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 ENERGÉTICO ARGENTINO: IMPLICANCIAS PARA LA SEGURIDAD NACIONAL

Integrantes del Equipo Nro: 8

HECTOR GERMÁN MEDINA GIMENEZ

SANDRA VERONICA MARTINEZ

GERARDO DANIEL ORTIZ

Títulos Profesionales / de grado

Técnico Superior en Telecomunicaciones

Licenciada en Conducción y Gestión Operativa-Orientación Armas

Licenciado en Administración

08 de noviembre de 2024

Resumen

El sector energético no sólo es extremadamente importante para todos los países, sino que también es vulnerable a posibles ciberataques. En vista del progreso tecnológico actual, la interconexión organizacional, la interconexión de redes y la globalización de la tecnología, es necesario lograr herramientas con resultados científicos en los campos de las tecnologías de la información y las comunicaciones (TIC) y la automatización industrial, y buscar ventajas tecnológicas e innovación. Y la Argentina no queda afuera de los avances, ventajas y desventajas al que se expone cuando decide ingresar dentro de las formas de desarrollos a nivel mundial.

Observando desde la protección de nuestros recursos y el desarrollo social y económico, es menester tomar posicionamientos y decisiones firmes que nos permita adelantarnos y adquirir poder al tener el control de ello. En razón de esto, en este trabajo se busca a través de la investigación y el análisis de datos, brindar algún sesgo y buscar respuestas frente a estos cuestionamientos de vulnerabilidades en las infraestructuras críticas, como logramos identificar que lo es “VACA MUERTA”, una formación geológica que se extiende por 30.000 kilómetros cuadrados, en la provincia argentina de Neuquén, alcanzando también Mendoza y Río Negro. Alberga el segundo reservorio mundial de gas no convencional y el cuarto de petróleo. Hoy en día se sabe sobre su potencialidad económica y por eso la importancia de investigar este sector.

El trabajo consiste en presentar y analizar conceptos claves del tema que nos permitirá comprender el contexto en donde investigaremos. Se analizará las bases legales, el avance tecnológico, todo entorno a las amenazas cibernéticas y nuestra capacidad de proceder y proteger la seguridad nacional que es lo que nos interesa.

Para acercarnos y justificar nuestra hipótesis en el marco teórico tomaremos ejemplos de incidentes ya ocurridos en otros países. Y en base a sus acciones se toma las miradas fundadas en hechos reales. Y finalmente dimensionaremos nuestra capacidad como nación y las posibles herramientas de las cuales nos valdremos para entender y en un futuro. responder a las vulnerabilidades no solo del sector, “VACA MUERTA”, sino de las infraestructuras críticas del país.

Palabras Claves: infraestructura critica, VACA MUERTA, globalización tecnológica, amenazas cibernéticas, sector energético.

Índice General

Justificación / Fundamentación / Aportes

Las nuevas formas de desarrollar la guerra han cambiado rotundamente a través del tiempo, el factor vital en esto son los avances tecnológicos, a partir de los cuales hay hablamos de los ataques cibernéticos y amenazas constantes, sin conocer claramente de donde proviene o no hay un enemigo declarado o peor aún el ataque va directamente a la población civil sin ningún remordimiento, hablamos del ciberterrorismo, donde la ética no existe. Razón por la cual no hay país que no esté pensando en prepararse y tomando las medidas necesarias para poder proteger sus bienes y el bien estar de la población civil.

Para iniciar a responder algunas preguntas sobre la protección y seguridad Nacional, referido y puntualmente sobre las infraestructuras críticas, este trabajo se va centrar y profundizar en el sector energético argentino, más específicamente una de las fuentes de energía, "VACA MUERTA", al considerarse un factor estratégico desde el punto de vista económico. Considerando también que hoy en día la argentina depende más de los recursos no renovables en el sector energético.

Al buscar el desarrollo a través de esta fuente de energía que brinda VACA MUERTA, somos altamente vulnerables ya que al ingresar al sistema de interrelación con el resto del mundo, es decir la interdependencia necesariamente que busca la globalización tecnológica para el nuevo desarrollo económico, nos deja descubiertos, es por eso que debemos ir protegidos ya que sabemos que abrimos puertas a amenazas y ataques cibernéticos, tal es la gravedad del tema que en un segundo podemos lamentar el robo de datos y la venta de los mismos o vernos afectados toda la población al no contar con los recursos que día a día son necesarios para la supervivencia básica.

Planteamiento del Problema

El problema principal identificado en Vaca Muerta es la vulnerabilidad de sus sistemas de control industrial (ICS/SCADA) frente a ciber amenazas. Al ser una infraestructura crítica de importancia estratégica para Argentina, su exposición a ciberataques que podrían comprometer la continuidad operativa y la seguridad nacional es un riesgo significativo. A medida que el yacimiento avanza en su digitalización, aumenta el riesgo de ataques dirigidos, tanto por parte de actores estatales como no estatales, lo que convierte este espacio en un objetivo relevante para

proteger. El carácter innovador de esta detección radica en la integración de un enfoque específico en infraestructuras críticas energéticas y la identificación de las brechas de seguridad en un entorno digitalizado altamente interdependiente.

Formulación del Problema

¿Según nuestras vulnerabilidades, quiénes y cómo podemos actuar frente a una amenaza o ataque cibernético? ¿Cuáles son las herramientas con la que contamos? ¿en caso de ser atacados con qué rapidez el gobierno recupera el centro de la infraestructura critica tomada?

Solución Propuesta

La solución propuesta para abordar este problema es el desarrollo de una estrategia integral de ciberdefensa para Vaca Muerta, que incluye la implementación de tecnologías avanzadas de seguridad y la creación de un equipo especializado de respuesta a incidentes cibernéticos (CSIRT) para infraestructuras críticas. Esta estrategia se basa en tres pilares fundamentales:

1. Segmentación de redes IT/OT para minimizar la exposición de los sistemas industriales a ciberataques.
2. Implementación de sistemas de detección de intrusiones (IDS) avanzados para detectar actividades anómalas en tiempo real.
3. Creación de un equipo especializado de ciberdefensa que supervise, evalúe y responda a incidentes cibernéticos específicos en Vaca Muerta.

El carácter innovador de la solución radica en su enfoque adaptado al entorno energético argentino, combinando la experiencia en infraestructuras críticas con las mejores prácticas globales en ciberseguridad industrial.

El sustento de la solución propuesta se realizará a través de un análisis detallado de las vulnerabilidades de los sistemas SCADA/ICS en Vaca Muerta y la implementación de un prototipo de sistema de detección de intrusiones. Este prototipo será evaluado en escenarios de prueba simulando ataques cibernéticos comunes en infraestructuras críticas, como ransomware o ciberespionaje. Además, se realizarán simulaciones de incidentes con el CSIRT propuesto para verificar su eficacia en la respuesta ante ataques.

Adicionalmente, se contrastará la solución mediante la revisión de estudios de casos internacionales (e.g., Colonial Pipeline) y se aplicarán modelos estadísticos para estimar el impacto potencial de los ciberataques y la efectividad de las medidas de mitigación propuestas. Estos estudios contribuirán a justificar la relevancia de la solución y su capacidad para proteger la seguridad nacional a través de la defensa de infraestructuras críticas.

Objetivos

Objetivo General

Analizar las amenazas cibernéticas que enfrenta el sector energético argentino, evaluando sus implicancias para la seguridad nacional y proponiendo estrategias para mitigar estos riesgos.

Objetivos Particulares

1. Identificar y clasificar los tipos de amenazas cibernéticas más relevantes que afectan a las infraestructuras críticas del sector energético en Argentina.

2. Evaluar el impacto potencial de estas amenazas en la seguridad nacional, considerando aspectos económicos, sociales y de infraestructura.

Marco Teórico

El sector energético en Argentina

La historia nos va a mostrar que la Argentina a través del tiempo sigue siendo dependiente de unos de las principales fuentes de energía, los hidrocarburos. (Véase Anexo A, Figura 1 y 2). Según estudios, más del 80% del total de los servicios es través de los recursos primarios de este tipo, además la Argentina desde el año 2013 según un informe se encuentra entre los países que consume dentro del 10% sobre la media mundial, solo un poco menos que China.

Esto nos lleva a reflexionar que deberíamos pensar en diversificar la matriz energética e ir invirtiendo en las fuentes renovables (Véase Anexo A, Figura 6). En el 2013 vemos que no había mucha participación mientras que hoy en día sabemos que se trabaja a través de nuevas políticas sobre todo en las energías, eólica y la solar (Véase Anexo A, Figura 3,4 y 5). Sin embargo, no cambio mucho nuestro panorama, observamos que vamos a seguir dependiendo principalmente de los hidrocarburos y la energía nuclear por lo cual es un problema a la hora de analizar los puntos vulnerables o las infraestructuras críticas para nuestra nación ya que, si se centran en un solo punto,

dándole una importancia significativa a este sector es más fácil realizar un daño y a grandes efectos, como lo es un ataque o amenaza cibernética.

Vaca Muerta y su importancia

Formación sedimentaria (Véase Anexo A, Figura 7) depositada en un mar de edad jurásica, en la Cuenca Neuquina, de más de 35 mil kilómetros cuadrados el 2° en el mundo en recurso no convencional de gas, hay 31 empresas con posición en el proyecto, 4° en el mundo en recurso no convencional de petróleo. Es un tesoro energético importante a nivel mundial.

Se extiende en cuatro provincias (Véase Anexo A, Figura 8), Neuquén, Rio Negro, La Pampa y Mendoza, la mayor parte se encuentra a más de 3000m de profundidad, ahí encontramos en 40% de gas y 60% de petróleo no convencionales del país. De ahí su importancia, ya que la población mundial fue creciendo multiplicándose por grandes números y del mismo modo el consumo de energía en todo el mundo. Según datos a nivel mundial hoy en día dependemos de estas fuentes de energía.

Datos Agencia Internacional De Energía (AIE)

Según datos de la Agencia Internacional de Energía (AIE), en 2019 se consumieron en todo el mundo más de 167.000 teravatios hora (TWh) de energía.

Según la AIE, en 2019 el petróleo representó el 33% del consumo mundial de energía primaria, seguido por el gas natural (24%), el carbón (27%) y la energía nuclear (4%).

El petróleo

El petróleo es una fuente de energía fósil que se utiliza para la producción de combustibles líquidos, como la gasolina y el diésel, así como para la generación de electricidad y la producción de plásticos y otros productos químicos. Su uso se ha vuelto esencial en el transporte, la industria y la generación de energía eléctrica en muchos países.

El mantenimiento de las redes y de los datos en Vaca Muerta.

1. Desde ocasionar un desperfecto o encriptar una máquina para pedir un rescate informático son posibilidades latentes.

2. Un ataque cibernético puede tener un alto costo para la empresa, llegando a millones de dólares
3. Se podría utilizar herramientas de inteligencia artificial para detectar fallas y ataques de manera proactiva.
4. Debido a la transformación digital y su integración con las redes actuales, necesariamente son más vulnerables.
5. Los ataques pueden afectar el tiempo y el dinero al paralizarse la actividad de generación de energía o bombeo de hidrocarburos durante minutos u horas.
6. Los ciberataques pueden darse:
    (1) en los sensores en todas las redes industriales, que están en los oleoductos, gasoductos y acueductos conectados a las redes. Al estar conectados empiezan a ser puntos de fallas y de ataques cibernético.
    (2) En las cualquier de las computadoras
    (3) Los líderes como Cisco, Tenable, CyberArk, Oracle y Dell, ofrecen servicios de monitoreo de datos, seguridad, cómputo, almacenamiento y dispositivos para ambientes hostiles en la industria.

Infraestructuras críticas

Según una de las definiciones que nos brinda el Poder Ejecutivo Nacional, las Infraestructuras Críticas son aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente.

Ejemplos de Infraestructura Critica (Ver Anexo B)

1. Sistema Financiero y Tributario (entidades bancarias, información, valores e inversiones).
2. Administración (servicios básicos, instalaciones, redes de información, principales activos y monumentos del patrimonio nacional).
3. Agua (embalses, almacenamiento, tratamiento y redes).

4. Alimentación (producción, almacenamiento y distribución).
5. Centrales y Redes de energía (producción y distribución).
6. Instalaciones relacionadas con el Espacio Exterior.
7. Centrales nucleares (producción, almacenamiento y transporte de mercancías peligrosas, materiales nucleares, radiológicos, etc.).
8. Industria Química (producción, almacenamiento y transporte de mercancías peligrosas, materiales químicos, etc.).
9. Investigación: laboratorios que por su idiosincrasia dispongan o produzcan materiales, sustancias o elementos críticos o peligrosos.
10. Salud (sector e infraestructura sanitaria).
11. Tecnologías de la Información y las Comunicaciones (TIC, ya sean infraestructuras críticas en sí mismas, como redes de telecomunicaciones, o den servicio de información y comunicaciones a otras infraestructuras críticas)
12. Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico).

Principales responsables de la protección de las infraestructuras críticas son:

1. Gobiernos.
2. Organismos competentes.

Medidas para evitar un ciberataque

1. Recolectar, analizar, integrar y evaluar la información aportada por las instituciones públicas, los servicios policiales, y sectores estratégicos.
2. Evaluar las amenazas y analizar los riesgos sobre las instalaciones estratégicas.
3. Diseñar y establecer la información, la comunicación y los mecanismos de alerta.

Tecnología de la información y Tecnologías de la operación

Internet Industrial de las cosas (IIoT), hay una integración física en las maquinas físicas sensores y programas que se conectan en red, esto une a Tecnologías de la información (TI) con tecnologías de la operación (TO) y hace que sea más accesibles a los ciberdelincuentes a las infraestructuras críticas.

Norma y Estándares para mitigar los Riesgos Cibernéticos -ISO/IEC 27001

La norma ISO/IEC 27001 es un estándar de gestión de la seguridad de la información que ayuda a las organizaciones a proteger sus datos mediante un enfoque sistemático para gestionar la seguridad de la información.

Mejores Prácticas para Proteger Infraestructuras Críticas

Además de seguir normas y estándares, las organizaciones pueden implementar una serie de mejores prácticas para mejorar su ciberseguridad y conocer los distintos tipos de amenazas (Véase Anexo C)

Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)

Un SGSI proporciona un marco para gestionar la seguridad de la información, ayudando a identificar, gestionar y reducir los riesgos cibernéticos.

Formación y Concienciación de los Empleados

Los empleados deben ser capacitados regularmente sobre las amenazas cibernéticas y las mejores prácticas de seguridad. La concienciación puede ayudar a prevenir ataques de phishing y otras intrusiones basadas en el error humano.

Segmentación de Redes

La segmentación de redes limita el movimiento lateral de los atacantes dentro de una infraestructura, dificultando el acceso a sistemas críticos una vez que se ha obtenido acceso no autorizado.

Monitoreo Continuo y Respuesta a Incidentes

El monitoreo continuo de redes y sistemas es esencial para detectar actividades anómalas. Tener un plan de respuesta a incidentes permite a las organizaciones reaccionar rápidamente ante un ataque, minimizando el daño.

Metodología

La metodología de investigación a emplear para desarrollar este trabajo es del tipo cualitativo, por la recopilación, análisis e interpretación de datos, narrativos y visuales. Se buscó realizar un estudio de muchos aspectos del objeto a investigar, utilizamos el razonamiento deductivo con inferencias inductivas a fin de obtener conclusiones parciales, que luego nos llevó a resolver nuestros objetivos planteados.

Capítulo 1

Tipos de amenazas cibernéticas que afectan las infraestructuras críticas del sector energético argentino.

Introducción

En el presente capítulo se analizarán las amenazas que afectan las infraestructuras críticas del sector energético, para lo cual es necesario definir el concepto de infraestructura crítica. Esta definición la encontramos en el Decreto Nro. 1523/2019 emitido por la Secretaría de Gobierno de Modernización, la cual nos menciona que: las Infraestructuras Críticas son aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente. De la mano con este concepto, el mismo decreto nos define lo que se entiendo como las Infraestructuras Críticas de Información que son las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas.

A su vez una directiva publicada por la Unión Europea (UE, 2008) nos define como infraestructura crítica a el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población, cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones.

Ahora muy bien, una vez definido el concepto de Infraestructura Crítica debemos mencionar que áreas estratégicas las contienen, y es ahí en donde encontramos el área de Transporte (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico), Tecnologías de la Información y de las Comunicaciones (TIC, ya sean infraestructuras críticas en sí mismas, como redes de telecomunicaciones, o den servicio de información y comunicaciones a otras infraestructuras críticas), Salud (sector e infraestructura sanitaria), Financiero (entidades bancarias, información, valores e inversión), Investigación (laboratorios que por su idiosincrasia dispongan o produzcan materiales, sustancias o elementos críticos o peligrosos), Administración (servicios básicos, instalaciones, redes de información, principales activos y monumentos del patrimonio nacional), Alimentación

(producción, almacenamiento y distribución), Agua (embalses, almacenamiento, tratamiento y redes), Químico (producción, almacenamiento y transporte de mercancías peligrosas, materiales químicos, etc.), Nuclear (producción, almacenamiento y transporte de mercancías peligrosas, materiales nucleares, radiológicos, etc.), Espacio y Energía (producción y distribución).

Dentro de estas áreas que son de carácter estratégico para una nación el sector energético en la Argentina es fundamental para su desarrollo, como nos menciona (Kosulj, 2015) los recursos energéticos de hidrocarburos son de vital importancia, porque constituyen una parte significativa de su matriz energética, con un elevado grado de dependencia del gas natural y de los hidrocarburos líquidos. Esta dependencia no solo asegura el suministro energético de la nación, sino que también influye en su economía, dado que el sector de hidrocarburos es crucial para la generación de ingresos y empleo. Sin embargo, esta alta participación de los hidrocarburos plantea desafíos importantes, como la vulnerabilidad ante el agotamiento de estos recursos no renovables y la necesidad de diversificación hacia fuentes de energía más sostenibles. Entendemos como Matriz Energética de Argentina a la combinación de fuentes de energía que se utiliza para satisfacer las necesidades energéticas. Esta matriz incluye tanto fuentes de energía primarias, como el petróleo, gas natural, carbón, energía hidráulica y renovables, como fuentes secundarias, que son aquellas que resultan de la transformación de las primarias, como la electricidad.

En el contexto del documento publicado por la Revista de la Bolsa de Comercio de Rosario (Cárdenas, 2009), la matriz energética de Argentina estaba compuesta en su mayoría por fuentes no renovables, con un 90,9% de la energía consumida proveniente de petróleo y gas natural. A pesar de la importancia de estos recursos, se señala que su producción ha comenzado a declinar, lo que plantea desafíos para la seguridad energética del país.

La matriz también se compara con la de otros países, como Brasil, que presenta una mayor diversificación en sus fuentes de energía, incluyendo un porcentaje significativo de energías renovables. El documento enfatiza la necesidad de diversificar la matriz energética argentina, incorporando más fuentes renovables y mejorando la eficiencia en el uso de la energía para lograr un desarrollo sostenible y enfrentar los desafíos del cambio climático.

Sabemos que la matriz energética de Argentina está compuesta principalmente por hidrocarburos, con el gas natural como la fuente predominante, seguido del petróleo y sus derivados, que son esenciales para el transporte y la industria. Aunque las energías renovables,

como la eólica y solar, fueron ganando participación, su aporte energético sigue siendo relativamente bajo en comparación con los hidrocarburos. Además, Argentina cuenta con una pequeña pero significativa participación de la energía nuclear en la generación de electricidad, mientras que el carbón tiene una presencia mínima. A pesar de que la matriz energética se considera "limpia" en términos de emisiones de CO2, la alta dependencia de los hidrocarburos, especialmente del gas natural, plantea desafíos importantes en términos de sostenibilidad y seguridad de suministro a largo plazo.

Las infraestructuras críticas en el sector energético

Las infraestructuras críticas en el sector energético de Argentina juegan un papel vital en la vida cotidiana de cada ciudadano y en el funcionamiento de la economía nacional. Estas estructuras, que abarcan desde las redes de transporte y distribución de gas y electricidad hasta las refinerías y plantas de generación, son esenciales para asegurar que la energía fluya de manera constante y eficiente a todos los rincones del país. En un contexto donde el gas natural representa más del 50% de la matriz energética, la importancia de contar con infraestructuras robustas y bien mantenidas se vuelve aún más evidente. No solo son responsables de satisfacer la creciente demanda energética, sino que también deben ser capaces de resistir desafíos como eventos climáticos extremos, fallas técnicas o incluso amenazas cibernéticas. Por ello, es importante que se realicen inversiones significativas en la modernización, mantenimiento y defensa de estas infraestructuras. Y haciendo hincapié en la defensa de las Infraestructuras Críticas la Resolución 829/2019 de la Secretaría de Gobierno de Modernización nos menciona que a partir de los OCHO (8) objetivos centrales a fijar en la Estrategia Nacional de Ciberseguridad, se desplegarán planes de acción vinculados a la generación de un marco normativo acorde; al desarrollo y la articulación de capacidades de respuesta a incidentes de seguridad a gran escala; a la protección de infraestructuras críticas que habilitan la prestación de servicios esenciales para la sociedad y la economía; a la integración con otros países y a la creación de una cultura de ciberseguridad, a partir de la cual las personas aprovechen los beneficios de las nuevas tecnologías, minimizando los riesgos devenidos de su utilización. Y en particular el Decreto 50/2019 de la Administración Pública Nacional en su Anexo II dentro del apartado del Ministerio de Defensa, Secretaría de Estrategia y Asuntos Militares, Subsecretaría de Ciberdefensa nos plantea algunos de estos objetivos:

- Entender en los aspectos regulatorios del sistema de ciberdefensa para la Jurisdicción y las infraestructuras críticas de la Defensa.
- Entender en la coordinación con los organismos y autoridades de los Poderes del Estado para contribuir desde la Jurisdicción a la política nacional de ciberseguridad y de protección de infraestructuras críticas.
- Entender en la coordinación con las agencias u organismos reguladores de la prestación de los servicios esenciales y de producción de bienes de interés para la Defensa Nacional, como contribución para la elaboración de normas específicas relativas a la protección de la tecnología operacional (OT) de esas infraestructuras críticas y de los procesos productivos de interés para la Defensa Nacional.
- Promover políticas tendientes al fortalecimiento de la capacidad de asistencia a los sistemas de infraestructuras críticas.

Amenazas y vulnerabilidades de las Infraestructuras Críticas

Dentro de una publicación realizada por Lisa Institute en el año 2024 nos menciona algunas amenazas y vulnerabilidades a la cual las IICC de España están expuestas:

1. Terrorismo – Cada vez tiene mayores dimensiones, en la actualidad, el Daesh / ISIS es el principal protagonista por su modo de operar, su proyección mediática y su rápida expansión, pero cada vez están surgiendo otros movimientos terroristas con diferente ideología.

2. Crimen organizado – Es una amenaza de carácter transnacional, flexible y opaca. Tiene una gran capacidad desestabilizadora, cuyo fin es el ánimo de lucro, pero debilitando el Estado y minando la buena gobernanza económica. Una parte del Crimen Organizado es el llevado a cabo por los Grupos Violentos son los responsables de gran parte de las conductas violentas en las grandes ciudades.

3. Proliferación de armas de destrucción masiva – Supone una gran amenaza para la paz y la seguridad internacional, afectando de manera directa a la Seguridad Nacional.

4. Espionaje – Es una amenaza de primer orden para la seguridad tanto por el espionaje de otros países como por el realizado por empresas extranjeras. La Inteligencia en el ciberespacio coge el nombre de ciberinteligencia siendo su objetivo obtener cantidades

ingentes de información y datos confidenciales entre los que puedan estar los de Infraestructuras Críticas.

5. Vulnerabilidad del ciberespacio – Las amenazas en el ciberespacio han adquirido una dimensión global que va mucho más allá de la tecnología. El objetivo es conseguir diferentes propósitos como, por ejemplo, la expansión de determinados intereses geopolíticos por parte de Estados, organizaciones terroristas y actores individuales.

6. Vulnerabilidad del espacio marítimo – Este espacio es de gran relevancia para España como potencia marítima, pues reviste un gran valor estratégico. Los factores que desafían la seguridad marítima se concentran en dos grupos:

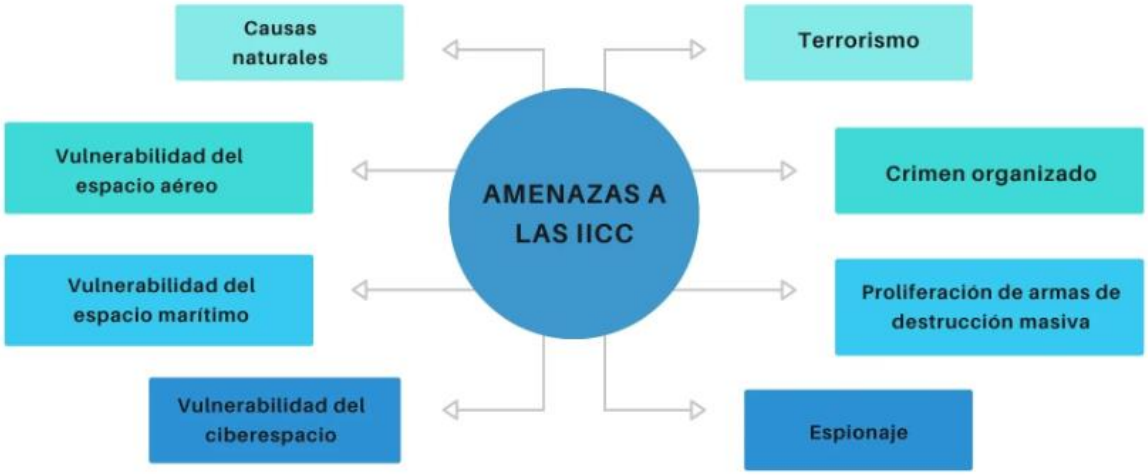
   Amenazas derivadas de actos intencionados y de naturaleza delictiva (la piratería, el terrorismo, los tráficos ilícitos, etc).

   Amenazas accidentales derivadas de las condiciones naturales del propio medio (accidentes marítimos y las catástrofes naturales).

7. Vulnerabilidad del espacio aéreo y ultraterrestre – El espacio aéreo puede ser comprometido por parte de actores estatales y no estatales. Algunos ejemplos son las acciones contra la aviación comercial, los sistemas de control de navegación y los tráficos ilícitos.

8. Causas naturales – El impacto de las catástrofes perjudica la vida de las personas, así como a los bienes patrimoniales, al medioambiente y al desarrollo económico. Por otro lado, las epidemias y las pandemias han aumentado su número y situaciones de riesgo. Y, finalmente, los efectos derivados del cambio climático tienen graves consecuencias. Por ejemplo, la subida de las temperaturas afecta a los niveles del mar, a la degradación del suelo y a la acidificación del océano, entre otros.

9. Otros – Cualquier tipo de perturbación en los servicios ofrecidos por estas infraestructuras de sectores estratégicos y esenciales podría conllevar riesgos en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, además de dar lugar a disfunciones en materia de seguridad.



Fuente: LISA Institute, Madrid, 2024.

Ahora bien, como se mencionó anteriormente en el Marco Teórico, dentro de las SEIS (06) principales amenazas de ciberseguridad podemos mencionar:

1. Phishing: Que se trata de correos electrónicos o mensajes disfrazados de entidades confiables que buscan engañar al usuario para que revele información personal o financiera. Y funciona de la siguiente manera, el atacante envía un enlace malicioso. La víctima lo abre y luego, a través de un formulario falso en una web apócrifa o un archivo infectado, envía o pone a disposición del atacante sus datos (información bancaria, datos personales, etc). Con esos datos, el ciberdelincuente puede ingresar a la computadora de la víctima, a su homebanking, a sus perfiles, etc. O puede incorporarlos a una base para luego venderlos en la dark web. Para evitar este tipo de ataques debemos no abrir enlaces sospechosos, verificar la dirección de los enlaces, desconfiar de mensajes con ofertas demasiado buenas, etc.
2. Ransomware: Que se trata del secuestro digital del siglo XXI. Este tipo de malware captura los datos del usuario y los encripta (los hace inaccesibles para el propietario). Así, los delincuentes del ataque exigen un rescate a cambio de su liberación. Empresas e instituciones públicas son blancos predilectos de estos ataques que pueden tener consecuencias devastadoras. Y funciona de la siguiente manera, el ransomware se instala en el dispositivo a través de un periférico infectado, una app o un enlace malicioso, se activa y encripta la información. Para tratar de evitar este tipo de ataques

hay que tratar de hacer copias de seguridad de la información en un disco o en un servidor, de forma regular, manteniendo actualizado los equipos y las aplicaciones.

3. DoS - Denegación de servicio: que se trata de un ataque de denegación de servicio (DoS) es un intento de interrumpir o deshabilitar un servicio o recurso para que los usuarios legítimos no puedan acceder a él. Puede causar graves inconvenientes, como interrupciones y pérdidas económicas. Estos ataques DoS pueden funcionar de diferentes maneras, pero en general se basan en sobrecargar el servidor o la red con una cantidad excesiva de tráfico, lo que provoca que se ralentice o se caiga por completo.
4. Ataque Man-in-the-Middle (MitM) o Intercepción en la red, se trata de un ataque cibernético en el que un ciberdelincuente se interpone en la comunicación entre dos partes, sin que ellas lo sepan, para interceptar y manipular el tráfico de datos. Se ejecuta a través de redes wi-fi públicas no seguras, phishing o un servidor infectado, un hacker se conecta en el medio de la transferencia de información entre dos personas o entre un usuario y una página web. Así, puede capturar contraseñas, información sensible, datos bancarios, etc.
5. Ataques de día cero o Zero-day exploits este tipo de ataque explota una vulnerabilidad de software que aún no es conocida por el fabricante ni por el usuario. Se llaman de día cero porque el desarrollador tiene cero días para solucionar la vulnerabilidad antes de que sea explotada por los atacantes. Funciona a través de diferentes técnicas, los ciberdelincuentes encuentran una vulnerabilidad en un sistema o en un soft y a partir de entonces inician el ataque.
6. DNS Spoofing o envenenamiento del caché DNS esta amenaza tiene como objetivo modificar las entradas de un servidor DNS para redirigir el tráfico web de los usuarios hacia sitios web falsos o maliciosos. El atacante modifica las entradas DNS en la memoria caché de un servidor DNS, que es una especie de directorio que almacena la correspondencia entre los nombres de dominio y las direcciones IP. Cuando un usuario intenta acceder a un sitio web, su dispositivo consulta al servidor DNS para obtener la dirección IP correspondiente. Si el servidor DNS ha sido envenenado, proporcionará al usuario la dirección IP de un sitio web falso en lugar del sitio web real.

Vaca Muerta como Infraestructura Crítica del sector energético argentino.

Vaca Muerta representa un pilar fundamental en la estrategia de infraestructura crítica energética de Argentina debido a sus significativos recursos de hidrocarburos no convencionales. El yacimiento ha impulsado obras estratégicas como el Gasoducto Néstor Kirchner, que permite conectar la producción de gas de Neuquén con los principales centros de consumo del país, mejorando la autonomía energética de Argentina y generando un impacto directo en la reducción de la importación de gas. Además, la reactivación del Oleoducto Trasandino ha favorecido la exportación de crudo hacia Chile, lo cual posiciona a Vaca Muerta en el comercio energético internacional (Redacción, 2023; Infobae, 2023).

El desarrollo de infraestructura en Vaca Muerta es crucial no solo para la autosuficiencia energética de Argentina, sino también para su rol como exportador, en especial mediante proyectos como el Oleoducto Vaca Muerta Norte, el cual aumentará la capacidad de transporte de crudo hacia Mendoza y Chile, asegurando rutas estratégicas para el comercio exterior. Además, la región cuenta con alianzas para implementar tecnologías sostenibles, como el uso de energías renovables en sus instalaciones, lo que apunta a una mayor sostenibilidad en el sector y resalta su relevancia tanto para la seguridad energética como para el desarrollo económico (Fundación Ambiente y Recursos Naturales, 2023; Infobae, 2023).

No obstante, Vaca Muerta enfrenta diversos riesgos y vulnerabilidades. Al tratarse de un sistema complejo de infraestructura energética, está expuesto a ciberataques que podrían interrumpir el suministro y afectar los sistemas de control industrial.

Con respecto a la protección de esta IC es fundamental establecer un marco de evaluación de riesgos que identifique las vulnerabilidades específicas de las instalaciones y sistemas tecnológicos involucrados en la explotación de Vaca Muerta. Esto incluye la implementación de medidas de ciberseguridad robustas que abarquen desde la capacitación del personal en la detección de amenazas hasta la adopción de tecnologías avanzadas de protección de datos y redes. Además, es crucial fomentar la cooperación público-privada, donde las empresas operadoras trabajen en conjunto con el gobierno y expertos en ciberseguridad para desarrollar protocolos de respuesta ante incidentes y garantizar la resiliencia de la infraestructura. La creación de un centro de monitoreo y respuesta a incidentes cibernéticos específico para Vaca Muerta podría ser una

estrategia efectiva para anticipar y mitigar posibles ataques, asegurando así la continuidad de las operaciones y la protección de este recurso vital para el desarrollo energético de Argentina.

Capítulo 2

Impacto de las Amenazas Cibernéticas en la Seguridad Nacional considerando los aspectos Económicos, Sociales y de Infraestructura.

Introducción

El Yacimiento Vaca Muerta es uno de los principales faros de proyección económica que tiene la Argentina, albergando el 40% de las reservas de gas no convencional del país. Su desarrollo ha impulsado la economía Nacional y ha posicionado a Argentina como un actor clave en el mercado energético global.

En la operación del petróleo y gas, intervienen muchas empresas que trabajan mancomunadamente para extraer el hidrocarburo y comercializarlo. Es preciso aclarar que las operaciones de campo están monitoreadas en forma remota, con lo cual son muchos los datos que se suben a la red, con los cuales se toman decisiones para continuar con la actividad Industrial.

La creciente digitalización de las operaciones en Vaca Muerta, con un incremento de dispositivos conectados a internet, la hace especialmente vulnerable a ciberataques. La interrupción de los sistemas de monitoreo remoto, que recolectan datos cruciales como presión, caudal y dirección del pozo, podría tener consecuencias catastróficas para la producción, la economía y la seguridad energética del país.

Recientes incidentes a nivel mundial, como el ataque a la empresa Colonial Pipeline (Uno de los principales proveedores de petróleo y gas de la Costa Este de los EE. UU), han evidenciado la vulnerabilidad de las infraestructuras críticas ante ciberamenazas. Un ataque exitoso a Vaca Muerta podría tener consecuencias devastadoras para la economía argentina, la seguridad energética y la estabilidad social.

Este capítulo tiene como objetivo analizar los riesgos cibernéticos que enfrentan las operaciones en Vaca Muerta, evaluando su impacto potencial y proponiendo medidas para mitigarlos. Considerando cómo estos riesgos afectan los ámbitos económicos, social y de infraestructura del país, y explorando las implicancias estratégicas de adoptar un enfoque integrado

de ciberseguridad en la Defensa Nacional. Un enfoque integrado para combatir el riesgo cibernético asegurando las operaciones industriales en el sector del petróleo y el gas.

El Yacimiento Petrolífero Vaca Muerta como infraestructura crítica depende de los Sistemas de Control de la Seguridad (ICS) para mantener operaciones seguras y confiables. Los ingenieros han diseñado e implementado con éxito ICS teniendo en mente la seguridad y la confiabilidad, pero no siempre la protección.

Los sistemas Corporativos (OT) se hallaban aislados y aptos para su propósito a la orden del día. Como estos sistemas operativos no estaban integrados a los sistemas empresariales o incluso entre sí, el riesgo de una falla en cascada a gran escala debido a un ataque, cibernético o de otro tipo, era extremadamente aislado. Veinte años después, la conectividad omnipresente de la Internet de las cosas (IoT) ha trastocado las suposiciones más básicas sobre seguridad operativa. Hoy en día, todo tipo de instalaciones industriales, incluidos yacimientos petrolíferos, oleoductos y refinerías, son vulnerables a ataques cibernéticos. Independientemente de su ubicación, los sistemas operativos pueden verse comprometidos por riesgos externos o internos, lo que provoca fallos de seguridad o producción y aumenta el riesgo comercial. Aunque los sistemas de control industrial suelen estar diseñados para funcionar a prueba de fallos, la creciente sofisticación de los cibercriminales aumenta el riesgo de incidentes catastróficos, junto con la magnitud de los impactos en aspectos económicos, sociales y de infraestructura.

Entendiendo los riesgos

Uno de los principales factores que genera una dificultad para proteger los sistemas de control industrial (ICS) es que fueron diseñados para no estar conectados; sin embargo, hoy están conectados en red. La digitalización de los procesos operativos en la industria del petróleo y el gas ha generado nuevas oportunidades para mejorar la productividad y reducir los costos. Asimismo, también ha abierto una nueva gama de riesgos cibernéticos. A continuación, se presentan los ataques más frecuentes a la Industria:

1) Explotación de vulnerabilidades: Muchas instalaciones petroleras utilizan sistemas industriales heredados que pueden contener vulnerabilidades conocidas donde una tecnología adquirida sin las debidas evaluaciones por ejemplo puede introducir una vulnerabilidad en los controladores lógicos programables (PLC), permitiendo a los

atacantes obtener acceso remoto y manipular los procesos de producción a voluntad. Esto podría resultar en paradas no programadas, daños a equipos o incluso accidentes industriales.

2) Ingeniería social y malware: Los ciberdelincuentes a menudo emplean técnicas de ingeniería social para engañar a los empleados y hacer que ejecuten software malicioso. Un ejemplo clásico es el caso de un contratista externo que introduce un virus en el entorno de producción, afectando sistemas críticos como los SCADA (Control de Supervisión y Adquisición de Datos) y creando condiciones de trabajo inseguras. Estos ataques pueden causar desde la pérdida de datos hasta la interrupción total de las operaciones.
3) Ataques de denegación de servicio (DoS): Estos ataques buscan saturar los sistemas informáticos de una organización, impidiendo el acceso a los servicios y aplicaciones. En el caso de la industria petrolera, un ataque DoS podría afectar los sistemas de control de procesos, los sistemas de seguridad o las comunicaciones internas, causando disrupciones significativas en las operaciones.
4) Ransomware: Este tipo de ataque consiste en el cifrado de los datos de una organización, exigiendo un rescate económico a cambio de la clave de descifrado. En la industria petrolera, un ataque de ransomware podría paralizar las operaciones, causar pérdidas financieras significativas y poner en riesgo la cadena de suministro.

Las amenazas son diversas y pueden tener consecuencias devastadoras, como pérdidas financieras, daños ambientales y hasta pérdida de vidas. La falta de conciencia sobre los riesgos cibernéticos y la dificultad para conciliar las perspectivas de TI y OT agravan la situación. Es fundamental que las empresas de este sector implementen medidas de seguridad robustas y colaboren estrechamente entre los equipos para proteger sus infraestructuras críticas.

Impactos de los ciberataques en la Industria Petrolífera

Según la Revista de Cibercrimen (Cybercrime Magazine) y el Foro Mundial de Economía (World Economic Forum) a nivel mundial, se estima que el costo del cibercrimen alcanzará los USD 10,5 billones anuales para 2025. Esta alarmante tendencia está impulsada por la creciente frecuencia y sofisticación de los ataques cibernéticos, incluyendo malware y ransomware.

Un ciberataque a la infraestructura crítica de una compañía de petróleo y gas puede tener repercusiones económicas devastadoras, las cuales se pueden agrupar en tres grandes categorías:

1) Interrupciones en la producción y distribución: Un ciberataque exitoso puede paralizar o ralentizar significativamente las operaciones de extracción, procesamiento y transporte de hidrocarburos. Esto genera una disminución en la producción de petróleo y gas, afectando directamente los ingresos de la compañía y los precios en el mercado. Además, las interrupciones en la cadena de suministro pueden causar escasez de combustibles, lo que a su vez impacta en la economía de un país y genera pérdidas para los consumidores.
2) Daños financieros y costos de recuperación: Los costos asociados a un ciberataque van más allá de las pérdidas directas por la interrupción de la producción. Las empresas afectadas deben invertir en la recuperación de sus sistemas, lo que implica gastos en hardware, software, servicios especializados y tiempo de inactividad. La pérdida de confianza de los inversores puede provocar una caída en el valor de las acciones de las empresas afectadas y generar inestabilidad en los mercados financieros. Asimismo, pueden enfrentar multas regulatorias, demandas legales y pérdidas reputacionales, lo que erosiona su valor de mercado y dificulta la obtención de financiamiento.
3) Impacto en la inversión extranjera: Un ciberataque puede generar una pérdida de confianza por parte de los inversores extranjeros, lo que dificulta la atracción de nuevas inversiones en el sector energético. Los inversores pueden percibir a la industria petrolera como un sector muy riesgoso. Además, la incertidumbre generada por un ciberataque puede desalentar a las empresas internacionales a establecer operaciones en el país.

Impacto Social:

Hoy en día, vivimos en una era digital, donde la infraestructura crítica se ha convertido en un objetivo principal para los ciberdelincuentes. Desde ataques de ransomware, hasta intrusiones en sistemas de energía que afectan el sector energetico de ciudades enteras, las amenazas cibernéticas representan una preocupación creciente para la estabilidad y seguridad de nuestra sociedad.

1) Disrupción en el suministro y aumento de precios: Un ciberataque a la industria petrolera puede paralizar operaciones clave como la refinación y el transporte de combustible. Esta interrupción genera escasez en las estaciones de servicio, lo que a su vez provoca largas

filas, tensiones sociales y un aumento significativo en los precios. Este incremento no solo afecta el costo de los combustibles, sino que se traslada a otros bienes y servicios, generando una inflación generalizada y afectando la economía de manera amplia.

2) Pérdida de clientes / integrantes: La paralización de operaciones puede llevar a despidos masivos, aumentando el desempleo en regiones dependientes de la industria petrolera. Además, la incertidumbre generada por estos incidentes puede desalentar la inversión y afectar negativamente. Las personas pueden dejar de confiar en la organización si no puede garantizar la seguridad de sus datos, afectando su percepción del valor, afectando su reputación.
3) Pérdida de confianza y consecuencias políticas: Los ciberataques a la industria petrolera erosionan la confianza pública en las instituciones gubernamentales y en las empresas responsables de la infraestructura crítica. Esto puede generar un sentimiento de inseguridad y desconfianza en las autoridades. Además, estos incidentes dañan la reputación de las empresas involucradas, la cobertura mediática adversa sobre un ciberataque puede amplificar el daño reputacional, especialmente en las redes sociales y medios de comunicación, lo que puede afectar su capacidad para atraer inversionistas y futuros clientes.

Impacto a las Infraestructuras Criticas:

Los ciberataques contra infraestructuras críticas se han convertido en una de las grandes amenazas actuales por sus graves consecuencias económicas y sociales.

1) Disrupción de servicios esenciales: Organizaciones en sectores clave como energía, salud, telecomunicaciones o finanzas pueden sufrir un daño grave a nivel nacional si sus sistemas son comprometidos, afectando la economía, la salud pública o la seguridad de la población.
2) Pérdida de datos: Si no se tienen copias de seguridad adecuadas, los datos importantes pueden perderse irremediablemente.
3) Debilidad: El ataque demostró vulnerabilidades en las infraestructuras críticas del País, exponiendo la facilidad con la que pueden ser manipuladas y afectadas por ciberataques.
4) Robo de la propiedad industrial: ciberataques contra infraestructuras críticas buscan menoscabar el funcionamiento de los sistemas ICS, manipularlo e, incluso, interrumpirlo.

Sin contar con que algunos ataques pueden tener como objetivo robar propiedad industrial y conseguir información confidencial sobre el funcionamiento de un ICS.

5) Daño ambiental: Algunos ciberataques pueden tener consecuencias ambientales significativas. Por ejemplo, un ataque puede provocar la liberación de contaminantes al medio ambiente, causando daños a ecosistemas y poniendo en peligro la salud humana.

Como mitigar estos ataques y prevenir su impacto

Esto requiere un programa unificado para abordar la ciberseguridad de manera sistemática en toda la empresa y las operaciones. Si bien la creación e implementación de un programa de esta naturaleza es un esfuerzo de transformación que lleva varios años, cada fase de la iniciativa debe tener el mismo objetivo en mente "avanzar en la escala de madurez para crear un entorno de ICS que sea seguro, resiliente y vigilante".

1) Análisis, Evaluación y Gestión del Riesgo de Ciberseguridad: Se identifican, evalúan y priorizan los riesgos, creando un perfil de riesgo personalizado para la organización. Esto permite enfocar los esfuerzos de seguridad en las amenazas más críticas.
2) Plan de Ciberseguridad Actualizado y Alineado a Riesgos: Se desarrolla un plan detallado que incluye políticas, procedimientos y roles, asegurando que esté alineado con los riesgos identificados y se actualice regularmente.
3) Fortalecimiento de la Conciencia: Se capacita al personal sobre las mejores prácticas de seguridad, se realizan simulacros y se promueve una cultura de seguridad para minimizar errores humanos.
4) Principio de Mínimos Privilegios: Se otorgan a los usuarios solo los permisos estrictamente necesarios para realizar sus tareas, reduciendo la superficie de ataque.
5) Segmentación de Redes: Se divide la red en segmentos más pequeños para limitar la propagación de un ataque en caso de una brecha.
6) Análisis de Vulnerabilidades – Pentests – Hacking Ético: Se realizan pruebas de penetración y análisis de vulnerabilidades de forma regular para identificar y corregir debilidades en los sistemas.
7) Revisión y Actualización de Sensores y Reglas Vigentes: Se mantienen actualizados los sistemas de detección de intrusos para garantizar una detección temprana de amenazas.

8) Actualización de Software y Parches: Se aplican de manera oportuna las actualizaciones de software y parches de seguridad para cerrar las vulnerabilidades conocidas.
9) Aplicación de Técnicas DFIR: Se utilizan técnicas de investigación forense digital para analizar incidentes de seguridad y obtener evidencia.
10) Adquisición y Aplicación de Agentes Endpoints con Microsegmentación: Se implementa una estrategia de confianza cero mediante el uso de agentes endpoints para monitorear y proteger los dispositivos.
11) Revisión Constante de Políticas de Seguridad: Se revisan y actualizan periódicamente las políticas de seguridad para garantizar su efectividad y cumplimiento.
12) Gestión de Incidentes de Ciberseguridad: Se establece un proceso claro para responder a incidentes de seguridad, incluyendo la contención, la erradicación y la recuperación.
13) Resiliencia Cibernética: Se implementan planes de continuidad del negocio, análisis de impacto del negocio y planes de recuperación ante desastres para garantizar la continuidad de las operaciones en caso de un incidente.

Conclusiones

En los últimos años, la industria del petróleo y gas ha experimentado una integración creciente entre los sistemas de TI corporativa y los sistemas de control industrial, acelerada por la digitalización del sector. Esta interconexión ha llevado a un aumento en la frecuencia y sofisticación de los ataques cibernéticos, para los cuales muchas empresas no están aún completamente preparadas.

El primer paso hacia una respuesta adecuada es evaluar la madurez del entorno de controles de ciberseguridad. Es crucial ir más allá de las medidas tradicionales de seguridad operativa y adoptar un enfoque que implemente un programa seguro, vigilante y resiliente. Esta transformación no solo fortalece la capacidad de una empresa de petróleo y gas para proteger su integridad operativa frente a la variedad creciente de amenazas, sino que también permite alcanzar la excelencia operativa y aprovechar los beneficios de productividad que ofrece un entorno de sistemas de control industrial (ICS) completamente digitalizado e integrado.

El entorno de amenazas cibernéticas que enfrenta el sector energético argentino, y en particular Vaca Muerta, demanda una evaluación exhaustiva de vulnerabilidades y la adopción de medidas de mitigación efectivas. La historia reciente de ciberataques a infraestructuras críticas en otras naciones subraya la urgencia de adoptar una postura proactiva en la defensa cibernética. La creación de un comando centralizado para la vigilancia y respuesta ante incidentes, junto con la formación continua del personal en tácticas de detección y prevención, permitirá no solo salvaguardar los recursos energéticos estratégicos, sino también preservar la estabilidad social y económica del país. La defensa cibernética debe ser considerada como un componente esencial en la estrategia de seguridad nacional, garantizando que Argentina mantenga su autonomía y capacidad operativa frente a amenazas emergentes en el ciberespacio.

La defensa de la infraestructura crítica energética de Argentina, específicamente en el yacimiento de Vaca Muerta, se presenta como un objetivo estratégico primordial para la seguridad nacional. La creciente digitalización y la interconexión de los sistemas de control industrial (ICS) han incrementado la superficie de ataque, convirtiendo a esta formación geológica en un blanco atractivo para actores cibernéticos hostiles. Es imperativo que se establezcan protocolos de

ciberdefensa robustos, que incluyan la segmentación de redes y la implementación de unidades de respuesta a incidentes (CSIRT) dedicadas a la protección de estas infraestructuras. La coordinación entre fuerzas de seguridad, entidades gubernamentales y empresas del sector energético es crucial para crear un frente unido que garantice la resiliencia operativa y la continuidad de las operaciones ante cualquier amenaza cibernética.

Referencia

Morgan, J. (29 de junio de 2022). Ciberseguridad en el monitoreo de procesos dentro de Petróleo y Gas. https://newsroom.axis.com/blog/cybersecurity-oil-gas

Almada, P. (2021). Impacto “real” de la ciberseguridad en los ambientes del Oil & Gas y su situación en la región. https://www.petrotecnia.com.ar/new/420/impacto.html

Petrobras (20 de noviembre de 2023). Ciberseguridad en la Industria del Petróleo: Protegiendo Activos Críticos. https://www.petrobras.com.ar/ciberseguridad-en-la-industria-del-petroleo-protegiendo-activos-criticos/

Dirección Nacional de Ciberseguridad (2023). Informe 2023 del CERT.ar https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/informes-de-la-direccion-7

Agencia de la Unión Europea para la Ciberseguridad (4 de diciembre de 2013). Good practice guide for CERTs in the area of Industrial Control Systems - Computer Emergency Response Capabilities considerations for ICS. https://www.enisa.europa.eu/publications/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems

Thomson, J. (2024). Perspectiva de la industria de energía y servicios públicos 2024 - Delo https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/power-and-utilities-industry-outlook.html

Shale en Argentina (2023). Vaca Muerta. http://www.shaleenargentina.com.ar/vaca-muerta

Aguirre Leiva, E. (15 de mayo de 2021). ¿Está protegida Vaca Muerta de los ciberataques? https://mase.lmneuquen.com/vaca-muerta/esta-protegida-vaca-muerta-los-ciberataques n797555

Arrieta, F. (29 de julio de 2024). Pérdidas millonarias en Argentina por delitos cibernéticos – Infobae. https://www.infobae.com/opinion/2024/07/29/perdidas-millonarias-en-argentina-por-delitos-ciberneticos/

Infosecurity México (21 de septiembre de 2023). ¿Cuál es el impacto económico de los ciberataques a nivel mundial? – Ciberlatam. https://www.segurilatam.com/actualidad/cual-es-el-impacto-economico-de-los-ciberataques-a-nivel-mundial_20230921.html

Reuters (11 de mayo de 2022). Cibercrimen ha costado 6 millones de dólares a las economías del mundo – El Economista. https://www.eleconomista.com.mx/tecnologia/Cibercrimen-ha-costado-6-millones-de-dolares-a-las-economias-del-mundo-20220511-0022.html

El Cronista (26 de marzo de 2024). Argentina, en la mira de los hackers: es el tercer país con más ciberataques de la región. https://www.cronista.com/infotechnology/actualidad/argentina-en-la-mira-de-los-hackers-es-el-tercer-pais-con-mas-ciberataques-de-la-region/

Almada, P. (26 de mayo de 2023). Cómo prevenir a las pymes de Vaca Muerta ante los ataques cibernéticos – Vaca Muerta news. https://vacamuertanews.com/actualidad/como-prevenir-a-las-pymes-de-vaca-muerta-ante-los-ataques-ciberneticos.htm

Fundación Ambiente y Recursos Naturales (2023). Infraestructura en Vaca Muerta: pieza clave en su explotación. https://www.farn.org.ar

Infobae. (2023). Vaca Muerta: un hito que demuestra el potencial de la Argentina para abastecer de energía sustentable al mundo. https://www.infobae.com

Redacción. (2023). Vaca Muerta y el año de las grandes obras de infraestructura. https://www.redaccion.com.ar

Eissa, S. G., Gastaldi, S., Poczynok, I., & Zacarías Di Tullio, E. (2014). El ciberespacio y sus implicancias para la defensa nacional. Aproximaciones al caso argentino. Revista de Ciencias Sociales de la Universidad Nacional de Quilmes, 6(25), 181-197.

Carbajales, J. J. (2023). El futuro de Vaca Muerta en el contexto energético global. Nueva Sociedad, (306), 86-107.

Kozulj, R. (2015). El sector energético argentino. Un análisis integrado de sus problemas, impactos y desafíos macroeconómicos. Editorial UNRN.

Cantamutto, F. J. (2020). Vaca Muerta y las elusivas promesas de desarrollo en Argentina. Ensayos de economía, 30(56), 185-209.

RUTZ, A. T. Y. G. (2021). Aportes a la ciberdefensa y ciberseguridad para la gestión de las infraestructuras críticas de la información en Argentina. Revista Defensa Nacional-Nro.

Miranzo, M., & del Río, C. (2014). La protección de infraestructuras críticas. Revista UNISCI, (35), 339-352.

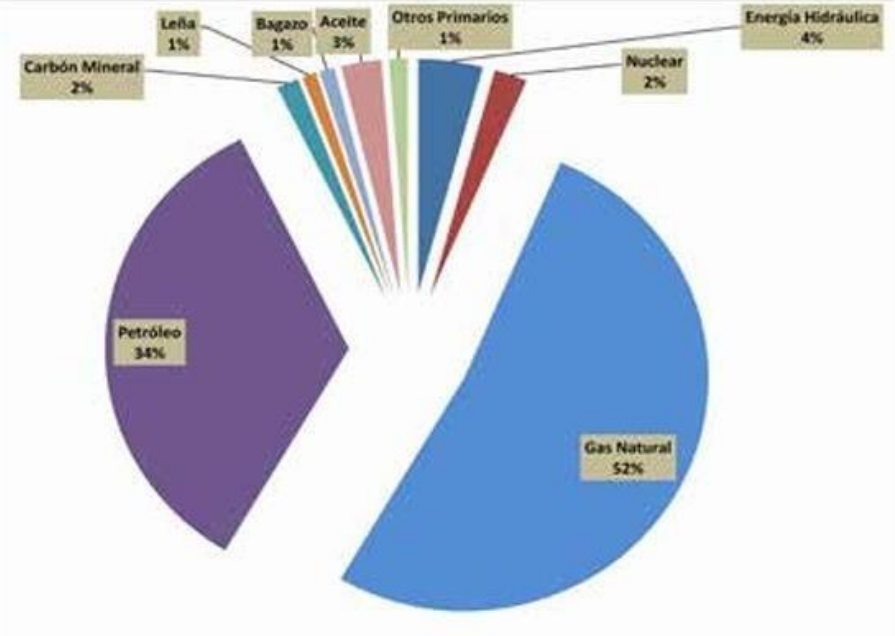
Cárdenas, G. J. (2011). Matriz energética argentina. Situación actual y posibilidades de diversificación. Revista de la Bolsa de Comercio de Rosario, 9, 32-36.

ANEXOS A (AL TRABAJO FINAL INTEGRADOR)

DEPENDENCIAS DE LOS COMBUSTIBLES FÓSILES. Uso de los recursos No Renovables en la producción de energía en Argentina desde el año 2013 a la actualidad.

Figura 1

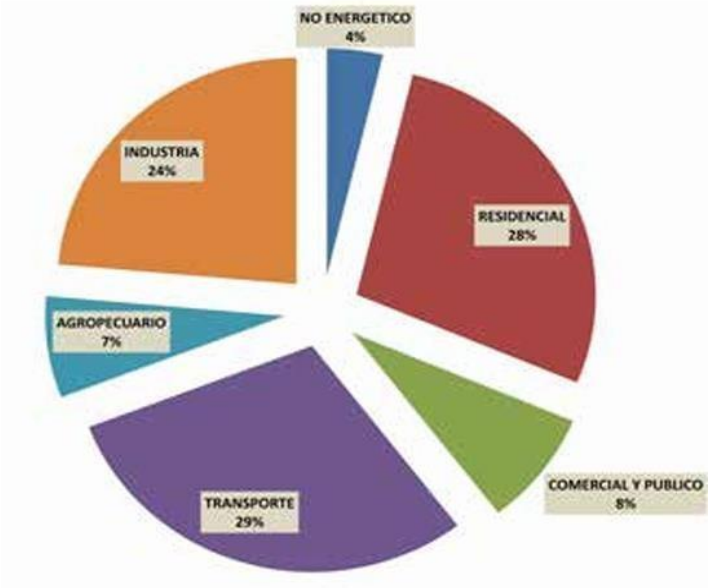
Oferta energética según fuentes primarias en Argentina. Año 2013



Nota. Datos de la Secretaria de Energia de la Nacion, Balances Energeticos 2013. Accedido en Marzo 2015 en http://www.energia.gov.ar/verpagina.php?idpagina=3366.

Figura 2

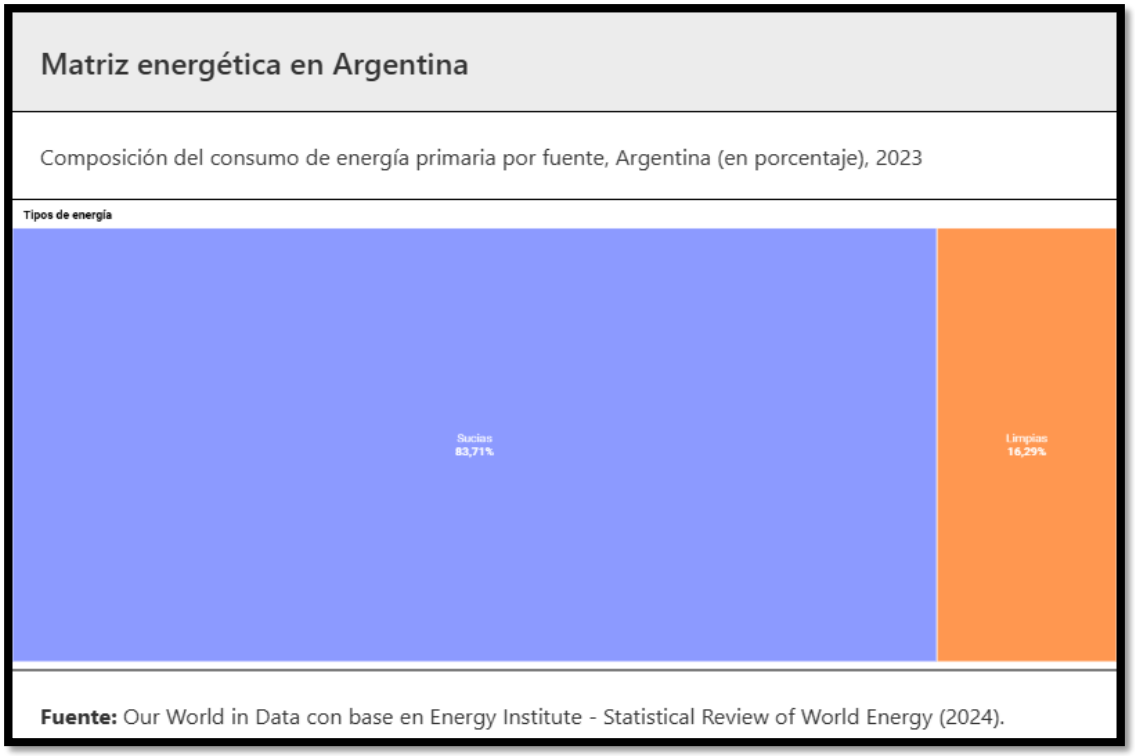
Datos del uso de la energía



Nota. Balance Energético noviembre 2013. Accedido en http://www.energia.gov.ar/contenidos/verpagina.php?idpagina=3366.

Figura 3

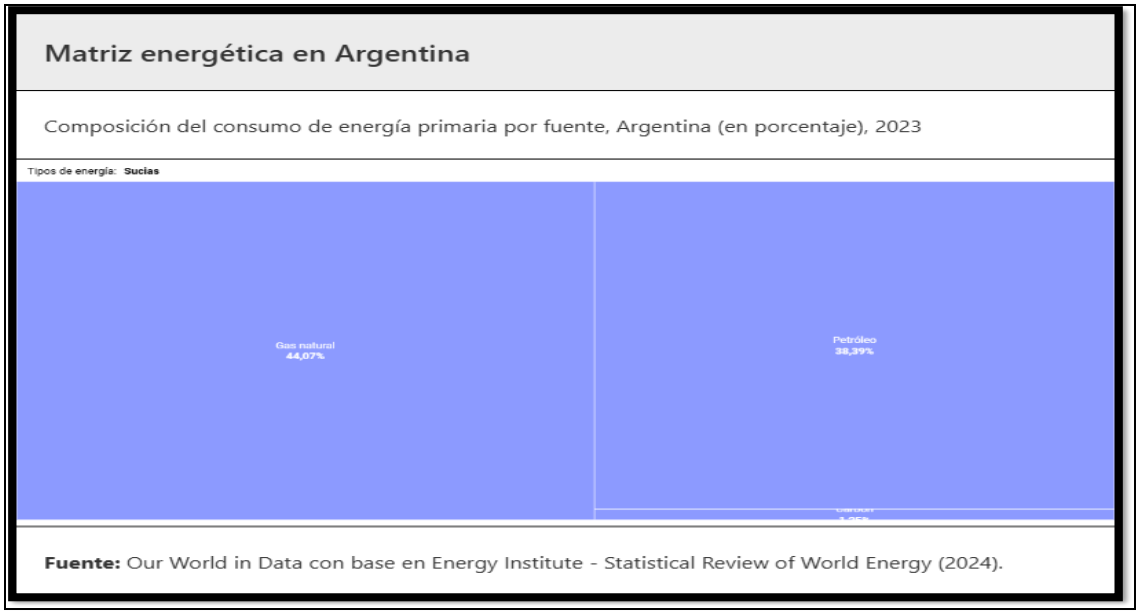
Porcentaje del consumo de energía primaria por fuente 2023- Energías sucias y limpias



Nota. Datos del porcentaje del uso de energías. Tomado de Statistical Review of world Energy (2024).

Figura 4

Total, de energías sucias



Nota. Datos del porcentaje del uso de energías sucias. Tomado de Statistical Review of world Energy (2024)

Figura 5

Total, de Energías limpias

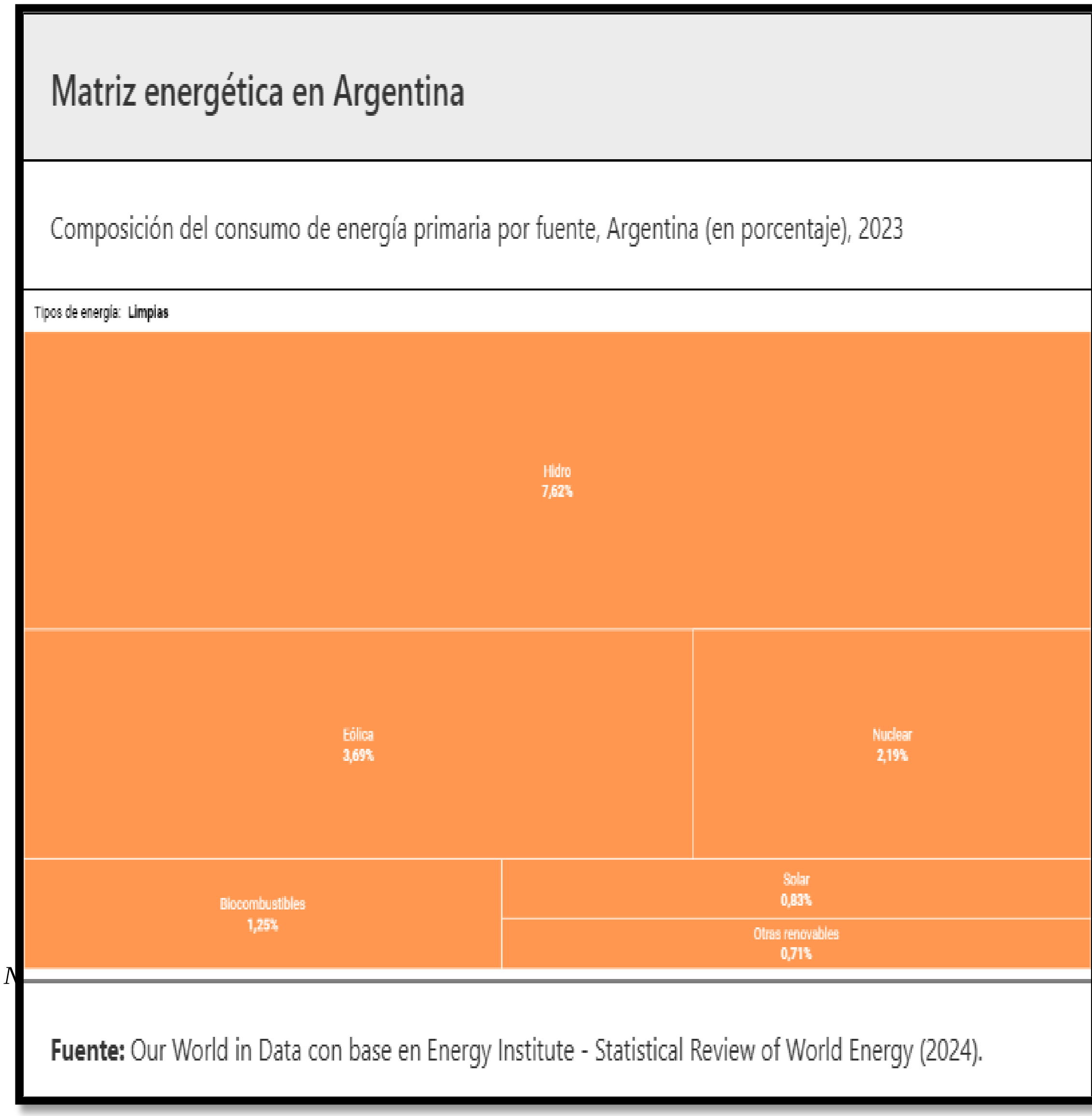
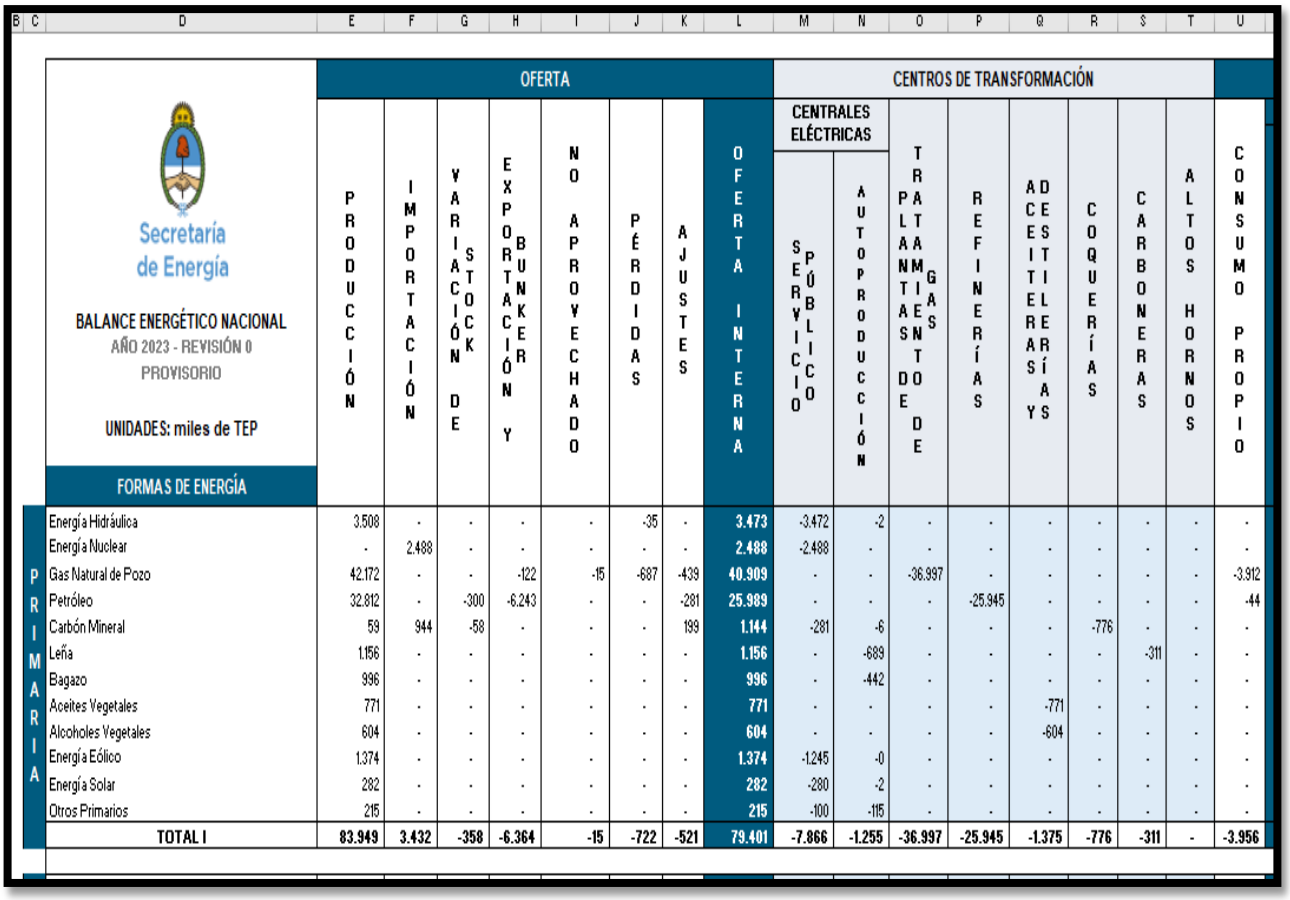


Figura 6

Balance Energético Nacional, formas de energía primaria



Secretaría de Energía

BALANCE ENERGÉTICO NACIONAL
AÑO 2023 - REVISIÓN 0
PROVISORIO

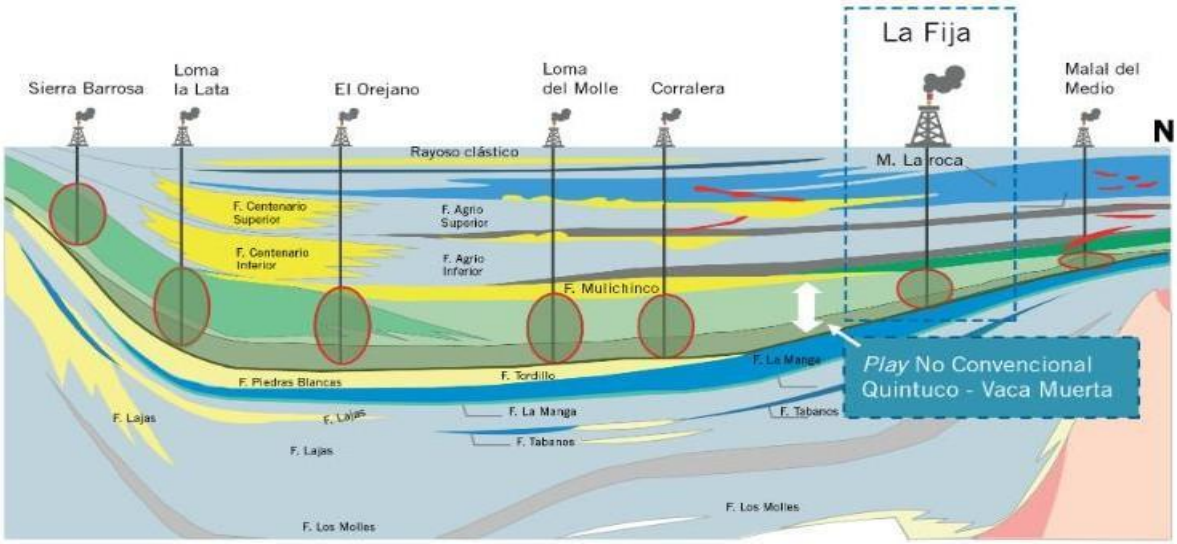
UNIDADES: miles de TEP

	FORMAS DE ENERGÍA	OFERTA								CENTROS DE TRANSFORMACIÓN								
										CENTRALES ELÉCTRICAS								
		PRODUCCIÓN	IMPORTACIÓN	VARIACIÓN STOCK DE	EXPORTACIÓN Y BUNKER	NO APROVECHADO	PÉRDIDAS	AJUSTES	OFERTA INTERNA	SERVICIO PÚBLICO	AUTOPRODUCCIÓN	TRANSFORMACIÓN DE GAS	REFINERÍAS	ADECESTIERASÍAYS	COQUERÍAS	CARBONERAS	ALTOS HORNOS	CONSUMO PROPIO
PRIMARIA	Energía Hidráulica	3.508	-	-	-	-	-35	-	3.473	-3.472	-2	-	-	-	-	-	-	-
	Energía Nuclear	-	2.488	-	-	-	-	-	2.488	-2.488	-	-	-	-	-	-	-	-
	Gas Natural de Pozo	42.172	-	-	-122	-15	-687	-439	40.909	-	-	-36.997	-	-	-	-	-	-3.912
	Petróleo	32.812	-	-300	-6.243	-	-	-281	25.989	-	-	-	-25.945	-	-	-	-	-44
	Carbón Mineral	59	944	-58	-	-	-	199	1.144	-281	-6	-	-	-	-776	-	-	-
	Leña	1.156	-	-	-	-	-	-	1.156	-	-689	-	-	-	-	-311	-	-
	Bagazo	996	-	-	-	-	-	-	996	-	-442	-	-	-	-	-	-	-
	Aceites Vegetales	771	-	-	-	-	-	-	771	-	-	-	-	-771	-	-	-	-
	Alcoholes Vegetales	604	-	-	-	-	-	-	604	-	-	-	-	-604	-	-	-	-
	Energía Eólico	1.374	-	-	-	-	-	-	1.374	-1.245	-0	-	-	-	-	-	-	-
	Energía Solar	282	-	-	-	-	-	-	282	-280	-2	-	-	-	-	-	-	-
	Otros Primarios	215	-	-	-	-	-	-	215	-100	-115	-	-	-	-	-	-	-
	TOTAL I	83.949	3.432	-358	-6.364	-15	-722	-521	79.401	-7.866	-1.255	-36.997	-25.945	-1.375	-776	-311	-	-3.956

Nota. Balance energético Nacional, formas de energía primaria. Uso del Petróleo y Gas Natural de Pozo. Año 2023. Accedido octubre 2024 en https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.argentina.gob.ar%2Fsites%2Fdefault%2Ffiles%2Fbalance_2023_v0_h.xlsx&wdOrigin=BROWS

Figura 7

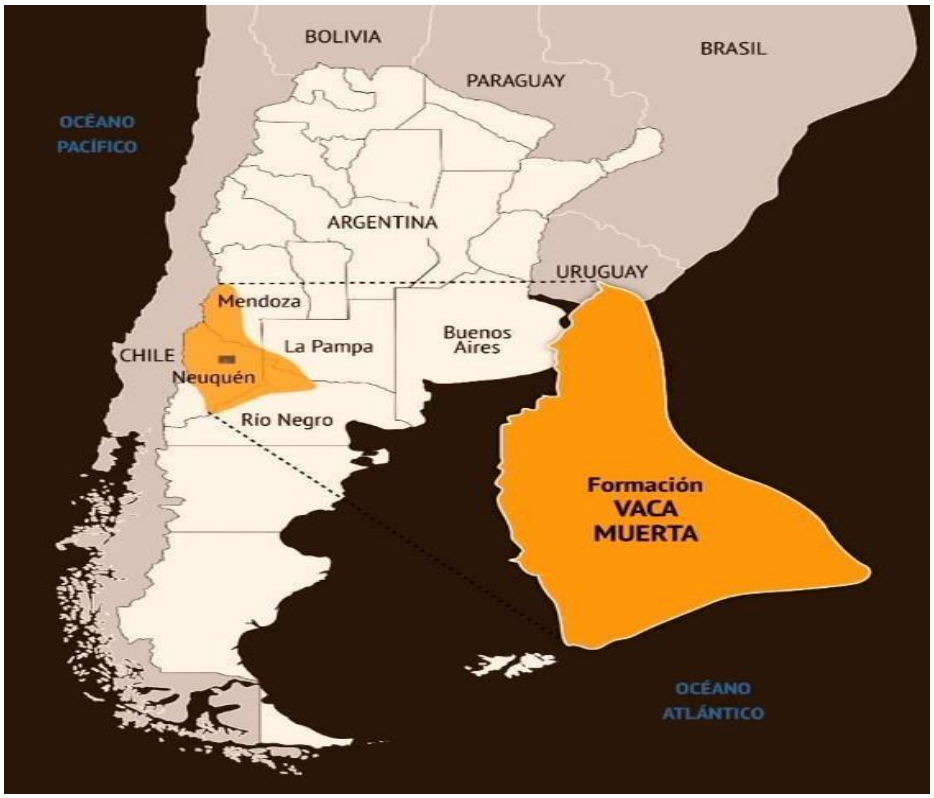
Corte sur a norte de la Cuenca Neuquina, donde se indica la sección sedimentaria, en la cual se podría realizar explotación de tipo no convencional.



Nota. Descripción gráfica del corte de la cual se puede realizar la explotación. Accedido octubre 2024 en https://www.argentina.gob.ar/economia/energia/vaca-muerta/historia.

Figura 8

Extensión de "VACA MUERTA"



Nota. Ubicación en el mapa de "VACA MUERTA".

ANEXO B (AL TRABAJO FINAL INTEGRADOR) EJEMPLOS DE CIBERATAQUES

IRAN

Ataque	IICC	DAÑOS	AÑO
El ataque permaneció 30 días observando el funcionamiento de la centrifugadoras (tiempo en que tardan en llenarse de uranio) y reprogramo su velocidad.	Motores de las centrifugadoras que enriquecen uranio en la planta nuclear de NATANZ (IRAN)	Deshabilitar 1000 centrifugadoras	2010

UCRANIA

Ataque	IICC	DAÑOS	AÑO
Programa malicioso BLACKENREGY 3. La distribución del programa se realizó mediante PHISHING personalizado, se trataba de un correo electrónico con un adjunto falso de Microsoft, el cual, al abrirlo, infectaba el equipo.	Compañías energéticas	Tres regiones sin electricidad en pleno invierno, un total de 250.000 personas afectadas.	2015

ARABIA SAUDITA

Ataque	IICC	DAÑOS	AÑO
Ciber terroristas, A través de un programa malicioso llamado TRITON, este controla el sistema de seguridad instrumentado (SIS). Introducido mediante PHISHING.	Se toma control de una estación de trabajo	No se llevó a cabo, pero se buscaba por medio del sabotaje, provocar una explosión al atacar los sistemas de seguridad que prevenían los accidentes industriales catastróficos.	2017

EL ATAQUE A LA RED ELÉCTRICA DE UCRANIA

Ataque	IICC	DAÑOS	AÑO
Ataque cibernético dirigido.	Red eléctrica.	Dejo a cientos de miles de personas sin electricidad.	2015

EL INCIDENTE DE COLONIAL PIPELINE (ESTADOS UNIDOS)

Ataque	IICC	DAÑOS	AÑO
Ataque de RANSOMWARE.	Colonial Pipeline, red de transporte de combustible.	Dejo a cientos de miles de personas sin electricidad. Obligo a empresas a cerrar sus operaciones durante varios días, causando	2021

		escasez de gasolina en varias regiones.	

ANEXO C (AL TRABAJO FINAL INTEGRADOR) TIPOS DE AMENAZAS

	Dimisión	**Modo de operar**	**Identidad/ organización**
Terrorismo	Fue progresando. Ca da vez hay nuevos movimientos	A nivel global Mediática	Yihadista Daesh/ISIS
Crimen organizado	Transnacional	Capacidad desestabilizadora, ánimo de lucro, debilitar es Estado, minar la gobernanza económica.	Grupos violentos
Proliferación de armas de destrucción masiva	Amenaza de la paz y seguridad a nivel internacional.	Ataque NBQR	
Espionaje	Nacional e Internacional, a empresas extranjeras.	Obtiene información y datos confidenciales, ej: como las infraestructuras críticas.	
Vulnerabilidad del ciberespacio	Global	Conseguir diferentes propósitos, depende los intereses geopolíticos de estados,	

		organizaciones terroristas y actores individuales.	
Vulnerabilidad del espacio marítimo, aéreo, y ultraterrestre	Acciones que van contra los sistemas de control de navegación y los tráficos ilícitos.	Piratería, terrorismo, trafico ilícitos, etc. A través de drones, realizar espionajes, atentados y riesgos para la seguridad ciudadana, física y patrimonial.	

Datos sobre el aumento de ciberataques al sector energético

	Propone	**Vulnerabilidad**	**Datos**
Foro Económico Mundial (WEF)	Apela a la Ciberseguridad	La interconexión y digitalización de las empresas en el desarrollo	En 2021, sufrió más de 451 mil ciberataques en el mundo, un incremento de 28% respecto al año anterior.
Informe de X-Force Threat Intelligence Index 2022		Ransomware, 25% Troyanos DDos Phising	cuarta posición en relación a las industrias más afectadas por los ataques en el ciberespacio. Actividades en relación al gas y petróleo

Principales Riesgos Cibernéticos en el Sector Energético

Tipos de ataques	**Efectos**
Malware y Ransomware	Programas maliciosos pueden infiltrarse en sistemas críticos, cifrando datos vitales y exigiendo un rescate para su liberación.
Ataques DDoS	Buscan saturar los sistemas con tráfico, haciendo que los servicios en línea se vuelvan inaccesibles. Podría interrumpir la comunicación y el control de las infraestructuras
Intrusiones en Sistemas de Control Industrial (ICS)	Pueden acceder a sistemas y manipular los procesos industriales, con potenciales consecuencias catastróficas.
Phishing	A través de correos electrónicos engañosos, buscan robar credenciales de acceso.