UNCUYO
UNIVERSIDAD NACIONAL DE CUYO

FACULTAD DE INGENIERÍA

Sector Energético

Infraestructura Crítica

Grupo Gardel:

Cuello, Juliana
Di Rocco, Constanza
Ferre Lo Castro, Iván
Nieto, Augusto

Grupo Metaverso2022:

Aguilera, José
Amodeo, Marianela
López, Lucía
Trípoli, Natalia

ÍNDICE:

1 Introducción

El presente informe abordará el tema de Infraestructuras Críticas y Resiliencia, y la importancia de ellas para garantizar el óptimo funcionamiento de los servicios prestados por el Estado y las empresas privadas.

También, se hará el análisis de un caso particular que amenazó con la integridad de una de las infraestructuras críticas esenciales de Argentina, recalcando las posibles consecuencias frente a dicho suceso.

1.1 ¿Qué es una infraestructura crítica?

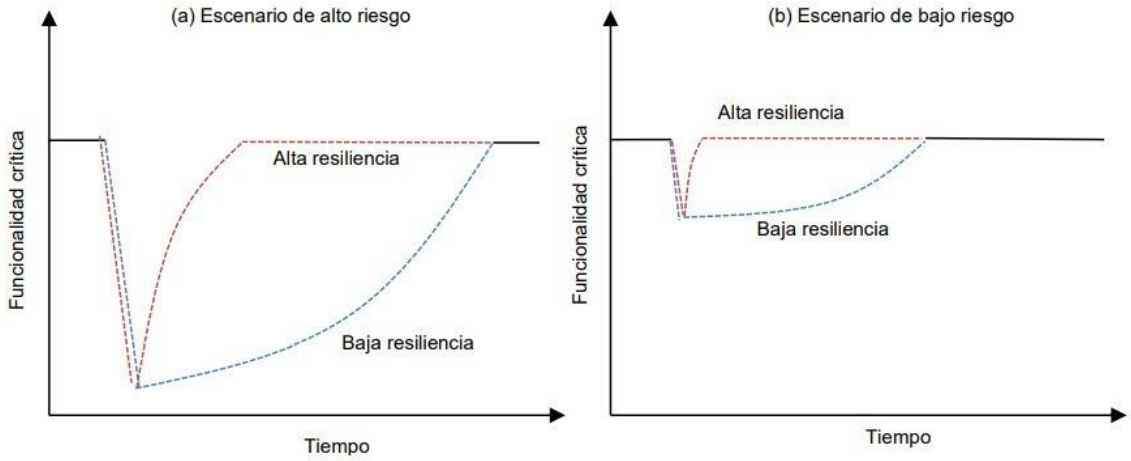
Son todos aquellos sistemas físicos o virtuales que hacen posible las funciones y servicios considerados esenciales y que contribuyen al buen desempeño de los sistemas más básicos a nivel social, económico, medioambiental y político. Cualquier alteración o interrupción en su suministro, debido a causas naturales (una catástrofe climática, por ejemplo) o provocada por el factor humano (como un ataque cibernético a una central de energía eléctrica) podría acarrear graves consecuencias.

RESILIENCIA

Es la capacidad de una infraestructura (y sus sistemas relacionados) para mitigar, adaptarse o responder positivamente a nuevas condiciones, transformándose de manera de poder restaurar, mantener e incluso mejorar sus funciones esenciales.

La resiliencia se define con base en la presencia de cuatro propiedades: robustez, redundancia, recursos y rapidez.

Propiedad	Descripción
Robustez	Resistencia, o la capacidad de los elementos, sistemas y otras unidades de análisis para soportar un determinado nivel de estrés o demanda sin sufrir degradación o pérdida de su función.
Redundancia	Medida en que existen elementos, sistemas u otras unidades de análisis que son sustituibles, es decir, capaces de satisfacer requisitos funcionales en caso de interrupción, degradación o pérdida de funcionalidad.
Recursos	Capacidad de identificar problemas, establecer prioridades y movilizar recursos cuando existen condiciones que amenazan perturbar algún elemento, sistema u otra unidad de análisis. También llamado "ingenio", este atributo puede conceptualizarse adicionalmente como la capacidad de aplicar recursos materiales (es decir, monetarios, físicos, tecnológicos e informativos) y humanos para cumplir con las prioridades alcanzar los objetivos establecidos.
Rapidez	Capacidad de cumplir con las prioridades y alcanzar los objetivos de manera oportuna para contener las pérdidas y evitar futuras interrupciones.



Representación teórica de la resiliencia de un sistema en escenarios de alto y bajo riesgo

1.2 Tipos de Infraestructuras Críticas

Las infraestructuras críticas suelen ser similares en todos los países, aunque puede haber diferencias en función de los recursos, necesidades y nivel de desarrollo que tengan. Suelen agruparse por sectores o áreas estratégicas como:

- Administración: Instalaciones, servicios básicos, redes de información, patrimonio nacional y monumentos.
- Financiero-tributario: Entidades bancarias, sistemas informáticos gubernamentales.
- Alimentación: Empresas u organismos dedicados al almacenamiento, producción y distribución.
- Agua: Instalaciones de tratamiento, de redes, embalses, almacenamiento.
- Producción y distribución de redes de energía: Oleoductos, centrales energéticas, gasoductos, etc.
- Centrales nucleares: Almacenamiento, producción y transporte de materiales nucleares, radiológicos, mercancías peligrosas.

- Industrias químicas: Transporte, almacenamiento y producción de materiales químicos.
- Salud e infraestructura sanitaria.
- Investigación: Laboratorios productores de sustancias peligrosas o críticas.
- Transportes: Toda la infraestructura relativa a aeropuertos, ferrocarriles, puertos, redes de transporte público, instalaciones intermodales, sistemas de regulación y control de tráfico.
- Tecnologías de la comunicación e información: Redes de telecomunicaciones, centralitas y aquellas que puedan dar información a otras infraestructuras críticas.
- Instalaciones relacionadas con los espacios exteriores.

2 Producción y distribución de redes de energía

La infraestructura energética se divide en tres segmentos interrelacionados: electricidad, petróleo y gas natural. La dependencia de prácticamente todas las industrias con respecto a la energía eléctrica y los combustibles implica que todos los sectores se ven influenciados. Esto resalta la importancia que debe ser dada a la infraestructura crítica y a su planificación y preparación frente a posibles riesgos. La cooperación a través de grupos de la industria ha dado como resultado un intercambio sustancial de información sobre las mejores prácticas en todo el sector.

Medir el progreso en el avance de los objetivos de seguridad y resiliencia es uno de los principios rectores centrales que deben ser considerados por los estados de todo el mundo en el marco de gestión de riesgos para la infraestructura crítica. Muchos propietarios y operadores del sector han adquirido una amplia experiencia con respecto a la protección de la misma y han centrado su atención en la ciberseguridad.

3 Caso de Estudio: ciberataque contra el sistema de gestión virtual de la red de gasoductos de TGS.

TGS (Transportadora de Gas del Sur) es una transportadora de gas natural, responsable de 9.231 kilómetros de gasoductos distribuidos en siete provincias del sur de la República Argentina. Es la transportadora más importante del país y opera el sistema de gasoductos más extenso de América Latina. Pertenece al sector de Producción y distribución de redes de energía.

Dicha compañía, sufrió un ciberataque contra su sistema SPAC, la plataforma de procesamiento de solicitudes, asignación y programación de los volúmenes de gas que se cargan en la red de gasoductos que opera la empresa.

El SPAC permite, entre otras cosas, efectuar un seguimiento preciso de los volúmenes recibidos y entregados. TGS ofrece una página web en la que se puede seguir el esquema diario de nominaciones. Esta interfaz es la que fue hackeada. Sin embargo, el sistema de transporte de gas no se vio afectado en ningún momento. Es decir, el ciberataque dejó fuera de servicio la página web de TGS, pero no hubo riesgo para la operación en sí misma del sistema de gas. A través del equipo IT de la empresa el sistema se fue normalizando progresivamente.

El sabotaje informático también afectó parcialmente a los compradores de gas ya que el SPAC es una herramienta vital para realizar una gestión diaria del gas que se toma del sistema y a partir del mismo obtener información valiosa a la hora de tomar decisiones técnicas.

3.1 Ciberataque

Los ciberataques contra sistemas estratégicos del sector energético, cada vez más interconectado gracias a la digitalización, son una realidad que se repite cada vez con mayor asiduidad a nivel mundial. En la mayoría de esos casos, los hackers exigen a los propietarios de esos programas una suma de dinero para restablecer el control de la operación.

La ciberseguridad para los sistemas de suministro de energía requiere la colaboración entre diversas partes interesadas del sector energético: incluidos los servicios públicos, los proveedores, los laboratorios nacionales, las universidades y el gobierno, que trabajan en la informática de la ciberseguridad.

3.2 ¿Qué hubiese pasado si la amenaza hubiese sido más dañina?

En caso de que el riesgo hubiese sido de mayor escala, esta amenaza no solo estaría violando la privacidad de una empresa, sino que estaría perjudicando la distribución de gas en gran parte del país.

Consecuencias y principales sectores afectados:

- Centrales térmicas para la generación de energía eléctrica. Por ende, desabastecimiento energético.
- Plantas cementeras, se pararía la construcción.
- Suministro domiciliario. Si el corte perdura esta es la consecuencia más grave de todas ya que las cañerías, una vez restablecido el flujo de gas, pueden llegar a arrastrar mucha suciedad y taponar filtros de la entrada de los reguladores y otros equipos. Las válvulas reguladoras no se activan, produciendo colapso de sistemas de mantenimiento.
- Industrias donde la producción es continua y los paros de planta requieren procesos paulatinos y no bruscos.
- Los dirigentes de las empresas no pueden tomar decisiones porque hay incertidumbre y entonces se genera el caos.

Distribución de los gasoductos de TGS (en rojo)

4 Conclusión

Tanto empresas estatales como privadas forman parte de la infraestructura crítica del sector de energía; siendo la empresa analizada un actor principal en el transporte de gas dentro del país, podría considerarse que una parte específica del sector mostró una respuesta positiva frente a una amenaza inminente. La comunicación e interrelación entre el estado y empresas genera la base de una infraestructura resiliente. El estado en conjunto con los diferentes agentes partícipes del sector debería crear políticas que mejoren la resiliencia de la infraestructura crítica, minimizando las consecuencias adversas de los incidentes a través de esfuerzos combinados de planificación y mitigación. Logrando así respuestas efectivas y asegurar la rápida recuperación de servicios esenciales.

Se hace hincapié en la importancia del sector para un normal funcionamiento de la vida en sociedad debido a que puede considerarse a este como excepcionalmente crítico porque proporciona servicios fundamentales en todos los sectores de infraestructura crítica.

5 Bibliografía

https://microsegur.com/seguridad-en-infraestructuras-criticas/

https://www.cisco.com/c/m/es_cl/articles/infraestructuras-criticas-cda.html

https://econojournal.com.ar/2022/04/tgs-logro-resolver-un-ciberataque-que-afecto-un-sistema-virtual-de-gestion-del-sistema-gasifero/

https://drive.google.com/drive/folders/1DuPIxot6LUGts2lELxfbr181ApQnKE_T (Link de cátedra)

https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19

https://repositorio.cepal.org/bitstream/handle/11362/46646/1/S2000675_es.pdf