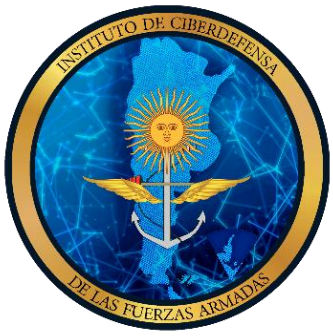


INSTITUTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS

DIPLOMATURA UNIVERSITARIA EN GERENCIAMIENTO DE LA CIBERDEFENSA

TRABAJO FINAL INTEGRADOR

ANÁLISIS DE LA AMENAZA CIBERNÉTICA EN EL SECTOR ELÉCTRICO ARGENTINO: IMPLICANCIAS

Integrantes del Equipo Nro 2:

DRA MÓNICA BORETTO

CR CARLOS MARTÍN

CR DIEGO MARGHEIM

CR JOSÉ BRUSA

MY EUGENIA ROTELA

Títulos Profesionales / de grado

Abogacía

Licenciados en Estrategia y Organización

Ingeniería Electrónica

08 de noviembre de 2024

Resumen

Este trabajo analiza las vulnerabilidades críticas del Sistema Argentino de Interconexión (SADI), con especial foco en la Compañía Administradora del Mercado Mayorista Eléctrico Sociedad Anónima (CAMMESA), y propone estrategias de ciberseguridad para mejorar su resiliencia operativa. Se identifican factores de riesgo en sistemas eléctricos, clasificados en externos, tecnológicos, operativos, de mercado e intencionales, como los ciberataques. A nivel internacional, se examinan incidentes como los ciberataques a Ucrania (2015-2022), que afectaron gravemente su infraestructura energética, y el apagón de 2019 en Argentina, causado por fallas operativas y la falta de protocolos de seguridad que expusieron el sistema a riesgos cibernéticos.

Se argumenta que el SADI debe considerarse como una infraestructura crítica, protegiendo tanto sus componentes materiales (plantas, líneas de transmisión) como los intangibles (información y flujos virtuales). Para mejorar su seguridad, se propone un enfoque integral de ciberseguridad que incluya la segmentación de redes, la identificación de activos críticos, la capacitación del personal y protocolos operativos robustos.

El trabajo emplea un enfoque metodológico deductivo, complementado con análisis inductivos. Utilizando los modelos Kill Chain y MITRE ATT&CK, se analiza el impacto de ciberataques previos y la situación actual de la ciberseguridad del SADI y CAMMESA. Los objetivos específicos incluyen la identificación de vulnerabilidades, el análisis de incidentes internacionales y la propuesta de un marco de ciberseguridad adaptado a las mejores prácticas internacionales.

En conclusión, se subraya la necesidad urgente de fortalecer la ciberseguridad del SADI para mitigar los riesgos de ciberataques y garantizar la fiabilidad del suministro eléctrico, protegiendo las infraestructuras críticas de Argentina.

***Palabras Claves**:* Infraestructura Crítica, Ciberataque, Sistema Argentino de Interconexión, Riesgos cibernéticos, Ciberdefensa, Segmentación de redes, Protocolos operativos, Capacitación del personal, Respuesta a incidentes, CAMMESA, Mercado Eléctrico Mayorista, Riesgos de ciberamenazas, Kill Chain, MITRE ATT&CK, Amenazas persistentes avanzadas (APT), Red OT (Operational Technology), Red IT (Information Technology), Aislamiento de redes, Spear-phishing, Sabotaje, Brecha IT/OT, Modelo Purdue, Control de acceso lógico, Sandworm, BlackEnergy, Industroyer .

ÍNDICE GENERAL

Justificación / Fundamentación / Aportes

A la hora de clasificar **factores de riesgo** para sistemas eléctricos, en Bo et al (2015) contextualizándolos a nivel internacional se proponen los siguientes: *externos, tecnológicos, operativos, de mercado e **intencionales**.* Dentro de estos últimos, puede haber hechos de vandalismo, incluyendo **ciberataques**…[1]

Con la intención de tener una dimensión del porqué se trata de una ***Infraestructura Crítica (IC),*** en el anexo 1 se enumeran los mayores colapsos eléctricos en el mundo, previo a que, en diciembre de 2015 alrededor de la mitad de los hogares en la región ucraniana de Ivano-Frankivsk (con una población de 1,4 millones de habitantes), se quedaran sin electricidad durante unas horas...[2]. Las acciones ofensivas se intensificaron en 2016 y en 2022, bajo tácticas y técnicas que fueron mutando en pos del objetivo buscado.

En el caso de nuestro país, si bien hubo apagones importantes registrados[3], el ocasionado el 16 de junio de 2019 afectó prácticamente a todo el territorio argentino con repercusiones en Paraguay y Uruguay, por una falla en la línea Colonia Elía (ER) - Campana (BA).

De acuerdo con los especialistas, el origen de la interrupción energética de 2015 el en el país europeo, "…fue un "virus" utilizado en un "ataque de hackers" (…) utilizando una familia de malware (…): **BlackEnergy**[4]. En concreto, este backdoor se utilizó para instalar un componente **KillDisk** en los equipos de destino, cuya función fue impedir que arranquen…"[5]. Al año siguiente, se usó el malware **Industroyer**[6] con el objetivo de disrupción distribuida sobre la matriz energética, focalizándose sobre los procesos que operan los ICS en subestaciones eléctricas.

Ya en 2022, utilizaron una combinación de los malware **GEOGETTER**, **Neo-REGEORG, CadyWiper** y otras técnicas de acceso a la Supervisión, Control y Adquisición de Datos (SCADA, por sus siglas en inglés, Supervisory Control and Data Acquisition), del mercado eléctrico para su afectación.

Para el caso argentino, expertos que estudiaron el caso concluyeron que los motivos de este fue un equilibrio inestable causado por menor demanda, a raíz de una falla en cascada a través de factores externos, tecnológicos y operativos o de gestión.[7.]

---

[1] CALCAGNO, D.L. et al. Análisis de vulnerabilidades e interrupciones del sistema argentino de interconexión. **Rev. Tecnol. Soc**., Curitiba, v. 18, n. 54, p. 53-73, out./dez., 2022. Pág 6.
[2] https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/
[3] Entre paréntesis, se enumeran los factores que influyeron: En AMBA, de febrero 1999, 160.000 personas afectadas durante 11 días (externos y operativos). En CABA, AMBA, Córdoba, La Pampa, Neuquén, Río Negro y Santa Fe, de noviembre de 2002 dejó sin luz por 4 hs, a 16 millones de personas (externos y tecnológicos).
[4] https://attack.mitre.org/software/S0089/
[5] https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/
[6] https://attack.mitre.org/software/S0604/
[7]https://www.infobae.com/sociedad/2019/06/16/la-secretaria-de-energia-atribuyo-el-apagon-al-clima-y-fallas-en-el-sistema-de-proteccion/

En las consideraciones finales, pusieron de relieve al **Sistema Argentino de Interconexión** (**SADI) como IC**, debiendo focalizarse en su componente material (plantas, líneas de transmisión y todo tipo de equipamiento) e intangibles (tales como la información y los flujos virtuales), así como en el personal interviniente. La realización de evaluaciones periódicas debiera permitir anticipar las falencias y fallas, de manera de minimizar sus consecuencias, trabajando sobre los sistemas operativos…[8]

¿Ciberseguridad o ciberdefensa?

"…La Organización del Tratado del Atlántico Norte (OTAN) ha declarado oficialmente el 16 de junio de 2016 al espacio cibernético como una zona de guerra (…) Este posee ciertas características: no tiene límites geográficos como lo puede tener el espacio terrestre o marítimo; es de fácil acceso económico y virtual; se difuman los conceptos tradicionales de ataque y defensa; puede ser usado para fines loables o, por el contrario, para fines delictivos o para afectar la seguridad de un Estado; es anónimo (…) se desdibuja la diferencia civil – militar…[9]

En Argentina, por Resolución del Ministro de Defensa 343/2014 se creó el Comando Conjunto de Ciberdefensa. Y a través del decreto 577/2017, el Gobierno Nacional creó el Comité de Ciberseguridad. En ambos documentos se hace hincapié en la necesidad de "proteger las **IICC**". Los autores concluyen que "…en un mundo continuamente cambiante (…) se adopta el concepto de ***Seguridad del Estado***, en los términos establecidos por la Asamblea General de la Organización de las Naciones Unidas (ONU) en su Documento A 40/553 del año 1986; es decir, "la condición en que los estados pueden libremente continuar con su desarrollo y progreso, al no existir peligro de un ataque militar, presión política o coerción económica" …[10]

El Consejo Mundial de la Energía, recomienda que las empresas energéticas consideren los riesgos cibernéticos como riesgos empresariales fundamentales, (…) y elaborar normas y mejores prácticas para hacer frente a estas amenazas actuales.[11] Aquí también se define como Infraestructuras Críticas de la Información (ICI), a las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud, el bienestar de los

[8] CALCAGNO, D.L. et al. y otros. Ibíd. Pág 17.
[9] Operaciones militares cibernéticas: planeamiento y ejecución en el nivel operacional / Gustavo Adolfo Trama; Evergisto Arturo de Vergara. - 1a ed . - Ciudad Autónoma de Buenos Aires : Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, 2017. Pág 12, 16/17.
[10] Ibíd. Pág 118/9
[11] Deloitte (Corrado, Nicolás – Socio de Ciberseguridad; Pizarro, Carolina – Senior Manager Ciberseguridad; Gorena Cristian – Gerente Ciberseguridad) – Fortinet (Aguayo Fuentealba, Pablo – SE Territorio Enterprise Industrias, RRNN y Utilities; Cuadrado Corsse, Luz María – MAM Territorio Enterprise Industrias, RRNN y Utilities; Arias Aparicio, Juan Pablo – SE Manager Fortinet Chile; Salas Varela, Pía – Country Manager Fortinet Chile. Diciembre 2022. Pág 4.

ciudadanos y el efectivo funcionamiento del Estado y del sector privado."[12] Adicionalmente, se dice que "las ICI se deberán diseñar con una arquitectura que maximice su robustez y resiliencia frente a eventos que las puedan inhabilitar, adaptándose a fenómenos de la naturaleza, intervenciones humanas o interferencias informáticas tales como incidentes involuntarios o ciberataques."

Como ya se ha afirmado, resulta casi imposible identificar al agresor cibernético, considerándose necesario adoptarse un enfoque basado en efectos. "…Es decir, la intervención del Sistema de Defensa en el ciberespacio debe estar definida no por quien produce el ataque, sino en base a qué infraestructura o sistema está siendo afectado…", adhiriendo al "Programa Nacional de ICI y Ciberseguridad" a fin de incrementar la seguridad de las redes del sistema.[13]

Además, los Estados tienen que promover las denominadas ***Operaciones Interagenciales***. En este ámbito "…la cooperación entre las distintas agencias del gobierno, las compañías privadas y el público para combatir las ciberamenazas es mucho más complicada de lo que debiera ser. (…) La mayoría de las estrategias reconocen que la seguridad de los sistemas de información que comprenden la Internet requiere de una alianza entre el gobierno, las universidades y la industria. La sociedad política y la sociedad civil deben unificar esfuerzos…".[14]

Planteamiento del Problema

El presente trabajo integrador final analizará si el SADI enfrenta vulnerabilidades críticas que comprometen su operatividad y fiabilidad, evidenciadas en el apagón de 2019, donde fallas operativas y el incumplimiento de protocolos de seguridad expusieron el sistema a riesgos significativos, incluyendo posibles amenazas cibernéticas.

Formulación del Problema

¿Cuáles son las vulnerabilidades críticas del SADI que afectan su operatividad y fiabilidad, y cómo pueden las amenazas cibernéticas y los fallos en la implementación de protocolos de seguridad incrementar el riesgo de colapsos, como el apagón de 2019?

Solución Propuesta

Para dar respuesta al interrogante planteado y dado el carácter y la diversidad de los ciberataques modernos, se considera necesario para mitigar estas vulnerabilidades, adoptar un enfoque integral de ciberseguridad que contemple la segmentación de redes, la identificación y

[12] Ibíd. De la Política Nacional de Ciberseguridad de Chile.
[13] Ibíd. Pág 135
[14] Ibíd. Pág 120

priorización de activos críticos, y el fortalecimiento de la capacitación del personal. Esto debe complementarse con los protocolos operativos robustos y el establecimiento de respuesta a incidentes, en línea con las acciones que lleve adelante CAMMESA.

Asimismo, para alcanzar dicha solución a la problemática planteada, el equipo pretende alcanzar los objetivos según el siguiente detalle:

Objetivos

Principal o General

Analizar las vulnerabilidades del SADI, con foco en CAMMESA y proponer estrategias de ciberseguridad que mejoren su resiliencia y fiabilidad operativa.

Particulares o Intermedios

Objetivo Particular Nro 1

Identificar y evaluar las principales vulnerabilidades del SADI, incluyendo factores operativos como ciberamenazas, y su impacto en la seguridad del suministro eléctrico, a través del desarrollo del marco

Objetivo Particular Nro 2

Analizar los ciberataques al sistema eléctrico sufridos por Ucrania en los años 2015, 2016 y 2022; utilizando las modelizaciones Kill Chain y MITRE ATT&CK.

Objetivo Particular Nro 3

Estudiar la situación actual de ciberseguridad del SADI en general y de CAMMESA en particular a través de las modelizaciones Kill Chain y MITRE ATT&CK, a fin de proponer un marco de ciberseguridad, en línea con las mejores prácticas necesarias llevar adelante por esa Compañía.

Metodología

El método a emplear para desarrollar el trabajo de investigación será del tipo deductivo, con ciertas inferencias inductivas, para ello se realizarán análisis y descripciones durante el desarrollo de cada capítulo a fin de obtener conclusiones parciales surgidas de cada uno de ellos y que permitan dar respuesta al objetivo general planteado por la investigación. Para lo cual, se utilizarán los modelos de análisis Kill Chain y MITRE ATT&CK, como herramientas para el estudio del caso Sistema Eléctrico Argentino (SEA), con foco en CAMMESA.

Capítulo 1 - MARCO TEÓRICO

Sección 1: Breve descripción de la matriz energética y del Sistema Eléctrico Argentino (SEA)

La matriz energética nacional está conformada principalmente por fuentes termoeléctricas (59%), hidroeléctrica (25%), renovables (12%) y nuclear (4%)[15]

Las primeras surgen de las cuencas del Noroeste (3% del aporte de gas), Cuyana (3% del petróleo), Neuquina (principal fuente, Vaca Muerta), Golfo de San Jorge (30% del petróleo) y Austral (20% del gas natural, fuente off-shore). Por su parte, el caudal hidroeléctrico no solo proviene de la Cuenca Mesopotámica (Paraná y Uruguay, y sus afluentes), siendo sus emblemas las centrales binacionales de Yacyretá y Salto Grande (3.600 MW de potencia instalada). Además, existen otras casi cien centrales distribuidas en todo el país.[16]

La energía nuclear es aportada a través de tres centrales: Atucha I y II (Lima – Buenos Aires) y Embalse Río III (Córdoba).

Las renovables son aportadas por el sol y el viento. Las primeras, tienen su mayor aprovechamiento en el noroeste de nuestro país (a partir del norte de Mendoza). La eólica proviene de la Patagonia principalmente y del Noroeste Argentino (NOA) en menor medida. En el opuesto del cuidado medioambiental, funcionan en nuestro país dos centrales a carbón: Central Térmica San Nicolás[17] y Río Turbio (Santa Cruz).

Para unir las fuentes a las centrales productoras, la distribución de las fuentes precitadas se realiza a través de gasoductos, oleoductos, poliductos y tendidos de alta tensión (que luego, se transforma en media y baja, a partir de transformadores).

El SADI está formado por estas líneas de alta tensión, que transportan energía eléctrica uniendo cinco áreas (Cuyo, Comahue, Buenos Aires, Noroeste, Noreste y la región patagónica, excepto Tierra del Fuego).

La empresa de Transporte de Energía Eléctrica en Alta Tensión (TRANSENER), en tanto, es la encargada del sistema de transporte de alta tensión en todo el sistema de 500 kV y de algunas líneas del Sistema del Litoral de 220 kV. El resto corresponde a empresas de transporte regional, como Transnoa, Districuyo, Transba, Transnea y COTDT Comahue.

CAMMESA, formada por el Estado y privados, como cabeza del sistema es la responsable de coordinar y supervisar la operación del SADI, ya que ordena el despacho de generación en tiempo real y la coordinación de maniobras de mantenimientos o de adecuación de la configuración de las redes…”[18].

Sección 2: Marco jurídico y normativo

[15] https://www.argentina.gob.ar/sites/default/files/2022/01/energias_renovables_2021_se-c.pdf
[16] https://www.argentina.gob.ar/economia/energia/energia-electrica/hidroelectrica/centrales-hidroelectricas
[17] Que dejaría de operar a partir de 2026, según la operadora, AES; como parte de su estrategia del cuidado mediambiental.
[18] https://www.infobae.com/sociedad/2019/06/16/que-es-el-sistema-de-interconexion-electrica-y-por-que-su-falla-dejo-sin-luz-a-todo-el-pais/

Sector eléctrico

Más allá que la normativa nacional en este ámbito es amplia y se encuentra en permanente actualización, se consideran de incumbencia para este trabajo las siguientes:

- **Ley 24.065/91 (Marco Regulatorio Eléctrico)**[19], los Decretos reglamentarios y las Resoluciones de la Secretaría de Energía, comenzó a generarse durante 1992 la nueva estructura del mercado eléctrico, cuyas principales características son la segmentación vertical en función de las diferentes necesidades regulatorias de cada actividad: **Generación, Transmisión y Distribución**.

Por su parte, los consumidores se dividen en Grandes usuarios y Usuarios Finales. Los primeros se constituyen asimismo en agentes del Mercado Eléctrico Mayorista (MEM), tal como los integrantes de los subsectores anteriormente citados.[20]

En la misma Ley se determina la creación del Ente Nacional de Regulación de la Electricidad (ENRE), que tiene como funciones, entre otras: controlar la prestación de los servicios, dictar reglamentaciones, prevenir conductas monopólicas y establecer bases de cálculo de tarifas y fiscalizar las concesiones de jurisdicción federal.

Finalmente, define al transporte y la distribución de electricidad como servicio público, y establece las funciones del despacho nacional a través de CAMMESA.

- **Ley 23.696**: Declaró en estado de emergencia la prestación de diversos servicios y llevó a la reestructuración del sector de la energía.[21]
- **Resolución N° 508/15**: Establece requisitos para los materiales de instalaciones eléctricas, máquinas y herramientas para disminuir el riesgo eléctrico.[22]

Además, existen lineamientos y manuales que proporcionan orientación para el desarrollo integral del sector eléctrico, como el Manual de Buenas Prácticas 23 que define términos y expresiones aplicados en el ámbito de la tecnología eléctrica.

Ciberdefensa

La ciberdefensa en Argentina no tiene una regulación técnica específica, sino que surge de un conjunto de normas generales del ámbito de la Defensa, sobre la base de los principios

---

[19] Generación, transporte y distribución de electricidad, objeto - política general y agentes - transporte y distribución - provisión de servicios modifica a la ley 15336 en los incisos e) y g) del art.30 y el art.31, art. 4,11,14,18 inciso 8 y 28; deroganse los art. 17,20,22,23, los incisos a), b), c), d), y k) del 30 y los incisos e) al h) inclusive del 37,38,39,40,41,42 y 44.- promulgada por dec. 13 del 3-1-92, observada - los párrafos 3 y 4 del art. 93. (nota: "protocolo adicional al acuerdo de complementación económica nro. 16 entre argentina y chile sobre normas que regulan la interconexión eléctrica y el suministro de energía eléctrica" - bo 30/8/00, pag. 17; presupuesto enre 2001 - bo 15/9/00, pag. 14).

[20] https://servicios.infoleg.gob.ar/infolegInternet/anexos/5000-9999/9615/norma.htm

[21] Lineamientos para el desarrollo integral y sostenible del sector eléctrico al corto y mediano plazo PDF (www.argentina.gob.ar)

[22] MANUAL DE BUENAS PRÁCTICAS. MBP-Industria-Eléctrica.
PDF (www.srt.gob.ar)

[23] Ibíd.

fundamentales de la Constitución Nacional, base fundamental del marco jurídico argentino y disposiciones complementarias de ciberseguridad:

Leyes:

- Ley 23.554: Defensa Nacional.
- Ley 24.059: Seguridad Interior.
- Ley 25.506: Firma Digital.
- Ley 25.326: Protección de Datos Personales.
- Ley 26.388: Delitos Informáticos.
- Ley 26.904: Grooming.
- Ley 27.411: Convenio sobre Ciberdelito del Consejo de Europa (Convención de Budapest).[24]

Decretos:

- Decreto 1558/2001: Reglamentario de la Ley de Protección de Datos Personales.
- Decreto 2628/2002: Reglamentario de la Ley de Firma Digital.
- Decreto 577/2017: Creación del Comité de Ciberseguridad.
- Decreto 50/2019: Determina la responsabilidad primaria en materia de ciberseguridad y protección de ICI. [25]
- Decreto 1523/2019: se aprueba la definición de IICC y de IICCI.[26]
- Decreto DNU 614/2024: se disuelve la Agencia Federal de Inteligencia (AFI), … se crean organismos desconcentrados, entre ellos la Agencia Federal de Ciberseguridad (AFC).[27]

Decisiones Administrativas:

- DA 641/2021: Aprueba los Requisitos Mínimos de Seguridad de la información para organismos del Sector Públicos Nacional.
- DA 893/2022: Asigna funciones a la Dirección Nacional de Ciberseguridad, de la Secretaría de Innovación Pública.

Resoluciones:

- Resolución 829/2019: Infraestructuras Críticas e Infraestructuras Críticas de Información

[24] Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas. Argentina y la Unión Europea unen esfuerzos para combatir el ciberdelito. El ministro de Seguridad de la Nación, Aníbal Fernández, firmó hoy en Francia la adhesión de la Argentina al Segundo Protocolo Adicional del Convenio de Budapest de la Unión Europea, sobre ciberdelito, una herramienta que permitirá reducir el tiempo de las investigaciones de los ciberdelitos a nivel internacional.
https://www.argentina.gob.ar/noticias/argentina-y-la-union-europea-unen-esfuerzos-para-combatir-el-ciberdelito#:~:text=El%20ministro%20de%20Seguridad%20de,los%20ciberdelitos%20a%20nivel%20internacional.

[25] Guía técnica de prevención - 02 PREVENCIÓN DEL RIESGO ELÉCTRICO.2019.
2_guia_prevencion_riesgo_electrico_ok_PDF (www.argentina.gob.ar)

[26] https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-1523-2019-328599

[27] https://www.argentina.gob.ar/normativa/nacional/decreto-614-2024-401512

- Resolución 144/2020 Ministerio de Seguridad Protocolo general para la prevención policial del delito con uso de fuentes digitales abiertas.
- Resolución 44/2023: Aprueba la Segunda Estrategia Nacional de Ciberseguridad.
- Resolución 15/2024: Aprueba Lineamientos para el uso seguro de herramientas digitales.

De la misma manera que en el sistema eléctrico, el marco legal ciber está en proceso evolutivo. Ello también se ve reflejado en la dinámica organizacional del Estado para atender esta problemática.[28]

Normas técnicas:

- **ISO 27001**: Esta norma internacional proporciona directrices y un marco para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (ISMS, por sus siglas en inglés Information Security Management System). La implementación de esta norma ayuda a mitigar el riesgo de ciberataques y garantiza la integridad, confidencialidad y disponibilidad de los datos.

Algunos de los beneficios de su implementación en IC incluyen:

  - Mejora de la seguridad: Protege contra vulnerabilidades, amenazas de malware y ataques DDoS.
  - Cumplimiento normativo: Ayuda a cumplir con otras normativas de protección de datos, como el Reglamento Europeo de la Protección de Datos (RGPD) y el Marco de Ciberseguridad (CSF por sus siglas en inglés Cybersecurity Framework) del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés, National Institute of Standards and Technology)
  - Confianza y reputación: Demuestra a los clientes y partes interesadas que se toma en serio la seguridad de la información.
  - Reducción de riesgos: minimiza riesgos de ciberataques y exposición accidental de datos. [29]

- **ISO 62443**: Proporciona un marco para proteger la IC y los sistemas industriales para que sean robustos y resilientes frente a amenazas cibernéticas. Algunos de sus objetivos principales son:
  - Evaluación de Riesgos: Ayuda a identificar y evaluar riesgos relacionados con la ciberseguridad en entornos industriales.
  - Políticas de Seguridad: Establece directrices para el desarrollo de políticas de seguridad efectivas.
  - Arquitectura de Seguridad: Proporciona un marco para diseñar arquitecturas de seguridad que integren las medidas necesarias para mitigar riesgos.

[28] https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa
[29] https://www.akamai.com/es/glossary/what-is-iso-27001

- Gestión de Incidentes: Promueve la implementación de procesos para gestionar incidentes de seguridad.
- Concienciación y Formación: Enfatiza la importancia de la formación del personal en temas de ciberseguridad.

Sección 3: Ciberataques al sector eléctrico. Amenazas para Sistemas de Tecnologías de la Información y Tecnologías Operativas del SADI

Para el adecuado dimensionamiento de la problemática, es importante entender que el SADI integra tecnologías con brechas tecnológicas de más de 30 años en un marco operativo 24x7, es decir que no es factible "parar la máquina". Las soluciones deben implementarse a caballo de su funcionamiento.

Ahora sí, adentrándonos en la integración de redes de tecnología de la información (IT) y de tecnología operativa (OT)[30], resulta hoy necesario incorporar ya la seguridad por defecto en toda nueva incorporación de medios al sistema, por ejemplo, a través de medidores inteligentes que tengan incorporados mecanismos de detección de vulnerabilidades que aseguren estándares específicos de acuerdo con el tipo y marca del fabricante. En particular, es indispensable el monitoreo de ellas para la detección de incidentes, el compartir información a través de redes formales (Equipo de Respuesta ante Emergencias Informáticas (CSIRT por sus siglas en ingles Computer Security Incident Response Team), Plataforma para Compartir Información sobre Malware (MISP por sus siglas en inglés, Malware Information Sharing Platform, etc.) y sobre todo el tener un plan de respuesta ante incidentes de ciberseguridad dentro de un plan de Gestión de Crisis.

Entre las *principales amenazas* al sector energético se encuentra el acceso no autorizado (mediante métodos tradicionales (correos electrónicos con archivos adjuntos -*phishing*), el *ransomware* y las amenazas al almacenamiento en la nube, a partir de la naturaleza operativa continua del mercado eléctrico (24x7); así como y las Amenazas Persistentes Avanzadas (APT por sus siglas en inglés *Advanced Persistent Threats*).[31]

Vulnerabilidades de una red OT y su integración a una red IT[32]:

[30] Los ambientes OT contemplan tanto el software como hardware que ejerce cambios a través de un monitoreo directo o control de un dispositivo físico, proceso y/o eventos. La vida útil de los medios solía ser de 20/30 años, tendiendo a reducirse producto de la convergencia con los ambientes IT, con procesos limitados y que se tornan desactualizados en el tiempo, con anclaje hacia el fabricante y dificultades para la incorporación de parchajes. Por su parte, los ambientes IT se enfocan en la capacidad para almacenar, obtener, transmitir y manipular información. Su vida útil cada vez es menor (3/5 años) producto de la evolución tecnológica. Se trata de un entorno que facilita una alta escalabilidad de procesamiento, y dinámico a la hora del parchado, a través de equipos de personas dedicadas a ello. Deloitte – Fortinet, autores varios precitados. Pág 13.

[31] Deloitte – Fortinet, autores varios precitados. Pág 5/6.

[32] Deloitte – Fortinet, autores varios precitados. Pág 8.

Cuando los controles de los dispositivos físicos de una red OT se conectan con otras redes de datos, la superficie de ataque disponible para que un adversario comprometa a una organización industrial se expande. Entre las principales vulnerabilidades, encontramos las siguientes:

- Aislamiento: Tradicionalmente, la red OT se encontraba aislada de la red IT. Dado esto, la ciberseguridad no era usualmente una prioridad para la red OT.
- Vector de entrada (Spear-phishing, estaciones de trabajo comprometidas y el robo de credenciales): concientización hacia los empleados y monitoreo continuo de indicadores de compromiso (IoC).
- Sabotaje: a través de herramientas especializadas para penetrar redes OT, representando un mayor riesgo.
- La falta de segmentación dentro de una red OT es una de las vulnerabilidades más explotadas.
- Brecha IT/OT: administración de ambas áreas divididas son más susceptibles a sufrir ciberataques.
- Actores externos patrocinados por entes estatales.

Su integración con las redes IT, generan mayor vulnerabilidad para las OT por ser el eslabón más débil en la cadena de seguridad. Por lo tanto, amerita atender las debilidades que ambas presentan, de manera de asegurar la robustez de los sistemas operativos y de gestión, donde confluyen modelos de fuerza laboral remotos, uso de terceros para la gestión y mantenimiento de sistemas, incremento en uso de tecnología móvil y el uso de soluciones IT.[33] En el Anexo 2 se puede observar el modelo Kill Chain esquemático, donde la amenaza comienza a configurarse desde el ambiente IT.

Las posibles herramientas que se utilizan para llevar a cabo ciberataques en el sector eléctrico pueden ser maldocss, Troyano de Acceso Remoto (RAT), el empleo de la fuerza bruta, validadores de cuentas, Wipers, Malware IOT y Ransomware, entre otros.

Ahora bien, en el SADI, el Sistema de Operación en Tiempo Real (SOTR, por sus siglas en inglés, Real Time Operating System)[34] funciona a través de:

- Los sistemas de adquisición de datos de los Agentes del Mercado Eléctrico Mayorista (MEM) que participan del SOTR.
- Los medios de comunicación de datos y voz.

[33] "…Un estudio reciente indica que aproximadamente dos tercios de sistemas OT están conectados — 32% directamente a internet, y otro 32% por medio de un Gateway a la organización 1 . Si bien la tendencia es incuestionablemente hacia la convergencia, muchas organizaciones han encontrado que esta transición es más complicada —y riesgosa— que lo esperado…" (¿John Maddison, "Is Converging Your IT and OT Networks Putting Your Organization at Risk?" Fortinet, May 9, 2018. Pág 10

[34] https://cammesaweb.cammesa.com/inicio-sotr/

- El SCADA del Sistema Monetario Europeo (EMS, por sus siglas en inglés, European Monetary System) del **Centro Operativo de Control de CAMMESA (COC)**[35].

De esta manera, el SCADA del COC está bajo la responsabilidad directa de CAMMESA y el resto, incluyendo las comunicaciones, bajo la responsabilidad de cada uno de los Agentes. A aquella le compete, además, la coordinación del conjunto a través de las funciones que le confiere el marco normativo establecido por la Secretaría de Energía. Este proceso se divide en cuatro partes:

- Mantenimiento de los Equipos del SOTR de CAMMESA.
- Ingreso de Nuevos Enlaces.
- Gestión de Base de Datos SCADA/EMS.
- Control de los Enlaces de Datos.

En síntesis, se integran procesos **SCADA** con Sistemas de Control Distribuido, Controladores Lógico Programable (CLP), Sistemas de Control de Automatización Industrial (SCAI) y Unidades Terminales Remotas (UTR).

Arquitectura para fomentar la seguridad en OT[36]:

Los autores promueven el uso del modelo Purdue en el desarrollo de un plan de ciberseguridad en un ambiente OT. En el cual, se establecen ***5 niveles de seguridad***, divididos en ***3 zonas*** (de mayor a menor nivel de seguridad):

- Célula/ Área: 0 activos físicos de alto valor en el proceso; 1 dispositivos básicos inteligentes que manejan procesos físicos (CLP, UTR); 2 sistemas de control de área supervisores de procesos (HMI, maestros SCADA)
- De fabricación: 3 sistemas de operaciones de fabricación del producto in situ.
- Empresarial: 4 planificación del negocio, incluida la logística; 5 Infraestructura IT que controla el negocio.

Recomendaciones generales[37] (en el marco del modelo Purdue)

1. **Identificar activos**, clasificarlos y priorizar su valor.
2. **Segmentar la red (con diagramas actualizados) y generar soluciones antivirus/antimalware, sistemas de respaldo y parches de seguridad actualizados**, básico y fundamental en ambientes OT, de manera dinámica y no estática.
3. **Monitorear el tráfico** en cada segmento, de manera de minimizar las consecuencias que puedan ocasionar las vulnerabilidades

[35] El COC, a su vez se divide en el COC propiamente dicho, y en el **Centro Operativo de Control de Emergencias (COCE)**, el cual resulta clave para la Seguridad de la Información (propia del negocio y la operativa).
[36] Deloitte – Fortinet, autores varios precitados. Pág 22.
[37] Deloitte – Fortinet, autores varios precitados. Pág 23 y 24.

4. **Control de acceso lógico a plataformas y dispositivos** es un punto muy vulnerable desde el punto de vista ciber. Se deben establecer procesos de autenticación de usuarios y contraseñas seguras.
5. **Proteger puntos de acceso controlando el acceso físico**, normalmente con dispositivos administrados desde una interfaz central con conexión alámbrica (los medios inalámbricos son usados progresivamente, más allá de sus ineficiencias y vulnerabilidades) a través del establecimiento de reglas de seguridad en equipos perimetrales.
6. **Gestionar los incidentes de ciberseguridad** a través de un responsable**.** Al respecto, la experiencia en la implementación de programas de educación y concientización en seguridad y ciberseguridad resultan un eslabón necesario.

Sección 4: Análisis de vulnerabilidades de sistemas eléctricos a través del modelaje Kill Chain[38] y Mitre Att&Ck

A la hora de estudiar las debilidades de sistemas eléctricos, a las siete fases tradicionales de la Kill Chain IT (Reconocimiento, Armamento, Entrega, Explotación, Instalación, Comando y Control (C^2) y Acción sobre el Objetivo), se agregan las adicionales OT: Preparación (antes del Reconocimiento) e Impedir Respuesta (después de Acción sobre el Objetivo). (Anexo 2)

Por su parte, MITRE Tácticas, Técnicas y Conocimientos Comunes Adversarios (ATT&CK[39] por sus siglas en inglés, Adversarial Tactics, Techniques, and Common Knowledge), (Anexo 3) modeliza las operaciones cibernéticas a través de tres tipos de Framework: focalizadas en la Empresa[40], los Celulares[41] y los Sistemas de Control Industrial (SCI). Dentro de cada uno, se agrupan las tácticas[42] (es decir, los objetivos de los atacantes) en una estructura que permite entender el flujo de los ataques. Finalmente, por táctica existen técnicas asociadas, generándose de esta manera un modelo escalable exponencial. En este caso en particular, un sistema eléctrico es un ambiente IT/OT que se encuentra desplegado a lo largo y ancho de una amplia geografía, cualquiera sea ella.

Por ser el eslabón más débil, resulta de particular interés hacer foco **en el** modelo MITRE ATT&CK para ICS, que proporciona un marco estructurado de **tácticas y técnicas** específicas para entender las amenazas a que está expuesto. Este enfoque es particularmente adecuado

[38] Ver Anexo 2.
[39] Ver Anexo 3
[40] Para entornos PRE, Windows, macOS, Linux, Cloud, Network, Containers. (https://attack.mitre.org/matrices/ics/)
[41] Para entornos Android e Ios. (Ibíd).
[42] Para los entornos Empresarial y Celulares, se tipifican 14 tácticas y 12 en el ámbito ICS. A modo de ejemplo, encontramos Reconocimiento, Acceso inicial, Persistencia, Movimiento lateral, Comando y Control, Exfiltración. (https://attack.mitre.org/tactics/enterprise/)

para evaluar los ciberataques en IC, donde los atacantes buscan manipular, interrumpir o destruir sistemas de energía.

Capítulo 2 – Caso de estudio: Ataque cibernético a IC en Ucrania de 2015/2016/ 2022

Sección 1: Introducción

Este ataque fue uno de los primeros que impactó significativamente una red eléctrica, causando un apagón temporal en varias regiones de Ucrania mediante técnicas ciber avanzadas. El grupo responsable de los ataques es conocido como **Sandworm**[43], que se lo asoció a una unidad perteneciente a la inteligencia militar rusa, cuyos inicios data de 2009. En 2020 fue acusado en EEUU de haber ejecutado los ciberataques contra compañías eléctricas y organismos públicos de Ucrania en 2015, 2016 y 2022, entre otros.

En 2015, emplearon los malware **BlackEnergy**[44] y **KillDisk**. La **versión 3** del primero, dispone de un conjunto de herramientas que crea botnets para ser empleados para Ataques de Denegación de Servicios Distribuidos (DDoS), que fue evolucionando para soportar varios plug-ins. El segundo se trata de un software de destrucción permanente de datos a través de archivos sobre escritos con datos aleatorios a fin de impedir la ejecución de sistemas operativos. Inicialmente era parte del BlackEnergy y que fue usado de manera independiente con diferentes variantes.

Como se enunciara en el comienzo del trabajo, al año siguiente se usó el malware **Industroyer**[45] con el objetivo de disrupción distribuida sobre la matriz energética. Se focalizó sobre los procesos que operan los ICS en subestaciones eléctricas.

En el último caso, utilizaron una combinación de los malware **GOGETTER, Neo-REGEORG, CaddyWiper** y otras técnicas de acceso a los sistemas SCADA del mercado eléctrico para su afectación.

Sección 2: Uso de Kill Chain para analizar los ataques al Sistema Eléctrico de Ucrania

Para analizar el ciberataque de 2015 al sistema eléctrico de Ucrania con el modelo integrado Kill Chain IT/OT, que incluye las dos fases adicionales OT (Preparación e Impedir Respuesta), podemos desglosarlo en cada una de las etapas ya enumeradas en el capítulo 1, identificando cómo avanzaron los atacantes para comprometer la IC.

1. **Preparación (fase OT):** El objetivo inicial fue identificar los sistemas SCADA y los puntos críticos que permitirían afectar la distribución eléctrica. Entre las acciones ejecutadas, se

[43] "Gusano de arena", traducido del inglés. (https://attack.mitre.org/groups/G0034/)
[44] https://attack.mitre.org/software/S0089/
[45] https://attack.mitre.org/software/S0604/

dedicaron a recopilar información sobre los procedimientos operativos y tecnologías específicas empleadas por las empresas de energía. Para ello, realizaron ingeniería social y usaron otras técnicas de inteligencia para identificar debilidades en los sistemas de acceso remoto y prácticas de los empleados.

2. **Reconocimiento:** Los atacantes llevaron a cabo una investigación previa para identificar las redes y sistemas críticos. Esto incluyó la recolección de información sobre los empleados y la arquitectura de la red a través de ingeniería social y análisis de las conexiones remotas que usaba el personal técnico. De esta manera, lograron entender su topología y los accesos de usuarios clave para comprometer la infraestructura. A través de tácticas de phishing, accedieron a esas cuentas y lograron mapear la estructura de los sistemas críticos y las redes de control industrial.
3. **Armamento:** Su objetivo fue crear y personalizar herramientas para la infiltración y manipulación de ICS. Usaron para ello el malware BlackEnergy con módulos específicos para SCADA, enfocados en controlar sistemas de distribución. También desarrollaron KillDisk, un módulo adicional para captura de credenciales y destrucción de datos, con el fin de dificultar la recuperación.
4. **Entrega:** Utilizaron campañas de phishing para enviar correos electrónicos maliciosos a empleados clave. Los archivos adjuntos contenían el malware, que se activó una vez abiertos, infectando las computadoras de la red.
5. **Explotación**: Buscaron aprovechar vulnerabilidades en el sistema para ejecutar el malware y ganar acceso a los sistemas críticos. Cuando los empleados abrieron los archivos adjuntos maliciosos, el malware se activó y permitió a los atacantes obtener acceso inicial a las redes de control sin ser detectados.
6. **Instalación:** Implantaron el malware de manera persistente para asegurar el acceso continuo. Una vez comprometidos los sistemas, se instalaron herramientas adicionales para obtener y mantener acceso remoto a los sistemas SCADA. KillDisk se implementó para borrar registros y archivos críticos, impidiendo así una respuesta rápida.
7. **Comando y Control (C^2):** Lograron mantener el control y la comunicación con los sistemas comprometidos por medio de conexiones con servidores C^2 externos, permitiendo a los atacantes monitorear y controlar los sistemas infectados a distancia. Esta fase fue clave para ejecutar acciones precisas sobre los sistemas de distribución de energía.
8. **Acción sobre el Objetivo:** Tomaron el control de los sistemas SCADA, desde los cuales desconectaron subestaciones y estaciones de distribución. Esto provocó el corte en el suministro eléctrico en varias regiones de Ucrania. Asimismo, enviaron comandos para manipular y desactivar los sistemas de respaldo, dificultando la intervención de los operadores.
9. **Impedir Respuesta (fase OT):** Con el objetivo de asegurar que el impacto del ataque sea duradero y obstaculizar la recuperación, utilizaron KillDisk para borrar registros y archivos

esenciales en los sistemas afectados. Esto fue clave para prolongar el impacto del apagón y complicar la restauración de los sistemas afectados lo cual complicó los esfuerzos de recuperación.

Sección 3: Uso de Mitre ATT&CK para analizar los ataques al sistema eléctrico en Ucrania

Como se ha venido explicando, a lo largo de los tres años de ciberataques, los mismos fueron evolucionando/mutando/complementándose, en la intención que los mecanismos de ciberdefensa no pudieran neutralizar las agresiones. De esta manera, a continuación, se enumeran técnicas identificadas para cada oportunidad, agrupadas por ámbito de aplicación (en este caso, empresa e ICS).

Mitre ATT&CK - Técnicas utilizadas en 2015[46]

1. **Focalizas en Empresas:**
   - ✓ Protocolos de capas de aplicaciones Web: para afectar la comunicación de los hosts y sus servidores C^2, vía requerimientos a puertos HTTP.
   - ✓ Intérpretes de comandos y encriptación de Visual Basic (VB) en entorno Windows.
   - ✓ Creación de cuentas dominio.
   - ✓ Servicios remotos externos.
   - ✓ Modificación/desactivación de ajustes de seguridad de Web profunda.
   - ✓ Detección de archivos para su borrado.
   - ✓ Transferencia de herramientas maliciosas en sistemas infectados para usar lateralmente credenciales sustraídas a fin de destruir datos.
   - ✓ Logeo a través de datos pre capturados.
   - ✓ Transferencia de herramientas de manera lateral a través de los sistemas corporativos, con compromiso de los ICS.
   - ✓ Modificación de registros, previos a su envío a través de los sistemas C^2.
   - ✓ Network sniffing: captura de credenciales de usuario durante la comunicación entre la LAN y la matríz ICS.
   - ✓ Phishing: archivos enviados a través de correos electrónicos.
   - ✓ Inyección de procesos maliciosos, a través de archivos ejecutables.
   - ✓ Localización de procesos OT, a partir de ambientes IT.
   - ✓ Empleo de backdoor para afectar directorios raíz.
   - ✓ Ejecución de archivos maliciosos.
   - ✓ Validación de cuentas en ambientes corporativos.

[46] https://attack.mitre.org/campaigns/C0028/

2. **Apuntadas a ICS (en ambientes OT):**
   - ✓ Bloqueo de mensajes de comando, de reportes y de comunicaciones seriales.
   - ✓ Afectación de puertos usados por los sistemas, de conexiones proxy y de servicios remotos externos.
   - ✓ Manipulación y/o denegación de control y de servicios remotos.
   - ✓ Apagado y restauración de dispositivos.
   - ✓ Transferencia lateral de herramientas en entorno ICS.
   - ✓ Pérdida del control de equipos, de disponibilidad de sitios infectados y/o corte de suministro de energía.
   - ✓ Pérdida de productividad y ganancias.
   - ✓ Afectación de firmware (denegación/apagado provocando su no recuperación).
   - ✓ Mensajes de comando no autorizados.
   - ✓ Validación de cuentas.

Mitre ATT&CK - Técnicas utilizadas en 2016[47] (complementan el listado anterior).

1. **Focalizadas en Empresas:**
   - ✓ Intérpretes de comandos y encriptación PowerShell, Windows Command Shell, VB.
   - ✓ Fuerza Bruta.
   - ✓ Manipulación de cuentas dominios.
   - ✓ Uso de troyanos.
   - ✓ Servicios de Windows: creación o modificación de procesos de sistemas.
   - ✓ Desactivación de eventos de logeo en sistemas comprometidos.
   - ✓ Ofuscación de información o archivos.
   - ✓ Captura de credenciales legítimas.
   - ✓ Manipulación de administración compartida.
   - ✓ Afectación de software de servidores.
2. **Apuntadas a ICS (en ambientes OT):**
   - ✓ Afectación de interfaces de comandos en línea.
   - ✓ Enmascaramiento/renombrado de archivos.
   - ✓ Encriptación.

Mitre ATT&CK - Técnicas utilizadas en 2022[48] (complementan el listado anterior).

1. **Focalizadas en Empresas:**
   - ✓ Destrucción de datos.

[47] https://attack.mitre.org/campaigns/C0025/
[48] https://attack.mitre.org/campaigns/C0034/

- ✓ Modificación de políticas de dominio (GPOs).
- ✓ Afectación y tunelamiento de protocolos.
- ✓ Afectación de Tareas/Trabajos predefinidos (GPOs).
- ✓ Ataque a componentes de software de servidores.

2. **Apuntadas a ICS (en ambientes OT):**
   - ✓ Imágenes auto arrancables en servidores SCADA.
   - ✓ Modificación de ejecución del proxy de sistemas binarios en ambiente SCADA.

Capítulo 3 - Análisis de vulnerabilidades del SEA a ataques cibernéticos

Sección 1: Vulnerabilidades de CAMMESA y su mitigación

Volviendo al origen del presente trabajo, el apagón de 2019 dejó expuestas las vulnerabilidades del SADI. (…) En el caso de Argentina, los fallos que han desembocado en apagones se han debido principalmente a *factores climáticos, desastres naturales y vandalismo*. En el caso en cuestión, el factor humano fue el más importante… Si bien existían los protocolos de acción y que, además, los mismos fueron aprobados y habían nacido del consenso del Estado con las empresas transportistas, generadoras y distribuidoras, los mismos no fueron cumplidos acabadamente.

Pudo definirse como un evento excepcional, en el cual todos los sistemas de seguridad que debían proteger el funcionamiento del SADI funcionaron incorrectamente. Se trató de un fallo en cascada que condujo al colapso total del sistema de interconexión. Lo verdaderamente notable es que cada una de las fallas que se produjeron fue consecuencia de errores operativos, que pudieron haber sido evitados si se hubieran seguido todos los protocolos legalmente establecidos o si se hubieran detectado de manera temprana como posibles causas de fallos…Los autores afirmaron que CAMMESA, siendo el organismo responsable de la coordinación y supervisión de su funcionamiento, debería desarrollar **nuevos sistemas de control** de todas las empresas que forman parte de la generación, transporte y distribución de energía eléctrica.[49]

La respuesta a esta situación se concretó a través del **Procedimiento Técnico 29**[50] que se implementó en 2021 a fin de "…es determinar los controles y las acciones a instrumentar sobre aquellos procesos y sistemas asociados a la seguridad de la operación del SADI…" y es **producto de un trabajo conjunto entre CAMMESA y los Agentes del Mercado** en el marco

[49] CALCAGNO, D.L. et al. Análisis de vulnerabilidades e interrupciones del sistema argentino de interconexión. **Rev. Tecnol. Soc**., Curitiba, v. 18, n. 54, p. 53-73, out./dez., 2022. Pág 16.
[50] https://cammesaweb.cammesa.com/2024/01/29/pt-29-control-de-condiciones-de-seguridad-del-sadi/

del plan de acciones preventivas y de control para reducir riesgos de colapso y mejorar la confiabilidad operativa de este.

Son alcanzados por dicho Procedimiento todos los equipos, sistemas y procesos que se encuentren activos en instalaciones de los Agentes del MEM con el objetivo de realizar funciones específicas para cumplir con los requisitos estipulados, referentes a la seguridad de la operación e integridad del sistema. También son alcanzadas aquellas actividades que tengan por objeto recuperar en el menor tiempo posible el funcionamiento del sistema luego de un colapso parcial o total. Ello no incluyó la temática ciber.

De las últimas averiguaciones practicadas, CAMMESA actualmente se encuentra abocado a un proceso de mejora continua. A partir de una serie de entrevistas en cinco áreas[51], se definieron más de 160 oportunidades de evolución, convenientemente clasificadas y priorizadas[52]; con una hoja de ruta trazada para los próximos dos años a través de un Plan de Ejecución.

Dentro de ello, sí tienen previsiones para 2025 de desarrollar un Proyecto de Ciberseguridad (adoptando como marco la NORMA ISO 27.001:2022, focalizada en la Seguridad de la Información), que buscará mitigar una serie de hallazgos[53] de naturaleza Organizacional[54] y de Comunicaciones. De estos últimos surgen entre otras, las siguientes dimensiones donde focalizarán los esfuerzos: Redes y enlaces[55], **COCE[56]**, Servidores SCADA[57] y Continuidad Operativa[58].

De esta manera, se plantearon las siguientes iniciativas en materia de Seguridad (duración de cada proceso en meses):

- ✓ Primer semestre: Validar condiciones de continuidad del negocio (8), Ciberseguridad (5) y Continuidad operativa (6).
- ✓ Segundo semestre: Marco Normativo (3), Gobernanza Seguridad de la Información (2), Plan Estratégico Seguridad Informática (2) y Concientización (4).

[51] Ellas son: •Transparencia, Control y Trazabilidad; •Productividad y Procesos Colaborativos; •Seguridad y Continuidad Operacional; •Disponibilidad de información e interacción con los Agentes del Mercado y •Optimización y Desarrollo del Talento Organizacional.

[52] Las iniciativas se agruparon de la siguiente manera: 1. Oficina de transformación, 2. Colaboración y productividad, **3. Seguridad**, 4. Gestión administrativa, 5. Data/Cloud, 6. People, 7. Gestión tecnológica.

[53] Principalmente en el ámbito IT.

[54] Se definió la creación de un CONSEJO DE SEGURIDAD, cuya ausencia se visualiza de alto impacto. Del cual se deberá establecer rol y responsabilidades.

[55] Si bien el SCADA dispone de una red independiente y securizada, **hoy los agentes del mercado no tienen la obligación de comunicarse al COC y al COCE**. Esto impacta en la disminución de disponibilidad de la red SOTR del OT, ante una eventual caída del COC.

[56] No se encuentra totalmente integrado al proceso comunicacional, aspecto que se buscará generar para minimizar el riesgo que genera (no solo en materia de seguridad, sino principalmente, al modelo de negocios).

[57] Se trata de un conjunto de 2 servidores en el COC y otros 2 en el COCE. A estos últimos últimos, los agentes no tienen la obligación expresa de conexión. Además, la red administrativa no se encuentra convenientemente segmentada.

[58] Entre las necesidades detectadas, está la necesidad de no sacrificar seguridad en pos de velocidad de implementación, generar un plan de continuidad de negocios integral (operaciones y sistemas, incluida la seguridad)

Sección 2: Análisis de un supuesto Ciberataque en el SEA mediante MITRE ATT&CK – Caso: CAMMESA

A continuación, se analizan posibles vectores de ataque y vulnerabilidades en la infraestructura de CAMMESA usando el framework MITRE ATT&CK para sistemas ICS, considerando el impacto potencial en la operación y estabilidad del SEA. Como operador clave de esta IC, CAMMESA gestiona el despacho de energía eléctrica en Argentina y mantiene la estabilidad del sistema interconectado.

Framework MITRE ATT&CK para los ICS de CAMMESA

Se examinarán algunas de las **tácticas** más relevantes desde el reconocimiento hasta el impacto, analizando **técnicas específicas** que pueden aplicarse a sistemas de control de generación y distribución eléctrica en CAMMESA.

1. **Reconocimiento (Reconnaissance):**

   Técnicas: Recolección de información sobre la infraestructura de CAMMESA, incluyendo configuraciones de red, proveedores y topología de red.

   Métodos posibles: Ingeniería social, phishing a empleados y contratistas, escaneo de redes públicas y privadas.

   Ejemplo de Amenaza: Un atacante podría recolectar datos sobre puntos de acceso remoto utilizados por operadores, como VPNs o sistemas de acceso remoto a los sistemas SCADA.

2. **Desarrollo de Recursos (Resource Development):**

   Técnicas: Desarrollo o adquisición de herramientas específicas para acceder y manipular sistemas SCADA o DCS.

   Métodos posibles: Uso de malware especializado (como Industroyer) adaptado para interrupciones eléctricas.

   Ejemplo de Amenaza: Creación de malware similar a BlackEnergy para infiltrarse y control remoto.

3. **Acceso Inicial (Initial Access):**

   Técnicas: Abuso de accesos remotos, uso de cuentas comprometidas o explotación de vulnerabilidades.

   Métodos posibles: Campañas de spear-phishing dirigidas a empleados de CAMMESA, explotación de vulnerabilidades en software de terceros o accesos mal configurados.

   Ejemplo de Amenaza: Compromiso de credenciales de acceso al sistema SCADA de CAMMESA para controlar los sistemas de energía.

4. **Ejecución (Execution):**

   Técnicas: Scripts maliciosos o comandos para manipular los sistemas operativos y aplicaciones críticas.

   Métodos posibles: Inyección de scripts o uso de herramientas como PowerShell en sistemas Windows para ejecutar comandos específicos.

Ejemplo de Amenaza: Un atacante ejecuta comandos para desactivar protecciones en estaciones de subtransmisión.

5. **Persistencia (Persistence):**

   Técnicas: Instalación de backdoors o herramientas de acceso remoto en sistemas clave de CAMMESA.

   Métodos posibles: Creación de cuentas ocultas, modificación de servicios de Windows o Linux, instalación de malware persistente.

   Ejemplo de Amenaza: Instalar puertas traseras en sistemas SCADA para retomar el control de manera inmediata después de un reinicio del sistema.

6. **Escalada de Privilegios (Privilege Escalation):**

   Técnicas: Aprovechamiento de vulnerabilidades para ganar permisos de administración.

   Métodos posibles: Ataques a través de vulnerabilidades en el software de control o explotación de credenciales con permisos elevados.

   Ejemplo de Amenaza: Escalación de privilegios en servidores para manipular sistemas de distribución de energía.

7. **Evasión de Defensa (Defense Evasion):**

   Técnicas: Uso de software legítimo para ocultar actividades maliciosas o deshabilitar herramientas de seguridad.

   Métodos posibles: Modificación de logs o instalación de programas de monitoreo en modo oculto.

   Ejemplo de Amenaza: Desactivar alertas en sistemas de monitoreo para evitar la detección de actividades sospechosas.

8. **Descubrimiento (Discovery):**

   Técnicas: Identificación de recursos de red, perfiles de usuario y sistemas operativos en la red de CAMMESA.

   Métodos posibles: Escaneo de puertos internos, exploración de topologías de red y búsqueda de dispositivos específicos de ICS.

   Ejemplo de Amenaza: Mapear la red interna de CAMMESA para encontrar sistemas SCADA críticos y vulnerables.

9. **Movimiento Lateral (Lateral Movement):**

   Técnicas: Uso de credenciales robadas para acceder a otros sistemas y extender el control.

   Métodos posibles: Transferencia de credenciales entre equipos, uso de herramientas de acceso remoto.

   Ejemplo de Amenaza: Acceso a sistemas adyacentes para controlar dispositivos adicionales en la red eléctrica.

10. **Recopilación (Collection):**

    Técnicas: Acceso y recolección de datos sensibles del sistema SCADA y el estado de la red.

Métodos posibles: Monitoreo de tráfico y almacenamiento de información sobre los parámetros de operación.

Ejemplo de Amenaza: Recopilación de datos sobre la red de distribución y estado de subestaciones.

11. **Comando y Control (C^2):**

Técnicas: Establecimiento de canales seguros para controlar los sistemas comprometidos a distancia.

Métodos posibles: Uso de VPNs o comunicación cifrada para enviar comandos al sistema comprometido.

Ejemplo de Amenaza: Control remoto de sistemas SCADA y cambios en el flujo de energía.

12. **Inhibición de Respuesta (Inhibit Response Function):**

Métodos posibles: Impedir las funciones de respuesta automática,

Ejemplo: apagar alarmas.

13. **Daño o Pérdida (Impair Process Control):**

Métodos posibles: Alterar el control de procesos para dañar o alterar sistemas.

14. **Impacto (Impact):**

Técnicas: Manipulación de sistemas para causar daños físicos o interrupciones.

Métodos posibles: Manipulación de controladores para provocar apagones, daños físicos en equipos, o sobrecargas en la red.

Ejemplo de Amenaza: Sobrecargar los sistemas de distribución para provocar apagones en áreas extensas de Argentina.

Sección 3: Conclusiones

1. **IC y Vulnerabilidades del SADI:**

El SADI es una IC que no solo enfrenta riesgos tradicionales (climáticos, operativos y técnicos) sino también amenazas cibernéticas. Estas últimas han mostrado su potencial destructivo en eventos globales, como fueron los ataques en Ucrania en 2015, 2016 y 2022. La creciente interconexión de las redes IT y OT aumenta la exposición a ciberataques, haciendo más vulnerables sistemas clave como el SCADA, que controla el flujo de energía en tiempo real.

2. **Impacto de los Ciberataques en Sistemas OT y TI:**

Un ciberataque exitoso en el sector energético trae consecuencias devastadoras, no solo por la interrupción del servicio eléctrico, sino también en términos de daño ambiental, pérdidas económicas, riesgo a la seguridad nacional y afectaciones a la vida de las personas. Además, los ataques a sistemas OT tienen impacto en la economía y en la infraestructura física, lo que podría amplificar las consecuencias a largo plazo.

El modelo integrado Kill Chain IT/OT del caso de estudio Ucrania, permitió dimensionar el ataque que destacó por su sofisticación y planeación meticulosa en cada fase mismo. Subrayó la vulnerabilidad de las IC frente a ataques bien organizados y patrocinados por actores estatales sobre ICS. Al añadir las fases de Preparación e Impedir Respuesta, pone de relieve la sofisticación del ataque a su sistema eléctrico, logrando no solo la interrupción temporal del servicio, sino también la intención de los atacantes de dificultar cualquier recuperación rápida y cubrir sus rastros al mismo tiempo.

El análisis con MITRE ATT&CK en CAMMESA revela cómo un atacante podría comprometer y controlar el SEA mediante técnicas avanzadas de ciberataque en IC e intenta generar la concientización de la necesidad de fortalecer la seguridad ante amenazas ciber de CAMMESA y minimizar las vulnerabilidades del SEA.

3. **Necesidad de fortalecer la Ciberseguridad:**

Si bien el país ha avanzado en el establecimiento de medidas de ciberdefensa, como el Comando Conjunto de Ciberdefensa y el Comité de Ciberseguridad, persisten vulnerabilidades. El informe menciona la importancia de implementar arquitecturas robustas, como el modelo Purdue, para segmentar redes y fortalecer los sistemas de monitoreo y protección. Sin embargo, el Procedimiento Técnico 29, implementado tras el apagón de 2019, parece no haber avanzado lo suficiente en términos de mitigación de ciberamenazas específicas.

La iniciativa de CAMMESA de octubre de 2024 empieza a desandar este camino, que dependerá mucho de la proactividad que tenga el Comité de Crisis por crearse y las acciones proyectadas para 2025.

4. **Desafíos Operativos y de Coordinación:**

El apagón de 2019, si bien no fue causado por un ataque cibernético, reveló deficiencias en la gestión de crisis y coordinación operativa. Estos mismos problemas podrían ser explotados por actores cibernéticos malintencionados si no se fortalece la adherencia a protocolos y se mejora la comunicación entre las diversas empresas que integran el sector.

5. **Recomendaciones para Mitigar el Riesgo Cibernético:**

El procedimiento 29 y la última iniciativa prevé la ejecución de simulacros que facilitarán la definición de las tareas necesarias llevar adelante, en el marco de las operaciones Interagenciales, que permitan trabajar en un ambiente cooperativo win-win.

En este contexto, a continuación se sugieren algunas acciones:

1. **Conformar el Comité de Crisis**: que permitirá asesorar en las acciones Interagenciales necesarias para mitigar los riesgos cibernéticos.
2. **Identificar y clasificar activos críticos**: para establecer un orden de prioridades de atención.
3. **Segmentar redes**: que minimice los riesgos de los ataques.
4. **Incrementar el vínculo de los agentes del MEM al COCE**: asegurando la doble comunicación del MEM con CAMMESA.

5. **Mejorar el Monitoreo de Seguridad**: Implementación de herramientas avanzadas de detección en entornos SCADA y monitoreo continuo del tráfico.
6. **Capacitar al Personal**: Entrenamiento constante en identificación de amenazas y phishing.
7. **Asegurar Accesos Remotos**: Verificación en dos pasos y restricciones en VPN para sistemas SCADA.
8. **Actualizar Equipos y Software**: Parches de seguridad periódicos y pruebas de penetración.
9. **Cooperar entre agencias del gobierno, universidades y empresas privadas**: para crear un frente común contra las ciber amenazas.

Consideraciones finales

Relacionado al Procedimiento Técnico 29[59] de CAMMESA surgido luego del gran apagón de 2019 y haciendo un análisis documental de los informes de evaluación y anuales (y sus respectivos anexos) de los años 2021 al 2023, se concluye que los mismos focalizan el esfuerzo en garantizar el funcionamiento del SADI de manera eficiente, en términos de eficiencia operativa y económica. No es factible definir si también se apuntó a reducir las amenazas cibernéticas, foco de interés de este trabajo final.

Del último documento estudiado, que reúne las previsiones de CAMMESA para 2025, se extraen las siguientes ideas fuerza:

- En el marco de la matriz de priorización de iniciativas que elaboraron, con un alto nivel de impacto y mediana complejidad, la prioridad del esfuerzo estará en “Validar condiciones de continuidad del negocio”. Seguido por el “Plan de ciberseguridad” y la “Continuidad operativa”, con la misma valoración de impacto, pero de baja complejidad. Mientras que el “Marco Normativo”, la “Gobernanza y Seguridad de la Información”, el “Plan Estratégico Seguridad Informática” y la “Concientización del personal” se perciben de mediano impacto y baja complejidad.
- En función de esta priorización, se buscará asegurar la continuidad de los principales servicios IT y ante contingencias en el COC, en los nodos de comunicación y/o en la infraestructura.
- Se buscará incrementar acciones tendientes a las buenas prácticas[60], con el objetivo de reforzar medidas de ciberseguridad defensivas (de naturaleza activa y pasiva) a fin de minimizar los impactos de potenciales agresiones cibernéticas.

En función de esto último, si bien la seguridad de la información y operación ante amenazas cibernéticas comenzó a estar en la agenda de mejora de CAMMESA (utilizando la

[59] https://cammesaweb.cammesa.com/2024/01/29/pt-29-control-de-condiciones-de-seguridad-del-sadi/
[60] Por ejemplo, validar correcta configuración de soluciones de seguridad existentes, desarrollar ejercicios de ethical hacking y de modelado de amenazas, actualizar playbooks de accionar ante incidentes y mejorar los procesos de obsolescencia y vulnerabilidades.

Norma ISO 27.001:2022), aún no se la aprecia debidamente valorizada, en función que la misma afecta la rentabilidad del negocio.

La completa integración del COCE con los agentes del Mercado Eléctrico Mayorista (MEM) y la consideración de la Norma ISO 62.443 aplicable a IC (que se centra en la ciberseguridad de los sistemas de automatización y control industrial) debieran ser las principales meta por conquistar…

Todo esto se debe llevar adelante en un contexto técnico que condiciona la eficiencia y los tiempos asociados a su implementación: se trata de un sistema que opera 24/7 con una brecha tecnológica de treinta años en el equipamiento instalado.

Finalmente, el SEA enfrenta crecientes amenazas cibernéticas que, si no se abordan integralmente, podrían causar graves interrupciones en el suministro eléctrico y poner en riesgo la seguridad nacional, aspecto que traspasa los límites normativos en materia de seguridad y defensa, obligando a su estudio desde el punto de vista del impacto y no de la causa que lo genera. Las soluciones requieren una mejora en la infraestructura de ciberseguridad, la adopción de protocolos robustos y una coordinación más efectiva entre el sector público y privado, en el marco de las Operaciones Interagenciales que se lleven adelante en el Comité de Crisis por conformar.

Anexos

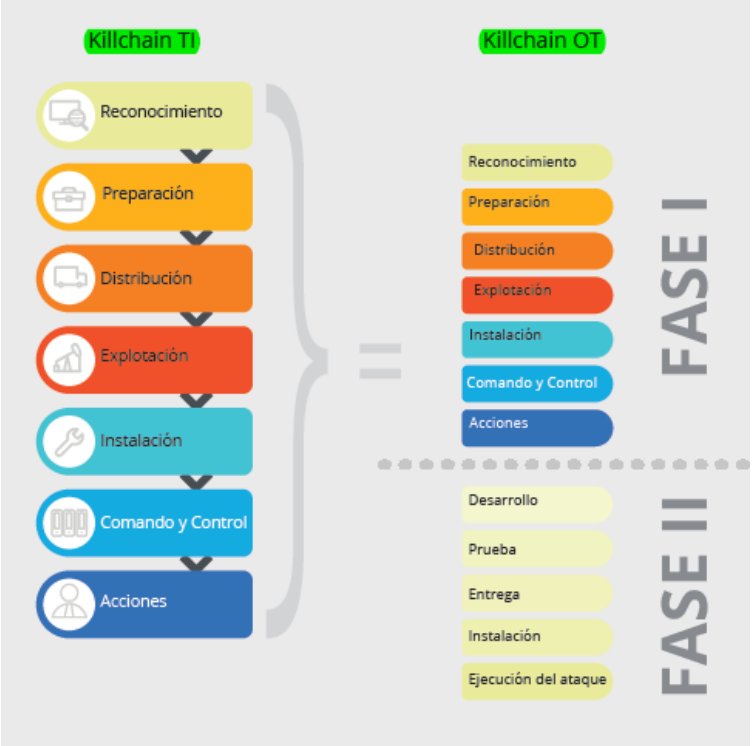
Anexo 1 - Principales colapsos eléctricos a nivel mundial[61]

(previo al ataque en Ucrania de 2015)

AÑO	ZONA	MW CORTADOS	POBLACION (millones)	TIEMPO DE REPOSICION
1977	NEW YORK y ZONAS CERCANAS	6,000	9	26 hs
1982	COSTA OESTE DE E.E. U.U.	12.000	5	
1996	MALASIA	10.000	21	
1996	COSTA OESTE DE E.E. U.U.	12.000	2	
1996	COSTA OESTE DE E.E. U.U.	28.000	7	9 hs
2003	NORESTE DE E.E.U.U.	62.000	50	3 DIAS
2003	ITALIA	24.000	57	24 hs
2009	BRASIL	25000		8 hs
2012	INDIA	30.000	350	21 Hs
2015	TURQUÍA		70	8 HS

[61] CAMMESA

Anexo 2 - Modelo de Kill Chain aplicado a ambientes IT/OT[62]



Impacto por ciberataques:

En el ambiente TI, las consecuencias pueden ser disrupción de operaciones, fuga de Información (la cual puede también ser sensible) y daño reputacional. Mientras que en el entorno OT, a las anteriores, se suman daño ambiental, pérdidas de vida, pérdida de ingresos por minuto/hora, riesgo a la seguridad nacional, disrupción a cadena de suministro y penalidades regulatorias.

[62] "…La kill chain de TI es típicamente utilizada como la primera fase de un ataque modelado bajo la kill chain de OT…" Deloitte – Fortinet, autores varios precitados. Figura X. Pág 10 y 13.

Anexo 3 – Empleo del Modelo de Mitre ATT&CK[63] en ambientes IT/OT

A continuación, se presentan las Tácticas para IT y OT (ICS), entendidas como los "pasos" que los atacantes suelen seguir para comprometer un sistema.

1. **Tácticas para IT:**
   a. **Reconocimiento (Reconnaissance)**: Recopilación de información sobre el sistema objetivo.
   b. **Desarrollo de Recursos (Resource Development)**: Preparación de herramientas, infraestructura y cuentas.
   c. **Acceso Inicial (Initial Access)**: Obtener acceso inicial al sistema o red objetivo.
   d. **Ejecución (Execution)**: Ejecutar comandos o software malicioso en el sistema.
   e. **Persistencia (Persistence)**: Mantener acceso en el sistema objetivo después de un reinicio o cambio de credenciales.
   f. **Escalada de Privilegios (Privilege Escalation)**: Aumentar privilegios para controlar más recursos o datos.
   g. **Evasión de Defensa (Defense Evasion)**: Eludir la detección y medidas de seguridad.
   h. **Acceso a Credenciales (Credential Access)**: Obtener credenciales del sistema para avanzar en el ataque.
   i. **Descubrimiento (Discovery)**: Recopilar información sobre el sistema y la red para identificar más objetivos.
   j. **Movimiento Lateral (Lateral Movement)**: Moverse a otros sistemas dentro de la red comprometida.
   k. **Recopilación (Collection)**: Obtener datos relevantes del sistema.
   l. **Comando y Control (Command and Control)**: Establecer un canal de comunicación para controlar los sistemas comprometidos.
   m. **Exfiltración (Exfiltration)**: Transferir datos fuera de la red objetivo.
   n. **Impacto (Impact)**: Alterar, destruir o manipular datos o el sistema para causar interrupciones o pérdidas.
2. **Tácticas para ICS**
   a. **Reconocimiento (Reconnaissance)**: Similar a TI, enfocada en obtener información específica de ICS.
   b. **Desarrollo de Recursos (Resource Development)**: Preparar herramientas y recursos para ICS.
   c. **Acceso Inicial (Initial Access)**: Obtener acceso a los ICS.

[63] https://attack.mitre.org

d. **Ejecución (Execution)**: Ejecutar comandos o malware en el entorno ICS.
e. **Persistencia (Persistence)**: Mantener el acceso a sistemas ICS a largo plazo.
f. **Evasión de Defensa (Defense Evasion)**: Evadir la detección en redes y dispositivos ICS.
g. **Escalada de Privilegios (Privilege Escalation)**: Adquirir mayores permisos para el control de ICS.
h. **Descubrimiento (Discovery)**: Recopilar información en la red de ICS para avanzar en el ataque.
i. **Movimiento Lateral (Lateral Movement)**: Desplazarse hacia otros dispositivos o redes dentro del entorno ICS.
j. **Recolección (Collection)**: Obtener información o datos críticos de ICS.
k. **Comando y Control (Command and Control)**: Comunicar y controlar los sistemas industriales comprometidos.
l. **Inhibición de Respuesta (Inhibit Response Function)**: Impedir las funciones de respuesta automática, por ejemplo, apagar alarmas.
m. **Daño o Pérdida (Impair Process Control)**: Alterar el control de procesos para dañar o alterar sistemas.
n. **Impacto (Impact)**: Causar efectos negativos en el proceso industrial (interrupciones, daños físicos, etc.).

Estas tácticas brindan un marco estructurado para identificar, entender y responder a las acciones de los atacantes en sistemas tanto de TI como de ICS. De esta manera, a través de esta plataforma podemos simular diferentes tipos de ataques con sus tácticas y técnicas, los que nos lleva a evaluar una matriz de vulnerabilidades, por ejemplo:

Tácticas	Initial Access	Execution	Persistence	Defense Evasion	Impact
Técnicas	Spearphishing Attachment (T1566.001)	Command-Line Interface (T1059.003)	Remote Access Software (T1219)	Masqueradi ng (T1036)	Inhibit Response Function (T0813)

Explicación del proceso

1. **Acceso Inicial**:

   Técnica: **Spearphishing Attachment (T1566.001)**

   Esto cae bajo la táctica "Initial Access", ya que es una forma en la que los atacantes podrían obtener acceso al sistema enviando archivos maliciosos.
2. **Ejecución**:

   Técnica: **Command-Line Interface (T1059.003)**

Una vez que los atacantes tienen acceso, pueden usar la línea de comandos para ejecutar scripts maliciosos, una técnica asociada con la táctica "Execution".

3. **Persistencia**:

   Técnica: **Remote Access Software (T1219)**

   Para mantener acceso continuo, los atacantes podrían instalar software de acceso remoto, que cae en la táctica "Persistence".

4. **Evasión de Defensas**:

   Técnica: **Masquerading (T1036)**

   Los atacantes pueden enmascarar procesos maliciosos para que parezcan legítimos, evadiendo así las defensas del sistema.

5. **Impacto**:

   Técnica: **Inhibit Response Function (T0813)**

   Finalmente, los atacantes podrían inhibir las funciones automáticas del sistema para causar daños, técnica que cae bajo la táctica "Impact".

Anexo 4 – Abreviaturas

- Agencia Federal de Ciberseguridad (AFC).
- Agencia Federal de Inteligencia (AFI)
- Ataques de Denegación de Servicios Distribuidos (DDoS, por sus siglas en inglés, Distributed Denial of Service).
- Centro Operativo de Control de Emergencias (COCE)
- Comando y Control (C^2, por sus siglas en inglés, Command and Control).
- Compañía Administradora del Mercado Mayorista Eléctrico Sociedad Anónima (CAMMESA).
- Ente Nacional de Regulación de la Electricidad (ENRE).
- Equipo de Respuesta ante Emergencias Informáticas (CSIRT, por sus siglas en inglés, Computer Security Incident Response Team).
- Infraestructuras Críticas (IC).
- Infraestructuras Críticas de la Información (ICI).
- Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés, National Institute of Standards and Technology).
- Marco de Ciberseguridad (CSF, por sus siglas en inglés, Cybersecurity Framework).
- Mercado Eléctrico Mayorista (MEM).
- MITRE Tácticas, Técnicas y Conocimientos Comunes Adversarios (ATT&CK, por sus siglas en inglés, Adversarial Tactics, Techniques, and Common Knowledge).
- Noroeste Argentino (NOA).
- Organización del Tratado del Atlántico Norte (OTAN).
- Organización de las Naciones Unidas (ONU).
- Plataforma para Compartir Información sobre Malware (MISP, por sus siglas en inglés, Malware Information Sharing Platform).
- Reglamento Europeo de la Protección de Datos (RGPD).
- Sistema Argentino de Interconexión (SADI).
- Sistema de Control Supervisor y Adquisición de Datos (SCADA, por sus siglas en inglés, Supervisory Control And Data Acquisition).
- Sistema de Gestión de Seguridad de la Información (ISMS, por sus siglas en inglés, Information Security Management System).
- Sistema de Operación en Tiempo Real (SOTR).
- Sistema Eléctrico Argentino (SEA).
- Transporte de Energía Eléctrica en Alta Tensión (TRANSENER).
- Tecnologías de la Información (IT, por sus siglas en inglés, Information Technology).
- Tecnologías Operativas (OT, por sus siglas en inglés, Operational Technology).

- Troyano de Acceso Remoto (RAT, por sus siglas en inglés, Remote Access Trojan).
- Sistemas de Control Industrial (ICS, por sus siglas en inglés, Industrial Control Systems).

Referencias

- CALCAGNO, D.L. et al. Análisis de vulnerabilidades e interrupciones del sistema argentino de interconexión. **Rev. Tecnol. Soc**., Curitiba, v. 18, n. 54, p. 53-73, out./dez., 2022.
- Deloitte (Corrado, Nicolás – Socio de Ciberseguridad; Pizarro, Carolina – Senior Manager Ciberseguridad; Gorena Cristian – Gerente Ciberseguridad) – Fortinet (Aguayo Fuentealba, Pablo – SE Territorio Enterprise Industrias, RRNN y Utilities; Cuadrado Corsse, Luz María – MAM Territorio Enterprise Industrias, RRNN y Utilities; Arias Aparicio, Juan Pablo – SE Manager Fortinet Chile; Salas Varela, Pía – Country Manager Fortinet Chile. Diciembre 2022.
- ESET. Welivesecurity. Crisis en Ucrania - Centro de Recursos de Seguridad Digital, Investigaciones. Liposvsky, Robert. https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/ . 05 de junio de 2.016.
- Guía técnica de prevención - 02 PREVENCIÓN DEL RIESGO ELÉCTRICO.2019
- Manual de Buenas Prácticas. MBP - Industria-Eléctrica. PDF (www.srt.gob.ar)
- Operaciones militares cibernéticas: planeamiento y ejecución en el nivel operacional / Gustavo Adolfo Trama; Evergisto Arturo de Vergara. - 1a ed . - Ciudad Autónoma de Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, 2017.
- POLÍGONO INDUSTRIAL. Revista Industrial Bahía Blanca. Conocé como se conforma la matriz energética Argentina. https://poligono.com.ar/2024/05/30/conoce-como-se-conforma-la-matriz-energetica-argentina/ . 30 de mayo de 2024
- https://attack.mitre.org
- https://cammesaweb.cammesa.com
- https://www.welivesecurity.com
- https://www.akamai.com/es/glossary/what-is-iso-27001
- https://www.argentina.gob.ar/economia/energia/energia-electrica/hidroelectrica/centrales-hidroelectricas
- https://www.argentina.gob.ar/economia/energia/energia-electrica/hidroelectrica/centrales-hidroelectricas
- https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa
- https://www.enel.com.ar/es/Historias/a201802-biomasa-en-argentina-con-80-plantas.html
- https://www.infobae.com/sociedad/2019/06/16/la-secretaria-de-energia-atribuyo-el-apagon-al-clima-y-fallas-en-el-sistema-de-proteccion/
- https://www.infobae.com/sociedad/2019/06/16/que-es-el-sistema-de-interconexion-electrica-y-por-que-su-falla-dejo-sin-luz-a-todo-el-pais/

- https://servicios.infoleg.gob.ar/infolegInternet/anexos/5000-9999/9615/norma.htm
- https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/
- https://www.argentina.gob.ar/normativa/nacional/decreto-614-2024-401512
- https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-1523-2019-328599
- https://www.argentina.gob.ar/sites/default/files/2022/01/energias_renovables_2021_sec.pdf