuras críticas, interoperabilidad y estándares: ejes para una administración electrónica efectiva. Pág. 12. Noviembre de 2010.Obtenido el 23/06/2015 del sitio web http://siare.clad.org/fulltext/0065716.pdf
[23] CNPIC (Centro Nacional para la Protección de las Infraestructuras Críticas). ¿Qué es una infraestructura crítica? Sin indicación de fecha pub. Obtenido del sitio web http://www.cnpic.es/Preguntas_Frecuentes/Que_es_una_Infraestructura_Critica/index.html

holandeses hacia el año 2003[24], quienes propusieron un inventario de cada sector, agrupando en cada uno los productos o servicios abarcados. Nótese que el sector Energía aparece en primera posición y dentro del mismo la electricidad también ocupa el lugar inicial.

| # | Sector | Producto o servicio vital |
|---|---|---|
| 1 | **Energía** | **Electricidad** |
| 2 | | Gas Natural |
| 3 | | Petróleo |
| 4 | Telecomunicaciones | Infraestructura permanente (postes, cables, microondas) |
| 5 | | Telecomunicaciones móviles |
| 6 | | Comunicación y navegación por radio |
| 7 | | Comunicaciones satelitales |
| 8 | | Radiodifusión (broadcasting) |
| 9 | | Infraestructura de Internet y acceso |
| 10 | | Correo electrónico y mensajería |
| 11 | Agua potable | Provisión de agua potable |
| 12 | Alimentación | Provisión de comida. Seguridad alimentaria |
| 13 | Salud | Servicios de salud |
| 14 | Financiero | Infraestructura financiera privada (bancos, servicios financieros) |
| 15 | | Infraestructura financiera pública (impuestos, servicios sociales) |
| 16 | Aguas superficiales | Calidad del agua |
| 17 | | Gestión de la cantidad de agua (diques, bombas, compuertas) |
| 18 | Seguridad y orden | Mantenimiento del orden público (policía) |
| 19 | públicos | Mantenimiento de la seguridad pública (bomberos) |
| 20 | Justicia | Jurisdicción y detención |
| 21 | | Mantenimiento de la Justicia |
| 22 | Gobierno estatal | Servicios diplomáticos |
| 23 | | Servicios de información pública |
| 24 | | Fuerzas Armadas / Defensa |
| 25 | | Gobierno civil |
| 26 | Transporte | Rutas y autovías |
| 27 | | Ferrocarriles |
| 28 | | Transporte aéreo |
| 29 | | Transporte marítimo / fluvial |
| 30 | | Cargas |
| 31 | | Ductos / tuberías (acueductos, oleoductos, gasoductos) |

**Tabla 1: Lista de 11 sectores y 31 productos y servicios vitales (2003)**

[24] Luiijf, Eric et al. Critical Infrastructure Protection in The Netherlands: A Quick-scan. Pág. 15. Ene 2003. Obtenido el 24/06/2015, URL: https://www.emsec.rub.de/media/crypto/attachments/files/2011/03/bpp_13_cip_luiijf_burger_klaver.pdf (texto adaptado)

El propio Ministerio del Interior de Holanda cita en 2004 una versión similar, a modo de segunda fase y amplía la misma tabla, agregando una categoría y cuatro servicios, lo cual se observa en la tabla 2.

| 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 |
| IV Alimentación | 12 Provisión de comida. Seguridad alimentaria |
| V Salud | 13 Urgencias y atención en hospitales |
| | 14 Medicamentos |
| | 15 Sueros y vacunas |
| | 16 Medicina nuclear |
| VI Financiero | 17 Estructura de pagos y servicios (privado) |
| | 18 Asignación financiera de Gobierno |
| VII Represas y control | 19 Calidad de las aguas superficiales |
| | 20 Represas y control de la cantidad de agua |
| VIII Seguridad y orden públicos | 21 Mantenimiento del orden público |
| | 22 Mantenimiento de la seguridad pública |
| IX Ordenamiento jurídico | 23 Administración de justicia y detención |
| | 24 Mantenimiento de la ley y el orden |
| X Administración civil | 25 Comunicación diplomática |
| | 26 Difusión de información gubernamental |
| | 27 Fuerzas Armadas |
| | 28 Administración civil |
| XI Transporte | 29 Rutas y autovías |
| | 30 Ferrocarriles |
| | 31 Transporte aéreo |
| | 32 Transporte fluvial |
| | 33 Transporte marítimo |
| | 34 Control de ductos |
| XII Industria nuclear y química | 35 Transporte, almacenamiento, producción y procesamiento de sustancias químicas y nucleares. |

**Tabla 2: Lista de 12 sectores y 35 productos y servicios (2004)**

Los cambios introducidos, aunque menores, muestran algunas vetas interesantes. Desaparece en el título la palabra “vital”, lo cual surge un tanto contradictorio al ver que se subdivide el sector Salud en cuatro grupos separados. Y en lo atinente a Industria nuclear y química, se la incluyó a pesar de que ciertos especialistas opinan que se trata de un sector con su propio régimen de seguridad, completo y autónomo. El foco de la protección está puesto en los desastres naturales, por sus efectos en cadena; y los actos humanos intencionales.

A modo de aprendizaje puede decirse entonces que los servicios esenciales dependen de las infraestructuras críticas para su normal prestación, y que éstas no tienen razón de existir sin las necesidades y exigencias de las sociedades modernas.

**Realidad en Argentina**

En 2011 la Jefatura de Gabinete de Ministros del Gobierno Nacional creó el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), pensado y diseñado con el fin de sostener un estructura para crear y adoptar un marco regulatorio que permita identificar, inventariar y proteger infraestructuras críticas estratégicas necesarias para el correcto funcionamiento del Sector Público Nacional, las organizaciones de jurisdicción provincial, la sociedad civil y las organizaciones privadas.

Tratándose de una cuestión incipiente que plantea nuevos desafíos y luego de sucesivos cambios en la burocracia estatal, se ha creado durante junio de 2015 (Decreto 1067/2015) la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Uno de los considerandos del decreto sostiene “Que una de las premisas del Gobierno Nacional es lograr el perfeccionamiento de la utilización de los recursos públicos con miras a una mejora sustancial en la calidad de vida de los ciudadanos, focalizando su accionar en la producción de resultados que sean colectivamente compartidos y socialmente valorados” [25]. En cuanto a los objetivos, se destacan los tres iniciales:

- “1. Asistir a la Secretaría de Gabinete en la formulación de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras críticas del Sector Público Nacional, y a las organizaciones civiles, del sector privado y del ámbito académico que así lo requieran, fomentando la cooperación y colaboración de los mencionados sectores.
- 2. Entender en la elaboración de la Estrategia Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.

[25] Administración Pública Nacional. Decreto 1067/2015. 10/06/2015. Obtenido el 23/06/2015 del sitio web: http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/247971/norma.htm

- 3. Entender en las acciones de supervisión, monitoreo, análisis y detección de los activos críticos de información, dentro del alcance de su competencia" [26].

Referido a las acciones propias de la Dirección se resaltan las siguientes:

- "4. Colaborar con el sector privado para elaborar en conjunto políticas de resguardo de la seguridad digital con actualización constante, fortaleciendo lazos entre los sectores público y privado; haciendo especial hincapié en las infraestructuras críticas.
- 5. Establecer prioridades y planes estratégicos para liderar el abordaje de la Ciberseguridad, asegurando la implementación de los últimos avances en tecnología para la protección de las infraestructuras críticas.
- 7. Monitorear los servicios que el Sector Público Nacional brinda a través de la red de Internet y aquellos que se identifiquen como infraestructura crítica para la prevención de posibles fallas de seguridad.
- 8. Alertar sobre casos de detección de intentos de vulneración de infraestructuras críticas así como de las vulnerabilidades encontradas" [27].

La mencionada Dirección lidera el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), conformado por cuatro grupos de trabajo:

- Infraestructuras críticas.
- Acción preventiva.
- ICIC CERT.
- Internet sano.

Interesa aquí el primero: "Tiene por objeto el relevamiento, identificación y clasificación de las infraestructuras estratégicas y criticas de Información. […]. Asimismo es el encargado de desarrollar políticas y estrategias tendientes a la protección de las infraestructuras críticas de información" [28]

No se encontró ninguna explicación o declaración acerca de qué entiende el Estado Argentino por infraestructuras críticas, o al menos una enumeración de los sectores abarcados, más allá del propio Sector Público Nacional. Haciendo un paralelo con el caso español, puede que una parte de la respuesta provenga del razonamiento que hace Eduardo A. Thill al referirse al Catálogo Nacional de Infraestructuras Críticas: "El criterio por el cual se incluyen dichas instalaciones sensibles en el Catálogo es una mezcla de factores: rango, escala y efectos en el tiempo y de parámetros: daños causados, impacto económico y en

[26] Administración Pública Nacional. Ibid.
[27] Administración Pública Nacional. Ibid.
[28] ICIC – Programa Nacional de Infraestructuras Críticas. Qué hacemos / Grupo de Infraestructuras Críticas. Sin indicación de fecha de publicación. Obtenido el 23/06/2015 del sitio web: http://www.icic.gob.ar/

servicios esenciales. Dada la criticidad de la información, el listado de las infraestructuras que integran el Catálogo es secreto" [29]. El status "secreto" tiene que ver con que las instalaciones de las fuerzas armadas también son consideradas infraestructuras críticas. Por cuestiones de seguridad nacional y soberanía de cada país, muchos datos relativos al mundo castrense no son públicos ni accesibles por el ciudadano común.

**Protección de Infraestructuras Críticas, un asunto de larga data**

Pese a que los historiadores difieren en algunas teorías y existen variadas hipótesis respecto a la caída del Imperio Romano, una de ellas cita los cortes del suministro de agua por parte de los bárbaros como uno de los principales factores de la debacle en las mayores poblaciones de lo que en aquel momento era la potencia mundial dominante. Los desafiantes "bárbaros" apelaron al ingenio antes que a la fuerza y su supuesto poderío militar para darse cuenta que los habitantes de las ciudades sitiadas no podrían ofrecer resistencia por mucho tiempo sin hidratarse: el agua potable fue (lo es y será) estratégicamente un elemento de mayor valor que cualquiera de las defensas, arcos, flechas, catapultas y demás armas o ejércitos de la época.

Aun siendo la vida humana el activo más destacado, los jerarcas romanos no mensuraron en su justa magnitud la necesidad de proteger físicamente sus acueductos, probablemente porque confiaron en sus huestes antes que en la provisión ininterrumpida de algo tan básico e indispensable como el líquido elemento bebible. Evidentemente no se les ocurrió que, además de diseñar y construir semejante infraestructura de recolección, transporte, almacenamiento, distribución y desecho de agua, tendrían que haber tomado medidas para la defensa de la misma. En definitiva, la función y el servicio que prestaban tales acueductos eran más importantes que las acequias, fuentes, arcadas de piedra, cañerías y estanques. De allí el requisito incumplido de evitar que terceros ajenos accedieran a la "operación" de la red de saneamiento.

Este antiguo y paradigmático ejemplo es una muestra de la preponderancia que tiene la protección. No obstante, muchos autores sostienen que no se trata de un fin en sí mismo, por lo que es preciso considerar un principio de economía: el costo de la salvaguarda no debiera exceder el valor del activo a preservar.

Son tres los objetivos básicos de la protección:

- Garantizar la continuidad del servicio prestado.
- Implementar medidas para la prevención de fallas y ataques.

[29] Thil, Eduardo A. Op. cit.

- Ante un incidente, dar respuesta para lograr la rápida restitución del servicio.

A tal punto debe tenerse presente la protección que en el campo militar se agregó recientemente un nuevo dominio. A los tradicionales campos de batalla posibles (tierra, aire, agua, espacio) se sumó el llamado quinto elemento: el ciberespacio.

### Vulnerabilidades

Hablar de vulnerabilidad implica referirse a algo que se asume previamente como vulnerable, que puede ser dañado. Esta visión sitúa a toda infraestructura crítica como una entidad susceptible de ser golpeada, rota, deteriorada, aislada, quemada, inundada o afectada de cualquier forma para que no cumpla su función principal, antes que considerarla como un conjunto de elementos diseñado y organizado para fabricar un producto o prestar un servicio.

### Interdependencias

La salida de servicio por parte de una infraestructura crítica puede afectar directa o indirectamente otras infraestructuras, impactar determinadas regiones geográficas, e incluso propagar sus efectos en la economía nacional y global.

Básicamente una **interdependencia** puede definirse como la relación de dependencia recíproca entre dos personas o cosas. Ampliando el alcance a la temática del presente trabajo y considerando la inevitable interacción que existe entre dos o más infraestructuras críticas, en 2001 los investigadores Rinaldi, Peeremboom y Kelly propusieron 6 dimensiones en función de las cuales identificar, entender y analizar los desafíos que se presentan (Figura 4) y de las cuales quiero hacer foco en las interdependencias. Tales dimensiones abarcan:

- Características de la Infraestructura
- Estado de operación
- **Tipos de interdependencias**
- Ambiente / Entorno
- Comportamiento de acoplamiento y respuesta
- Tipo de falla

Los citados autores pusieron en evidencia una nueva perspectiva al momento de la publicación: la de los sistemas adaptables complejos[30]. Según esta visión el universo de las infraestructuras críticas posee una propiedad en común, y es que todas ellas son colecciones

[30] Rinaldi S., Peeremboom J. y Kelly T., Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. Pág. 13. Diciembre 2001. Obtenido el 01/09/2015 del sitio web: http://user.it.uu.se/~bc/Art.pdf

complejas de componentes dinámicos que interactúan entre sí. A menudo los cambios en los mismos o en la forma en que se relacionan son el resultado de procesos de aprendizaje; de allí el nombre dado a estos sistemas. Se desprenden tres implicancias de esta tesis: a) aporta beneficios para el análisis y modelado, b) confirma que cada elemento es parte de una intrincada red que conforma una infraestructura general y c) revela que todos los componentes están influenciados por experiencias pasadas.

La mayoría de los elementos son individualmente capaces de "aprender" tomando como referencia sucesos previos; y adaptarse a expectativas futuras. Ejemplos de ello son el personal de mantenimiento que intenta mejorar su desempeño a partir de métricas propias y los sistemas informáticos que ajustan en tiempo real los valores de las salidas en generadores eléctricos para satisfacer las diferentes cargas requeridas. Desde la óptica de los sistemas adaptables complejos una infraestructura es mucho más que la suma de sus componentes.

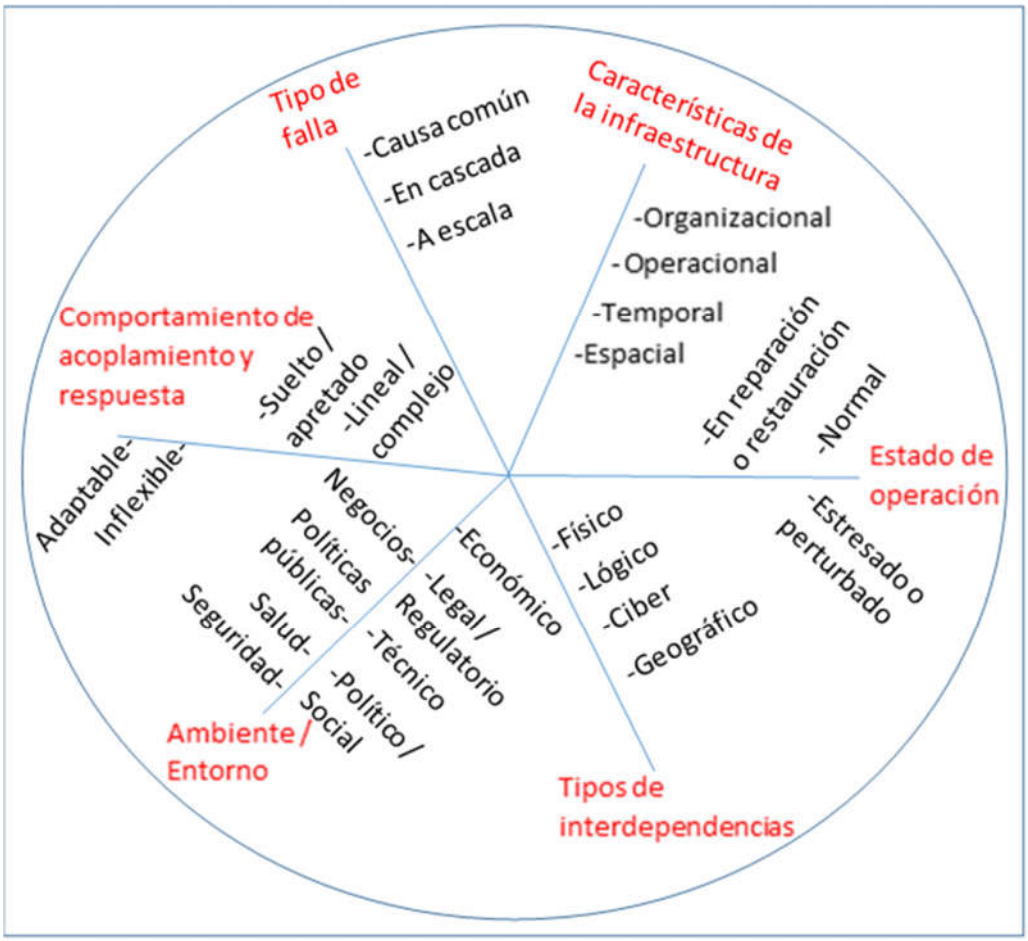


**Figura 4: Seis dimensiones para describir interdependencias entre infraestructuras**[31]

[31] Rinaldi S., Peeremboom J. y Kelly T., Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. Figure 1: Dimensions for describing infrastructure interdependencies. Pág. 12. Diciembre 2001. Traducido y adaptado al castellano. Obtenido el 01/09/2015 del sitio web: http://user.it.uu.se/~bc/Art.pdf

Una forma efectiva de investigar estos sistemas es verlos como una población de agentes interactivos. Un agente es una entidad con ubicación (espacio físico: región geográfica; o espacio abstracto: Internet; o ambos), capacidades (qué acciones puede llevar a cabo desde su ubicación) y memoria (cuáles han sido sus experiencias: las variables).

Se llega entonces a una definición más elaborada y específica de **dependencia**: es un vínculo o conexión entre dos (o más) infraestructuras, de modo que el estado de una infraestructura produce una influencia o se correlaciona con el estado de otra (u otras). En cuanto a los **tipos de interdependencias** mostrados en la Figura 4, son cuatro, para los cuales se proponen modelos de la industria eléctrica:

- Físico: Dos infraestructuras son físicamente interdependientes cuando el estado de cada una es dependiente de la salida de un material, producto o servicio de la otra. Por ejemplo: una planta de generación eléctrica a carbón y una red ferroviaria se relacionan físicamente dado que los trenes, señales, vías y centros de control necesitan de la electricidad generada para funcionar; mientras que la planta requiere de carbón, piezas de recambio y herramientas que son trasladados por dicho ferrocarril.
- Geográfico: Se produce cuando los elementos de múltiples infraestructuras están en estrecha proximidad espacial. Caso concreto: conductores de líneas eléctricas y fibras ópticas que comparten la misma postación (ubicación geográfica) para ofrecer respectivamente servicios de energía eléctrica, telecomunicaciones e infraestructuras de transporte.
- Ciber: Situaciones en que el estado de una infraestructura depende de la información transmitida usando mecanismos informáticos automatizados. El paradigma ciber está representado por los sistemas SCADA y EMS (*Energy Management System*, por sus siglas en inglés, traducido como Sistemas de Gestión de Energía) para el control de las redes eléctricas. Nota: desde el punto de vista de la administración mediante recursos informáticos, los EMS se dividen en tres segmentos: generación (GMS), transporte (TMS) y distribución (DMS).
- Lógico: Se trata de aquellas interdependencias cuyos mecanismos no son físicos, geográficos ni ciber. Es poco común hallar este tipo y para citar casuística pueden mencionarse sucesos en los cuales la oferta de generación eléctrica no alcanza a cubrir la demanda de los consumidores debido a decisiones políticas (monopolios) o falta de inversiones económicas (carencia de financiamiento por parte de los Bancos u organismos de crédito).

## La electricidad en el centro de la escena

Si bien no puede considerarse en forma aislada, la electricidad por sí misma posee un dinamismo y una versatilidad únicos. La evolución en cuanto a sus usos y aplicaciones ha logrado hacerla llegar hasta casi cualquier lugar en el mundo donde pueda tenderse un cable; aunque esto podría cambiar si se hace realidad el sueño de Nikola Tesla referido a la transmisión inalámbrica. La infraestructura que le otorga entidad como servicio público alimenta a otras actividades cuyos productos y servicios necesitan del fluido eléctrico para funcionar, nutriéndose de elementos que provienen de tales actividades.

La Figura 5 muestra ejemplos de interdependencias, centradas en la electricidad.

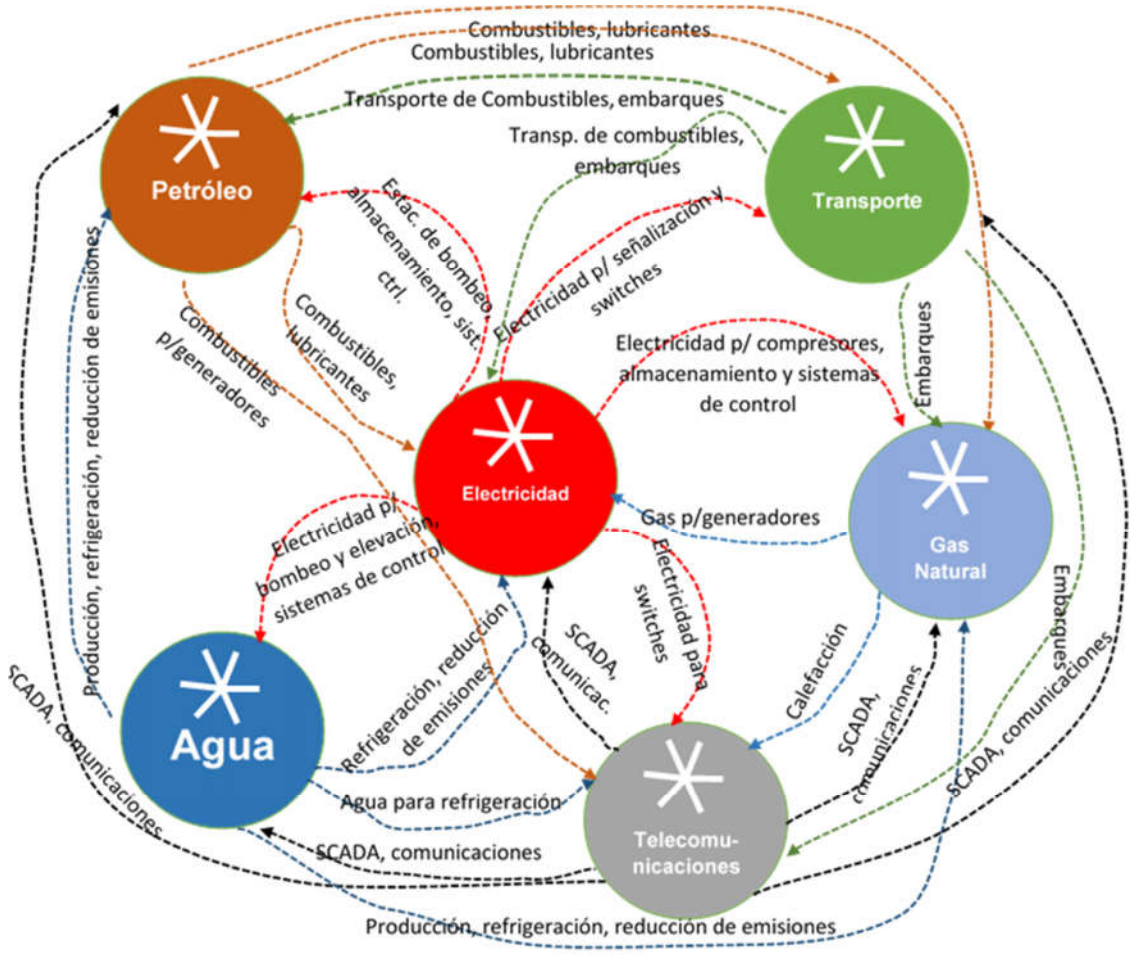


**Figura 5: Ejemplos de interdependencias en infraestructuras**[32]

[32] Rinaldi S., Peeremboom J. y Kelly T., Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. Figure 3: Examples of infrastructure interdependencies. Pág. 15. Diciembre 2001. Traducido y adaptado al castellano. Obtenido el 01/09/2015 del sitio web: http://user.it.uu.se/~bc/Art.pdf

Es tan amplio el nivel de inserción e incorporación de la electricidad en la vida diaria que en muchos casos sólo notamos su importancia cuando se produce un corte, aunque su duración sea de unos pocos minutos. El impacto de una interrupción en el servicio eléctrico se hace sentir con fuerza debido a la masificación de su uso. Un apagón puede tener consecuencias diversas: aumento de la natalidad (*baby boom*), vandalismo en las ciudades, indisponibilidad de otros servicios públicos, etc.

### Infraestructuras que dependen del servicio eléctrico

El concepto de dependencia visto anteriormente puede extrapolarse al caso de la electricidad. La Figura 6 muestra ejemplos de actividades en 8 infraestructuras. Esas actividades no pueden desarrollarse sin suministro de electricidad.

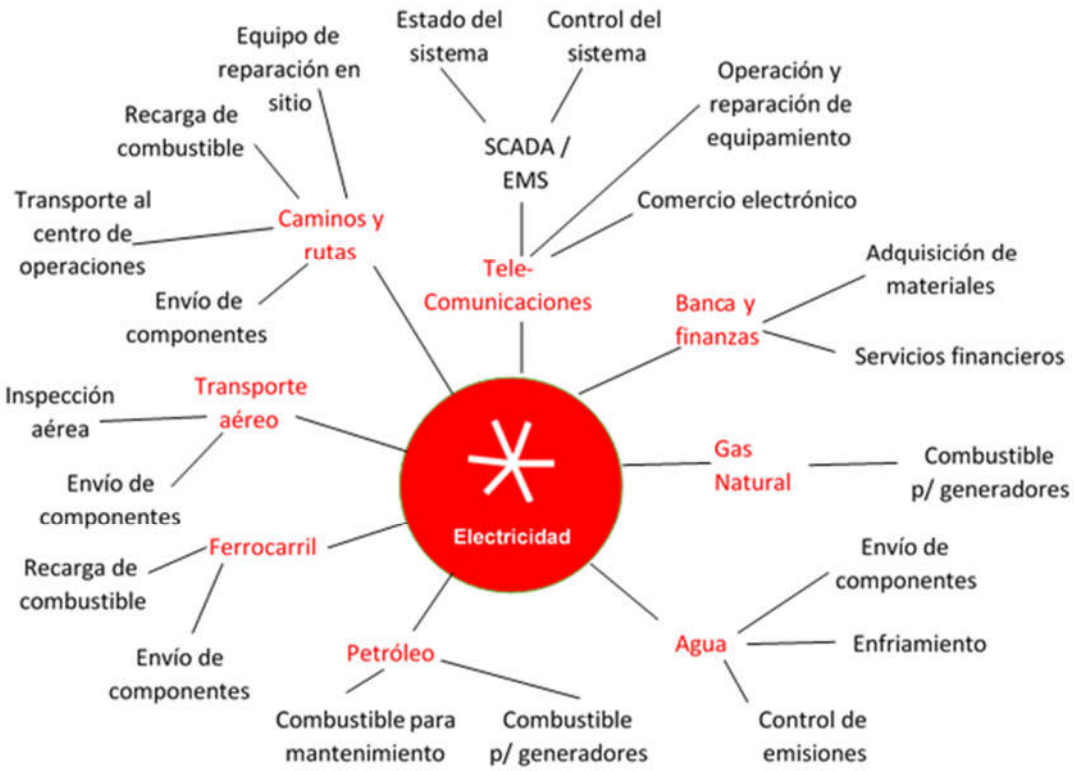


**Figura 6: Ejemplos de infraestructuras que dependen del servicio eléctrico**[33]

[33] Rinaldi S., Peeremboom J. y Kelly T., Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. Figure 2: Examples of electric power infrastructure dependencies. Pág. 14. Diciembre 2001.Traducido y adaptado al castellano. Obtenido el 01/09/2015 del sitio web: http://user.it.uu.se/~bc/Art.pdf

**Estado del arte y desafíos**

Con el paso del tiempo la identificación, el análisis y una mejor comprensión de las interdependencias entre infraestructuras ha cobrado una creciente relevancia. Los principales asuntos clave pasan por cambios económicos, marcos regulatorios, además de ciencia y técnica aplicadas que han alterado en forma radical las relaciones entre las diversas infraestructuras. Sumado a esto, la revolución planteada por las tecnologías de la información ha contribuido a multiplicar la cantidad de infraestructuras interconectadas, aportando por un lado complejidad y por otro una mayor centralización del control. Es poco probable que esta tendencia disminuya.

La búsqueda del funcionamiento continuo y fiable de las infraestructuras críticas otorga un papel preponderante a la electricidad como servicio público esencial. Ya sea que se la considere un engranaje de una gran maquinaria o se la sitúe en el rol de un producto / servicio imprescindible del cual depende infinidad de actividades, las preocupaciones en materia de seguridad y gestión del riesgo van en aumento.

# Capítulo III

## Sistema eléctrico en Argentina

*“Los adversarios tienen tres cosas de las que tu careces:*

*personal, tiempo y dinero”*

**Patrick Miller (@patrickcmiller)**

**en el Congreso #CCICon2, 2013**

*"Es hora de encontrar una alternativa al prefijo 'ciber-' antes de que*

*-como el término 'google'- se convierta en un verbo"*

**John B. Dickson**

**Director, Denim Group Ltd. 2015**

**Energía eléctrica. Definiciones.**

Los griegos denominaron con el término *élektron* a una resina orgánica con apariencia de piedra mineral conocida en castellano como ámbar, la cual tiene la particularidad de producir estática al ser frotada con un paño; atrayendo pequeñas partículas. Del vocablo original surgió la palabra electricidad, que alude en su forma básica a un flujo de cargas magnéticas. Más allá de los fenómenos y propiedades físicas, lo que interesa a los efectos del presente trabajo es la forma de manejar o dominar la misma y sus aplicaciones.

Considerando la acción deliberada del ser humano para aprovechar sus características, la electricidad se puede obtener artificialmente (producción o generación), trasladar físicamente (transmisión o transporte), entregar en lugares específicos (distribución) y en algunos casos conservar (almacenamiento). A escala industrial, tal como la conocemos actualmente, comenzó a finales del siglo XIX y su primer destino fue la iluminación eléctrica de calles y casas.

**Modelo eléctrico argentino. Breve historia reciente.**

La Ley 15336 de 1960 estableció el llamado Régimen de Energía Eléctrica, sentando las bases para el ordenamiento de la actividad. A la fecha se han publicado 58 Normas que la modifican y/o complementan. Las primeras áreas definidas, demarcadas y separadas fueron la Generación y la Transmisión, las cuales se mantenían bajo la influencia de la jurisdicción nacional. El hito principal consistió en calificarlas como Servicio Público. La Distribución y Subtransmisión eran de competencia provincial, con excepción de la Capital Federal (actual Ciudad Autónoma de Buenos Aires) y el llamado Gran Buenos Aires. El despacho nacional de cargas estaba a cargo de un ente conocido como Agua y Energía, con participación de las empresas HidroNor y SEGBA, entre otras. Las funciones de planificación y regulación eran ejercidas por la Secretaría de Energía de la Nación.

En el funcionamiento del servicio eléctrico se observaban algunas deficiencias[34]:

- Dispersión institucional en las empresas del sector.
- Fallas en el planeamiento estratégico.
- Politización de la gestión empresarial.
- Inexistencia de mínimos mantenimientos.
- Crisis de abastecimiento 1988/89.
- Ausencia del concepto costo - precio.

[34] Fundelec (Fundación para el desarrollo eléctrico). El sector eléctrico. Situación anterior a la transformación, Ley 15336. Sin indicación en cuanto a fecha de publicación. Obtenido el 07/01/2016 del sitio web: http://www.fundelec.com.ar/el_sector.htm

- Colapso de los planes de expansión.
- Interrupción en la relación Empresa Pública-Servicio Público.

A partir de 1990 se produjo una gran transformación en el sector eléctrico argentino. El Estado Nacional llevó adelante la privatización de parte de la prestación del servicio eléctrico y estableció su funcionamiento en tres etapas: generación (empresas que producen la energía eléctrica), transporte (firmas que trasladan la energía desde el lugar en que se genera hasta los centros urbanos), y distribución (organizaciones que llevan el fluido eléctrico desde los centros urbanos hasta los hogares de los usuarios, industrias, comercios, etc.). Varias Provincias aplicaron un modelo similar de privatizaciones en sus respectivas jurisdicciones, emitiendo las leyes correspondientes desde las legislaturas.

Se permitió la libre competencia para la generación y se liberó el precio de la electricidad a nivel mayorista. Por una cuestión de infraestructura y al no poder existir más de una empresa en una misma área de concesión; el transporte y la distribución tomaron la forma de monopolios. Debido a esto y en base a la experiencia del modelo norteamericano se crearon los Entes Reguladores: uno a nivel nacional: ENRE y al menos uno por cada Provincia, como manera de garantizar equilibrio entre las empresas y los usuarios del servicio regulado. Originalmente cada Ente Regulador gozaba de autarquía respecto al Estado, aunque en algunos casos fueron intervenidos debido a cuestiones coyunturales. Otro actor que apareció es la Secretaría de Energía de la Nación, entidad que también fue replicada en las Provincias.

En 1991 se publica el Marco Regulatorio Eléctrico (Ley 24.065). Las inversiones recibidas permitieron salir de los cortes programados que a diario interrumpían el servicio entre dos y cuatro horas y después apuntaron a mejorar la seguridad, la calidad y la potencia energética.

Las tres actividades principales fueron encomendadas a empresas públicas y privadas[35], tomando el Estado Nacional el rol de fijar las políticas del mercado y condicionar el accionar de las empresas mediante la regulación y las señales económicas. Los conjuntos de actores activos, como así también los Grandes Usuarios, son los únicos autorizados a participar del Mercado Eléctrico Mayorista (MEM) previa calificación como "Agentes del Mercado".

El MEM está administrado por CAMMESA (Compañía Administradora del Mercado Mayorista Eléctrico Sociedad Anónima) y asociado al SADI (Sistema Argentino de Interconexión), el cual cuenta con líneas en Extra Alta Tensión que se extienden por el norte

[35] Fundelec (Fundación para el desarrollo eléctrico). El sector eléctrico. El nuevo escenario. Sin indicación en cuanto a fecha de publicación. Obtenido el 08/01/2016 del sitio web: http://www.fundelec.com.ar/el_sector.htm

y centro del país. A partir de 2006 se integró el SIP (Sistema Interconectado Patagónico) que cubre la zona sur de Argentina. El MEM abastece al 99% de la demanda del sistema eléctrico argentino, (92% de zona norte y centro, 7% perteneciente al SIP, y 1% correspondiente a las demandas locales y rurales dispersas por todo el país que son atendidas por cooperativas).

### Actores

La figura 7 resume y agrupa los principales participantes del sistema eléctrico argentino.


**Figura 7: Actores principales del sistema eléctrico argentino**[36]

### Secretaría de Energía

A este organismo le corresponde fijar las políticas en materia energética. Esta repartición pasó a la órbita del Ministerio de Energía y Minería en diciembre de 2015, dividiéndose en varias entidades, una de las cuales cambió su denominación por Secretaría de Energía Eléctrica, con 5 subsecretarías en su estructura. De los 15 objetivos propuestos para la misma, los más relevantes son[37]:

1. Participar en la elaboración de las propuestas sectoriales y en la ejecución de la política nacional en materia de energía eléctrica, así como en el control de su

[36] Fundelec (Fundación para el desarrollo eléctrico). Adaptación. Actores del Sistema eléctrico argentino. Sin indicación de fecha de publicación. Obtenido el 08/01/2016 del sitio web: http://www.fundelec.com.ar/el_sector.htm
[37] Administración Pública Nacional. Decreto 231/2015. Fecha publicación 22/12/2015. Obtenido el 11/01/2016 del sitio web: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257246/norma.htm

ejecución, asistiendo al Ministro de Energía y Minería en el ejercicio de sus atribuciones de autoridad de aplicación del marco regulatorio eléctrico.

4. Asistir en la elaboración de la regulación de la actividad de transporte de energía eléctrica y de los procedimientos y financiamiento de la red de transmisión.
7. Asistir en la elaboración de las propuestas relativas a las normativas específicas para las distintas etapas de la industria eléctrica […].
10. Participar en la actuación que corresponda al Ministerio de Energía y Minería en relación con los entes u organismos de control de los servicios públicos que tengan una vinculación funcional con el área.

**ENRE**

El Ente Nacional Regulador de la Electricidad ejerce su función de contralor sobre la generación, el transporte y la distribución eléctrica en Ciudad Autónoma de Buenos Aires y Gran Buenos Aires. Las dos concesionarias del servicio son EDENOR y EDESUR. Es un organismo autárquico que tiene como referencia el Marco Regulatorio y los Contratos de Concesión para hacer valer sus atribuciones. La intervención del Estado se justifica dado que se trata de servicios públicos considerados monopolios naturales.

Entre los objetivos con los que debe cumplir el ente, se destacan los siguientes[38]:

- Proteger adecuadamente los derechos de los usuarios.
- Promover la competitividad en la producción y alentar inversiones que garanticen el suministro a largo plazo.
- Promover el libre acceso, la no discriminación y el uso generalizado de los servicios de transporte y distribución.
- Regular las actividades del transporte y distribución asegurando tarifas justas y razonables.
- Incentivar y asegurar la eficiencia de la oferta y la demanda por medio de tarifas apropiadas. Alentar la realización de inversiones privadas en producción, transporte y distribución, asegurando la competitividad de los mercados donde sea posible.

## Estados provinciales

En forma análoga, la estructura y funciones del ENRE se replican en las jurisdicciones provinciales para regular y controlar las áreas de concesión, garantizar la calidad del producto

[38] Ente Nacional Regulador de la Electricidad. ¿Qué es el ENRE? Sin indicación de fecha de publicación. Obtenido el 12/01/2016 del sitio web: http://www.enre.gov.ar/web/web.nsf/home

y del servicio, auditar la frecuencia y duración de las interrupciones, además de ofrecer a los usuarios una instancia para la defensa de sus derechos como consumidores, equilibrando la relación de fuerzas, especialmente entre las distribuidoras y los usuarios, en base a la legislación vigente, los reglamentos, el esquema regulatorio, los contratos, etc.

En muchas provincias las respectivas Secretarías de Energía asumen, en el marco de la temática eléctrica, funciones tales como la planificación y financiamiento de obras rurales, el desarrollo de tecnologías alternativas y sustentables, junto con la gestión de programas especiales (tarifa social, inclusión al consumo, subsidios a pequeñas empresas, supervisión de personas "electrodependientes" con enfermedades que exigen aparatología eléctrica, entre otras).

**CAMMESA**

El objeto de La Compañía Administradora del Mercado Mayorista Eléctrico Sociedad Anónima se halla definido en el artículo 3 de su estatuto[39]:

- El despacho técnico del Sistema Argentino de Interconexión (SADI) de acuerdo a lo previsto por la Ley 24.065 y sus normas complementarias y reglamentarias. A estos fines tendrá a su cargo: (a) determinar el despacho técnico y económico del SADI propendiendo a maximizar la seguridad del sistema y la calidad de los suministros y a minimizar los precios mayoristas en el mercado horario de energía ("Mercado Spot"); (b) planificar las necesidades de potencia y optimizar su aplicación conforme reglas que fije de tiempo en tiempo la Secretaría de Energía; (c) supervisar el funcionamiento del mercado a término y administrar el despacho técnico de los contratos que se celebren en dicho mercado.
- Representaciones, Mandatos y Comisiones: Podrá actuar como mandatario de los diversos actores del Mercado Eléctrico Mayorista (MEM) y/o cumplir las comisiones que aquellos le encomienden en lo relativo a la colocación de la potencia y energía; satisfacción de las curvas de cargas a los distribuidores y organización y conducción del uso de las instalaciones de transporte en el Mercado Spot; las gestiones de cobro y/o pago y/o acreditaciones de las transacciones que se celebren entre los diversos actores del MEM, incluyendo aquellas operaciones en las que la Sociedad actúe en nombre propio. A esos fines la Sociedad podrá actuar como agente de comercialización de la energía y potencia proveniente de importaciones y de emprendimientos binacionales, realizará el cálculo de las transacciones económicas

[39] CAMMESA. Estatuto de Compañía Administradora del Mercado Mayorista Eléctrico S.A. Sin indicación de fecha de publicación. Obtenido el 11/01/2016 del sitio web: http://portalweb.cammesa.com/pages/institucional/agentes/estatuto.aspx

y producirá la información necesaria para la facturación respectiva de los actos y operaciones que se realicen en el Mercado Spot del MEM.

- Actuar como mandatario del Estado Nacional como consecuencia de situaciones que pudieren generar riesgos de desabastecimiento y afectar la seguridad y la calidad habituales del sistema eléctrico. Tal actuación sólo podrá ser aceptada siempre que se reúnan en forma simultánea los tres requisitos establecidos y en la medida que tenga la transitoriedad necesaria para superar situaciones excepcionales que le dieron origen y no implique asumir la generación, el transporte o la distribución de energía eléctrica. En ningún caso el ejercicio del mandato podrá comprometer patrimonialmente a la Sociedad.
- Compra y Venta de Energía: Desde o hacia el exterior, realizando las operaciones de importación y exportación, así como la generada por entes binacionales.
- Servicios y Consultoría: la prestación de servicios relacionados con las actividades aludidas en los Párrafos I, II y III y en particular, sin que ello implique limitación, proveer servicios de consultoría en las áreas antedichas.

Desde el punto de vista práctico, CAMMESA administra la compra-venta de energía en el MEM, despachando el fluido eléctrico de acuerdo a las fuentes de generación, eligiendo en primer lugar las centrales más baratas, hasta cubrir la demanda en tiempo real. Su composición accionaria se divide en 5 partes iguales, controladas por las siguientes Organizaciones: AGEERA, ATEERA, ADEERA, AGUEERA, Secretaría de Energía de la Nación.

**Agentes del MEM**

Se trata de aquellos jugadores que integran el Mercado Mayorista Eléctrico, autorizados por CAMMESA para tomar energía eléctrica del Sistema Argentino de Interconexión y actuar en las etapas de creación, comercialización, traslado y entrega.

El sistema se inicia cuando un generador (1) fabrica energía, después un transportista (2) se encarga de llevarla a los centros urbanos donde es obtenida por las distribuidoras (3) que se ocupan de transformarla y adecuarla para entregarla en los suministros domiciliarios urbanos y rurales. Los grandes usuarios (4) son agentes que se encuentran directamente conectados a la red y tienen la capacidad de adquirir energía sin la obligación de tener una distribuidora como intermediaria. Casi siempre son grandes industrias, que deben cumplir con ciertos requisitos previos para acceder a esta categoría.

## 1. Generadoras

La generación implica transformar una forma de energía (térmica, hidráulica, nuclear, eólica, etc.) en energía eléctrica y es considerada una actividad de interés público, además de estar sujeta a competencia, en contraposición con la distribución. En cada central el precio es establecido de acuerdo a los costos de producción.

En Argentina las empresas que producen electricidad son en su mayoría privadas. El producto obtenido se vende en el mercado mayorista. Ninguna generadora posee más del 15% de la capacidad instalada total del sistema, lo cual propicia un ámbito de fragmentación para lograr un mercado competitivo.

En la actualidad existen 46 generadoras fijas en el territorio argentino. Bajo la normativa vigente puede ingresar al negocio cualquier empresa que cumpla con los requisitos de despacho, operación, seguridad y cuidado del medioambiente. La Asociación de Generadores de Electricidad de la República Argentina concentra a 40 firmas del rubro. La visión de AGEERA apunta a la evolución del desarrollo tecnológico que permite más y mejor eficacia en el servicio que brinda, junto con la implementación de políticas en el desarrollo que permitan mejorar la calidad de vida de los ciudadanos.

Según datos de CAMMESA, a diciembre de 2015 la capacidad de generación en el país era superior a los 33 000 MW (*MegaWatts*)[40]. A esa fecha, como referencia, la composición de las fuentes o balance energético estaba integrado en un 60,60% por petróleo y gas (ciclo combinado, turbinas-gas, turbinas-vapor y motores diésel), un 33,52% por fuerza hidráulica (represas), un 5,3% por tecnología nuclear (centrales atómicas), un 0,56% por aplicaciones eólicas (aerogeneradores) y un 0,02% proveniente de radiaciones solares (paneles fotovoltaicos). La alta dependencia de recursos no renovables derivados del petróleo plantea desafíos a mediano y largo plazo, sobre todo en lo relativo al desarrollo de fuentes sustentables.

## 2. Transportistas

La transmisión es el servicio que posibilita el transporte del fluido eléctrico desde su fuente de generación hasta redes locales a través de conductores o cables que soportan alto voltaje.

En el país las empresas transportistas tienen una concesión para transportar energía eléctrica desde el punto de suministro (generador) hasta el punto de recepción (distribuidora).

[40] CAMMESA. Informe Anual 2015. Pág. 30. Fecha de publicación: 02/06/2016. Obtenido el 24/10/2016 del sitio web: http://portalweb.cammesa.com/Documentos%20compartidos/Informes/Informe%20Anual%202015.pdf

La actividad de transporte en la Argentina está subdividida en dos sistemas: el sistema de transporte de energía eléctrica de extra alta tensión –que opera a 500 kV y transporta energía eléctrica entre regiones– y el sistema de distribución troncal –que presta un servicio público y, al ser un monopolio, opera a 132/220/330 kV, conectando generadores, distribuidores y grandes usuarios dentro de la misma región[41].

El 95% de las líneas de alta tensión son operadas por la empresa Transener.

La transmisión se considera un monopolio natural a nivel nacional, dadas las características de la actividad y la extensión territorial del país.

Una parte importante en cuanto a la función de las firmas transportistas consiste en informar al MEM sobre probables limitaciones en los sistemas, con una anticipación mínima de 8 años. Esto permite prever inversiones y medidas para garantizar el abastecimiento. Ante cortes de suministro, problemas de disponibilidad o deficiencias de calidad, las empresas de transporte son penalizadas por parte de la autoridad de aplicación. El valor de las multas guarda una relación de 100 a 1 respecto a la tarifa exigible en condiciones normales de operación.

La Asociación de Transportistas de Energía Eléctrica de Argentina (ATEERA) constituye una asociación sin fines de lucro conformada por 11 empresas con la responsabilidad de operar, mantener y supervisar de más de 28.000 km de líneas de alta tensión que conforman el Sistema Argentina de Interconexión (SADI).

### 3. Distribuidoras

La distribución permite la entrega de electricidad en el punto final de la cadena: el usuario, consumidor, cliente o usuario-cliente, previa reducción del voltaje a niveles requeridos por los contratos de concesión.

La comercialización del servicio tiene varias etapas: compra mayorista, contratación, venta, lectura periódica del suministro, atención al cliente, facturación, control de la calidad del producto y del servicio, cobro, cálculo de pérdidas técnicas, reducción del fraude por pérdidas no técnicas, etc.

Para tener una idea en cuanto a la dimensión y el alcance de toda la distribución en Argentina, el último reporte oficial disponible indica que a diciembre de 2012 existían

[41] Pampa Energía. Transmisión. Sin indicación de fecha de publicación. Obtenido el 13/01/2016 del sitio web: http://www.pampaenergia.com/sp/NUE_TRANSMISION.ASP

14.900.009 de acometidas[42] (puntos de entrega de electricidad en cada domicilio, a razón de uno por usuario del servicio), consolidados en los siguientes agrupamientos tarifarios: Residencial, Comercial, Industrial, Servicio Sanitario, Alumbrado, Riego, Ente Gubernamental Oficial, Establecimiento Rural y Otros. Esto impacta en al menos 33.000.000 de habitantes que gozan de los beneficios del servicio eléctrico conforme a la legislación y normativa vigentes. Aunque también debe mencionarse que existe aproximadamente un 10% de hogares, fundamentalmente carenciados, que no poseen acometidas normalizadas (llamadas conexiones directas), lo cual expone a riesgos de electrocución, atenta contra la disponibilidad del servicio, deteriora la calidad del fluido, y produce pérdidas no técnicas a consecuencia del fraude. Por ende, a los números expuestos deben sumarse 1.5 millones de suministros y 3.3 millones de personas.

En resumen: unos 16.5 millones de acometidas y 36 millones de personas dan cuenta del universo atendido y servido por el último eslabón de la cadena eléctrica.

ADEERA es la sigla de la Asociación de Distribuidoras de Energía Eléctrica de la República Argentina, la cual agrupa a 47 organizaciones del sector y explica el 97% de la electricidad consumida en el territorio nacional.

El presente trabajo descriptivo hace foco en la ciberseguridad industrial de este actor, representado por las distribuidoras, como la etapa postrera entre la creación de electricidad y su consumo por parte de los distintos usuarios, independientemente de las aplicaciones.

La actividad de distribución es una parte del proceso eléctrico y no podría existir por sí misma. Entre otros muchos factores, depende de la generación y el transporte previos. Un tramo del TFI va de lo general a lo particular, por lo que se hace necesario desarrollar este capítulo para situar al lector y contextualizar los próximos conceptos, especialmente el potencial impacto derivado de las brechas de seguridad sobre estas infraestructuras críticas. Cualquier tipo de sabotaje, fenómeno meteorológico o daño, independientemente de su origen, puede ser catastrófico para mucha gente y modificar sus hábitos, hasta el extremo de amenazar su medioambiente, su salud y en definitiva su vida.

## 4. Grandes usuarios

Son aquellos agentes habilitados a contratar energía eléctrica para consumo propio y en forma independiente. Por lo general se trata de grandes industrias, demandantes de altos

[42] Ministerio de Energía y Minería. Series históricas de energía eléctrica / Cantidad de usuarios total país 1991-2012. Fecha de publicación: 27/12/2013 Obtenido el 25/10/2016 de la URL: http://www.energia.gob.ar/contenidos/archivos/Reorganizacion/informacion_del_mercado/publicaciones/mercado_electrico/historicos/Serie%20cantidad%20de%20usuarios%201991-2012.xls

volúmenes de electricidad. Para ser alcanzadas por esta categoría, las empresas deben cumplir con los requisitos establecidos por la ley 24065, lo cual las habilita para contratar suministro sin pasar por una distribuidora y así disminuir sus costos de operación.

Dicha ley fija, entre otros valores, los topes de potencia y consumo, las necesidades técnicas y las condiciones contractuales.

Este agrupamiento se divide a su vez en dos conjuntos: GUMa (Gran Usuario Mayor) y GUMe (Gran Usuario Menor). La figura 8 grafica la relación de fuerzas entre la demanda de las distribuidoras y los grandes usuarios, según datos de 2015.

Por otro lado, AGUEERA (Asociación de Grandes Usuarios de Energía Eléctrica de la República Argentina) nuclea a 69 empresas de este tipo. Uno de sus principales objetivos es velar por la libre contratación, ejecución y cumplimiento por parte de los prestadores en lo atinente a contratos relativos a la actividad de sus asociados.

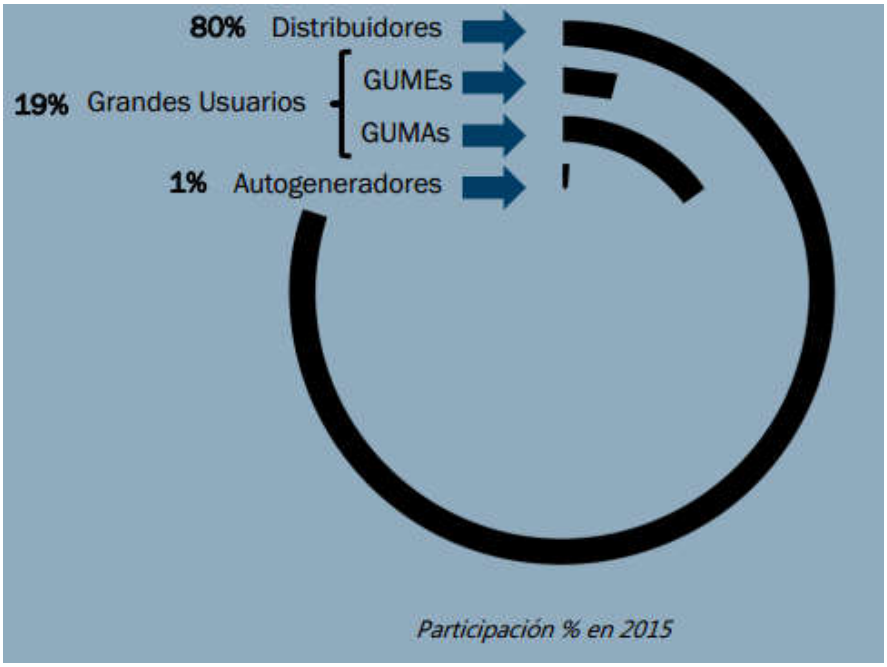


**Figura 8: Composición de la demanda anual 2015 por Tipo de Agente MEM**[43]

## Consumidores

Los usuarios hogareños del servicio eléctrico pueden ser categorizados en base a los niveles de consumo de energía eléctrica, expresados en kiloWatt / hora (kWh) por bimestre.

[43] CAMMESA. Informe Anual 2015. Pág. 17. Fecha de publicación: 02/06/2016. Obtenido el 24/10/2016 del sitio web: http://portalweb.cammesa.com/Documentos%20compartidos/Informes/Informe%20Anual%202015.pdf

Pueden hallarse muchas escalas para mensurar los valores. Por cuestiones de coherencia se menciona la utilizada por CAMMESA, que consta de 4 categorías de clientes residenciales (tomando como referencia un período bimestral):

- Menores o iguales a 1000 kWh
- Entre 1001 kWh y 1400 kWh
- Entre 1401 kWh y 2800 kWh
- Mayores a 2800 kWh

Siendo la electricidad un servicio público esencial y de acuerdo a la legislación vigente, los usuarios tienen la obligación de cumplir con todas las normativas para utilizar racionalmente el recurso. Además pueden exigir la defensa de sus derechos como consumidores y participar activamente en las Audiencias Públicas.

**Otros participantes**

Dadas las particularidades del mercado eléctrico en Argentina, se describen a continuación organismos adicionales relevantes en el campo eléctrico[44], que agregan su impronta y enriquecen al conjunto.

**CFEE**

El Consejo Federal de la Energía Eléctrica fue creado en el año 1960 por la mencionada ley Nº 15.336 y Decreto Reglamentario Nº 2073/60. Ha adquirido un papel relevante debido a su doble responsabilidad[45]:

- Administrar fondos específicos cuyo destino único es el sector eléctrico.
- Asesorar al Poder Ejecutivo Nacional y los Gobiernos Provinciales en lo referido a la industria eléctrica, los servicios públicos o privados de energía, las prioridades en la ejecución de estudios y obras, concesiones y autorizaciones, precios y tarifas del sector eléctrico. Aconsejar las modificaciones que requiera la legislación en materia de industria eléctrica

El CFEE está presidido por el Secretario de Energía de la Nación o el Subsecretario, en su reemplazo y dos representantes (un titular y un suplente) por cada una de las Provincias Argentinas. Estos últimos son propuestos por los Poderes Ejecutivos Provinciales y

[44] Fundelec (Fundación para el desarrollo eléctrico). Enlaces. Sin indicación de fecha de publicación. Obtenido el 26/10/2016 del sitio web: http://www.fundelec.com.ar/enlaces.htm
[45] CFEE. Perfil del Organismo. Sin indicación de fecha de publicación. Obtenido el 24/10/2016 del sitio web: http://www.cfee.gov.ar/perfil-organismo.php

designados por el Poder Ejecutivo de la Nación. Este Consejo compatibiliza las realidades de las diferentes jurisdicciones provinciales en lo relativo al desarrollo de políticas energéticas en este marco institucional.

**FUNDELEC**

Es el acrónimo para identificar a la Fundación para el Desarrollo Eléctrico, una entidad sin fines de lucro que nació en 1992, cuando el Gobierno Nacional decidió transformar el sector eléctrico a través de la Ley 24.065, privatizándolo parcialmente.

Nació por iniciativa de un grupo de 100 técnicos que habían pertenecido a Agua y Energía (empresa pública, del Estado Nacional, creada en 1947 y disuelta en 1996) autoconvocados, con el objetivo de contribuir al sano desarrollo del sector. Es una fuente de información técnica, objetiva y veraz para la promoción de la sustentabilidad en el ámbito eléctrico.

**FACE**

La Federación Argentina de Cooperativas Eléctricas agrupa a más de 240 cooperativas de servicios públicos en quince provincias, ejerciendo su representación en defensa de los principios y la acción cooperativa.

**Instituto Argentino de la Energía "General Mosconi"**

El propósito del IAE es propender a un aprovechamiento racional de los recursos energéticos y a un coherente desarrollo de sus actividades conexas que satisfagan los intereses de la población, destinataria final de los bienes y servicios que las mismas generan. Para el cumplimiento del objetivo general enunciado, el IAE realiza todas las actividades tales como:

- Investigación y estudios;
- Difusión y extensión;
- Asistencia y asesoramiento a organismos públicos, empresas e instituciones sobre las actividades de hidrocarburos, energía eléctrica, energía nuclear, energías no convencionales y alternativas, conservación y uso racional de la energía.
- Análisis de los aspectos tecnológico, económico-financiero, jurídico-legal, institucional y regulatorio, ambiental y social, en el marco de una adecuada planificación sectorial.

- Capacitación y especialización de recursos humanos.

**CACIER**

El Comité Argentino de la CIER es una asociación civil sin fines de lucro que aglutina a empresas y organismos del sector eléctrico argentino y tiene por misión vincularlos entre sí y con otras asociaciones similares de carácter nacional e internacional en general y en particular con la Comisión de Integración Energética Regional (CIER), entidad internacional que agrupa a los países sudamericanos, centroamericanos y España.

Sus objetivos son coordinar y hacer ejecutar las tareas que se le encomiendan en su condición de representante en la Argentina de la CIER, así como también promover y favorecer la integración del Sector Eléctrico Argentino mediante acciones que tiendan a lograr entre otras:

- Eficiencia de las organizaciones vinculadas al Sector Eléctrico en el país.
- Asistencia y cooperación técnica.
- Formación y capacitación de personal e intercambio entre empresas y países.
- Transferencia de conocimientos, informaciones, experiencias y estudios en los campos técnico, económico y jurídico.
- Desarrollo de proyectos con alcance nacional.
- Orientación y la coordinación de actividades de interés común.
- Adopción de especificaciones generales y normas técnicas.
- Utilización de técnicos y tecnologías nacionales y de la región.
- Fomento de la unidad estadística del país mediante un banco de datos.
- Promoción de proyectos que posibiliten interconexiones eléctricas con los Estados miembros de la CIER.

**Asociación Electrotécnica Argentina**

Organización sin fines de lucro fundada en 1913 por Jorge Newbery juntamente con otros 25 profesionales de la ingeniería. Su objetivo es fomentar el desarrollo de todos los campos de la electrotecnia en el país. Su función es el estudio e información de los aspectos teóricos de la Ingeniería Eléctrica, el establecimiento de Reglamentaciones y prácticas, según las reglas del buen arte, en todo lo referente a las aplicaciones tecnológicas y a los avances e innovaciones en este campo dentro de la República Argentina.

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

Desde su diseño original, la red eléctrica tradicional ha sido desplegada a lo largo y a lo ancho del territorio nacional, tratando de adaptarse a las exigencias de la sociedad civil, el comercio y la industria, recorriendo un camino poco planificado, sujeto a los avatares de la economía y la política, alimentando un círculo virtuoso de avances tecnológicos en prácticamente todas las actividades humanas. Sin una hoja de ruta precisa, de modo subyacente se persiguen los conceptos de progreso, innovación y mejora continua que realimentan el circuito, volcando sus aplicaciones al ámbito de la electricidad y profundizando su carácter de servicio esencial; aunque ello obliga a realizar inversiones estratégicas en recursos financieros, técnicos y humanos.

No obstante, las necesidades actuales y futuras del mercado eléctrico desnudan al menos tres implicancias[46]:

- Desde el punto de vista estructural, la red no ha evidenciado una transformación que le permita hacer frente a los nuevos requerimientos del mercado eléctrico. Hasta hace poco tiempo atrás, el principal paradigma dominante era la universalización del servicio. La excepción, debido a su criticidad, estuvo dada por la infraestructura de alta tensión.
- La red eléctrica del futuro reclama un salto cualitativo, no cuantitativo. Asuntos tales como el cuidado del medioambiente, la optimización del uso de los recursos energéticos, entre ellos la generación distribuida, y el cumplimiento de regulaciones más estrictas en cuanto a calidad del producto y del servicio; han dado origen al concepto “Redes Eléctricas Inteligentes” (*Smart Grids*).
- En base a la situación actual, la red del mañana será un “híbrido”, ya que a la red tradicional se le agregan progresivamente dispositivos electrónicos (mandos, sensores, medidores); vinculados mediante diversas tecnologías de comunicación a el fin de:
    - Centralizar la gestión de los elementos, vía automatización.
    - Usar la información, para provecho de los involucrados.
    - Permitir a las empresas una administración eficiente de sus activos.
    - Proveer herramientas a los usuarios para que gestionen sus consumos de manera racional.

[46] Asociación Electrotécnica Argentina. Redes Eléctricas Inteligentes. Fecha de publicación: Agosto de 2013. Página 7.

# PARTE 2

## Tecnología de la Información y Tecnología de Operación. Buenas prácticas, Normas y estándares.

## El universo SCADA.

# Capítulo IV

## Tecnología de la Información y Tecnología de Operación.

## Buenas prácticas, Normas y estándares

*"Existe una combinación de factores*

*que están redibujando dramáticamente las Tecnologías de Operación (TO).*

*Un mayor número de dispositivos de automatización industrial conectados a Internet*

*y la convergencia de las infraestructuras de TO con las de TI,*

*unido a la carencia de especialistas en seguridad,*

*hacen que una evaluación y mitigación precisas de los riesgos de seguridad*

*resulten cada vez más difíciles"*

**Robert Westervelt**

**Gerente de Investigación en Seguridad de la Información. IDC. 2016**

*"Cualquier rincón del planeta civilizado cuenta con infraestructuras*

*que resultan críticas para mantener el estilo de vida actual"*

**Tom Patterson (@TomTalks)**

**Director de Confianza, Unisys. 2016**

**"TITO": ¿Choque de planetas?**

Tal vez por su masificación, para el ciudadano de a pie acostumbrado a interactuar con herramientas informáticas, redes sociales y banca en línea no resulta raro escuchar el término "TI" y relacionarlo rápidamente a Tecnologías de la Información. Los medios de comunicación se han encargado de ponerlo en boga y hacerlo parte de la realidad cotidiana. En espacios educativos se habla con naturalidad de las "TICs", para abreviar Tecnologías de la Información y Comunicación, que son una parte de las TI. Una de las tantas aproximaciones a modo de explicación 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.

No tan conocidas, las "TO" representan a las Tecnologías de Operación propias del ámbito industrial, y pueden definirse desde dos perspectivas complementarias[47]:

- Tradicional: Son aquellas que integran la información, la interoperabilidad y la 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.

A continuación se consideran 4 factores para comparar las realidades de TI y TO.

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

**Tabla 3: Comparación entre factores de TI y TO**[48]

[47] CCI. CCI lanza una nueva serie de documentos sobre las tecnologías de operación inteligentes, "Smart OT". Fecha publicación 06/05/2016. Obtenido el 26/10/2016. URL: https://www.cci-es.org/web/cci/detalle-actividad/-/journal_content/56/10694/232182

[48] CCI. Curso taller "Aplicando ISA99 para proteger las infraestructuras industriales". Adaptado del Slide 3, titulado "Diferencias en Seguridad". Fecha de publicación 04/06/2015. Nombre del archivo: 03-0930-1030-IT-vs-OT-TALLERISA99.pdf.

La vertiginosa evolución de las TI les ha permitido irrumpir en los Sistemas de Control Industrial (SCI). El personal a cargo de TO no siempre está adecuadamente formado y entrenado en el manejo de las TI, no posee plena conciencia de los riesgos y problemas. Por otro lado, los gestores de TI desconocen los rudimentos de los sistemas industriales; tienen la falsa percepción de que los mismos son ajenos a sus funciones y responsabilidades, aunque los límites aparecen cada vez más difusos y en algunos casos los perímetros han dejado de existir.

Históricamente las implementaciones tecnológicas y la introducción de aplicaciones o programas informáticos (*software*) sobre sistemas industriales se focalizaban en tres aspectos: disponibilidad, funcionalidad y rendimiento, sin considerar ni mucho menos incorporar a la seguridad de la información. La línea de tiempo muestra en el pasado algunas postales a modo de ejemplo: sistemas aislados, redes de datos propietarias, interfaces de usuario en formato caracter (sólo texto y números, no se conocían ventanas, cuadros de diálogo ni gráficos de calidad), transmisiones en texto plano, “aplicaciones” construidas en planillas de cálculo con macros, etc. En general se echaba mano a la idea de seguridad por oscuridad, es decir creer que la protección más eficaz reside en el mero ocultamiento del diseño o los detalles, asumiendo que los posibles atacantes desconocen los mismos o, lo que es peor aún: carecen de habilidades, métodos y mecanismos informáticos para radiografiar el estado real de los recursos supuestamente bien encubiertos.

La misma línea de tiempo revela un presente caracterizado por determinados hitos: altos niveles de integración entre el universo de los SCI y los sistemas corporativos, procesos sostenidos de estandarización y convergencia en las comunicaciones (la norma *Ethernet* y el protocolo TCP/IP son paradigmáticos en este sentido respectivamente), predominio de interfaces y plataformas web, adopción masiva de la virtualización, entrada en vigencia de regímenes regulatorios y de cumplimiento legal, aumento de los ciberataques tanto aleatorios como dirigidos; crecimiento de las llamadas amenazas persistentes avanzadas (APT, *Advanced Persistent Threat*), cuya complejidad, sigilo y capacidad de permanencia plantean serios desafíos al futuro de la ciberseguridad industrial.

A la hora de intentar determinar las causas que motivan los desacoples entre TI y TO, los especialistas coinciden en tres probables fuentes[49]:

- La administración de ambos terrenos como si fueran compartimentos estancos.

[49] CCI. Curso taller “Aplicando ISA99 para proteger las infraestructuras industriales”. Fecha de publicación 04/06/2015. Adaptado de los Slides 4, 5 y 6. Fecha de publicación 04/06/2015. Nombre del archivo: 03-0930-1030-IT-vs-OT-TALLERISA99.pdf.

- La falta de atención hacia los canales de comunicación entre uno y otro dominio.
- La 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*). Ocurre que bajo determinadas circunstancias –casi siempre consideradas ilegales o que implican la comisión de un delito– es factible que alguien sin autorización trate de atacar y acceder desde Internet a una red corporativa. Si consigue ingresar, buscará uno de estos puntos de contacto e intentará usarlo como puente para llegar hasta el SCI, aunque éste no tenga vinculación con el mundo exterior.

**Estado de situación actual**

Al contrastar el estado de la TI tradicional a cargo de los sistemas informáticos empresariales y la TO que gestiona los SCI, los supervisores de cada grupo humano deben dialogar con el fin de alcanzar objetivos comunes. La visión clásica enfocada en marcar similitudes y diferencias ya no es suficiente, debe ser complementada y ampliada. De hecho, se ha sumado una tribu al juego: los profesionales de la seguridad informática y de la información. La realidad evidencia algunas tendencias interesantes, a saber:

- Incremento sostenido de los ataques dirigidos a sistemas corporativos y los basados en *malware*.
- Creciente nivel de interconexión entre a) sistemas de control y automatización industrial y b) redes corporativas. Este fenómeno es disruptivo, ya que debilita el paradigma por el cual muchos responsables de TO creen estar seguros a partir del aparente aislamiento de los SCI. Tal interconexión los expone a los mismos ataques de software diseñados originalmente para equipos de computación empresariales y de escritorio, en gran parte debido a la adopción del protocolo TCP/IP.
- Existencia de herramientas y servicios para buscar sistemas conectados y automatizar ataques se encuentran disponibles en Internet. El pionero es, sin dudas, Shodan ( https://www.shodan.io/; una captura de pantalla se muestra en la Figura 9).
- Complejidad en cantidad y tamaño de los socios y contratistas de los cuales depende una empresa. Tal condición dificulta sobremanera la aplicación de medidas de seguridad.

- Mayor protagonismo del factor humano. Las principales amenazas son los intentos de acceso por parte de atacantes aficionados, empleados descontentos o ex empleados.

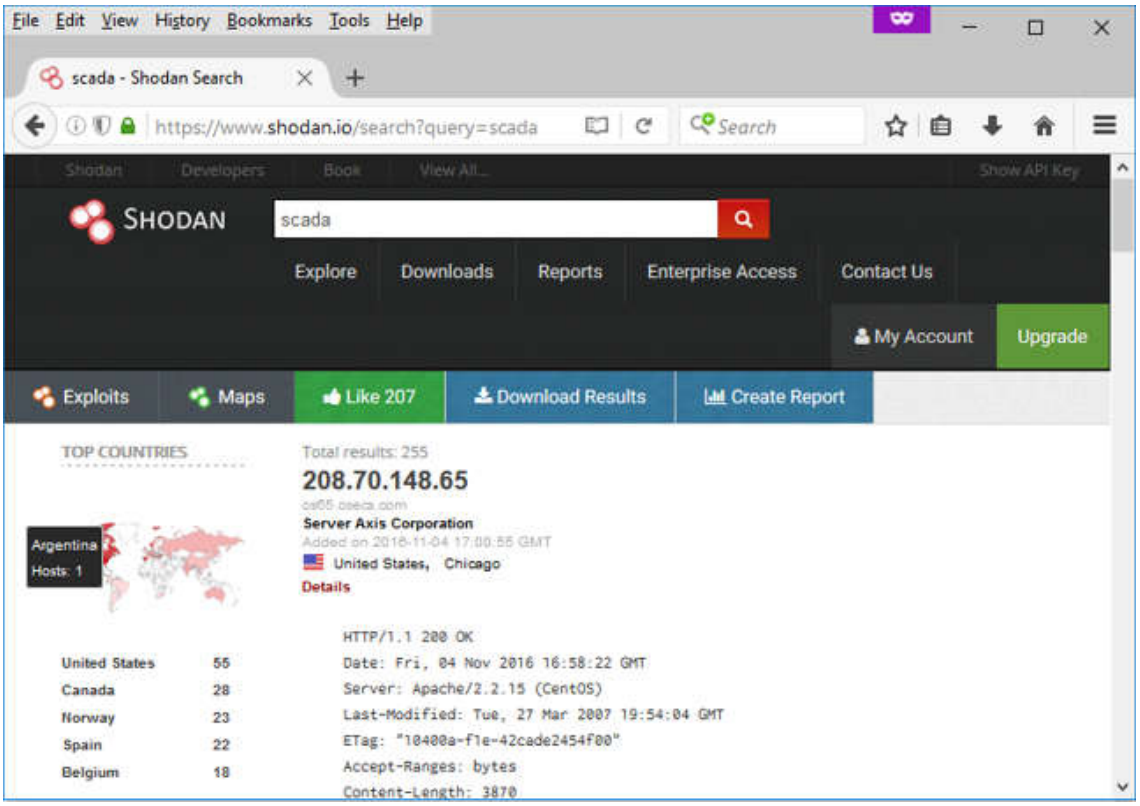


**Figura 9: Shodan en acción, búsqueda de la palabra "scada"**

### Falta de coordinación entre TI y TO, consecuencias

Mientras los ámbitos TI y TO se gestionen en forma separada e inconexa, el impacto potencial derivado puede tomar formas concretas:

- Interrupción de las operaciones. Como ya fue mencionado, para TO la principal prioridad es la disponibilidad, con todo lo que ello significa.
- Publicación de datos en medios o lugares indebidos.
- Cambios sin control en los procesos industriales, que afectan la calidad del producto o servicio, la funcionalidad de los programas informáticos, la capacidad de producción, etc.
- Sustracción y/o filtración de datos confidenciales a partir de accesos no autorizados.

- Daños en el equipamiento por mala configuración de parámetros funcionales.
- Incumplimiento de disposiciones legales, ordenanzas o reglamentaciones.
- Lesiones físicas, accidentes laborales, incidencia sobre la salud pública.
- Materialización de amenazas sobre infraestructuras críticas y la seguridad nacional.
- Afectación de la imagen y la confianza de las organizaciones ante los ciudadanos.

**Carencias más comunes en Tecnologías de Operación**

El CCI identifica las fallas de seguridad[50] que se repiten con más frecuencia en el mundo industrial:

- Escasez de dispositivos dedicados al control de tráfico en las redes de datos. Lo usual es hallar un firewall que se encarga de establecer una separación básica entre la red corporativa y la zona desmilitarizada (DMZ) correspondiente a la supervisión.
- Cuando existen, los procesos de filtrado en las redes de datos no son consistentes y no se establecen en los diferentes niveles.
- La seguridad por oscuridad se encuentra embebida en algunos integrantes de TO, lo cual dificulta analizar cuestiones tales como:
    - Cualquier sistema o protocolo industrial puede ser interpretado o decodificado mediante ingeniería inversa. La documentación generalmente se halla en Internet.
    - Los sistemas de control son similares a los de TI.
    - Ciertos ataques, como la denegación distribuida de servicios (DDoS), pueden ser llevados a cabo por personas sin conocimientos técnicos
- Hay un falso desinterés basado en creer que nadie se siente atraído para atacar a la organización, desechando argumentos válidos:
    - Ciertos ataques no apuntan a la empresa como fin, sino como medio para cometer otros actos ilícitos o no autorizados.
    - Determinadas intrusiones no son dirigidas, más bien buscan sistemas vulnerables para aprovechar sus recursos.
    - La empresa puede sufrir daños aunque el atacante no obtenga beneficios.

[50] CCI. Curso taller “Aplicando ISA99 para proteger las infraestructuras industriales”. Fecha de publicación 04/06/2015. Adaptado de los Slides 72 a 77. Fecha de publicación 04/06/2015. Nombre del archivo: 03-0930-1030-IT-vs-OT-TALLERISA99.pdf.

- Subsisten instalaciones que utilizan direccionamiento público para uso interno, algo habitual en implementaciones de algunos fabricantes y riesgoso:
    - Usado a veces por cuestiones de escala, menor esfuerzo y con la premisa falaz de homogeneizar el despliegue de los dispositivos.
    - No es raro que las redes de una planta se construyan en base a direcciones públicas, lo cual causa innumerables problemas y conflictos de conectividad con Internet.
- Persiste la errada fe en "sistemas inmunes", a prueba de todo. Ello no es cierto, por los siguientes aspectos:
    - Los sistemas de TO, no solo se encuentran frente a las mismas amenazas que los sistemas de TI, sino que existen programas maliciosos (*malware*) específicamente desarrollados para comprometer la seguridad de TO.
    - Resulta imperativo que los SCI incorporen medidas de protección: *firewall*s, antivirus, *antimalware*, etc. y sean incluidos en los procesos de gestión de parches. Ningún motivo justifica la ausencia de estas salvaguardas.
- Depositar la confianza en un dispositivo (*hardware*). Aquellos que todavía ven a la seguridad como un mero producto o servicio creen, a modo de ejemplo, que la sola existencia de un *firewall* "per se" es la panacea de la protección. Ello también carece de fundamentos porque:
    - Un "cortafuegos" debe estar correctamente configurado, gestionado y mantenido, con el objeto de adaptarse a nuevas amenazas.
    - Este tipo de aparatos, ¡no puede inspeccionar aquel tráfico que no lo atraviesa!

Por cierto, la mejor aproximación a la seguridad, tanto informática como de la información, consiste en considerarla y tratarla como un proceso, con todo lo que ello implica.

**Otros jugadores importantes**

La constelación se completa con participantes cuyo protagonismo no puede obviarse:

- Fabricantes de dispositivos industriales y sistemas de control.
- Integradores. Consultoras de ingeniería especializadas en el 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. Normalmente contratan a integradores para implementar soluciones y sistemas.
- 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. Estos cuerpos escritos se establecen con el objetivo de lograr niveles óptimos de ordenamiento en procesos y procedimientos.
- Usuarios finales. La "capa 8 del modelo OSI". Tendría poco sentido pergeñar infraestructuras, sistemas o programas informáticos sin el factor humano que los maneje. Por más alto que sea el nivel de automatización, las personas son el principio y fin de este circuito.
- El Estado. En argentina la forma de gobierno es representativa, republicana y federal. Ya sea en su poder ejecutivo (nacional, provincial y municipal), legislativo o judicial, su influencia alcanza sobre todo a los servicios públicos e infraestructuras críticas, tanto por acción como por omisión.

**Buenas prácticas, Normas y estándares: uniendo las partes**

Es lógico pensar que muchas de las problemáticas surgidas de una pobre o nula interacción entre los departamentos de TI y TO se podrían mitigar si ambos grupos trabajaran juntos. Ciertamente, además de promover el diálogo inter-organizacional, existen herramientas que contribuyen a tender puentes, estableciendo un lenguaje común, definiendo términos, especificando cuestiones técnicas, etc. Ellas surgen de al menos tres fuentes:

- Buenas o mejores prácticas. Una vez más, la castellanización de una expresión en inglés. En este caso: "*best practices*". En un sentido amplio aluden a los mejores métodos, los procedimientos más adecuados, o las acciones que se llevan a cabo en forma coherente y producen resultados de excelencia, superlativos, por encima del rendimiento esperado. Deben ser repetibles en contextos semejantes, por lo que se esperan resultados similares. Las buenas prácticas se extienden a un sinnúmero de disciplinas profesionales. Aquí se las considera en función de la temática abordada.

- Normas. La palabra norma deriva del latín y se refiere a escuadra[51], una clase de regla utilizada por los carpinteros para marcar ángulos rectos. Son pautas establecidas para ajustar ciertas actividades. Cuando algo cumple con una norma, se dice que es normal, o está normalizado. Por el contrario, se habla de anormal o sin normalizar ante aquello que aparece como fuera de regla o medida.
- Estándares: El vocablo estándar se originó en el francés “standort”[52], integrada por “stand” (parado), y “ort” (lugar alto), donde los francos colocaban su bandera para que no la tomaran los enemigos en la época de las invasiones bárbaras. Es también el origen de estandarte. Los estándares son construcciones culturales; para este caso son gestionadas por entidades con autoridad técnica. Dictan patrones a seguir, condiciones mínimas a las que debe adherir un producto o servicio con el fin de ser eficaz, positivo, útil y/o confiable.

Habiendo detallado los conceptos previos, se presentarán brevemente 4 normas, las cuales a mi criterio resultan las más representativas y de mayor adopción a nivel mundial; yendo de lo general a lo particular, de lo industrial a lo eléctrico, con el hilo conductor impuesto por la ciberseguridad y la seguridad de la información:

- ISA 99 / IEC-62443
- ISO/IEC 27001 y 27002
- Serie 800 de NIST
- NERC

Ciertamente existen otras, tales como ETSI, IASME, RFC 2196, ISO 15408, ISO 38500, Standard of Good Practice, BS 27999, etc. que no se incluyen aquí por ser consideradas complementarias al tema competente en el presente TFI.

**ISA 99, del automatismo a la seguridad**

En el capítulo 1 se realizó una breve introducción a la historia de la *International Society of Automation*. El conjunto de Normas arrancó en 2005 con la serie ISA 95, mutando en 2007 a ANSI / ISA 99, mientras que en 2009 comenzó la transición a ISA / IEC 62443 con motivo de adecuar su nomenclatura a las exigencias de la *International Electrotechnical Commission*, para devenir a IEC 62443 en 2010. A partir de 2013 su masificación es notoria,

[51] ConceptoDefinicion. Definición de Norma. Sin indicación en cuanto a fecha de publicación. Obtenido el 05/11/2016 del sitio web: http://conceptodefinicion.de/norma/
[52] DeConceptos. Definición de Estándar. Sin indicación en cuanto a fecha de publicación. Obtenido el 05/11/2016 del sitio web: http://deconceptos.com/ciencias-sociales/estandar

en gran parte debido a la presencia de ISO (*International Organization for Standarization*) a nivel mundial. En Argentina el representante es IRAM (Instituto de Racionalización Argentino de Materiales, actualmente identificado como Instituto Argentino de Normalización y Certificación).

Los objetivos originales del comité ISA 99 fueron desarrollar y establecer estándares, informes técnicos e información relacionada que definirá los procedimientos para implementar SCI seguros, prácticas de seguridad y evaluaciones de desempeño. La Norma está dirigida a los responsables de diseñar, implementar o administrar los SCI. Esta guía también se aplica a usuarios, integradores de sistemas, profesionales de la seguridad, fabricantes y vendedores. El fin de ISA 99 es mejorar la confidencialidad, integridad y disponibilidad de los componentes o sistemas utilizados para la automatización y el control industriales; proporcionar criterios para adquirir e implementar SCI seguros. El cumplimiento de las directrices ISA 99 tiene por norte asegurar las prestaciones, ayudar a identificar y abordar las vulnerabilidades y reducir el riesgo de comprometer información confidencial o causando degradación o falla del equipo de proceso bajo control.

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

Resumiendo el espíritu de esta normativa, la misma se basa en dos ideas bien concretas[53]:

- Zonas de seguridad (*security zones*). Conjunto de activos, tanto físicos como lógicos, que tienen en común ciertos requisitos de seguridad. Una zona establece un borde lógico o físico para delimitar claramente los agrupamientos y separar los componentes internos de los externos.
- Conductos (*conduits*). Son puentes de comunicación entre dos zonas de seguridad. Brindan las funciones de seguridad que permiten a dos zonas comunicarse de forma segura. Toda comunicación entre zonas diferentes ha de efectuarse mediante un conducto.

Los documentos generados desde 2007 fueron elaborados por diferentes grupos de trabajo. A continuación, lo nombres y la cronología:

- ANSI/ISA-99.01.01-2007 *"Security for Industrial Automation and Control Systems: Concepts, Terminology and Models*". Sienta las bases a usar a lo largo de la serie.

[53] CERTSI. IEC 62443: Evolución de la ISA 99. Definición de Norma. Publicado el 25/08/2015. Obtenido el 06/11/2016 del sitio web: https://www.certsi.es/blog/iec62443-evolucion-isa99

- ANSI/ISA-TR99.01.02-2007 "*Security Technologies for Manufacturing and Control Systems*". Informe técnico revisado periódicamente. Recoge las novedades del mercado. Contiene diversas herramientas de seguridad destinadas a los SCI.
- ANSI/ISA-99.02.01-2009 "*Establishing an Industrial Automation and Control Systems Security Program*". Último de la serie ISA99. Describe los elementos necesarios para implantar un sistema de gestión de la ciberseguridad y ofrece una guía para conocer los requerimientos de las partes que lo componen.
- ANSI/ISA-99.02.02 "*Operating an industrial automation and control system security program*". Nunca se publicó ningún borrador. Su objetivo se fijaba en la operación del programa de seguridad luego del diseño e implementación. Incluía aspectos como la definición de métricas y cuantificar la efectividad del programa.
- ANSI/ISA–99.03.xx "*Technical security requirements for industrial automation and control systems*". No llegó a iniciar su desarrollo. Abarcaba la definición de las características de los SCI que los diferencian de los sistemas de tecnologías de la información desde el punto de vista de la seguridad, definiendo requerimientos de seguridad únicos para estos sistemas.

A partir de 2010 se paralizaron los desarrollos ISA 99 y comenzaron a publicarse los trabajos con la denominación IEC 62443. La figura 10 muestra la evolución en el tiempo.

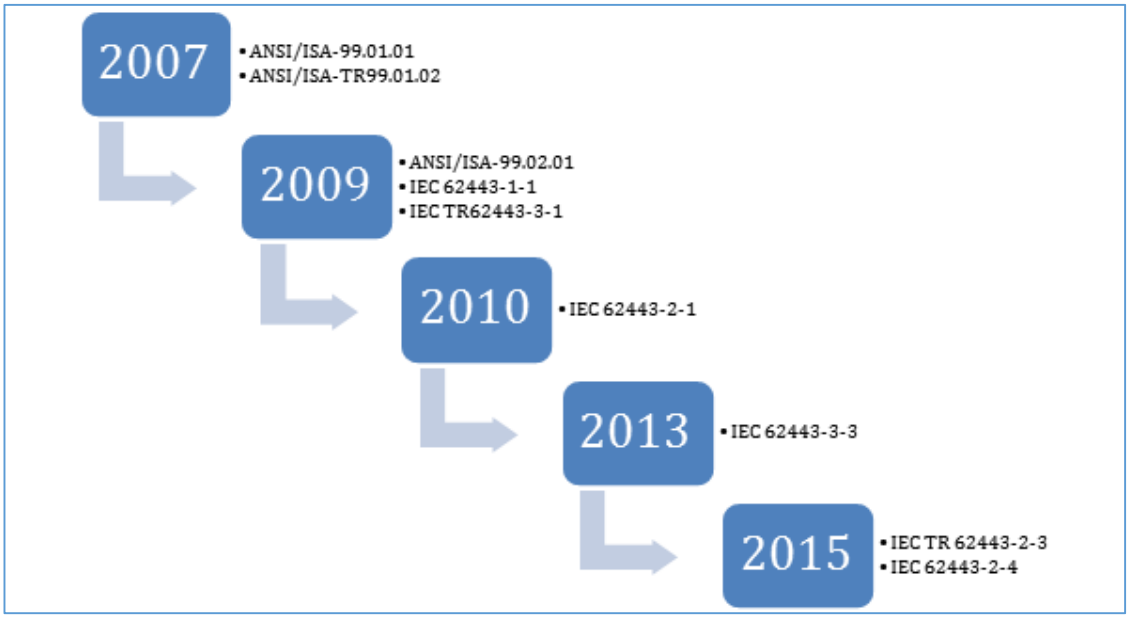


**Figura 10: Publicaciones ISA 99 e IEC 62443**[54]

[54] CERTSI. IEC 62443: Evolución de la ISA 99. Definición de Norma. Publicado el 25/08/2015. Obtenido el 06/11/2016 del sitio web: https://www.certsi.es/blog/iec62443-evolucion-isa99

**IEC 62443, un enfoque innovador e integrador**

Esta norma recoge la totalidad de las cuestiones planteadas por su antecesora, proponiendo una nueva estrategia y ampliando el campo de aplicación, desde los 4 documentos + 1 informe técnico que conforman ISA 99 hacia los 8 documentos + 5 informes técnicos en IEC 62443.

La principal novedad de este estándar es el paradigma de la defensa en profundidad, extendiendo sus alcances a todo el circuito: desde los fabricantes hasta los operadores.

Los 13 cuerpos se organizan según detalle, resumido en la Figura 11:

- IEC 62443-1-1 "*Models and Concepts*": Coincide con el primero de la ISA99, revisado para alinearlo a la nomenclatura y el resto de la nueva serie IEC.
- IEC TR 62443-1-2 "*Master Glossary of Terms and Abbreviations*": Glosario de términos y abreviaturas. Los conceptos pueden verse en la wiki de la norma.
- IEC 62443-1-3 "*System Security Compliance Metrics*": Métricas de cumplimiento en la seguridad de los SCI. En fase de borrador, abierto para comentarios.
- IEC TR 62443-1-4 "*Security Life Cycle and Use Cases*": Centrado en el ciclo de vida y ejemplos de uso para aplicaciones típicas en los SCI. Resta ser aprobado.
- IEC 62443-2-1 "*Requirements for an IACS Security Management System*": Recoge la información publicada por ISA 99 en el 2° documento. Se halla en revisión de los contenidos de los requerimientos para alinearlos con la familia ISO 27000.
- IEC TR62443-2-2 "*Operating a Control Systems Security Program*": Aborda la operación eficiente de un programa de ciberseguridad en los SCI. En desarrollo.
- IEC TR 62443-2-3 "*Patch Management in the IACS Environment*": Guía práctica para la gestión de actualizaciones, desde las ópticas del propietario y del proveedor de soluciones. Aún en fase de desarrollo.
- IEC 62443-2-4 "*Certification of IACS supplier security policies and practices*": Enfocado en la certificación de proveedores de productos de seguridad para los SCI. Adaptación de los requerimientos propuestos por el WIB (*Werkgroup voor Instrument Beoordeling*, de Holanda) en su documento "*Process control domain - Security requirements for vendors*". Está en desarrollo.
- IEC TR62443-3-1 "*Security Technologies for IACS*": Actualización de ANSI/ISA-TR99.01.02-2007. Descripción de tecnologías existentes para la protección de redes y SCI, exponiendo sus ventajas y limitaciones. En fase de revisión.

- IEC 62443-3-2 "*Security Risk Assessment and System Design*": Describe las ideas *security zone* y *conduit* propuestas en ISA99 y cómo se debe aplicar segmentación teórica en base a ellas. La segmentación técnica se detalla en la IEC 62443-4-2.
- IEC 62443-3-3 "*System Security Requirements and Security Levels*": Apunta a definir el nivel de seguridad del activo analizado, estableciendo relación con los 7 requisitos fundamentales expuestos en IEC 62443-1-1. El rendimiento y la disponibilidad no deben afectarse en el intento de dar cabida a los mismos.
- IEC 62443-4-1 "*Product Development Requirements*": Define el proceso de desarrollo a seguir por los nuevos dispositivos que se creen para los SCI, aunque también puede ser aplicado a los equipos ya existentes. Para ello hace referencia a procesos de desarrollo tanto para el *software* como para el *hardware*.
- IEC 62443-4-2 "*Technical Security Requirements for IACS Components*": Se corresponde con ANSI/ISA-99.03.03. Agrupa los requisitos técnicos para mejorar la seguridad en componentes, de forma individual, dentro de un SCI y la segmentación para restringir flujos de datos dentro de la red y entre redes.

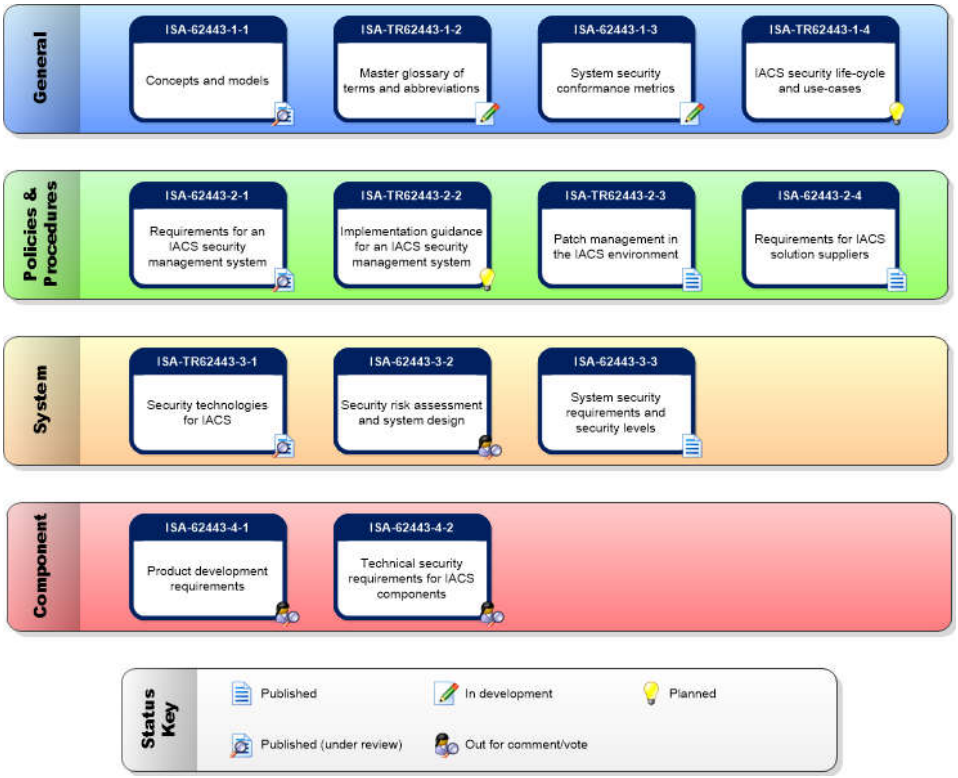


**Figura 11: Estado de las publicaciones IEC 62443 a setiembre de 2015**[55]

[55] ISA 99 Commitee. ISA99: Developing the ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security. Publicado el 04/09/2015. Obtenido el 06/11/2016 del sitio web: http://isa99.isa.org/ISA99%20Wiki/Home.aspx

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

Se trata de las dos primeras partes de la familia 27000, compuesta por 20 normas, basadas en el ciclo de Deming PDCA (*Plan, Do, Check, Act*) o bien Planear, Hacer, Verificar, Actuar. Originadas en el estándar BS 7799 de 2002 y luego de la transición a ISO/IEC 17799 en 2005, adoptan la actual denominación. Se dividen de la siguiente manera:

- 27001: (*Information technology - Security techniques - Information security management systems - Requirements*). Es la parte certificable y refiere a los requerimientos de un sistema de gestión de seguridad de la información (SGSI).
- 27002: (*Information technology - Security techniques - Code of practice for information security controls*). Es el código de práctica para los controles de seguridad de la información.

En cuanto a los objetivos, es la preservación de los establecidos por la tríada CIA (*Confidencility, Integrity, Availability*), los tradicionales: Confidencialidad, Integridad, Disponibilidad.

Dado que las Tecnologías de la Información se hallan embebidas en el mundo de las operaciones industriales, estas normas son aplicables a muchos procesos en los cuales la informática es indispensable. De hecho la Norma 27032 refiere a ciberseguridad, en general.

La versión vigente de las mismas data de 2013. En Argentina se titulan IRAM-ISO/IEC.

Si bien son complementarias, conviene establecer las particularidades de cada una:

- 27001:2013. Claves:
  - Establece los requisitos para implantar un SGSI, certificable.
  - Define las responsabilidades dentro del SGSI.
  - Sus dos pilares son la gestión del riesgo y la mejora continua.
- 27002:2013. Claves:
  - Detalla las buenas prácticas para gestionar la seguridad de la información.
  - Establece medidas con el fin de asegurar los sistemas de información.
  - Identifica los objetivos de control y recomienda los controles a implementar.

La organización documental abarca 5 capítulos introductorios, 14 dominios, 35 objetivos de control y 114 controles.

Capítulos introductorios:

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: procedimientos y responsabilidades; protección contra malware; resguardo; registro de actividad y monitoreo; control del software operativo; gestión de las vulnerabilidades técnicas; coordinación de la auditoría de sistemas
13. Seguridad de las Comunicaciones: gestión de la seguridad de la red; gestión de las transferencias de información
14. Adquisición de sistemas, desarrollo y mantenimiento: requisitos de seguridad en los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas
15. Relaciones con los Proveedores: seguridad de la información en las relaciones con los proveedores; gestión de la entrega de servicios
16. Gestión de Incidencias que afectan a la Seguridad de la Información: gestión de las incidencias que afectan a la seguridad de la información; mejoras
17. Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio: continuidad de la seguridad de la información; redundancias
18. Conformidad: conformidad con requisitos legales y contractuales; revisiones de la seguridad de la información

Debido a cuestiones de espacio no se detallan los objetivos de control ni los controles propiamente dichos. Estos últimos se enuncian en el Anexo A de la ISO 27001 y se desarrollan en profundidad en la ISO 27002. No todos son aplicables siempre, cada organización debe seleccionar aquellos que determine pertinentes, de acuerdo al tipo de negocio; diseñar sus propios procesos e implementar las salvaguardas correspondientes. Por lo general las normas dictan “qué” hacer, mientras que a las organizaciones les cabe el desafío de establecer “cómo” hacerlo.

**Serie 800 de NIST**

El NIST (*National Institute of Standards and Technology*) depende del departamento de Comercio de los Estados Unidos. Promueve la innovación y la competencia en el país del norte a través de avances en disciplinas asociadas a metrología, normas y tecnología, vehículos para mejorar las actividades económicas y la calidad de vida.

De la profusa biblioteca de Publicaciones Especiales que este Instituto genera y mantiene, interesa la serie 800 sobre Seguridad de la Información; y dentro de ella los documentos 53 y 61:

- *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. La última revisión añade una guía para la lucha contra las nuevas amenazas e incorpora nuevos hitos de privacidad en el marco de referencia que utilizan las agencias federales norteamericanas. Sirve para hacer frente a los peligros internos, el riesgo de la cadena de suministro, los celulares, la computación en la nube y otros desafíos. Agrega un apéndice de Confidencialidad con pautas de implementación asociada[56].
- *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. Esta publicación proporciona orientación sobre cómo asegurar los SCI, incluyendo sistemas SCADA, Sistemas de Control Distribuido (DCS), y otras configuraciones de un SCI tales como Controladores Lógicos Programables (PLC). El documento ofrece una visión general de los SCI y topologías típicas de sistemas, identifica amenazas y vulnerabilidades propias de estos sistemas y proporciona contramedidas de seguridad recomendadas para mitigar los riesgos asociados. La revisión 2 incluye nuevas directrices sobre cómo implementar los controles de seguridad de TI tradicionales para adaptarse a los requisitos únicos de rendimiento, fiabilidad y seguridad en los SCI, y actualizaciones de secciones sobre amenazas y vulnerabilidades, gestión de riesgos, prácticas recomendadas, arquitecturas de seguridad, capacidades y herramientas[57].

[56] Blog Segu-Info. Nueva revisión de NIST SP 800-53: ciberseguridad para organizaciones. Publicado el 12/03/2012. Obtenido el 06/11/2016 del sitio web: http://blog.segu-info.com.ar/2012/03/nueva-revision-de-nist-sp-800-53.html
[57] NIST. SP 800-82 Revision 2. Guide to Industrial Control Systems (ICS) Security. Publicado en mayo 2015. Obtenido el 06/11/2016 del sitio web: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

## 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. Desarrolla y hace cumplir las Normas de Confiabilidad, evalúa la fiabilidad estacional y a largo plazo; monitorea el sistema de energía a granel. Educa, entrena y certifica al personal de la industria. El área de responsabilidad de NERC abarca Estados Unidos, Canadá, y una porción de Baja California, México. Es la organización de confiabilidad eléctrica para América del Norte, sujeta a la supervisión de la Comisión Federal de Regulación de Energía (FERC) y autoridades gubernamentales en Canadá. La jurisdicción de NERC incluye usuarios, propietarios y operadores del sistema de energía a granel, que sirve a más de 334 millones de personas.

Los programas afectan a más de 1900 empresas operadoras de sistemas de energía a granel, se basan en cuatro pilares:

- 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.

| **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 |

**Tabla 4: Estándares de ciberseguridad NERC CIP vigentes a noviembre 2016** [58]

[58] NERC.CIP Standards. Sin indicación en cuanto a fecha de publicación. Obtenido el 06/11/2016 de la página web: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Dentro de sus iniciativas, sobresale la referida a protección de infraestructuras críticas, llama CIP (*Critical Infrastructure Protection*), actualmente en versión 5 y aprobada en Noviembre de 2013, cuyo principal objetivo es ofrecer un marco para la ciberseguridad en el sistema de energía mayorista (*BES, Bulk Energy System*). La misma propone un total de 12 estándares, que pueden verse en la tabla 4, de los cuales 11 son exigibles en el territorio de influencia de la NERC, y 1 se halla pendiente de aprobación.

Al ser documentos aplicables en el ámbito eléctrico deben marcarse sus particularidades:

- Se identifica, describe y categoriza a los cibersistemas utilizados por el sistema mayorista eléctrico y sus activos asociados. La finalidad es evaluar los requisitos de ciberseguridad en función del impacto adverso producido por la pérdida, compromiso o uso indebido de tales cibersistemas. Se busca evitar situaciones de mala operación o inestabilidad del sistema a granel.
- Hay una definición taxativa sobre la existencia de perímetros de seguridad electrónica. A partir de su reconocimiento se avanza en proponer medidas de protección.
- Existe un énfasis especial en las lecciones aprendidas. Analizando casos concretos se estudian las implicancias de los incidentes y se revisan los estándares para determinar si es necesario actualizar los mismos.
- Resulta loable la presencia de un estándar dedicado a prevenir y detectar cambios no autorizados en los cibersistemas del sistema mayorista eléctrico, especificando los requisitos para gestión de cambios de configuración y evaluación de vulnerabilidades; otorgándoles valor como actividades de apoyo a la protección de las infraestructuras.

**Obtener lo mejor de cada buena práctica, Norma y Estándar**

A falta de normativa local específica, es mucho lo que se puede aplicar de las 4 expuestas. Resulta imperioso buscar y encontrar motivos de consenso entre los departamentos dedicados a TI y los que gestionan TO. Las buenas prácticas, Normas y Estándares, incluso aquellas propias de la TI tradicional, como CObIT, ITIL o CMMI; esperan.

Finalizando el capítulo, un párrafo sobre “el negocio”, como sinónimo de la actividad desarrollada por cada organización. Sin un conocimiento pleno del mismo resulta imposible dar tratamiento adecuado a la ciberseguridad industrial. Una empresa que distribuye energía eléctrica no está exenta de elaborar, mantener y probar planes de continuidad.

# Capítulo V

## El universo SCADA

*"Una de las cosas que siempre enfatizamos son los cinco controles básicos.*
*Un 80 u 85 por cierto de los incidentes a los que damos respuesta*
*quedarían mitigados si tales controles se pusiesen en marcha*
*y se supervisasen de forma periódica.*
*Este año añadimos uno nuevo que es segmentación de las redes.*
*Los otros cuatro son:*
*reducción de privilegios de administración;*
*parcheo (tanto de sistemas operativos como aplicaciones);*
*y promoción de herramientas para administrar listas blancas de aplicaciones".*

***Ann Barron-DiCamillo (@Anni_BdC)***

***Directora, US-CERT. 2016***

"*Las organizaciones no pueden hacerse ciber-invulnerables;*
*pero pueden transformarse en ciber-resilientes*".

**Ricardo González**

**Responsable de Riesgo Operativo y Control de la firma Zurich España. 2016**

**Definiciones para SCADA**

Los conceptos relacionados con los Sistemas de Supervisión, Control y Adquisición de Datos; a veces citados como “Sistemas para Control de Supervisión y Adquisición de Datos” o “Sistemas de Control con Supervisión y Adquisición de Datos”, pueden ser tan amplios o acotados como sea necesario.

Analicemos algunos:

- Se trata de una aplicación *software* diseñada para funcionar sobre ordenadores en el control de producción, proporcionando comunicación con los dispositivos de campo (controladores autónomos, autómatas programables, etc.) y controlando el proceso de forma automática desde la pantalla del ordenador. Además provee toda la información que se genera en el proceso productivo a diversos usuarios, tanto del mismo nivel como de otros supervisores dentro de la empresa: control de calidad, supervisión, mantenimiento, etc. En este tipo de sistemas usualmente existe un ordenador, que efectúa tareas de supervisión y gestión de alarmas, así como tratamiento de datos y control de procesos. La comunicación se realiza mediante buses especiales o redes de área local. Todo esto se ejecuta normalmente en tiempo real, y están diseñados para dar al operador de planta la posibilidad de supervisar y controlar dichos procesos. Los programas necesarios, y en su caso el *hardware* adicional que se necesite, se denomina en general sistema SCADA[59].
- Es un mecanismo basado en computadoras que permite supervisar y controlar a distancia una instalación, proceso o sistema de características variadas[60].
- 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[61].

Las diversas aproximaciones muestran palabras que se repiten: sistemas, *software*, *hardware*, computadoras, datos, control, supervisión, gestión, local, remoto, interface, usuario, proceso, autómatas. A ello se agregan elementos específicos: señales de entrada y salida, realimentación (una señal de salida se usa como señal de entrada), sistemas complejos y sistemas expertos, interfaces hombre-máquina, bases de datos, controladores programables (lógicos y de automatización), unidades terminales remotas, sistemas de

[59] Automatas.org. SISTEMAS SCADA. Publicado el 02/03/2006. Obtenido el 12/11/2016 del sitio web: http://www.automatas.org/redes/scadas.htm
[60] Blog de Control de Accesos. ¿Qué es un sistema SCADA? Publicado el 23/04/2008. Obtenido el 12/11/2016 del sitio web: http://control-accesos.es/scada/%C2%BFque-es-un-sistema-scada
[61] Rodríguez Penin, Aquilino. Sistemas SCADA 2° Ed. 2007. Sección xiii y Pág. 19. Presentación / El Sistema Scada.

control distribuidos, sensores, actuadores, variadores, etc. Y en un mayor nivel de detalle aparecen los componentes propios del campo eléctrico, con foco en las particularidades de los SCADA implementados a nivel de la distribución de electricidad.

Antes de avanzar debo detenerme en una noción básica inherente a todo sistema de control: lazo abierto y lazo cerrado. Cuando hablamos de lazo abierto no existe realimentación pues una señal de salida no se convierte en señal de entrada; el proceso actúa sobre la señal de entrada y produce una señal de salida independiente de la primera, por ejemplo un temporizador. La idea de lazo cerrado aplica cuando la señal de salida depende de la señal de entrada, dando lugar a una realimentación; por ej. una válvula que se abre tras haberse excedido un umbral en los valores de presión y vuelve a cerrarse cuando los mismos caen por debajo del límite establecido. El cierre puede ser manual o automático.

Haciendo una simplificación introductoria, los principales módulos de un SCADA están constituidos por[62]: 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. Y lo más importante: operadores humanos.

a) La captura, recopilación y procesamiento de los datos se llevan a cabo por sensores, reguladores, registradores, etc.

b) El análisis y evaluación se realizan mediante clientes, buses de campo, controladores de procesos, servidores, etc. agrupados en 4 categorías:

b1) Interfaces hombre-máquina o HMI/MMI. Básicamente son pantallas para visualización de datos. En la actualidad se trata de monitores LCD o tipo LED.

b2) Unidad central o MTU. Gestiona el comando del sistema, las comunicaciones, la información, las estaciones remotas (RTU), el análisis, la impresión, la visualización, la seguridad, entre otras tareas.

b3) Unidades remotas o RTU. Son componentes que se hallan físicamente alejados del centro de control, aunque vinculados mediante enlaces de comunicación. A las RTU propiamente dichas se asocian los PLCs e IEDs.

b4) Sistema de comunicaciones. Su cometido es establecer el contacto y posibilitar el intercambio de señales entre los clientes – productores y los servidores – consumidores. Sobre los vínculos se ejecutan protocolos y mecanismos para el transporte de datos. Según el medio y la tecnología,

[62] Rodríguez Penin, Aquilino. Sistemas SCADA 2° Ed. 2007. Págs. 33-39. Arquitectura de un sistema Scada.

pueden ser líneas telefónicas, cable coaxil, multipar, onda portadora, fibra óptica, telefonía celular (ej. GPRS), radio (ej. VHF, UHF, microondas).

**Controladores lógicos programables, RTUs, computadoras industriales, PACs, IEDs**

Los mentados PLC (*Programmable Logic Controller*) o Controladores Lógicos Programables son, esencialmente, computadoras de propósito específico con capacidad de gestionar señales de entrada y salida, en tiempo real. Desde su diseño original se agregaron características especiales: tolerancia a rangos de temperatura ampliados, inmunidad a ruidos eléctricos y resistencia a vibraciones e impactos. Están pensados para operar en locaciones remotas, bajo condiciones climáticas a veces hostiles o bien con bajo o nulo mantenimiento. Algunos autores los llaman autómatas programables.

Sus funciones son variadas y han evolucionado con los años. Nos interesan especialmente las relacionadas con sistemas de control distribuido (DCS) y comunicación por red. Según Rodríguez Penin la incorporación de prestaciones mediante módulos de ampliación (especialmente los procesadores de comunicación) ha borrado la línea divisoria conceptual entre RTUs y PLCs. Hoy un PLC soporta todas las capacidades de una RTU.

A modo de desambiguación debe aclararse que existe una sigla idéntica referida a *Power Line Communications*, Comunicaciones a través de las líneas eléctricas.

Las computadoras industriales combinan el precio y la flexibilidad de una PC de oficina comercial con la durabilidad y el rendimiento de equipos industriales pesados. En algunos casos pueden asumir funciones de un PLC. En Argentina existe una iniciativa llamada CIAA (Computadora Industrial Abierta Argentina), una plataforma electrónica de *hardware* libre, multiprocesador, con una implementación propia del sistema operativo OSEK.

Los PAC (Programmable Automatic Controller) o Controladores Automáticos Programables incorporan tecnología industrial orientada al control automatizado avanzado, diseño de equipos para laboratorios y medición de magnitudes analógicas. Engloban un conjunto formado por una unidad central de procesamiento (controlador), módulos de entradas y salidas, y uno o varios buses de datos para interconexiones.

Este tipo de controlador combina eficientemente la fiabilidad de control de un autómata o PLC. junto a la flexibilidad de monitorización, cálculo y desempeño de una computadora industrial. Conjuga las prestaciones de varios dispositivos, transformándose en el último eslabón evolutivo de la automatización, agregando controles robustos como redes neuronales o lógica difusa. Los autómatas programables en general se hallan estandarizados mediante un conjunto de normas e informes técnicos aglutinados en la IEC 61131, que consta de ocho

documentos independientes: 1. Información general, 2. Especificaciones y ensayos de equipos, 3. Lenguajes de programación (son cinco los principales), 4. Guías de usuario, 5. Comunicaciones, 6. Seguridad funcional (actualizada en 2012), 7. Programación de control difuso, 8. Directrices para la aplicación e implementación de lenguajes de programación.

La tabla 5 recoge un cuadro comparativo de las características inherentes a diseño, arquitectura y prestaciones de un PLC, una PC estándar y un 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 |

**Tabla 5: Comparación entre características de PLC, PC estándar y PAC**[63]

El subgrupo restante se halla integrado por los Dispositivos Electrónicos Inteligentes o IED (*Intelligent Electronic Devices*), denominados también como periféricos inteligentes. Su singularidad reside en que cuentan con propiedades de decisión propia, a través de *software* embebido. Ejemplos: controladores de energía reactiva y transductores.

### Sistemas de Control Distribuido

Si bien poseen características similares a los SCADA en cuanto a funcionalidades, en los llamados DCS (*Distributed Control System*) la principal diferencia es que el lazo de control

[63] LogicElectronic. Qué es un PAC. Adaptado del Cuadro Comparativo. Sin indicación en cuanto a fecha de publicación. Obtenido el 20/11/2016 del sitio web: http://www.logicelectronic.com/BECKHOFF/Que%20es%20un%20PAC.htm

se cierra automáticamente, sin necesidad de intervención por parte de un operador humano. Dependiendo de factores tales como el tipo de actividad (manufactura o servicio), la ubicación y grado de dispersión geográfica de las locaciones, la fiabilidad de los vínculos de comunicaciones, el nivel de automatización de los componentes remotos; entre otros, se elegirá entre implementar un esquema SCADA o uno DCS.

La Tabla 6 ofrece una comparación entre ambos, basada en siete características.

| 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 |

**Tabla 6: Comparación entre SCADAs y DCSs**[64]

### SCADAs en el contexto organizacional

La ciberseguridad industrial ha reeditado el debate, los roles y la importancia del intercambio e interacción entre las Tecnologías de la Información (TI) y las Tecnologías de Operación (TO).

Una de las mejores y más claras representaciones jerárquicas de los sistemas industriales es la brindada por el especialista Maximilian Kon, Fundador y Director de la empresa WisePlant. Miembro del Comité ISA 99, ISA Secure y Homeland ICS-CERT, Kon propone un esquema de siete capas[65] (basado en la Norma ISA 99) cuyo detalle nos ayudará a visibilizar la ubicación de un SCADA en el marco organizacional y se encuentran graficados en la figura 12, a saber:

[64] Heffel, Walter. Comparación entre SCADAs y DCSs. Elaboración propia en base a contenidos de la entrada "What are the two major differences between DCS and SCADA systems?". Fecha publicación: 30/09/2014. Consultado el 20/11/2016.https://www.researchgate.net/post/What_are_the_two_major_differences_between_DCS_and_SCADA_systems

[65] Kon, Maximilian. ¿Qué hay de cierto, aciertos y desaciertos cuando se habla de convergencia IT/OT? Slide 2. Fecha pub: 29/06/2016. Obtenido el 26/11/2016. URL: http://wisecourses.com/wp-content/present/ConvergencialTOT/index.html

- En el nivel 0 se hallan los instrumentos de campo y mando que procesan datos y ejecutan funciones de control. Incluyen diagnóstico, autodiagnóstico, lógica de procesos, seguridad, comunicaciones inalámbricas, entre otras. Para dimensionar su crecimiento se menciona un ejemplo: en 2005 una refinería requería 10000 instrumentos de medición y mando, en 2015 necesitaba 30000 y hacia 2025 la misma usará entre 50000 y 70000. Dos tecnologías clave en esta instancia son los buses de campo y la comunicación inalámbrica implementadas mediante las especificaciones ISA 100 y Wireless Hart, distintas de los reconocidos estándares comerciales 802.11.
- En los estratos 1 y 2 se localizan los diferentes tipos de sistemas industriales, de control distribuido, de seguridad y SCADA. Los Sistemas de Automatización Industrial han evolucionado significativamente, ejecutan más funciones, son más veloces; capaces de procesar una cantidad creciente de entradas y salidas. Los *softwares* modernos han incorporado la ciberseguridad embebida o por diseño. Una particularidad actual de los SCADAs es que permiten la operación en modo dual: automático y manual. Se estima que las nuevas generaciones serán sólo automáticas.
- En la capa 3 aparecen los sistemas de gestión de la producción, de operación y de información industrial.
- La veta 3.5 se utiliza generalmente como lugar controlado de intercambio de datos entre Operaciones y los sistemas de información corporativos, típicamente regulados por la Norma ISA 95. En algunos casos se materializa a través de una zona desmilitarizada (DMZ, *demilitarized zone*). Si bien existen varias configuraciones posibles para este nivel, es de muy buena práctica evitar que los protocolos industriales crucen la frontera hacia la red corporativa y viceversa. Una de las principales funciones de los protocolos es vincular estratos que funcionan a distintas velocidades y anchos de banda.
- En el grado 4 se ubican las redes y los sistemas corporativos. Sus principales funcionalidades son el planeamiento del negocio y la logística.
- La capa 5 agrupa los sistemas para administración de la cadena de suministro, la planificación de recursos empresariales y las aplicaciones ofimáticas, correo electrónico, etc.

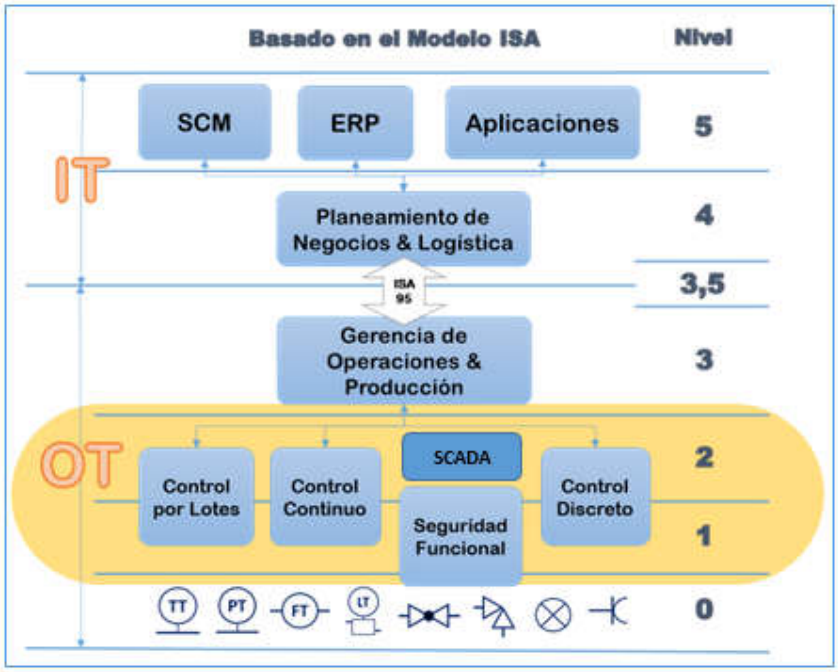


**Figura 12: Jerarquía de los sistemas industriales**[66]

### Partes principales del sistema eléctrico y sus misiones

Si bien se desarrolló un capítulo entero sobre el sistema eléctrico en Argentina, se resumen los 7 componentes básicos de la red y la finalidad principal de cada uno:

- Centros de generación. Producen la electricidad y elevan la tensión para transportarla.
- Líneas o conductores de alta tensión. Trasladan el fluido desde un lugar a otro.
- Estaciones transformadoras: subestaciones de transporte y distribución. Reducen el voltaje con el fin de adecuar su entrega de acuerdo al receptor.
- Líneas de distribución en media y baja tensión. Llevan la electricidad a los consumidores, mediante una acometida y un punto de medición.
- Suministros o instalaciones de los consumidores o clientes. Son los nodos finales de la cadena.
- Los centros de control de cada empresa generadora, transportista y distribuidora. Son gestionados por SCADAs.
- El centro de control principal nacional, operado por CAMMESA en la localidad de Pérez (oeste de Rosario). Mediante equipamiento *Bailey* de última generación se hace la gestión, supervisión y registración de eventos en la red, de manera centralizada

[66] Kon, Maximilian. Jerarquía de los Sistemas Industriales. Slide 2. Adaptación. Fecha pub: 29/06/2016. Obtenido el 26/11/2016. URL: http://wisecourses.com/wp-content/present/ConvergenciaITOT/index.html

**Funciones de un SCADA para distribución de electricidad**

Son tres los agrupamientos funcionales típicos para esta disciplina[67].

1. Aplicaciones de tiempo real y tiempo de respuesta crítico:
    a. Gestión de eventos en tiempo real. Adquisición de datos, conversión de unidades de ingeniería, detección, anuncio y registro de alarmas y eventos, chequeo de límites en valores analógicos, interacción con las estaciones de trabajo del operador, salida del control general y validación de cambio de estado, mantenimiento de la base de datos del sistema de tiempo real, monitoreo del funcionamiento, captura de datos para cumplir requerimientos de regulaciones y datos históricos.
    b. Procesos en aplicaciones específicas de tiempo crítico. Medición de volúmenes acumulados, generación de estadísticas sobre período de funcionamiento para cada equipo, cálculos: promedio para corriente, tensión, energía y potencia, número de maniobras, valores medios, máximos, mínimos y acumulados por períodos hora, día, mes y año.
    c. Soporte y aplicaciones en bases de datos de tiempo real. Cálculos en línea, valores derivados, utilitarios para guardar o transferir bases.
    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. Generación, navegación y edición de pantallas, presentación y manipulación de datos, acciones de control, presentación de alarmas, ingreso de parámetros o datos por el operador, generación de informes, mantenimiento del sistema.
    b. Interface del operador. Gestión de funcionalidades y configuraciones, con restricciones según perfiles predefinidos.
    c. Soporte a la interface. Comandos de control iniciados por el *software* y/o por la salida del operador, anuncio y registro de alarmas, actualización de pantallas, visualización de etiquetas sobre bloqueo de mandos en dispositivos, respuesta a requerimientos periódicos de las pantallas con datos en tiempo real.

[67] Enersa. Plataforma de gestión integrada, servicio de distribución de energía. Anexo C. Fecha pub: 06/06/2016. Págs. 10,11,12.

d. Registro de eventos cronológicos. Por lo general se mantienen tres libros de guardia: Uno para maniobras y actividades de transmisión; en otro se registran las novedades de subtransmisión y un tercero tiene como fin asentar los movimientos relativos a la distribución.

3. Almacenamiento de datos históricos:

   a. Captura de datos históricos. Recolección, lectura de valores en los dispositivos de campo.

   b. Bases de datos históricos. Archivado y recuperación de datos, almacenamiento de alarmas, eventos, acciones del operador, auditoria del sistema, tendencias de valores analógicos, acumuladores.

   c. Procesos de manipulación de datos históricos (aplicaciones específicas). Cálculos, tiempos de operación de dispositivos, estadísticas de comunicaciones, interface con la red corporativa, acceso y réplicas de los libros de guardia.

**Distribución eléctrica: SCADAs + Gestión Integral**

Las tendencias actuales en el campo de la distribución de electricidad ubican a estos sistemas con sus funciones tradicionales y nuevas características; en relación a otros que, conjuntamente, ofrecen servicios para la gestión integral del servicio público. Los engranajes de este gran mecanismo son:

- SCADA con arquitectura de n niveles, componentes distribuidos y modulares, conexiones vía bus de datos lógico (*middleware*). Multiplataforma operativa y de *hardware*, actualizable por nivel, escalable. Multitarea, multiusuario, multihilo (*multithreaded*). Redundante, altamente disponible y tolerante a fallas.
- GIS (*Geographic Information System*). El sistema de información geográfica ofrece al SCADA 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, componentes de las redes de comunicación, postación (postes) y alumbrado público, georreferenciamiento, 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. Entradas analógicas como mediciones de magnitud, voltaje, potencia activa y reactiva. Entradas de estado como situación de disyuntores, reconectadores,

conmutadores y bancos de capacitores. Administra la infraestructura de medición avanzada (Ej.: lectura remota de medidores correspondientes a grandes clientes).

- Módulo de informes. Al tratarse de un monopolio regulado, existe un contrato de concesión y un reglamento de suministro, entre otras exigencias, que definen los requisitos y condiciones para la prestación. Los principales destinatarios de los informes son los Entes Reguladores. El sistema correspondiente es capaz de generar reportes sobre calidad de producto, calidad del servicio técnico e interrupciones.
- 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.). Tiene una fuerte interacción con el SCADA y el GIS, con el fin de establecer el lugar físico de cada incidencia, dando tratamiento priorizado a los eventos y de esa forma mantener disponible el servicio público en óptimas condiciones.
- 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 y es compatible con los procesos de negocio de la empresa desde la recepción o construcción, puesta en servicio y explotación, hasta la baja. Operativamente, el EAM reporta desde la localización física de los activos, su condición y costos de explotación asociados; soporta la gestión de los recursos afectados a su operación y mantenimiento. Administra instalaciones, proyectos, obras, ensayos, calendario, órdenes de trabajo, incidentes, vehículos, personas, materiales, documentación, indicadores de desempeño, etc.
- Herramientas de administración. Posibilitan la modificación de los parámetros en el SCADA, con el objetivo de reflejar cambios operacionales, técnicos y organizacionales. Incluyen editores para bases de datos, pantallas e informes, y utilitarios para la gestión y monitoreo del *hardware* y las redes de comunicaciones.

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

El factor humano constituye una de las principales amenazas que se ciernen sobre cualquier sistema o instalación, y los SCADAs no son la excepción. El tipo de daño a infligir depende de muchos factores, lo cierto es que los medios informáticos e Internet ofrecen determinadas posibilidades, además de un engañoso manto de anonimato. Cabe a continuación realizar un análisis de los tres perfiles de atacantes probables a fin de aclarar algunas cuestiones.

Quizá por la influencia del cine o del periodismo no especializado, la palabra *hacker* es utilizada generalmente con un sentido y significado erróneos, al punto que la traducción al castellano realizada por la Real Academia Española la asocia a “pirata informático”, una idea total y groseramente equivocada. Proveniente del inglés, tiene varias acepciones. La que nos interesa y es actualmente la más difundida tiene su origen en el modismo *hack*, sinónimo de bromas inocentes entre los programadores integrantes del Laboratorio de Inteligencia Artificial en el MIT (Massachusetts Institute of Technology) a principios de los ‘60s. Desde el punto de vista de la seguridad informática hay tres grupos: *Black hat*, dedicados a intentos remotos de acceso, no autorizados. *Withe hat*, enfocados en depurar y arreglar errores en los sistemas. Y *Gray hat*, de dudosa moral. El uso adecuado y extendido del término alude a toda persona que implementa soluciones para cualquier sistema, de modo que un *software* o mecanismo puede utilizarse de maneras no previstas por sus creadores. Entiéndase *hackeado* como sinónimo de “modificado en sus fines para cumplir funciones diferentes”, antes que roto o manipulado para delinquir. Una última figura es la del *Ethical Hacker* o *hacker* ético, un profesional en seguridad de la información capacitado, entrenado y certificado ante organismos acreditados, preparado para realizar diversos tipos de análisis bajo condiciones controladas, previa contratación, firma de convenios de confidencialidad y plena comprensión de sus actividades y legislación vigente. Tiene la habilidad de ponerse en la piel de un intruso y pensar en formas de poner a prueba un sistema, un software o cualquier barrera protectora.

Aunque ha caído en desuso, la expresión *cracker* describe a una persona actuando desde la ilegalidad con el propósito de romper o quebrar (*crack*, en inglés) sistemas de seguridad. En sentido amplio, sus motivaciones pueden originarse en el lucro, la protesta política, racial, religiosa o el mero desafío. La finalidad es el daño, en forma de denegación de servicio, violación de propiedad intelectual, borrado o modificación de datos, afectación de la imagen pública de la víctima, incumplimiento de leyes, modificación del comportamiento del *software* o *hardware* con fines delictivos o lesivos, robo de secretos industriales, etc.

Un *insider* es un atacante interno, alguien que pertenece o fue parte de la organización y a su juicio tiene razones para, en algún momento o durante cierto lapso de tiempo, atentar contra la seguridad de la empresa o ente contratante. Sea por descontento, venganza o solamente probar sus conocimientos, es tal vez el perfil más peligroso, concreto y difícil de detectar. Corre con ventajas frente a *hackers* y *crackers* externos dado su conocimiento de las estructuras interiores, además de los puntos débiles. Se estima que cerca del 80% de los robos, fraudes, sabotajes e incidentes referidos a sistemas de información es generado por personal propio. El mayor énfasis puesto por las organizaciones apunta a implementar medidas para acotar el campo de acción de los *insiders*, tales como separar y rotar funciones,

dotar de conocimiento parcial al menos a dos personas con igual responsabilidad y conceder los mínimos privilegios a un empleado para que desarrolle sus actividades.

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

El riesgo más relevante y de mayor impacto al que está expuesta una empresa que distribuye electricidad es la interrupción del servicio, y sobre todo la imposibilidad de restablecer el mismo en un tiempo prudencial o, lo que es peor, en un tiempo indeterminado. A veces resulta inadmisible un corte de 2 minutos de duración, independientemente del motivo que lo originó. Si bien es cierto que la causa puede deberse a problemas en la generación o el transporte, la distribuidora evitará por todos los medios a su alcance cualquier tipo de interrupción. Es por ello que se implementan medidas que elevan el nivel de confiabilidad de los elementos de la red eléctrica: disposición mallada primaria y secundaria para transmisión con más de un paso para la alimentación de la carga, mecanismos que aíslan el elemento en falla con el fin de afectar la menor cantidad posible de clientes, transformadores de reserva para reemplazo ante averías, cables preensamblados e instalaciones subterráneas que reducen el peligro de electrocución en la vía pública, esquemas anillados que admiten la alimentación desde dos o más puntos, grupos de trabajo con tensión (TCT) que reparan y mantienen la red mientras los conductores siguen energizados, etc. Los sistemas SCADA actúan como los 5 sentidos que palpan, observan, degustan, escuchan y huelen cada incidencia, previniendo, reportando y actuando en consecuencia. En las áreas de concesión donde la regulación se aplica efectivamente, cada corte implica una multa onerosa cuyo monto debe ser pagado por la distribuidora en forma de devolución a los consumidores en concepto de mala calidad en el producto y/o servicio. También se aplican penalizaciones por eventos tales como sobretensión o baja tensión, reconociendo los daños a instalaciones, electrodomésticos, maquinaria de trabajo, etc. Aunque la mayoría de los riesgos son físicos, el creciente grado de automatización asigna cada vez más importancia a las amenazas cibernéticas, aumentando la superficie expuesta y la probabilidad de ciberataques.

La estructura y topología de una red eléctrica puede tomar diversas formas dependiendo de muchos factores. Su complejidad varía. Los tipos de ataques (físicos y ciber) también son numerosos, tantos como las combinaciones de eventos maliciosos para producir daños o alteraciones. Cabe señalar también que una adecuada implementación de un SCADA debe prever las contingencias que obligan a la operación manual parcial o completa del sistema, aunque ello obligue, por ejemplo, a garantizar el acceso físico a RTUs, PLCs, estaciones transformadoras, etc. mediante la movilización de los operadores de campo

correspondientes. Ello incluye variables de todo tipo: disponibilidad de vehículos frente a manifestaciones o piquetes, existencia de combustible que puede escasear ante un desastre natural, estado de los caminos en caso de inundaciones o tornados, funcionamiento de la telefonía fija, celular o radio para coordinar acciones, etc.

**El Estándar IEC 61850**

Se trata de una Norma específica sobre automatización de subestaciones eléctricas, organizada en 10 capítulos. Los temas principales son los requisitos generales del sistema, la gestión de proyectos de ingeniería y los requerimientos de comunicaciones. Incluye una propuesta referida a un modelo de datos definido mediante un lenguaje para descripción de subestaciones, a partir del cual se enumeran las capacidades de los IEDs. El modelado se realiza desde elementos llamados nodos lógicos que conforman la funcionalidad estándar de una subestación. A partir de clases y atributos de objetos se definen servicios e interfaces que se vinculan mediante protocolos, tales como MMS (Manufacturing Message Specification), GOOSE y Sampled Value. Una parte vital es el conjunto de pruebas de conformidad a aprobar por parte de un equipo o arquitectura para obtener la homologación de acuerdo al estándar. La primera versión data de 2005 y la última se publicó en 2013, conteniendo 3.364 páginas repartidas en 19 libros. Debe adquirirse, no es de uso libre.

**Referencia C37.240-2014**

Es una especificación que lleva el título *IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems*. La última versión fue publicada en enero de 2015 por la *IEEE Power and Energy Society* y auspiciada por los Comités *Power System Relaying* y *Substations*. Se trata de material pago, con costo.

A modo de resumen puede mencionarse que las medidas de ciberseguridad requieren lograr un equilibrio entre la factibilidad técnica y la viabilidad económica y que este balance responda a los riesgos que se espera se hallen presentes en una subestación eléctrica. Además, tales directivas deben diseñarse y aplicarse de manera que el acceso y el funcionamiento de las actividades legítimas no se vean obstaculizados, especialmente durante situaciones de emergencia o en procesos de restauración. Esta norma presenta un balance de los factores anteriores.

### El caso *BlackEnergy*

En diciembre de 2015 las empresas de servicio público eléctrico *Prykarpattya Oblenergo* y *Kyivoblenergo*, ambas con sede en Ucrania, sufrieron ciberataques. Los incidentes se materializaron mediante la introducción de un *backdoor* llamado *BlackEnergy*, el cual instala un componente identificado como *KillDisk*, cuya función es inutilizar el MBR (*Master Boot Sector*) o sector de booteo maestro en los equipos infectados, además de sobreescribir archivos en los discos rígidos y dejar inservibles las computadoras. En el primer caso el ciberataque provocó una interrupción que duró 3 horas, afectando unos 700.000 usuarios residenciales y cerca de 200.000 industrias. El segundo tuvo como consecuencia un corte de 6 horas y perjudicó a más de 80.000 consumidores hogareños, quienes dejaron de recibir fluido eléctrico usualmente suministrado por 30 subestaciones siniestradas. La restauración del servicio se llevó a cabo en forma manual, los SCADAs dejaron de operar.

Las investigaciones especulan con que los eventos fueron dirigidos y coordinados por un grupo ruso autodenominado *Sandworm Team*, movido por cuestiones de índole política. Previamente emprendieron ciberacciones contra empresas relacionadas con medios de comunicación, minería y ferrocarriles. La primera versión de *BlackEnergy*, también conocido como *DarkEnergy* data de 2008; la variante 2015 es más sofisticada, modular y con la capacidad de convocar componentes descargables para tareas puntuales. En los sucesos mencionados el vector de infección fueron archivos de Microsoft Office con macros maliciosas. Se combinaron técnicas, herramientas y explotación de vulnerabilidades; por ejemplo un *0-day exploit* de PowerPoint reportado bajo el código CVE-2014-4114.

Dentro de las metodologías usadas para infectar, la más rudimentaria resultó efectiva: un empleado recibe en su puesto de trabajo un correo electrónico conteniendo un archivo adjunto; un documento manipulado y destinado a modificar el comportamiento del equipo al que llegó. La empresa de seguridad CyS Centrum publicó capturas de pantalla correspondientes a *emails* en el marco de una campaña para diseminar *BlackEnergy*, donde se determina claramente cómo los atacantes suplantaron la dirección del remitente para que simulara pertenecer a la *Rada*, el Parlamento ucraniano. Esta modalidad de ingeniería social terminó de encadenar un conjunto de acciones tendientes a lograr la confianza del destinatario y que la persona siga las instrucciones. En la Figura 13 puede observarse la apariencia de un adjunto, una planilla Excel. En este caso, si la víctima ejecuta la macro termina infectada con la variante *BlackEnergy Lite*.

La evaluación pos mortem determinó 3 poderosas capacidades emanadas de los ataques: a) Apagar los sistemas críticos, en particular *software* industrial ELTIMA y ASEM, b) Acceder remotamente a los equipos infectados, c) Destruir archivos y evitar el re arranque.

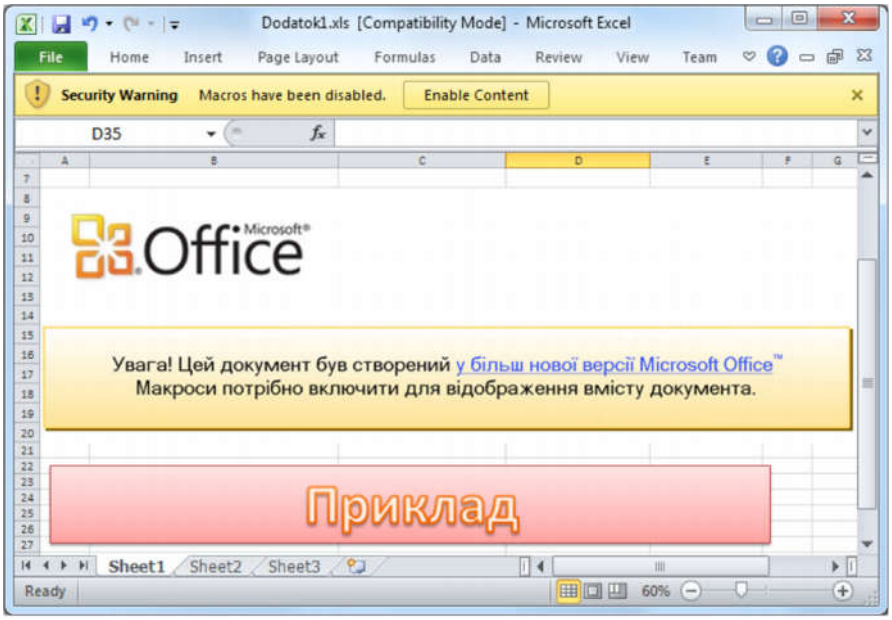


**Figura 13: Captura pantalla de archivo Excel con macros, vector de infección de *BlackEnergy*** [68]

Una investigación profunda de uno de los casos[69] reveló aristas inquietantes. El *malware* ingresó en computadoras del área IT, un ataque simultáneo afectó los sistemas telefónicos de otras empresas, los dispositivos de campo, RTUs y PLCs situados en las subestaciones siniestradas quedaron con su *firmware* y configuraciones corruptos o modificados, algunas estaciones de trabajo SCADA fueron accedidas remotamente sin autorización mediante conexiones VPN, los atacantes demostraron poseer gran conocimiento técnico sobre la actividad eléctrica y la operación de sistemas industriales, no se han revelado todos los detalles respecto al impacto real de los incidentes, el tiempo de recuperación fue mínimo en relación a la magnitud de los hechos, las principales fortalezas del sistema fueron la acción del grupo de respuesta formado por profesionales entrenados y los mecanismos de protección para evitar ingresos desde la red corporativa hacia OT.

El *software* malicioso fue un pequeño engranaje dentro de un plan estratégicamente desplegado. La correlación de eventos mostró intentos de acceso datados 9 meses antes de concretar el golpe, muchas de las acciones emprendidas fueron correctamente bloqueadas por mecanismos automáticos, la búsqueda de vulnerabilidades en los *firewalls* no tuvo éxito, ni siquiera ganar acceso a computadoras con perfil de administración. Medios alternativos como el robo de credenciales parecen haber sido una de las llaves. El único límite es la imaginación. 3 meses después los SCADAs no estaban aun plenamente operativos.

[68] WeLiveSecurity. Captura pantalla de archivo Excel con macros, vector de infección. Fecha pub: 05/01/2016. Obtenido 01/12/2016. URL: http://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/
[69] WisePlant. Caso de Estudio: Hackeo de la Red de Distribución Eléctrica en la zona oeste de Ukrania el pasado 23/12/2015. Fecha pub: 27/03/2016. Obtenido el 01/12/2016. URL: http://wiseplant.com/2016/03/27/analisis-del-hackeo-de-la-red-electrica-de-ukrania-el-pasado-23-de-diciembre-de-2015/

**Protección. ¿Por dónde empezar? Programa de Ciberseguridad Industrial**

Si bien lo descripto trata de situaciones extremas y diseñadas específicamente para dos empresas en particular, son una muestra nefasta del alcance que puede tener un ataque.

Un programa de ciberseguridad consiste en todas las acciones, actividades, tecnologías, metodologías, técnicas y esfuerzos realizados para proveer al dominio la seguridad necesaria o pretendida. Demanda es aquella generada por la inseguridad, vulnerabilidades y/o por los riesgos que las organizaciones deben asumir o enfrentar en sus operaciones. El mayor desafío para una empresa es identificar tal demanda y plasmarla en un plan, en este caso para mitigar las amenazas a la distribución eléctrica y a los SCADAs.

A continuación se describe a grandes rasgos una propuesta con 9 puntos[70] que deben estar incluidos en un programa de ciberseguridad, relacionando los dominios de TI y TO.

1. **Políticas**. En TI se desarrollan en torno a la información y su confidencialidad en un ámbito transaccional, mientras que en TO, para ser adecuadas y útiles es preciso que contengan y describan objetivamente, como mínimo: continuidad y disponibilidad de las operaciones industriales, evaluación de riesgos mediante una metodología, clasificación de proveedores, seguridad física, protocolos industriales, criterios para aceptación de pruebas y todas las cuestiones inherentes a los sistemas de control.
2. **Riesgos**. En TO se relacionan con el mundo físico: interrupción del servicio de distribución, afectación de la salud y la vida, etc. Las consecuencias son diferentes en comparación con el mundo TI, donde subyacen preocupaciones como la pérdida o robo de información y datos personales, cumplimiento de regulaciones, gestión de la infraestructura tecnológica, etc. Son dominios disímiles, por lo tanto poseen distintos riesgos. Un buen programa debe asumir las consecuencias y riesgos propios de TO.
3. **Análisis**. El inventario de los riesgos es una parte importante, debe ser actualizada periódicamente y acompañada del análisis correspondiente, a fin de contrastarlo con el nivel de aceptación fijado por la organización. Resulta imperioso que los profesionales encargados de llevar adelante esta tarea posean capacidades y habilidades acordes a los desafíos.
4. **Prioridades**. Aunque suene repetitivo, el peso de la disponibilidad en TO supera a las exigencias de confidencialidad en el campo TI. Aunque tampoco hay que dejar de considerar a la integridad. Es hora también de incorporar en

[70] Kon, Maximilian. ¿Qué hay de cierto, aciertos y desaciertos cuando se habla de convergencia IT/OT? Slide 5, adaptación. Fecha pub: 29/06/2016. Obtenido el 02/12/2016. URL: http://wisecourses.com/wp-content/present/ConvergencialTOT/index.html

TO a la autenticación, una característica ausente por diseño en las primeras generaciones de sistemas industriales.

5. **Tecnología**. Es el punto donde se presentan las mayores diferencias entre ambos dominios. La criticidad de TO no admite detener las operaciones para instalar un nuevo software, no es posible probar un parche en producción ni se aceptan latencias en las respuestas cursadas por determinados canales de comunicaciones. No es lo mismo una base de datos SQL relacional comercial de TI que una base de datos plana en TO. Las particularidades de TO deben ser conocidas, entendidas y difundidas en toda la organización.
6. **Vulnerabilidades**. La búsqueda de debilidades y pruebas de penetración, muy comunes y habituales en TI, no son viables en TO bajo los mismos criterios. Deben mensurarse cuestiones metodológicas, de ingeniería, configuración, conexión, interferencias, puestas a tierra y muchas otras puntuales del mundo eléctrico. Una simple búsqueda de puertos puede producir una denegación de servicio. Son requeridas competencias particulares, trabajo manual y gran conocimiento de los procesos industriales.
7. **Detección**. Las herramientas de detección y/o prevención no pueden ser intrusivas, un falso positivo o una disminución en los tiempos de proceso o respuesta no son opciones en instalaciones industriales; se necesitan homologaciones, pruebas y aprobaciones por parte de los fabricantes previo a su uso. En TI existe experiencia y desarrollo de herramientas para gestión de eventos: análisis de bitácoras, correlación, equipos de respuesta a incidentes, sistemas de prevención de intrusiones, etc.
8. **Mitigación**. Es la implementación de técnicas, herramientas, metodologías de diseño, configuración, monitoreo de eventos, etc. y toda acción encaminada a reducir los riesgos a niveles predeterminados por la empresa; y garantizar un estado razonable de seguridad en la prestación del servicio. En el ámbito TO los cambios son planificados, altamente gestionados y costosos.
9. **Protección**. Los recursos clave a proteger por TI son el conocimiento, información sensible, la continuidad del negocio, etc. mientras que TO busca preservar la disponibilidad, la seguridad física y de las personas, los procesos, el servicio público. Un programa de Cibserseguridad Industrial difiere significativamente de un programa de ciberseguridad de la información. Ante una misma demanda van a responder de maneras diferentes, aunque complementarias.

**Abordaje de la ciberseguridad en una empresa distribuidora**

El primer paso es realizar los diagnósticos interno y externo, con el fin de enumerar y detallas las amenazas específicas que acechan a la organización, con foco en las tecnologías de la operación, aunque sin dejar de lado a TI. Los resultados permitirán luego evaluar la situación actual y modelar escenarios basados en diferentes aspectos: regulatorio, político, de amenazas, en relación a Estándares y buenas prácticas, etc. Cada escenario se contrasta con metas o estados a los cuales la organización desea alcanzar. La comparación entre la actualidad y el futuro da como resultado un análisis de brecha (*gap analysis*) a partir del cual será necesario desarrollar un mapa de ruta y una estrategia para obtener los resultados planeados, dentro de un plazo razonable.

Una aproximación valiosa a considerar es el ES-C2M2 (*Electricity Subsector Cybersecurity Capability Maturity Model)*. La orientación proporcionada en esta publicación tiene por objeto tratar la implementación y gestión de prácticas de ciberseguridad asociadas con activos de tecnología de información y tecnología de operaciones, junto a los entornos en los que opera una empresa del sector eléctrico. No busca reemplazar o subsumir otras actividades, programas, procesos o enfoques relacionados con ciberseguridad que las organizaciones del subsector electricidad hayan implementado o tengan intención de implementar, incluidas actividades de ciberseguridad relativas a legislación, reglamentos, políticas o iniciativas de misión y visión, requisitos del negocio. Además, esta guía no es parte de ningún marco regulatorio ni está destinada al uso regulatorio. Más bien pretende complementar un programa integral de ciberseguridad.

ES-C2M2 comprende 10 dominios y se halla estructurada en 7 capítulos, además de 5 anexos. Los dominios son:

1. Gestión de riesgos. Establecer, operar y mantener un programa para identificar, analizar y mitigar los riesgos de ciberseguridad, incluyendo las unidades de negocio, subsidiarias, infraestructura interconectada relacionada y partes interesadas.

2. Gestión de Activos, Cambios y Configuración. Administrar los recursos de OT y de TI corporativos, incluyendo *hardware* y *software*, en consonancia con el riesgo para la infraestructura crítica y los objetivos organizacionales.

3. Gestión de Identidad y Acceso. Crear y administrar identidades para entidades a las que se les puede conceder acceso lógico o físico a los activos de la organización. Controlar el acceso a los activos de la organización.

4. Gestión de amenazas y vulnerabilidades. Establecer y mantener planes, procedimientos y tecnologías para detectar, identificar, analizar, gestionar y responder a las

amenazas y vulnerabilidades de ciberseguridad, proporcionalmente al riesgo para los objetivos de infraestructura de la organización (Ejemplo: críticos, informáticos, operativos).

5. Conciencia Situacional. Establecer y mantener actividades y tecnologías para recopilar, analizar, alarmar, presentar y utilizar información operativa y de ciberseguridad, incluyendo el estado y resumen de los otros dominios modelo, formando una imagen operativa común.

6. Intercambio de Información y Comunicaciones. Establecer y mantener relaciones con entidades internas y externas para recopilar y proporcionar información sobre ciberseguridad, incluyendo amenazas y vulnerabilidades, para reducir los riesgos y aumentar la resiliencia operacional, proporcionalmente al riesgo para la infraestructura crítica y los objetivos organizacionales.

7. Respuesta ante Eventos e Incidentes, Continuidad de Operaciones. Establecer y mantener planes, procedimientos y tecnologías para detectar, analizar y responder a eventos de seguridad cibernética y para mantener las operaciones a lo largo de un evento de ciberseguridad.

8. Gestión de la Cadena de Suministro y Dependencias Externas. Establecer y mantener controles para gestionar los riesgos de ciberseguridad asociados a los servicios y activos que dependen de entidades externas.

9. Administración de personal. Establecer y mantener planes, procedimientos, tecnologías y controles para crear una cultura de ciberseguridad y asegurar la idoneidad y competencia de los recursos humanos.

10. Gestión del Programa de Ciberseguridad. Establecer y mantener un programa de ciberseguridad empresarial que proporcione gobernabilidad, planificación estratégica y patrocinio para las actividades de seguridad cibernética de la organización de una manera que alinee los objetivos de ciberseguridad con los objetivos estratégicos de la organización y el riesgo para la infraestructura crítica.

**Ciber-resiliencia, en busca de nuevos paradigmas**

El genial Bruce Schneier ha acuñado su propia definición: “Cuando un sistema es capaz de soportar todo tipo de presiones sin cambiar su comportamiento, entonces es robusto. Cuando un sistema no es capaz de soportar más presiones, pero puede integrar cambios para disminuirlas y puede seguir adelante, entonces es ciber–resiliente”.

Probablemente sea este enfoque una de las claves a futuro para lograr que tanto los universos de Tecnología de la Información como Tecnología de la Operación (por ende los SCADAs) incorporen a la seguridad –en todas las acepciones aplicables– y a la Ciberseguridad Industrial como características intrínsecas. Ello les permitiría un mayor grado de preparación, protección y acceso a opciones ante ataques cada vez más sofisticados.

Un aporte concreto a esta visión es el documento "Ciber–resiliencia, aproximación a un marco de medición" de INCIBE, el cual no se analiza aquí por motivos de espacio, aunque se reproduce a modo de resumen la propuesta para la construcción de un marco integral de indicadores, basado en el *framework* del MITRE (Figura 14).

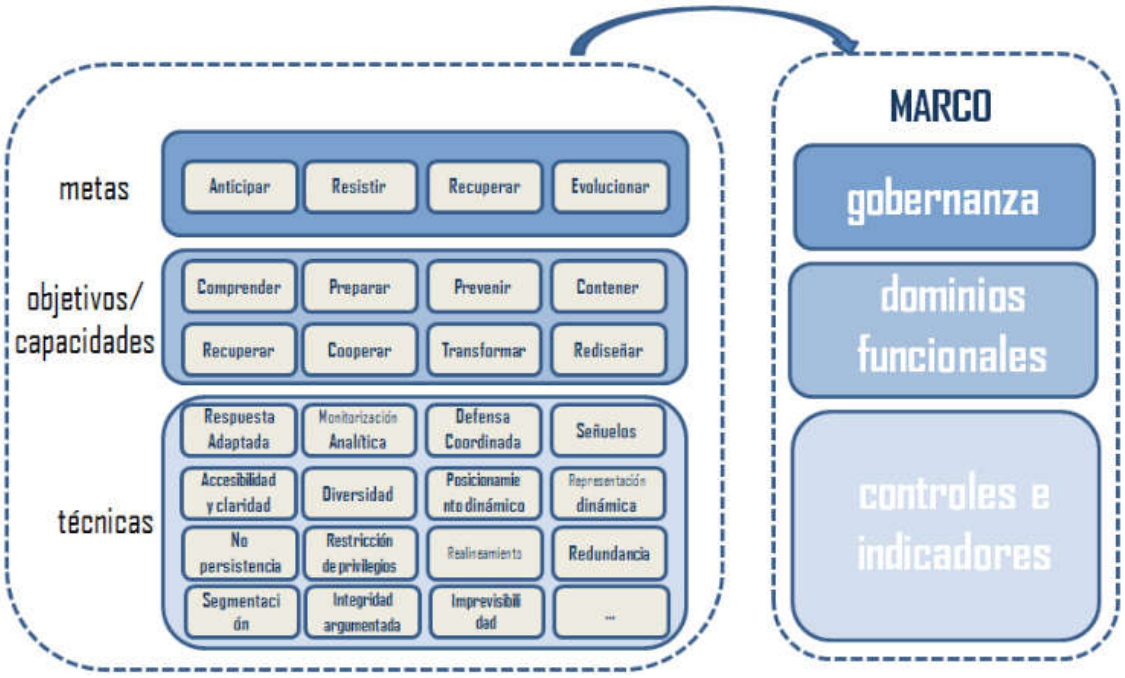


**Figura 14: Ciber-resiliencia, aproximación de la propuesta con base en el Framework del MITRE**[71]

[71] INCIBE. Ciber-resiliencia, aproximación a un marco de medición. Pág. 45. Fecha pub: 06/05/2014. Obtenido 02/12/2016. URL: https://www.incibe.es/extfrontinteco/img/File/Estudios/int_ciber_resiliencia_marco_medicion.pdf . URL de la fuente original: http://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework

# PARTE 3

## Medidores Inteligentes.

## Conclusiones y reflexiones

# Capítulo VI

## Medidores inteligentes

*"Combinar el aprendizaje automático con la simulación predictiva*
*y el control pre– o retro–alimentado puede ayudar a enfrentarse*
*a objetivos complejos de los sistemas de control,*
*y mejorar la capacidad para detectar ciberamenazas*
*u otro tipo de perturbaciones".*

**Dr. Anthony Skjellum**

**Facultad de Ingeniería "Samuel Ginn", Universidad Auburn, Alabama. 2016**

*"No es posible una Internet de las Cosas*
*ubicua, asequible, fiable, segura y sostenible*
*sin un suministro de energía eléctrica*
*ubicuo, asequible, fiable, seguro y sostenible.*
*LO CONTRARIO ES, IGUALMENTE, CIERTO:*
*No es posible un suministro de energía eléctrica …".*

**Steven E. Collier (@SmartGridMan).**

**Director de Estrategias para la Red Inteligente, MILSOFT Utility Solutions. 2016**

**Prosumidor: de consumidor a productor y viceversa**

El rol original de toda persona, comercio, industria y/o servicio que requiere energía eléctrica a una distribuidora es el de consumidor; conocido también como usuario o cliente.

Cuando existe la factibilidad de producir o almacenar electricidad en las instalaciones del usuario–cliente para consumo propio (por ejemplo, mediante paneles solares o generadores eólicos, bajo ciertas condiciones) y volcar el excedente a la red eléctrica, el rol se transforma dando paso al prosumidor. Esta palabra es el resultado de contraer y sumar dos términos: **pro**ductor + con**sumidor**. A lo largo de este capítulo expondré las características principales, condiciones previas y elementos destinados a establecer, mantener y gestionar la relación bidireccional entre el prosumidor y la distribuidora. Un dispositivo es el que permite coordinar esta "nueva" vinculación en la cual el tradicional usuario–cliente abandona su carácter pasivo mutando a un papel activo: el medidor inteligente.

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

Haciendo un desarrollo desde lo general a lo particular, lo primero a describir es la llamada red eléctrica inteligente. Según AEA[72] se trata de "la conjunción de la red eléctrica tradicional con tecnologías modernas de la información y comunicación. Permite integrar datos provenientes de los distintos puntos de la cadena eléctrica, desde el generador hasta el usuario final; y transformarlos en información y acciones que lleven a una mejora en su gestión. Su objetivo es elevar la eficiencia, confiabilidad, sustentabilidad, calidad de servicio y producto, para hacer frente a los nuevos desafíos de múltiples generadores diversos y estilos de consumo".

A nivel mundial el concepto *Smart Grid* nació en la década de 1980; siendo sus principales impulsores la dependencia de fuentes energéticas no renovables, los mayores costos en generación y operación, el aumento en la criticidad del servicio eléctrico, el cumplimiento de tratados internacionales y regulaciones, y la reducción de gases con efecto invernadero.

Muchos son los desafíos que plantea esta infraestructura híbrida. No obstante hay cuatro que sobresalen al considerarse en el presente trabajo:

- Generación distribuida, embebida o *in situ*. Es un modelo descentralizado para producir electricidad a pequeña escala, cuya potencia instalada va entre los 3 kW

[72] AEA. Redes Eléctricas Inteligentes. AEA 92559. Parte 1. Guía de conceptos, beneficios y desafíos para su implementación. Pág. 10. Edición: Agosto 2013.

y los 10 kW. Aspectos importantes: marco regulatorio, método de conexión y desconexión a la red, niveles de tensión y potencia, criterios de calidad, impacto ambiental.

- Seguridad (informática y de la información). La interconexión y comunicación de equipos es parte de la Internet de las Cosas, en este caso a nivel industrial (IIoT). Al transmitir datos relevados o generados se exponen puntos de acceso sobre los cuales es preciso prevenir intrusiones y pérdida de datos o modificaciones no autorizadas. Medidas como el cifrado y la validación de ingreso son necesarias, así como una fuerte concientización del factor humano: conductas basadas en buenas prácticas y resguardo de la información por parte del personal involucrado.
- Gestión de la información. El volumen de los datos, su granularidad y formas de obtención plantean retos para su procesamiento, traslado y resguardo. Son claves las políticas y procedimientos correspondientes. En un futuro no muy lejano deberá apoyarse en prácticas como *Big Data* si pretende dar respuestas acordes a las exigencias.
- Privacidad. Dada la cantidad de actores involucrados cobran relevancia los procesos de protección y administración. Debe garantizarse el cumplimiento de la legislación vigente y la correcta aplicación de perfiles de acceso a los datos.

**NISTIR 7628 Rev. 1: Ciberseguridad para *Smart Grid***

Conocidos como NIST *Internal or Interagency Reports*, los Informes Internos o Inter-agencias describen investigaciones de carácter técnico de interés para un público especializado. La lista incluye información sobre seguridad y privacidad.

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. Presenta un marco analítico que las organizaciones pueden utilizar a fin de desarrollar estrategias eficaces de seguridad cibernética adaptadas a sus combinaciones particulares de características relativas a la Red Inteligente, sus riesgos y vulnerabilidades. Las organizaciones en la diversa comunidad de partes interesadas en *Smart Grid*, desde servicios públicos hasta proveedores de servicios de administración de energía pueden usar los métodos e información de apoyo presentados en el informe como guía para evaluar el riesgo y los requisitos de seguridad para mitigarlo. Este enfoque reconoce que la red eléctrica está cambiando de un sistema relativamente cerrado a un entorno complejo y altamente interconectado. Los requisitos de ciberseguridad en cada organización deben evolucionar a medida que la tecnología avanza y las amenazas a la seguridad de la

red inevitablemente se multiplican y diversifican. Los tres tomos, que totalizan 668 páginas están disponibles en http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf .

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

Desde un punto de vista evolutivo, una distribuidora eléctrica pasa por 4 acciones en la migración hacia el paradigma *Smart Grid*, a saber:

1. Tele-medición. Con el objeto de implementar controles sobre la calidad del producto, el servicio y las pérdidas de electricidad, 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. En la figura 15 se resumen los tres niveles existentes, de menor a mayor escala: Lectura Automática de Medidores, Infraestructura de Medición Avanzada y Medición Inteligente.


**Figura 15: Niveles de Tele-Medición**[73]

[73] AEA. Redes Eléctricas Inteligentes. AEA 92559. Parte 1. Guía de conceptos, beneficios y desafíos para su implementación. Pág. 20. Edición: Agosto 2013.

2. Tele-supervisión. Es la recolección continua y remota de datos mediante sensores colocados en puntos sensibles de la red eléctrica. El monitoreo avanzado incluye indicadores y alarmas. El análisis se enfoca en la prevención de fallas y detección temprana de anomalías. Un centro de control aglutina la información en tiempo real para actuar rápidamente ante los eventos.
3. Tele-control o tele-gestión. Está soportado por el seguimiento y comando a distancia de diversos equipos para obtener agilidad en la operación. Incorpora funciones como: actuación remota, adquisición de datos y presentación de los mismos a otros sistemas integrados, automatización (menos fallas, menor impacto, mínimo lapso de tiempo de recuperación luego de un corte.
4. Sistema Integrado de Gestión. Estructura que posibilita agregar y recopilar datos, ordenar y compartir información. Una forma de intercambio entre sistemas son las interfaces. En la Figura 16 es posible apreciar un ejemplo de integración y los beneficios de implementar los tres sistemas mencionados por separado o en conjunto.

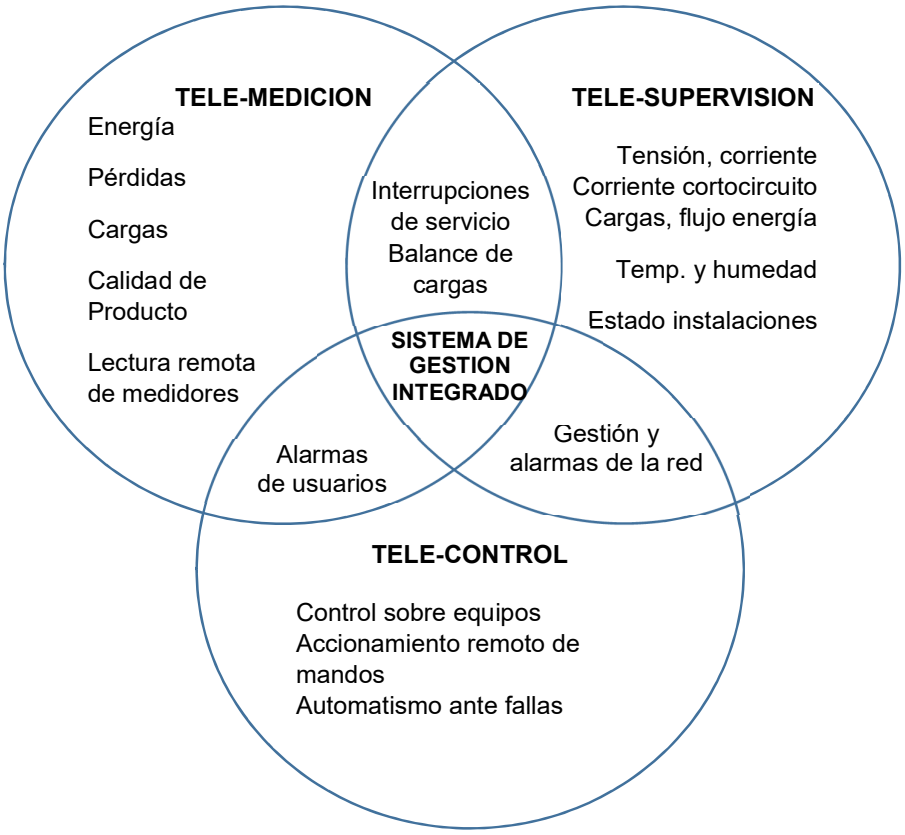


**Figura 16: Sistema de Gestión Integrado**[74]

[74] AEA. Redes Eléctricas Inteligentes. AEA 92559. Parte 1. Guía de conceptos, beneficios y desafíos para su implementación. Pág. 21. Edición: Agosto 2013.

### Principales componentes de la Distribución

Tratándose de la red más extensa y granular en comparación con la Generación y el Transporte, la mayoría de los cortes de suministro a los usuarios–clientes se producen en alguno de los niveles que la componen:

- Estación transformadora (de Alta a Media Tensión). Comprende transformadores, interruptores, bancos de capacitores, etc.
- Alimentador. Va desde el interruptor de salida de la ET hasta los transformadores de distribución (de Media a Baja Tensión). Incluye conductores (cables), capacitores, reguladores, reconectadores y seccionadores.
- Distribuidor. Constituye el “último cuarto de milla”, entre el alimentador y el usuario–cliente. Su complejidad está dada por la gran cantidad de elementos a controlar y por ende se convierten en potenciales puntos de falla.

### Comunicaciones

De poco servirían los dispositivos inteligentes, los centros de control y gestión o los prosumidores sin la posibilidad de establecer vínculos entre ellos, sean de una o dos vías.

Dependiendo de factores económicos, técnicos, legales y geográficos, existen a la fecha 8 tecnologías de comunicación que permiten enlazar las diversas clases de equipamiento, condensados en la Tabla 7.

| 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 |

**Tabla 7: Tecnologías de comunicación aplicables a *Smart Grid***[75]

## Medidores

Habiendo introducido los conceptos de prosumidor y red inteligente, puesto en contexto tanto la infraestructura de medición de una distribuidora como los canales disponibles para comunicar a todos los actores, pasemos al protagonista de este capítulo.

[75] AEA. Redes Eléctricas Inteligentes. AEA 92559. Parte 1. Guía de conceptos, beneficios y desafíos para su implementación. Pág. 45. Adaptación. Edición: Agosto 2013.

También llamado contador o registrador, se trata de un aparato encargado de medir el consumo de electricidad dentro de un circuito o suministro eléctrico. La unidad de medición impuesta es el kilovatio-hora (kWh).

Según la tecnología pueden ser:

- 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. Entre los usos extendidos puede mencionarse el soporte a esquemas tarifarios complejos y multitarifa, la conexión y desconexión remotas, el registro en tiempo real de eventos, magnitudes, alarmas, estados, la interacción con redes HAN (*Home Area Network*), FAN (*Field Area Network*) y LEN (*Local Energy Network*), la detección temprana del fraude y el control de la calidad del producto y del servicio. Dos de las características sobresalientes y estratégicas para las distribuidoras son la automatización de la red (las 3 “tele”: medición, control, supervisión) destinada a una total integración con los SCADAs; y el balance energético en instalaciones de los prosumidores, ayudando a prever la dinámica de la demanda.

**Un modelo para armar**

Las partes enumeradas conforman un entramado organizado de elementos cuya convergencia y destino apuntan a formar una red inteligente. Los medidores tradicionales eran el eslabón final en la relación entre una distribuidora y el usuario–cliente. Esta vinculación ha sido reformulada por los *Smart Meters*, al punto que los prosumidores pueden considerarse el eslabón inicial de la cadena. La Tabla 8 grafica la comparación entre la red eléctrica actual y la inteligente.

| Características | Red actual | *Smart Grid* |
|---|---|---|
| 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 |

**Tabla 8: Comparación entre una red eléctrica tradicional y una inteligente**[76]

### El aporte de TI y la importancia del *software*

El *hardware* de un medidor inteligente y las comunicaciones se complementan a partir del *software* disponible en el dispositivo. Considerando al aparato como un punto final (*end point*) su funcionamiento pleno es posible en principio gracias a un sistema operativo, por lo general una versión limitada y portable de Linux. Es probable que cuente con un cliente MQTT (*Message Queue Telemetry Transport*) para diversos tipos de conexiones, o bien se encuentre embebido en alguna aplicación específica utilizada por la distribuidora. A fin de tener una idea, por cada proceso de control remoto desde un centro de gestión, el protocolo MQTT admite hasta 50.000 dispositivos de medición. Otra de las funciones reside en utilizar el *Smart Meter* como concentrador de redes, donde cada adaptador existente en los aparatos hogareños (heladera, lavarropas, TV, etc.) puede actuar como un sensor. La conexión a un concentrador mediante MQTT permite agrupar los flujos de datos en una única sesión TCP/IP contra el punto de control central, administrado por la distribuidora desde un centro de gestión.

En noviembre de 2016 se anunció el lanzamiento del sistema operativo KasperskyOS, luego de 14 años de desarrollo. Según el fabricante, esta plataforma fue desarrollada desde

[76] G. Mercado, J.M. Da Peña, et.al. SG-SM - Smart Grid San Martin. Red de Distribución y Generación de Energía Inteligente en Ciudad Gral San Martin, Mendoza. Adaptación. Sin indicación en cuanto a fecha de publicación. Obtenido el 05/12/2016. URL: http://sedici.unlp.edu.ar/bitstream/handle/10915/45305/Documento_completo.pdf?sequence=1

cero pensando en equipamiento integrado, maquinaria industrial y sobre todo la Internet de las Cosas. Los pocos detalles que se conocen develan que se basa en arquitectura microkernel, seguridad por diseño y firmas digitales. Aun no hay fecha de salida al mercado.

En cuanto a las apps para dispositivos móviles, las primeras versiones interactúan con el medidor inteligente con el fin de hacer un seguimiento del uso, la tarifa variable y los hábitos de los usuarios clientes. Un par de ejemplos en los extremos:

- El poderoso grupo Unión Fenosa de España lanzó a mediados de 2015 la app "Mi Consumo" en busca de incrementar la calidad del servicio que la distribuidora presta, adelantándose a los requerimientos de la regulación y poniendo las curvas de carga a disposición de los usuarios – clientes domésticos con *Smart Meters*. La aplicación permite a los hogares conocer cómo utilizan la energía. Tras un proceso de registro en el sistema, el usuario accede a información gráfica y completa sobre su comportamiento energético en el intervalo de tiempo que seleccione: horario, diario, mensual. Cada 24 horas tiene a su disposición la curva de carga horaria de la jornada anterior.
- La comercializadora independiente Axpo Iberia ofrece a las PYMES una herramienta llamada eOpener desde fines de 2015, la cual recoge datos de consumo con varios fines: cobrar el monto exacto por el servicio, ofrecer asesoría personalizada para implementar medidas de ahorro, adecuar la tarifa al uso comercial o industrial, detectar ineficiencias, etc.

**Riesgos, amenazas y mitigación**

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.

Los medidores inteligentes recopilan gran cantidad de detalles sobre consumo de electricidad. Aunque también requieren asociarse a una acometida o punto de suministro y a un usuario–cliente en su carácter de titular del servicio; con lo cual ciertos datos personales están expuestos a la eventual divulgación no autorizada. Es posible además referenciar geográficamente la ubicación física de cada dispositivo.

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.

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

También conocido como Termeter[77], se trata de un *software open source* codificado en lenguaje Phyton que apareció a mediados de 2012. De acuerdo a su autor, Spencer McIntyre, de la firma Securestate, permite a cualquier persona con un poco de conocimiento conectarse a medidores de electricidad digitales o inteligentes mediante el puerto infrarrojo (ANSI Type 2). Implementa sus funciones mediante los protocolos C12.18 y C12.19.

Según el blog que publica la noticia original, Termineter potencialmente podría usarse para modificar el *software* del medidor y reducir las tarifas que los usuarios – clientes pagan por la electricidad, o simplemente ordenarle al aparato que reporte menos consumo de energía a la Compañía de distribución. Inicialmente brinda acceso limitado a los datos y configuración del medidor, aunque el usuario podría lograr un escalamiento y adquirir privilegios de administrador, lo que equivaldría a manejar el medidor a su antojo.

El creador del programa dijo que liberaron el software y el código (https://github.com/securestate/termineter) bajo licencia GNU con la idea de demostrar las

[77] Tecnomundo. Nuevo software permite hackear los medidores digitales de electricidad. Fecha pub.: 20/07/2012. Obtenido el 07/12/2016. URL: http://www.tecnomundo.net/2012/07/nuevo-software-permite-hackear-los-medidores-digitales-de-electricidad/

vulnerabilidades de los medidores, aunque admitieron que el programa podría ser usado por cualquier persona para beneficio propio. Tampoco detallaron o especificaron las debilidades.

El administrador del blog Tecnomundo agrega una nota al final de la noticia, textual: “He recibido decenas de mensajes de personas pidiendo comprar el *software*, u ofreciendo venderlo junto con el *hardware* necesario para modificar los medidores. Por favor, no continúen enviando estos mensajes porque no serán publicados. El artículo contiene el enlace para descargar el *software*, y en cuando el *hardware*, deben buscar otro sitio donde lo vendan, porque no voy a permitir que utilizan el blog para crear una compraventa de cosas que pueden resultar ilegal (sic) en muchos países.”

**Vulnerabilidades**

Las principales debilidades de los medidores inteligentes tienen que ver con exposición a factores climáticos, incorrecto montaje e instalación y configuraciones inadecuadas o por defecto. Debe tenerse en cuenta además que la medición del consumo es sólo una de varias funciones embebidas en el aparato. Un dispositivo con todas sus funciones implementadas es más apetecible para probables atacantes, sumadas a los datos personales que contiene.

El *hacking* es factible y depende del tiempo a invertir, el costo–beneficio del esfuerzo, las herramientas y el conocimiento de los intrusos. También es posible formar *Smart Users* que ayuden a reducir el campo de acción ante probables intentos de ataques.

**Legislación y regulaciones**

En Argentina, salvo honrosas excepciones, hay poco desarrollo y regulación de la generación distribuida cuando es originada por un particular en carácter de prosumidor, mucho menos la posibilidad de entregar la producción en exceso a la red pública. Sólo está autorizada para las distribuidoras. Aunque resulte obvio remarcarlo, la principal razón de existir para un medidor inteligente es la generación distribuida.

Como resultado de la promoción de energías renovables, a la fecha hay 6 provincias que poseen normativa sobre esta modalidad de producción de electricidad desde 2013: Santa Fe, Mendoza, Salta, San Luis, Neuquén y Misiones. Se trata de experiencias acotadas, de baja escala y a modo de prueba, entre las que sobresalen las vigentes en las ciudades de Armstrong (Santa Fe) –reconocida por ser la primera S*mart City* del país–, San Martín (Mendoza) y Centenario (Neuquén). En cuanto a los esquemas tarifarios, la opción mayoritaria el de balance neto (*net metering*) que suma el consumo y resta el excedente

saliente. No obstante, debido a los primeros resultados obtenidos, dos provincias, Santa Fe y Salta, han reorientado su estrategia hacia un sistema de tarifa diferencial (*feed in tariff*).

**Industrial Internet Consortium y su visión de la seguridad en *Smart Meters***

En noviembre de 2016 el IIC publicó la primera versión de su marco de seguridad: IISF (*Industrial Internet of Things, Volume G4: Security Framework*)[78], en la búsqueda de consensos acerca de cómo asegurar los sistemas que soportan a la Internet de las Cosas Industrial. Está conformado por 12 capítulos y 7 anexos.

En dicho *Framework* se destina un capítulo completo, el 8, a la protección de *endpoints*, entre los cuales se hallan los *Smart Meters*. Se pone especial énfasis en la seguridad física, heredada de los medidores tradicionales, adaptada a las "nuevas" necesidades: cajas contenedoras robustas y apropiadas, precintos de un solo uso en tapas y contratapas a modo de cerradura cuya rotura denote aperturas no autorizadas, protección ante condiciones climáticas adversas, blindaje de los conectores o enchufes ópticos y puertos USB, control del acceso físico a los mismos.

Dependiendo del modelo de amenaza, el medidor debe implementar componentes de seguridad duraderos o cualquier otro almacenamiento seguro para evitar la extracción de claves. El nivel de protección contra ataques de *hardware* a un dispositivo puede acreditarse usando certificaciones. Es posible que incorpore funciones físicas de protección contra manipulaciones, capaces de detectar y reportar cualquier cambio en el *hardware*, incluyendo sus subcomponentes.

Es recomendable etiquetar el medidor y ciertas partes con números de identificación únicos que previenen su uso fuera del contexto configurado. Los mecanismos deben ser capaces de detectar la sustitución de cualquier componente por reemplazos menos capaces o malintencionados.

En un entorno altamente controlado y regulado, el estado de seguridad del punto extremo debe monitorearse automáticamente como parte de las funciones de administración de la configuración; con la capacidad de detectar y reportar cualquier acceso no autorizado, modificaciones físicas o la integración del *hardware*.

[78] Industrial Internet Consortium. Industrial Internet of Things Volume G4: Security Framework Fecha pub.: 19/09/2016. Obtenido el 07/12/2016. URL: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

# Capítulo VII

## Conclusiones y reflexiones

*"Hablando con varios antiguos empleados de empresas contratistas del gobierno de los EEUU y expertos en guerra digital, he sabido que empresas como la ex empleadora de Edward Snowden: Booz Allen Hamilton, y otras similares (Northrup Grumman, Raytheon, Lockheed Martin y British Aerospace) cuentan con capacidades de sabotaje de sistemas SCADA.*
*No sorprende que todas ellas mantengan la discreción sobre lo que pueden hacer con dichas capacidades y a quién se las ofrecen".*

**Thomas Fox-Brewster (@IBlameTom)**

**Revista Forbes. 2015**

*"Si hoy se llegara a producir un ciberataque bien coordinado sobre la red eléctrica de los EEUU, el tiempo que llevaría restaurar el suministro eléctrico plantearía problemas de seguridad nacional de enormes proporciones".*

**John Everett**

**Director del Programa RADICS, DARPA. 2016**

**Respecto a la ciberseguridad industrial**

La ciberseguridad industrial es un asunto complejo, con muchas aristas, que involucra a diversos sectores y protagonistas.

En general por estas latitudes las responsabilidades en la materia no siempre se hallan claramente establecidas ni delimitadas. Tampoco hay en la sociedad civil un cabal entendimiento acerca del impacto o las consecuencias derivadas de hechos tales como sabotajes, fenómenos naturales, fallas, accesos no autorizados o negligencia en la gestión.

En algunas organizaciones el punto de partida que genera un cambio prometedor es reconocer la existencia de problemáticas asociadas a incidentes de seguridad. El ocultamiento deliberado de los mismos trae aparejada una involución que solo contribuye a mantener el estado de las cosas en un determinado momento, ofreciendo a la opinión pública una falsa sensación de normalidad y desperdiciando oportunidades para aprender tanto de los aciertos como los errores, conocer las formas en que actúan los ciberdelincuentes o, lo que es más motivante aún, capitalizar, compartir y multiplicar el conocimiento y la experiencia de los recursos humanos que a diario sostienen las infraestructuras críticas, tanto desde la operación como del mantenimiento y la gestión de los sistemas informáticos.

Los esfuerzos aislados o individuales están condenados de antemano al más estrepitoso fracaso. Es necesario incorporar a la mayor cantidad posible de actores interesados en el bienestar de los ciudadanos globales, establecer reglas de juego claras y sumar apoyos. 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.

Debe entenderse a la ciberseguridad industrial como una disciplina moderna, y a la vez contemporánea, ya que el grado en el cual la sociedad actual depende de la tecnología sigue aumentando en forma exponencial gracias a la investigación, el desarrollo y la innovación. Hace falta también un profundo debate sobre paradigmas como el mundo inteligente (hoy casi todo es *smart*), la Internet de las cosas (*Internet of Things*) y la Internet de las cosas Industrial (*Industrial Internet of Things*); que prometen convertir nuestra existencia en “auto–mágica”. ¿Qué aspectos estamos perdiendo de vista en el camino?, ¿cuáles son los peligros derivados de esa alta dependencia tecnológica?, ¿hasta qué punto es factible delegar a una máquina las decisiones que debería tomar un ser humano?, ¿puede un aparato cibernético reemplazar por completo a una persona?, ¿tienen los gobiernos la capacidad de neutralizar o contener ataques a gran escala?, ¿es posible eliminar por completo los errores humanos? Cientos de preguntas, sin respuestas a la vista en el corto plazo.

La ciencia y la técnica que motorizan los avances también están contribuyendo con herramientas para aumentar y mejorar la ciberseguridad industrial a través de la integración de disciplinas, la incorporación de metodologías relativas al análisis de riesgos, el desarrollo de estrategias sobre defensa en profundidad y mecanismos predictivos ante amenazas.

**Referidas a Infraestructuras Críticas**

En un extremo, 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. En otro, 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.

Citando un ejemplo reciente que evoca los acueductos romanos, las alarmas sonaron desde los medios de prensa el pasado 28 de setiembre de 2016 cuando se conoció una versión inquietante. Alertada por los servicios de inteligencia paraguayos, Gendarmería Nacional estaba investigando desde julio los pasos de un ex prefecto con antecedentes penales, quien habría vendido copias de planos correspondientes a tres plantas potabilizadoras de agua, ubicadas en Bernal, Tigre y Capital Federal. Los supuestos compradores son de origen libanés.

“Un problema central es que esos sitios no están catalogados, por lo tanto al día de hoy se sabe cuáles son, pero no más que eso”, dijo a un periódico un especialista en seguridad pública que pidió no ser identificado. Por ello, en el diseño original del ICIC iban a participar las universidades públicas para el relevamiento y evaluación de las infraestructuras críticas, cuyos responsables serían invitados a adherir voluntariamente al Programa. Pero eso nunca sucedió.

El especialista en ciberseguridad Mariano del Río enumera las amenazas: “virus, acceso indebido, mal uso, *hacking*, espionaje, robo de información o daño informático. Se debería hacer un análisis de los riesgos para priorizar aquellos activos más expuestos; este tipo de acciones se suelen llevar a cabo en el marco de una Estrategia Nacional de Ciberseguridad, algo que tampoco tenemos.” Del Río extiende las posibles fallas a los sistemas informáticos oficiales, que permitirían extraer información estratégica o valiosa para la seguridad de las instalaciones que es vital proteger.

Parafraseando la crónica del periodista Claudio Savoia, los hechos están a la vista: los planos de instalaciones sensibles supuestamente entregados a manos que no deberían

tenerlos podrían haberse obtenido por una debilidad en el acceso a ellos. Aún si la historia no fuera cierta, la alerta debería activar muchos planes.

¿Qué ocurriría si el Poder Ejecutivo obligara, bajo condición de anonimato, a los Estados Provinciales y a las empresas que gestionan infraestructuras críticas a reportar todas las brechas de seguridad físicas e informáticas?, ¿cuál sería el efecto de realizar simulacros de catástrofes naturales o ciberataques? Una ley no escrita considera al sentido común como el menos común de los sentidos: aquello que no se logra anticipadamente mediante planes o convencimiento, se hace de urgencia después de un incidente… si queda algo por proteger luego de perpetrado el mismo. En el caso de los planos, las recomendaciones apuntan al reemplazo de los cercos perimetrales de los predios cambiando alambrados por paredes, la elevación de la altura en los portones de ingreso, la colocación de caballetes los accesos para impedir la entrada de vehículos no identificados, el aumento en la cantidad de los puestos de vigilancia, el reemplazo de agencias privadas por fuerzas estatales y la colocación de cámaras y luces con sensores de movimiento. Claramente no es un problema tecnológico.

No debe soslayarse tampoco el fenómeno de las interdependencias entre estas infraestructuras. Una red de distribución carece de cualquier sentido sin electrones para repartir, a una represa hidroeléctrica se le hace imposible entregar su producción si las torres y líneas de transporte no existen. Independientemente del origen y modalidad de un ataque, el daño a cualquier eslabón de la compleja cadena eléctrica tiene consecuencias difíciles de mensurar. La “omnipresencia” de la electricidad en la vida moderna hace que la tengamos en cuenta ¡solamente cuando apretamos la tecla y la luz no se hace!

Una última observación en este asunto, para graficar la falta de comunicación y coordinación entre organismos de gobierno con injerencia en el mismo que derivan en ausencia de acciones básicas. Argentina es el único país en la región que aún no ha puesto en marcha el servicio de Hora Oficial en Internet para todo su territorio, con el fin de sincronizar relojes en los sistemas informáticos mediante enrutamiento de paquetes en redes con latencia variable; usualmente implementado vía NTP (*Network Time Protocol*). Por ley, el Observatorio Naval Buenos Aires –órgano de la Armada– es el ente a cargo de esta tarea. Luego de idas y vueltas, en 2008 adquirió un reloj atómico con salida digital y capacidad de transmitir señales a equipos remotos sin perder exactitud. Eso le permitirá contar con una homologación del Observatoire de Paris, autoridad en materia métrica a nivel mundial. No se conoce el estado actual de tal homologación. Bajo reserva de nombres, la única explicación textual emitida vía correo electrónico a mediados de 2014 es la siguiente: “el ONBA se encuentra en proceso de actualización tecnológica que demanda tiempos para su adquisición, instalación, pruebas de funcionamiento y puesta en servicio de los nuevos

equipos y programas a instalar. Al momento, no es posible precisar la fecha de su implementación. Se sugiere utilizar momentáneamente alguna solución alternativa".

Difícilmente se pueda avanzar consistentemente en ciberseguridad industrial si antes no se concretan medidas esenciales como la disponibilidad de al menos una fuente confiable, legalmente autorizada y exacta para sincronización de fecha y hora; mecanismo indispensable en la gestión de bitácoras e investigación de eventos, entre otros importantes requerimientos. ¡Ah!, ¿necesita sincronizar el reloj de un dispositivo conectado a Internet y vive en Argentina?, por favor telefonee al 113, o busque un método no oficial.

**Sobre el sistema eléctrico en Argentina**

Entre abril de 1988 y marzo de 1989 una grave crisis energética nacional tuvo como consecuencia la aplicación de cortes rotativos y programados en el suministro eléctrico, afectado a la población, los comercios y la industria. Durante ese período se implementaron interrupciones diurnas con una duración mínima de 5 horas por jornada. Según la explicación del gobierno de turno los motivos fueron una suma de "eventos desafortunados": la central Atucha I salió de servicio, se rompieron dos turbinas en la hidroeléctrica Embalse Río Tercero, un incendio afectó una red en La Pampa, encargada de distribuir electricidad producida en El Chocón –uno de cuyos diques presentaba una fisura, en reparación– y el lago de Salto Grande languidecía por falta de lluvias, sin poder alimentar a la represa homónima. El entonces Sistema Interconectado Nacional estaba colapsado. En menor escala y más cerca en el tiempo, durante períodos de muy altas o bajas temperaturas se pone a prueba todo el sistema eléctrico, al límite de sus prestaciones. La supuesta causa: falta de inversiones.

Mucha agua ha pasado bajo el puente: privatizaciones, nuevos marcos legales, desregulaciones en algunos sectores, regulaciones en otros, estatizaciones, congelamiento tarifario, sinceramiento de los valores hacia precios de mercado. Al período 1989 – 2000 de grandes transformaciones a partir de la segmentación en generación, transporte y distribución, le siguió una etapa de transición entre 2001 y 2003, tras lo cual se implementó una política de subsidios que se mantuvo hasta 2015, con resultados evidentemente nefastos: desequilibrios en toda la cadena de abastecimiento y deudas gigantescas, sobre todo para las distribuidoras. Las industrias también han sufrido las consecuencias en carne propia ya que ante la imposibilidad de cubrir la demanda de energía eléctrica, las autoridades gubernamentales deciden por lo general privilegiar el consumo residencial, determinando cortes a fábricas y grandes usuarios.

La producción de electricidad en el país depende fuertemente de la disponibilidad de combustibles fósiles, cuya capacidad de autoabastecimiento ha perdido la nación desde

2010. Según lo indicado por especialistas como Jorge Lapeña y otros ex ministros de Energía, hacia 2009 se conjugaban 3 situaciones complejas, que no han variado sustancialmente:

- El sector ha demostrado tener dificultades en ampliar la oferta de nueva generación. Las empresas privadas no cuentan con las condiciones mínimas para invertir y el Estado actúa sin previsión, recurriendo a unidades pequeñas, consumidoras de hidrocarburos líquidos importados, de alto costo.
- El funcionamiento del sistema se vuelve crítico ante situaciones de extremas temperaturas o cuando la hidraulicidad es mínima; debido a la insuficiente generación como a las limitaciones de los sistemas de distribución en las grandes ciudades.
- La visión es cortoplacista; con erogaciones retrasadas y, como consecuencia, exhibe un régimen basado en equipamiento y redes al límite de sus prestaciones.

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. Justificar estas inversiones, demostrar su retorno en un tiempo razonable y obtener los fondos para financiarlas constituyen desafíos para el futuro cercano.

Un alto grado de automatización e informatización en los procesos de generación, transporte y, sobre todo distribución tiene beneficios reales como la baja en los costos de operación, la mejora en los tiempos de respuesta, la disminución en la duración de los cortes, la preservación de la integridad física de los operadores, etc. Aunque también debe señalarse la aparición de nuevos riesgos, muchos de los cuales atraviesan el mundo cibernético para convertirse en amenazas tangibles, de alto impacto.

**En cuanto a TI, TO, buenas prácticas, Normas y Estándares**

El clásico síndrome de la Biblioteca de Alejandría alude a la historia ancestral de un aprendiz egipcio, quien viajó a la ciudad homónima en busca del conocimiento contenido en los volúmenes de sus famosas estanterías. Tras leer cientos de libros terminó por convencerse de una dura verdad: no le alcanzaría su vida, la de sus hijos y nietos para procesar todos los documentos allí existentes. Según su propia y particular visión, semejante colección de saberes constituía una maldición; por lo que decidió romper la misma incendiando el edificio junto a sus célebres archivos en “formato papel”. La versión actual del mítico hechizo se denomina *infoxicación*: gracias a los avances de la tecnología en bases de datos, motores de búsqueda, algoritmos, Internet, etc. nos hallamos intoxicados de

información, literalmente. Para algunos bendición, para otros desgracia, lo cierto es que a la hora de bucear en la web uno debe afinar el ingenio y aprender a distinguir lo sustancial de aquello que no aporta valor. Hay mucha y variada data sobre SCADAs. Se encuentra poco de Ciberseguridad Industrial aplicada en relación a seguridad de la información, menos en español y mucho menos aún relacionado con desarrollos o implementaciones en Argentina; y prácticamente nada en el ámbito de la distribución eléctrica a nivel local.

Uno de los dogmas sagrados en TO es el mito de la disponibilidad: “mientras la maquinaria continúe operando, lo demás pasa a segundo plano”. Esta aseveración tiene detractores, entre los cuales se halla Eric Byres. El fundador de la empresa Tofino Security sostiene que en los SCI el componente más importante de la tríada CID es la integridad, ya que debe garantizarse que el dato transmitido por el emisor llegue al receptor manteniendo su condición de fidedigno. Estoy de acuerdo, en parte, con Byres: la integridad, sin ser más importante que la disponibilidad y la confidencialidad, debe estar garantizada previamente. Un canal con alta disponibilidad no tiene mucho valor sin los mecanismos que certifiquen, como mínimo, la integridad de los datos transmitidos. Y la confidencialidad debería estar acompañada al menos por un mecanismo de autenticación.

Por cierto, 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 las necesidades de TO, brindando soluciones superadoras. Históricamente TI ha logrado insertarse transversalmente en las organizaciones, asumiendo un rol como área de servicios y soporte a la actividad principal. Una empresa distribuidora de electricidad no es la excepción; sus departamentos ligados a transmisión, subtransmisión, protecciones, despacho, etc. tampoco.

Las buenas prácticas, Normas y Estándares constituyen una hoja de ruta de gran valor. En su creación y mantenimiento intervienen miles de profesionales provenientes de diversas industrias, aportando experiencia, conocimiento y visión. Los desafíos a la hora de aplicarlas continúan intactos: transformar el “qué hacer” en “cómo hacerlo”, pasar de la letra muerta a la acción, interpretar las necesidades de una organización real, conseguir apoyo gerencial, obtener presupuesto, gestionar riesgos, producir métricas fiables para tomar decisiones, administrar los cambios, demostrar el retorno de las inversiones (sobre todo en materia de Ciberseguridad Industrial).

Asumiendo por un instante el rol de Ethical Hacker debe señalarse que el desarrollo de tecnología, amenazas y Estándares crece a ritmos diferentes. Por ejemplo, para proteger una infraestructura critica, seguir los Estándares no es suficiente ya que éstos tratan asuntos

básicos y se focalizan en gestionar problemas detectados hace años. Por citar un caso, Samuel Linares señala que IEC 62443 tiene lagunas en aspectos como el acceso remoto y la separación entre sistemas para *security* y *safety*. La moraleja es que las Normas y Estándares deben utilizarse como referencia, adoptando y adaptando sus contenidos, siendo necesario ir más allá de los mismos. La resiliencia puede ser un vehículo para ese viaje; de hecho existe el llamado CERT-RMM (*Resilience Management Model*) v1.2, desarrollado por el *Software Engineering Institute*, de la *Carnegie Mellon University*.

Una parte sensible es la referida a certificación de dispositivos y sistemas de control industrial. Para ISA-IEC62443 funciona desde 2007 el Instituto de Cumplimiento de Seguridad ISA, o ISCI (*ISA Security Compliance Institute*); más conocido por la marca ISA Secure (www.isasecure.org). Esta designación o sello garantiza que los productos de control de automatización industrial cumplan con los estándares de seguridad cibernética del consorcio de la industria, proporcionando confianza a los usuarios de los productos y sistemas ISA Secure y creando diferenciación de productos para proveedores que adhieren a la mencionada especificación. Fundado por 7 gigantes de la industria, es destacable la visión a futuro, aunque sería interesante una mayor injerencia de los gobiernos en áreas como esta.

**SCADAs**

Al decir del especialista Maximilian Kon, se da una paradoja que hasta ahora contribuye involuntariamente a proteger las instalaciones, los sistemas industriales y por ende a los SCADAs: existen cientos de protocolos, lo cual es una “ventaja” desde el punto de vista de la defensa. Les llevará mucho tiempo a los potenciales atacantes comprender la complejidad de los mismos; aunque tales protocolos no tengan en su origen y diseño la capacidad de gestionar autenticación, encriptación o validación. Quienes deploramos la seguridad por oscuridad vemos en este ejemplo cómo un riesgo se convierte en un elemento de protección. Los conversores TCP/IP están cambiando esta realidad, en parte a favor de potenciales intrusos, ya que permiten traducir casi cualquier protocolo a un estándar archiconocido.

Las consecuencias derivadas del incidente con el malware *BlackEnergy* y las lecciones aprendidas constituyen una oportunidad para generalizar siete conclusiones sobre ciberseguridad en SCADAs dentro de una empresa distribuidora de electricidad, a saber[79]:

[79] WisePlant. Caso de Estudio: Hackeo de la Red de Distribución Eléctrica en la zona oeste de Ukrania el pasado 23/12/2015. Una mirada cauta del incidente. Fecha pub: 27/03/2016. Obtenido el 02/12/2016. URL: http://wiseplant.com/2016/03/27/analisis-del-hackeo-de-la-red-electrica-de-ukrania-el-pasado-23-de-diciembre-de-2015/

- Los atacantes necesitaron entre 6 y 9 meses de reconocimiento, investigación, planificación y coordinación para lograr su objetivo. Con procesos internos de seguridad gestionada y herramientas informáticas adecuadas (muchas de uso libre y *open source*), las actividades de este grupo habrían sido detectadas.
- Idealmente las conexiones remotas a los Sistemas SCADA y/o Sistemas de Control deben implementar dos factores de autenticación. En la actualidad miles de sistemas de este tipo ni siquiera admiten o soportan el concepto de autenticación, menos su aplicación. La seguridad instrumentada o agregada es un paso inminente en estos casos.
- Las fuentes de alimentación y UPS de los sistemas de control son tan críticas como el propio SCADA. Deben ser seguras, confiables, monitoreadas y administradas.
- Las actualizaciones de *firmware* en los sistemas de control también son un vector de ataque válido, muy crítico. Muchos miembros de la comunidad TO y especialistas en seguridad informática y de la información aún no han incorporado este riesgo.
- Es preciso implementar un Sistema de Detección Comprensiva como así también de Protección Comprensiva. No basta con proteger solamente algunos de los puntos de ingreso.
- Es imperioso efectuar un estudio comprensivo de identificación de vulnerabilidades y evaluación de riesgos a la Ciberseguridad Industrial antes de implementar las medidas de protección. No hacerlo implica subestimar a los atacantes; malintencionados o no.
- La información, documentación y detalles que describen el funcionamiento de la red eléctrica como de la arquitectura de los Sistemas de Control deben ser asegurados. Tales recursos pueden brindar a terceros no autorizados la data necesaria para identificar las vulnerabilidades en los Sistemas de Control.

Por otro lado, sin ánimo de minimizar la problemática, según métricas del US-CERT hasta 2015, un 80 u 85 por cierto de los ciberincidentes a los que da respuesta quedarían mitigados a través de la aplicación de 5 controles básicos: 1. Segmentación de redes, 2. Reducción de privilegios para administración, 3. Parcheo de sistemas operativos. 4. Parcheo de aplicaciones, 5. Uso de herramientas para administrar listas blancas de *softwares*. Definir una estrategia para repensarlos en el ámbito industrial, comunicarlos adecuadamente, ponerlos en marcha y supervisarlos periódicamente no parece muy costoso a simple vista.

El mismo US-CERT, a través de su Centro Nacional de Ciberseguridad y Comunicaciones para Sistemas de Control Industrial publicó el informe anual de coordinación de vulnerabilidades reportadas para el año 2015, una de cuyas estadísticas revela que la

industria con mayor cantidad de debilidades denunciadas para ese período fue la energética, seguida por la fabricación crítica y los sistemas de agua y saneamiento. Una lectura rápida sugiere que a mayor cantidad de vulnerabilidades es mayor la probabilidad de explotación.

En cuanto a predicciones, la firma S21SEC pronostica que durante 2017 es probable la ocurrencia de importantes ciberataques contra grandes entidades bancarias y continuarán los actos de ciberespionaje y cibersabotaje a sectores como el industrial a través de Amenazas Persistentes Avanzadas (APT).

Finalmente, la ciber-resiliencia es un camino prometedor a seguir, aunque implica requisitos previos: un fuerte compromiso de toda la organización, cambios culturales, disciplina metodológica, entre otros menesteres de mediano y largo plazo.

**Medidores inteligentes**

En la segunda quincena de diciembre de 2013 se produjo una nueva oleada de cortes que perjudicaron a millones de usuarios–clientes, afectando principalmente a los habitantes de la Ciudad Autónoma de Buenos Aires, Conurbano bonaerense y La Plata. Un par de meses antes los directivos de las tres principales distribuidoras a cargo de la concesión del servicio público se reunieron con autoridades nacionales a fin de presentar un plan para la instalación masiva de medidores inteligentes en los hogares. El objetivo principal: impulsar un consumo más eficiente de la electricidad, aplicando esquemas ya maduros en otros países, una de cuyas premisas es el precio variable en función de bandas horarias. En un esquema progresivo la energía eléctrica debe ser más cara cuando se la consume durante horario pico (diurno o nocturno); de esta forma se incentiva a los usuarios–clientes a diversificar su consumo a lo largo del día para evitar la saturación del sistema de distribución en los períodos de mayor demanda. Aunque parezca contradictorio, las autoridades de turno rechazaron la idea argumentando que tal propuesta constituía un aumento encubierto de la tarifa eléctrica.

La realidad actual muestra iniciativas interesantes en forma de experiencias piloto, proyectos de ley y marcos regulatorios para incorporar y adaptar las tecnologías al mejoramiento en la calidad de vida de las personas. Ejemplos a mayor y menor escala como los emprendidos en las ciudades de Armstrong (Santa Fe), Centenario (Neuquén) y General San Martín (Mendoza) demuestran la factibilidad y los beneficios de las aplicaciones *smart*. Probablemente mientras no haya tarifa diferenciada en base a bandas horarias, no se logrará masificar el uso de medidores inteligentes.

El Estado Nacional Argentino, los provinciales y municipales deben generar las condiciones propicias para admitir la generación distribuida por parte de los prosumidores y

el volcado del excedente en la red eléctrica pública, promover la instalación de medidores inteligentes, proponer esquemas tarifarios que premien el uso racional de la electricidad y castiguen el derroche o la ineficiencia, gestionar la demanda y aumentar la oferta proveniente de fuentes renovables. Todo esto debe ser acompañado por una actualización en la legislación sobre Habeas Data y privacidad, considerando a las nuevas tecnologías "inteligentes" en materia eléctrica, poniendo en primer lugar la vida de los ciudadanos, protegiendo las infraestructuras críticas, regulando los servicios públicos monopólicos y garantizando un adecuado manejo de los datos personales. Los cambios a realizar implican un debate que debe incluir a todos los actores.

En noviembre de 2016 se conoció un proyecto del diputado nacional Villalonga que trata estas cuestiones y podría convertirse en ley a principios de 2017.

En cuanto a ciberseguridad, la Internet de las Cosas ha revolucionado muchos aspectos de la vida, al punto que una de sus vertientes más influyentes es la veta industrial (IIoT). Prácticamente la totalidad de los dispositivos inteligentes funcionan en base a electricidad, por lo que una estación transformadora, un auto, una heladera o un medidor *Smart* son electrodependientes, se comunican con los seres humanos y con otros aparatos. Si tienen una dirección IP son susceptibles de ser accedidos de forma no autorizada. No sólo pueden sufrir *hackeos*; su comportamiento, funciones y finalidad originales mutarán o simplemente dejarán de funcionar ante un ciberataque. La correcta gestión, una adecuada protección y un uso concienzudo de los datos son algunos de los desafíos planteados a corto y mediano plazo.

## Glosario de siglas

**ADEERA**. Asociación de Distribuidores de Electricidad de la República Argentina.

**AEA**. Asociación Electrotécnica Argentina.

**AGEERA**. Asociación de Generadores de Electricidad de la República Argentina.

**AGUEERA**. Asociación de Grandes Usuarios de Electricidad de la República Argentina.

**ANSI**. *American National Standards Institute*. Instituto Americano de Estándares Nacionales.

**APA**. *American Psychological Association*, Asociación Americana de Psicólogos.

**APN**. Administración Pública Nacional.

**APT**. *Advanced Persistent Threat*. Amenaza Persistente Avanzada.

**ATEERA**. Asociación de Transportadoras de Electricidad de la República Argentina.

**BES**. *Bulk Energy System*. Sistema Mayorista de Energía o Sistema de Energía a granel.

**BPL C**. Broadband Power Line. (Comunicaciones sobre) Líneas de Electricidad, Banda Ancha.

**BS**. *British Standards*. Estándares Británicos.

**BY-NC-SA**. *By-NonCommercial-ShareAlike*. Designa un tipo de licencia Creative Common. Se traduce como Atribución-NoComercial-CompartirIgual.

**CACIER**. Comité Argentino de la **CIER**.

**CAMMESA**. Compañía Administradora del Mercado Mayorista Eléctrico Sociedad Anónima.

**CARI**. Consejo Argentino de Relaciones Internacionales.

**CCI**. Centro de Ciberseguridad Industrial (España).

**CERT**. *Computer Emergency Response Team*. Grupo de Respuesta ante Incidentes "con computadoras" o ciberincidentes.

**CFEE**. Consejo Federal de la Energía Eléctrica

**CIA**. *Confidentiality, Integrity, Availabiliy*. **CID**. Confidencialidad, Integridad, Disponibilidad.

**CIAA**. Computadora Industrial Abierta Argentina.

**CIER**. Comisión de Integración Energética Regional.

**CIP**. *Critical Infrastructure Protection*. Protección de Infraestructuras Críticas.

**CMMI**. *Capability Maturity Model Integration*. Integración de modelos de madurez de capacidades.

**CNI**. *Critical National Infrastructure*. Infraestructura Nacional Crítica.

**CNPIC**. Centro Nacional para la Protección de Infraestructuras Críticas (España).

**CObIT**. *Control Objectives for Information and related Technology*. Objetivos de Control para Información y Tecnologías relacionadas.

**DCS**. *Distributed Control Systems*. Sistemas de Control Distribuido.

**EDENOR**. Empresa Distribuidora y Comercializadora Norte S.A.

**EDESUR**. Empresa Distribuidora Sur Sociedad Anónima.

**EMS**. *Energy Management System*, Sistema de Gestión de Energía.

**ENRE**. Ente Nacional Regulador de la Energía.

**ERP**. Enterprise Resource Planning.

**ESI**. Especialización en Seguridad Informática.

**ETH**. *Eidgenössische Technische Hochschule.* Escuela Politécnica Federal de Suiza.

**ETSI**. *European Telecommunications Standards Institute*. Instituto Europeo de Normas de Telecomunicaciones.

**FAA**. Fuerza Aérea Argentina.

**FACE**. Federación Argentina de Cooperativas Eléctricas.

**FAN**. Field Area Network. Red de Área de Campo.

**FERC**. *Federal Energy Regulatory Commission*. Comisión Federal Reguladora de la Energía.

**FI**. Facultad de Ingeniería.

**Fundelec**. Fundación para el Desarrollo Eléctrico.

**GMS**. *Generation Management System*. Sistema de Gestión de Generación (de electricidad).

**GPRS**. *General Packet Radio Service*. Servicio General de Paquetes Vía Radio.

**GSM**. *Global System for Mobile Communications*. Sistema Global para Comunicaciones Móviles.

**GUMa**. Gran Usuario Mayor.

**GUMe**. Gran Usuario Menor.

**HAN**. Home Area Network. Red de Área Hogareña.

**HidroNor**. Hidroeléctrica Norpatagónica S.A.

**IACS**. *Industrial Automation and Control Systems*. Sistemas de Control y Automatización Industrial.

**IAE**. Instituto Argentino de la Energía “General Mosconi”.

**IASME**. *Information Assurance for Small and Medium Enterprises*. Aseguramiento de Información para Pequeñas y Medianas Empresas.

**ICIC**. Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (Argentina).

**ICS-ISAC**. *Industrial Control System Information Sharing and Analysis Center*. Centro de Análisis e Intercambio de Información sobre Sistemas de Control Industrial.

**IEC**. *International Electrotechnical Commision*. Comisión Electrotécnica Internacional.

**IED**. *Intelligent Electronic Device*. Dispositivo Electrónico Inteligente.

**IIoT**. *Industrial Internet of Things*. Internet de las Cosas Industrial.

**INCIBE**: Instituto Nacional de CIBerseguridad de España.

**IoT**. *Internet of Things*. Internet de las Cosas.

**IRAM**. Instituto de Racionalización Argentino de Materiales.

**ISA**. *International Society of Automation*. Sociedad Internacional de Automatización.

**ISO**. *International Organization for Standarization*. Organización Internacional para la Estandarización.

**ITIL**. *Information Technology Infrastructure Library*. Biblioteca de Infraestructura de Tecnologías de Información.

**ITU**. *International Telecommunication Union*. Unión Internacional de las Telecomunicaciones.

**IUA**. Instituto Universitario Aeronáutico.

**KW**. *KiloWatt*. KiloVatio. Unidad equivalente a mil vatios. Un vatio es la potencia eléctrica producida por una diferencia de potencial de 1 volt y una corriente eléctrica de 1 amperio (1 voltamperio).

**LCD**. *Liquid Crystal Display*. Pantalla de Cristal Líquido.

**LED**. *Light-Emitting Diode*. Diodo Emisor de Luz.

**LEN**. *Local Energy Network*. Red de Energía Local.

**LTE**. *Long Term Evolution*. Evolución de Largo Término.

**MEM**. Mercado Eléctrico Mayorista.

**MinCyT**. Ministerio de Ciencia y Técnica (Argentina).

**MITRE**. Massachusetts Institute of Technology Research and Engineering. MIT Investigac. e Ingeniería

**MQTT**. *Message Queue Telemetry Transport*. Protocolo para Transporte de Telemetría en colas de Mensajes.

**MTU**. *Master Terminal Unit*. Unidad Terminal Maestra o Unidad Central.

**MW**. *MegaWatt*. MegaVatio. Unidad equivalente a un millón de vatios. Un vatio es la potencia eléctrica producida por una diferencia de potencial de 1 volt y una corriente eléctrica de 1 amperio (1 voltamperio).

**NERC**. *North American Electric Reliability Corporation.* Corporación Norteamericana para la confiabilidad eléctrica.

**NIST**. *National Institute of Standards and Technology*. Instituto Nacional de Estándares y Tecnología.

**NTP**. Network Time Protocol. Protocolo de tiempo de red.

**OEA**. Organización de los Estados Americanos. **OAS**. *Organization Of American States*.

**ONBA**. Observatorio Naval Buenos Aires.

**OSEK**. *Offene Systeme und deren Schnittstellen für die Elektronik in Kraftfahrzeugen*. Sistemas abiertos y sus interfaces para la electrónica en automóviles.

**PAC**. *Programmable Automatic Controller*. Controlador Automático Programable.

**PDCA**. *Plan, Do, Check, Act*. Planificar, Hacer, Controlar, Actuar.

**PLC**. *Programmable Logic Controller*. Controlador Lógico Programable.

**PLC**. *Programmable Logic Controller*. Controlador Lógico Programable. Alt. *Power Line Communications*, Comunicaciones a través de las líneas eléctricas.

**RAE**. Real Academia Española.

**RFC**. *Request for Comment*. Solicitud de comentarios.

**RFID**. *Radio Frequency IDentification*. Identificación por Radio Frecuencia.

**RTU**. *Remote Terminal Unit*. Unidad Terminal Remota.

**SADI**. Sistema Argentino de Interconexión.

**SCADA**. *Supervisory Control And Data Acquisition*. Sistemas para Supervisión del Control y Adquisición de Datos. Alt. Sistemas de Supervisión, Control y Adquisición de Datos.

**SCI**. Sistemas de Control Industrial. En inglés, **ICS**: *Industrial Control Sytems*.

**SEGBA**. Servicios Eléctricos del Gran Buenos Aires.

**SGP**. *Standard of Good Practice*. Normas de buenas prácticas.

**SIP**. Sistema Interconectado Patagónico.

**TCP/IP**. *Transmission Control Protocol / Internet Protocol*. Protocolo de control de transmisión / Protocolo de Internet.

**TFI**. Trabajo Final Integrador.

**TI**. Tecnología de la Información.

**TIC**. Tecnologías de la Información y las Comunicaciones.

**TMS**. *Transportation Management System*. Sistema de Gestión del Transporte (de electricidad).

**TO**. Tecnología de Operaciones.

**Transener**. Compañía de Transporte de Energía Eléctrica en Alta Tensión Transener S.A.

**UMTS**. Universal Mobile Telecommunications System. Sist. de Telecomunicaciones Móviles Universal.

**VHF-UHF**. Very High Frequency – Ultra High Frequency. Frecuencia Muy Alta – Ultra Alta Frecuencia.

**WIB**. *Werkgroup voor Instrument Beoordeling* Grupo de trabajo para Habilitación de Instrumentos (Holanda).

**WiMAX**. Worldwide Interoperability for Microwave Access. Interoperab. Mundial Acceso Microondas.

## Bibliografía. Fuentes


1. Real Academia Española, Diccionario de la lengua española, 22° edición. 2012. Obtenido el 28/01/15 desde el sitio web http://lema.rae.es/drae/?val=cibernética
2. Rouse, Margaret. Cyber. Sin indicación de fecha de publicación. Obtenido el 30/01/15 del sitio web http://searchsoa.techtarget.com/definition/cyber
3. Real Academia Española. Diccionario de la lengua española, 22° edición. 2012. Obtenido el 26/03/15 del sitio web http://lema.rae.es/drae/?val=seguridad
4. Real Academia Española, Diccionario de la lengua española, 22° edición. 2012. Obtenido el 26/03/15 del sitio web http://lema.rae.es/drae/?val=seguro
5. Stein, Abraham. El concepto de Seguridad multidimensional. Pág. 31. Sin indicación de fecha de publicación. Obtenido el 26/03/2015 del sitio web http://www.fundacionpreciado.org.mx/biencomun/bc176-177/A_Stein.pdf
6. Linares, Samuel. Presentación titulada “Implementando la Ciberseguridad desde la realidad: Perspectiva desde Europa, América y Medio Oriente”. Pág. 5. Junio 2015. Programa del evento obtenido el 01/06/2015 del sitio web https://www.cci-es.org/documents/10694/0/IV+Congreso+Iberoamericano+de+Ciberseguridad+ESP/cbfc6f0d-9210-417d-bdcf-60692ad77c4c
7. International Telecommunication Union (ITU). Decisiones destacadas de Guadalajara, Ciberseguridad, Resolución 181. Noviembre 2010. Obtenido el 27/05/2015 del sitio web https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx
8. Consejo Argentino de Relaciones Internacionales (CARI). Ciberdefensa: los riesgos que plantea. Pág. 2. Noviembre 2013. Obtenido el 27/05/2015 del sitio web http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf
9. Brunner, Elgin, et al. Focal Report 3, Critical Infrastructure Protection, Cibersecurity – Recent Strategies and Policies: An Analysis. Pág 6. Agosto 2009. International Relations and Security Network (ISN). Obtenido el 11/06/2015 del sitio web http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=108743
10. Pillajo, C. Sierra, J. Importancia del estudio del control para los sistemas cyber-físicos. Pág. 1. Diciembre 2014. Obtenido el 27/10/2015. URL: http://carlospillajo.info/wp-content/uploads/sites/1369/2014/12/Importancia-del-estudio-de-control-para-los-CPS_RevCP.pdf
11. Pillajo, C. Sierra, J. Importancia del estudio del control para los sistemas cyber-físicos. Pág. 2. Diciembre 2014. Obtenido el 27/10/2015. URL: http://carlospillajo.info/wp-content/uploads/sites/1369/2014/12/Importancia-del-estudio-de-control-para-los-CPS_RevCP.pdf
12. Paredes, Ignacio. Tsunami: ¿Vas a quedarte mirando la ola? Panorama actual de ciberseguridad industrial. Slide 7. Sin fecha de publicación. Obtenido el 27/10/2016. URL: http://es.slideshare.net/NextelSA/tsunami-vas-a-quedarte-mirando-la-ola-panorama-actual-de-ciberseguridad-industrial
13. Industrial Control Systems Information Sharing and Analysis Center. About ICS-ISAC, párrafo 3. Sin indicación de fecha de publicación. Obtenido el 12/06/2015 del sitio web http://ics-isac.org/blog/home/about/ (adaptado al castellano).
14. International Society of Automation. Cybersecurity. Home / Technical Topics / Cybersecurity. Sin indicación de fecha de publicación. Obtenido el 12/06/2015 del sitio web https://www.isa.org/technical-topics/cybersecurity/ (adaptado al castellano).
15. Jefatura de Gabinete de Ministros. Resolución 580/2011, Art. 2°. Julio de 2011. Obtenido el 12/06/2015 del sitio web http://www.infoleg.gov.ar/infolegInternet/anexos/185000-189999/185055/norma.htm
16. Centro de Ciberseguridad Industrial. Portal CCI, El Centro. Sin indicación de fecha de publicación. Obtenido el 27/01/2015 del sitio web https://www.cci-es.org/el-centro
17. WisePlant. Servicios para la Ciberseguridad Industrial, Pág. 3. Fecha de publicación: junio 2014. Obtenido el 27/10/2015 del sitio web http://docplayer.es/1228551-Servicios-para-la-ciberseguridad-industrial-ics.html
18. Definición ABC. Definición de infraestructura. Sin indicación de fecha de publicación. Obtenido el 16/06/2015. URL:http://www.definicionabc.com/general/infraestructura.php

19. Moteff, John D. Critical Infrastructures: Background, Policy, and Implementation. Pág. 2. Sin indicación de fecha de publicación. Obtenido el 10/06/2015 del sitio web https://www.fas.org/sgp/crs/homesec/RL30153.pdf (adaptado al castellano).
20. Thil, Eduardo A. Infraestructuras críticas, interoperabilidad y estándares: ejes para una administración electrónica efectiva. Pág. 12. Noviembre de 2010.Obtenido el 23/06/2015 del sitio web http://siare.clad.org/fulltext/0065716.pdf
21. CNPIC (Centro Nacional para la Protección de las Infraestructuras Críticas). ¿Qué es una infraestructura crítica? Sin fecha de publicación. Obtenido el 23/06/2015. URL: http://www.cnpic.es/Preguntas_Frecuentes/Que_es_una_Infraestructura_Critica/index.html
22. Luiijf, Eric et al. Critical Infrastructure Protection in The Netherlands: A Quick-scan. Pág.15. Fecha publicación: Enero 2003. Obtenido el 24/06/2015 del sitio web: https://www.emsec.rub.de/media/crypto/attachments/files/2011/03/bpp_13_cip_luiijf_burger_klaver.pdf (texto adaptado)
23. Administración Pública Nacional. Decreto 1067/2015. 10/06/2015. Obtenido el 23/06/2015 del sitio web: http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/247971/norma.htm
24. Administración Pública Nacional. Ibid.
25. Administración Pública Nacional. Ibid.
26. ICIC – Programa Nacional de Infraestructuras Críticas. Qué hacemos / Grupo de Infraestructuras Críticas. Sin indicación de fecha de publicación. Obtenido el 23/06/2015 del sitio web: http://www.icic.gob.ar/
27. Thil, Eduardo A. Op. cit.
28. Rinaldi S., Peeremboom J. y Kelly T., Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. Pág. 13. Diciembre 2001. Obtenido el 01/09/2015 del sitio web: http://user.it.uu.se/~bc/Art.pdf
29. Rinaldi S., Peeremboom J. y Kelly T., Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. Figure 1: Dimensions for describing infrastructure interdependencies. Pág. 12. Diciembre 2001. Traducido y adaptado al castellano. Obtenido el 01/09/2015 del sitio web: http://user.it.uu.se/~bc/Art.pdf
30. Rinaldi S., Peeremboom J. y Kelly T., Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. Figure 3: Examples of infrastructure interdependencies. Pág. 15. Diciembre 2001. Traducido y adaptado al castellano. Obtenido el 01/09/2015 del sitio web: http://user.it.uu.se/~bc/Art.pdf
31. Rinaldi S., Peeremboom J. y Kelly T., Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. Figure 2: Examples of electric power infrastructure dependencies. Pág. 14. Diciembre 2001.Traducido y adaptado al castellano. Obtenido el 01/09/2015 del sitio web: http://user.it.uu.se/~bc/Art.pdf
32. Fundelec (Fundación para el desarrollo eléctrico). El sector eléctrico. Situación anterior a la transformación, Ley 15336. Sin indicación en cuanto a fecha de publicación. Obtenido el 07/01/2016 del sitio web: http://www.fundelec.com.ar/el_sector.htm
33. Fundelec (Fundación para el desarrollo eléctrico). El sector eléctrico. El nuevo escenario. Sin indicación en cuanto a fecha de publicación. Obtenido el 08/01/2016 del sitio web: http://www.fundelec.com.ar/el_sector.htm
34. Fundelec (Fundación para el desarrollo eléctrico). Actores del Sistema eléctrico argentino. Sin indicación de fecha de publicación. Adaptación. Obtenido el 08/01/2016 del sitio web: http://www.fundelec.com.ar/el_sector.htm
35. Administración Pública Nacional. Decreto 231/2015. Fecha publicación 22/12/2015. Obtenido el 11/01/2016. URL: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257246/norma.htm
36. Ente Nacional Regulador de la Electricidad. ¿Qué es el ENRE? Sin indicación de fecha de publicación. Obtenido el 12/01/2016 del sitio web: http://www.enre.gov.ar/web/web.nsf/home
37. CAMMESA. Estatuto de Compañía Administradora del Mercado Mayorista Eléctrico S.A. Sin indicación de fecha de publicación. Obtenido el 11/01/2016 del sitio web: http://portalweb.cammesa.com/pages/institucional/agentes/estatuto.aspx

38. CAMMESA. Informe Anual 2015. Pág. 30. Fecha de publicación: 02/06/2016. Obtenido el 24/10/2016 del sitio web: http://portalweb.cammesa.com/Documentos%20compartidos/Informes/Informe%20Anual%202015.pdf
39. Pampa Energía. Transmisión. Sin indicación de fecha de publicación. Obtenido el 13/01/2016 del sitio web: http://www.pampaenergia.com/sp/NUE_TRANSMISION.ASP
40. Ministerio de Energía y Minería. Series históricas de energía eléctrica / Cantidad de usuarios total país 1991-2012. Publicación: 27/12/2013 Obtenido el 25/10/2016 de la URL: http://www.energia.gob.ar/contenidos/archivos/Reorganizacion/informacion_del_mercado/publicaciones/mercado_electrico/historicos/Serie%20cantidad%20de%20usuarios%201991-2012.xls
41. CAMMESA. Informe Anual 2015. Pág. 17. Fecha publicación: 02/06/2016. Obtenido el 24/10/2016. URL: http://portalweb.cammesa.com/Documentos%20compartidos/Informes/Informe%20Anual%202015.pdf
42. Fundelec (Fundación para el desarrollo eléctrico). Enlaces. Sin indicación de fecha de publicación. Obtenido el 26/10/2016 del sitio web: http://www.fundelec.com.ar/enlaces.htm
43. CFEE. Perfil del Organismo. Sin indicación de fecha de publicación. Obtenido el 24/10/2016 del sitio web: http://www.cfee.gov.ar/perfil-organismo.php
44. Fundelec (Fundación para el desarrollo eléctrico). Enlaces. Sin indicación de fecha de publicación. Obtenido el 26/10/2016 del sitio web: http://www.fundelec.com.ar/enlaces.htm
45. CFEE. Perfil del Organismo. Sin indicación de fecha de publicación. Obtenido el 24/10/2016 del sitio web: http://www.cfee.gov.ar/perfil-organismo.php
46. Asociación Electrotécnica Argentina. Redes Eléctricas Inteligentes. Fecha de publicación: Agosto de 2013. Página 7.
47. CCI. CCI lanza una nueva serie de documentos sobre las tecnologías de operación inteligentes, "Smart OT". Fecha publicación 06/05/2016. Obtenido el 26/10/2016. URL: https://www.cci-es.org/web/cci/detalle-actividad/-/journal_content/56/10694/232182
48. CCI. Curso taller “Aplicando ISA99 para proteger las infraestructuras industriales”. Adaptado del Slide 3, titulado “Diferencias en Seguridad”. Fecha de publicación 04/06/2015. Nombre del archivo: 03-0930-1030-IT-vs-OT-TALLERISA99.pdf.
49. CCI. Curso taller “Aplicando ISA99 para proteger las infraestructuras industriales”. Fecha de publicación 04/06/2015. Adaptado de los Slides 4,5 y 6. Fecha de publicación 04/06/2015. Nombre del archivo: 03-0930-1030-IT-vs-OT-TALLERISA99.pdf.
50. CCI. Curso taller “Aplicando ISA99 para proteger las infraestructuras industriales”. Fecha de publicación 04/06/2015. Adaptado de los Slides 72 a 77. Fecha de publicación 04/06/2015. Nombre del archivo: 03-0930-1030-IT-vs-OT-TALLERISA99.pdf.
51. ConceptoDefinicion. Definición de Norma. Sin indicación en cuanto a fecha de publicación. Obtenido el 05/11/2016 del sitio web: http://conceptodefinicion.de/norma/
52. DeConceptos. Definición de Estándar. Sin indicación en cuanto a fecha de publicación. Obtenido el 05/11/2016 del sitio web: http://deconceptos.com/ciencias-sociales/estandar
53. CERTSI. IEC 62443: Evolución de la ISA 99. Definición de Norma. Publicado el 25/08/2015. Obtenido el 06/11/2016 del sitio web: https://www.certsi.es/blog/iec62443-evolucion-isa99
54. CERTSI. IEC 62443: Evolución de la ISA 99. Definición de Norma. Publicado el 25/08/2015. Obtenido el 06/11/2016 del sitio web: https://www.certsi.es/blog/iec62443-evolucion-isa99
55. ISA 99 Commitee. ISA99: Developing the ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security. Publicado el 04/09/2015. Obtenido el 06/11/2016 del sitio web: http://isa99.isa.org/ISA99%20Wiki/Home.aspx
56. Blog Segu-Info. Nueva revisión de NIST SP 800-53: ciberseguridad para organizaciones. Publicado el 12/03/2012. Obtenido el 06/11/2016 del sitio web: http://blog.segu-info.com.ar/2012/03/nueva-revision-de-nist-sp-800-53.html
57. NIST. SP 800-82 Revision 2. Guide to Industrial Control Systems (ICS) Security. Publicado mayo 2015. Obtenido el 06/11/2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
58. NERC.CIP Standards. Sin indicación en cuanto a fecha de publicación. Obtenido el 06/11/2016 de la página web: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
59. Automatas.org. SISTEMAS SCADA. Publicado el 02/03/2006. Obtenido el 12/11/2016 del sitio web: http://www.automatas.org/redes/scadas.htm

60. Blog de Control de Accesos. ¿Qué es un sistema SCADA? Publicado el 23/04/2008. Obtenido el 12/11/2016 del sitio web: http://control-accesos.es/scada/%C2%BFque-es-un-sistema-scada
61. Rodríguez Penin, Aquilino. Sistemas SCADA 2° Ed. 2007. Sección xiii y Pág. 19. Presentación / El Sistema Scada.
62. Rodríguez Penin, Aquilino. Sistemas SCADA 2° Ed. 2007. Págs. 33-39. Arquitectura de un sistema Scada.
63. LogicElectronic. Qué es un PAC. Adaptado del Cuadro Comparativo. Sin indicación en cuanto a fecha de publicación. Obtenido el 20/11/2016 del sitio web: http://www.logicelectronic.com/BECKHOFF/Que%20es%20un%20PAC.htm
64. Heffel, Walter. Comparación entre SCADAs y DCSs. Elaboración propia en base a contenidos de la entrada "What are the two major differences between DCS and SCADA systems?". Publicación: 30/09/2014. Consultado el 20/11/2016. https://www.researchgate.net/post/What_are_the_two_major_differences_between_DCS_and_SCADA_systems
65. Kon, Maximilian. ¿Qué hay de cierto, aciertos y desaciertos cuando se habla de convergencia IT/OT? Slide 2. Fecha pub: 29/06/2016. Obtenido el 26/11/2016. URL: http://wisecourses.com/wp-content/present/ConvergenciaITOT/index.html
66. Kon, Maximilian. Jerarquía de los Sistemas Industriales. Slide 2. Adaptación. Fecha pub: 29/06/2016. Obtenido el 26/11/2016. URL: http://wisecourses.com/wp-content/present/ConvergenciaITOT/index.html
67. ENER. Plataforma de gestión integrada, servicio de distribución de energía. Anexo C. Fecha pub: 06/06/2016. Págs. 10,11,12.
68. WeLiveSecurity. Captura pantalla de archivo Excel con macros, vector de infección. Fecha pub: 05/01/2016. Obtenido 01/12/2016. URL: http://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/
69. WisePlant. Caso de Estudio: Hackeo de la Red de Distribución Eléctrica en la zona oeste de Ukrania el pasado 23/12/2015. Fecha pub: 27/03/2016. Obtenido el 01/12/2016. URL: http://wiseplant.com/2016/03/27/analisis-del-hackeo-de-la-red-electrica-de-ukrania-el-pasado-23-de-diciembre-de-2015/
70. Kon, Maximilian. ¿Qué hay de cierto, aciertos y desaciertos cuando se habla de convergencia IT/OT? Slide 5, adaptación. Fecha pub: 29/06/2016. Obtenido el 02/12/2016. URL: http://wisecourses.com/wp-content/present/ConvergenciaITOT/index.html
71. INCIBE. Ciber-resiliencia, aproximación a un marco de medición. Pág. 45. Fecha pub: 06/05/2014. Obtenido 02/12/2016. URL: https://www.incibe.es/extfrontinteco/img/File/Estudios/int_ciber_resiliencia_marco_medicion.pdf. URL de la fuente original: http://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework
72. AEA. Redes Eléctricas Inteligentes. AEA 92559. Parte 1. Guía de conceptos, beneficios y desafíos para su implementación. Pág. 10. Edición: Agosto 2013.
73. AEA. Redes Eléctricas Inteligentes. AEA 92559. Parte 1. Guía de conceptos, beneficios y desafíos para su implementación. Pág. 20. Edición: Agosto 2013.
74. AEA. Redes Eléctricas Inteligentes. AEA 92559. Parte 1. Guía de conceptos, beneficios y desafíos para su implementación. Pág. 21. Edición: Agosto 2013.
75. AEA. Redes Eléctricas Inteligentes. AEA 92559. Parte 1. Guía de conceptos, beneficios y desafíos para su implementación. Pág. 45. Adaptación. Edición: Agosto 2013.
76. G. Mercado, J.M. Da Peña, et.al. SG-SM - Smart Grid San Martin. Red de Distribución y Generación de Energía Inteligente en Ciudad Gral San Martin, Mendoza. Adaptación. Sin indicación en cuanto a fecha de publicación. Obtenido el 05/12/2016. URL: http://sedici.unlp.edu.ar/bitstream/handle/10915/45305/Documento_completo.pdf?sequence=1
77. Tecnomundo. Nuevo software permite hackear los medidores digitales de electricidad. Fecha pub.: 20/07/2012. Obtenido el 07/12/2016. URL: http://www.tecnomundo.net/2012/07/nuevo-software-permite-hackear-los-medidores-digitales-de-electricidad/

78. Industrial Internet Consortium. Industrial Internet of Things Volume G4: Security Framework. Fecha de publicación: 19/09/2016. Obtenido el 07/12/2016. URL: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf
79. WisePlant. Caso de Estudio: Hackeo de la Red de Distribución Eléctrica en la zona oeste de Ukrania el pasado 23/12/2015. Una mirada cauta del incidente. Fecha pub: 27/03/2016. Obtenido el 02/12/2016. URL: http://wiseplant.com/2016/03/27/analisis-del-hackeo-de-la-red-electrica-de-ukrania-el-pasado-23-de-diciembre-de-2015/

El presente documento fue editado con Microsoft Word Professional Plus 2016 e impreso en formato PDF usando el complemento Foxit Reader PDF Printer incluido en la versión 7.3.6.321 de Foxit Reader.

La entrega final es acompañada de un archivo llamado Hash-SHA-512.PDF, conteniendo la cadena correspondiente al cálculo de la función de resumen o digesto sobre el archivo **IUA-FI-ESI-TFI-Heffel-Walter.PDF**, realizado con la herramienta WinHasher 1.6. Dicho Hash garantiza la integridad del archivo PDF original que contiene el Trabajo Final Integrador.