INSTITUTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS

DIPLOMATURA UNIVERSITARIA EN GESTIÓN DE LA CIBERDEFENSA

TRABAJO FINAL INTEGRADOR

GESTIÓN DE LA RESILIENCIA EN INFRAESTRUCTURAS CRÍTICAS: UN ENFOQUE BASADO EN RIESGOS Y CIBERDEFENSA

Integrantes del Equipo Nro 9 :

Rocha José

Canevaro Juan

Velez Gabriel

Barbera Marcela

Títulos Profesionales / de grado

Licenciado en Seguridad

Licenciado en Conducción y Gestión Operativa

Licenciado en Conducción y Gestión Operativa

Abogada/Lic en Ciencias de la Educación

08 de noviembre de 2024

Índice General

Resumen

La gestión de la resiliencia en infraestructuras críticas, que incluye la ciberdefensa y la mitigación de riesgos, es esencial para garantizar la seguridad y la continuidad de los servicios clave en una sociedad moderna.

Busca asegurar que los sistemas y servicios esenciales (como energía, transporte, agua y comunicaciones) puedan resistir, adaptarse y recuperarse de interrupciones, ya sean provocadas por desastres naturales, fallos técnicos o ataques deliberados. La resiliencia en este contexto es crucial para minimizar el impacto de estos eventos en la sociedad.

Este tipo de gestión implica evaluar y reducir vulnerabilidades, implementar planes de contingencia, desarrollar redundancias en sistemas críticos y capacitar a los operadores. También requiere una colaboración constante entre sectores público y privado para mejorar la respuesta ante incidentes, la recuperación y la adaptación de las infraestructuras frente a nuevas amenazas.

Justificación / Fundamentación / Aportes

Elegir la gestión de la resiliencia en infraestructuras críticas es crucial porque estas infraestructuras son esenciales para el funcionamiento y la seguridad de la sociedad, la economía y el bienestar general de la población.

Cualquier interrupción en estos servicios esenciales, como energía, agua, transporte o comunicaciones, puede tener consecuencias graves y de gran alcance, desde afectar la salud y seguridad de las personas hasta impactar la economía y la estabilidad social.

Implementar un enfoque de resiliencia permite reducir la vulnerabilidad, identificar y fortalecer puntos débiles en infraestructuras críticas, se minimizan las posibilidades de que fallos o ataques causen interrupciones graves

Además, la gestión de la resiliencia en infraestructuras críticas ofrece beneficios a largo plazo que justifican su implementación y la optimización de recursos y reducción de costos. Aunque invertir en resiliencia puede implicar costos iniciales, a largo plazo se ahorran recursos al reducir la necesidad de reparaciones extensas, minimizar interrupciones y evitar pérdidas económicas. Asimismo, la capacidad de recuperación rápida disminuye el tiempo en el que el sistema está fuera de servicio, lo que reduce el impacto financiero.

Para profundizar en los beneficios de la gestión de la resiliencia en infraestructuras críticas, se puede considerar también sus impactos en innovación, sostenibilidad y desarrollo de capacidades. Al enfocarse en la resiliencia, las organizaciones y gobiernos se ven motivados a innovar y adoptar tecnologías avanzadas que puedan fortalecer las infraestructuras críticas. Esto puede incluir inteligencia artificial para la detección temprana de amenazas, blockchain para asegurar registros, o el Internet de las Cosas (IoT) para mejorar la disponibilidad y monitorear sistemas en tiempo real. Esta inversión en tecnología no solo mejora la resiliencia, sino que también abre oportunidades para mejorar la eficiencia y optimizar el funcionamiento diario de los sistemas críticos.

Planteo del problema

En cualquier sociedad se depende en gran medida del funcionamiento eficaz y eficiente de los sistemas de infraestructuras críticas para prestar servicios públicos, enriquecer la vida y estimular el crecimiento económico.

Las infraestructuras críticas nacionales son el eje central de una economía moderna, y la resiliencia de las infraestructuras críticas es esencial para un desarrollo sostenible. Una infraestructura robusta y resiliente es un motor clave del crecimiento económico. La fiabilidad, el rendimiento, el funcionamiento continuo, la seguridad, el mantenimiento y la protección de las infraestructuras críticas son prioridades nacionales y locales en todo el mundo.

La pandemia COVID-19 aceleró las previsiones tecnológicas por la necesidad de interconectar personas y sistemas con sus actividades normales. Al realizarse por urgencia y no con un planeamiento adecuado, sumado a los fenómenos meteorológicos extremos y a los atacantes que día a día mejoran sus técnicas con la motivación de obtener dinero, han puesto de manifiesto las vulnerabilidades y la exposición de los sistemas de infraestructuras en todo el mundo. Los sistemas de infraestructuras existentes y los servicios que prestan se ven cada vez más afectados por los desastres de origen natural o de origen humano.

Las políticas, las estrategias y los marcos normativos deben basarse en análisis de riesgos y en una clara comprensión de las vulnerabilidades de los sistemas nacionales de infraestructuras. Para mejorar la resiliencia de las infraestructuras mediante el fortalecimiento de la gobernanza es necesario comprender el rendimiento de las infraestructuras existentes, su exposición, el entorno normativo actual, los retos y las barreras, la coordinación entre las distintas partes interesadas y las opciones para integrar la resiliencia. Este proceso también requiere que se construya un entendimiento común de la «resiliencia de las infraestructuras críticas», basado en ciertos criterios que puedan servir de orientación para los gobiernos y el sector privado.

Una de las principales fisuras es la falta de comprensión de lo que significa y supone realmente una «infraestructura resiliente» en términos de política, planificación y medidas prácticas, a las que los sectores público y privado pueden referirse cuando planifican y gestionan políticas y proyectos de infraestructuras

Las acciones no pretenden limitar las intervenciones y las mejoras, sino fomentar un acuerdo innovador que resuelva los retos de resiliencia de las infraestructuras que son exclusivos de las distintas naciones del mundo. A medida que nuestras infraestructuras económicas se vuelven más variadas, interconectadas e innovadoras, y que nuestros entornos (por ejemplo, natural, social, construido) se vuelven más diversos, se esperan nuevas acciones clave que surjan con el tiempo. Además, como ocurre con todos los sistemas de innovación orientados a la mejora, existe el riesgo de que se produzcan consecuencias no deseadas. Esto exige una evaluación continua de la eficacia nacional de estos principios.

Formulación del Problema

¿Cuáles son los principales desafíos para implementar una estrategia efectiva de resiliencia en infraestructuras críticas?

Solución Propuesta

Para dar respuesta al interrogante y dado el carácter y la diversidad de la temática se considera que las infraestructuras críticas sustentan nuestra calidad de vida y bienestar social debido a la prestación de servicios esenciales en una amplia gama de sectores, desde la sanidad, el transporte, la energía, las telecomunicaciones, la seguridad pública, los servicios de emergencia y el funcionamiento efectivo del estado.

Una Infraestructura resiliente ofrece un enfoque integral para garantizar que la resiliencia se integre en la planificación y ejecución de los proyectos de infraestructuras. Contribuye a crear un acuerdo común sobre cómo mejorar la resiliencia de las infraestructuras en un contexto de riesgo con conmociones y desastres con efecto dominó, cada vez más enmarañados que pueden producirse en todo el sistema de infraestructuras. Con este enfoque se asegura de que todo lo que se hace sea resiliente y que todas las inversiones en infraestructuras manifiesten el avance de la resiliencia general de las mismas.

En el caso de las infraestructuras que fueron ideadas hace años y que día a día nos brindan servicios es necesario adoptar todas las medidas necesarias tanto administrativas como técnicas que nos permitan tener una resiliencia acorde a nuestros tiempos.

En un mundo cada vez más interconectado las políticas, la legislación, la cooperación entre entes estatales y privados, es fundamental para una resiliencia efectiva, teniendo en cuenta que cada infraestructura crítica va afectar en mayor o menor medida a otras. Por lo que su rápida recuperación favorece a la estabilidad de una sociedad.

Objetivos

Objetivo General

Desarrollar e implementar un marco integral de gestión de la resiliencia en infraestructuras críticas que permita identificar, evaluar y mitigar los riesgos cibernéticos y físicos, garantizando así la continuidad operativa, la seguridad de los sistemas y la protección de los servicios esenciales ante amenazas y vulnerabilidades emergentes.

Objetivos particulares

- Identificar riesgos, amenazas y vulnerabilidades que afectan a las infraestructuras críticas.
- Analizar las medidas tecnológicas y organizativas para proteger los sistemas y redes críticas de ataques cibernéticos.
- Analizar planes de continuidad y recuperación que aseguren la rápida recuperación y continuidad de las operaciones en caso de incidentes.
- Entender sobre la formación del personal involucrado en la gestión de infraestructuras críticas sobre las mejores prácticas en ciberseguridad y resiliencia.
- Entender sobre la cooperación entre distintos sectores y con entidades gubernamentales para mejorar la respuesta ante amenazas y cumplir con las normativas de seguridad vigentes.

Marco Teórico

Iniciando este momento del trabajo es menester citar las reflexiones iniciales de Alejandro Corletti Estrada Manual de la Resiliencia" (Una guía práctica de Ciberresiliencia en Redes y Sistemas de TI) 2020.

"El poder del siglo XXI se llama "Información".

El quinto escenario militar "Ciberespacio" tiene como límites la "Información". El tesoro es la "Información", no la infraestructura que la sustenta".

Una infraestructura, se la puede resumir en un conjunto de hardware (de red y TI) y software (sistemas operativos, aplicaciones y bases de datos). A medida que se interconectan, configuran y prueban, los mismos van entrando en producción y desempeñando su rol sobre la base de los servicios que deben ofrecer.

En definitiva esta es la parte menos problemática, pues si sufrieran cualquier tipo de incidente, natural o artificial, los mismos se reponen o se reinstalan y el problema, con sus más y sus menos, queda resuelto en un tiempo aceptable o no, en la medida que tengamos bien implantados nuestros planes de recuperación de desastres y/o planes de continuidad de negocio. Estos mismos planes se complican a la hora de entrar en juego la "Información" que a lo largo de los años se procesa en estas infraestructuras.

En Occidente, las libertades individuales han sido pilares de las sociedades, hoy esas libertades individuales están cada vez más coartadas por los controles sociales necesarios para vivir en orden en una población en constante aumento. Eso es contradictorio en sociedades donde la democracia, entendida como la opinión de las mayorías, se adopta por una opinión pública que en realidad se ha transformado en opinión mediática que puede ser manipulada por el poder político y económico que busca mantener o conquistar el poder. La información es poder, y habrá que aceptar una intromisión cada vez más frecuente en esferas que antes se reservaban exclusivamente a las libertades individuales.

Hay que asumir que el mundo está bajo constante ataque. Los países no están solos, y necesitan conformar alianzas con países poderosos que serán competidores. Este sistema de alianzas es de un equilibrio inestable, porque los países periféricos recibirán una cuota de poder del país repartidor de poder que se refleja en bienestar para sus ciudadanos. Como cada actor pugnará para obtener más beneficios, el equilibrio será inestable. El riesgo más grande es que la desinformación, la manipulación y las redes sociales venzan el espíritu de resistencia de los hombres a la dominación, haciéndoles ver como favorables a situaciones que van encontrar de sus intereses legítimos, y su bienestar.

Es este el momento para marcar diferencias y definirlas.

La resistencia a los desastres enfatiza la importancia de las medidas de mitigación previas al desastre que mejoran el desempeño de estructuras, elementos de infraestructura e instituciones para reducir las pérdidas por un desastre.

La resiliencia refleja una preocupación por mejorar la capacidad de los sistemas físicos y humanos para responder y recuperarse de eventos extremos.

La resiliencia es:

- La capacidad de recuperación.
- Una herramienta con un límite (umbral) elástico, plástico o de rotura.
- Una herramienta con un equilibrio entre rigidez y flexibilidad.
- Un sistema no es resiliente “per sé”, sino que debemos considerar “Resiliente a qué”.
- Presenta una justa relación entre “amortiguación" y un mero “rebote”.
- Su tiempo de respuesta es óptimo.
- Para que el concepto de resiliencia pueda ser estable a lo largo del tiempo, es necesario valorar qué esfuerzo de mantenimiento requiere.
- Cualquier anomalía o incidente, deseado o no, impacta directamente en la capacidad de recuperación del mismo.

Relacionándolo con la Informática y Telecomunicaciones respecto a la “Resiliencia”. Una infraestructura de redes y sistemas de TI no se puede catalogar de resiliente o no resiliente, es preferible manejarse por valores de “tolerancia” o porcentajes de cumplimiento.

El análisis de riesgo es un proceso crítico que permite identificar, evaluar y priorizar riesgos asociados a un sistema, proyecto o infraestructura, con el objetivo de gestionar y mitigar sus impactos potenciales. En el contexto de infraestructuras críticas, este análisis es fundamental para garantizar la seguridad y la continuidad operativa.

Los estándares mundialmente reconocidos para este análisis de riesgo tienen como punto de partida las normas ISO pero ninguna incluye metodologías para la gestión de riesgos, es decir no dan pautas acerca de cómo desarrollar el análisis de riesgo, pero sí son muy detalladas en los aspectos clave a considerar y por qué deben ser considerados.

MAGERIT es una metodología robusta y práctica que permite a las organizaciones gestionar de manera efectiva los riesgos relacionados con la seguridad de la información. Su enfoque sistemático y estructurado facilita la identificación y tratamiento de riesgos, contribuyendo así a la protección de los activos de información críticos.

La matriz de la resiliencia es una herramienta que permite evaluar y visualizar la capacidad de una infraestructura, organización o sistema para resistir y recuperarse de eventos adversos. Esta matriz ayuda a identificar áreas de mejora y establecer estrategias para aumentar la resiliencia ante diferentes tipos de riesgos, tanto físicos como cibernéticos.

Beneficios de la Matriz de Resiliencia: proporciona una representación visual que facilita la comprensión de las relaciones entre riesgos y capacidades, ofrece un enfoque sistemático para evaluar la resiliencia de una organización o infraestructura y permite realizar un seguimiento de las mejoras en la resiliencia a lo largo del tiempo y ajustar las estrategias según sea necesario.

Metodología

En la metodología de recopilación de datos bibliográficos se apoya el desarrollo del presente trabajo. Está orientada a la selección, análisis, interpretación de resultados y conclusiones plasmadas en bibliografía y artículos científicos sobre el tema de elección con el fin de obtener información que contribuya a la solución del problema.

Capítulo I

Las Infraestructuras críticas

Como se formulara en la introducción, el presente capítulo tiene como objetivo conceptualizar la Infraestructura crítica.

Se plantean definiciones de Infraestructuras críticas abordadas por distintos países y organismos internacionales, con el objetivo de identificar características distintivas e intentar conseguir conclusiones.

En la adopción de definiciones de IICC válida para referentes como el General Evergisto de Vergara, lo crítico no es la infraestructura, sino la información.

Sección 1

Conceptos y definiciones en el Ámbito Internacional.

Al abordar el tema de las infraestructuras críticas, se puede percibir una abundancia de conceptos y/o definiciones, según el país u organismo; por lo cual es necesario adoptar un concepto que sirva como base de análisis.

A continuación se exponen algunos conceptos más expuestos o definidos:

Comisión Europea: 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 y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones. [1]

España: son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales. [2]

Estados Unidos: “La infraestructura crítica de la nación proporciona los servicios esenciales que sustentan la sociedad estadounidense y sirven como columna vertebral de la economía, la seguridad y la salud de nuestra nación. Lo conocemos como la energía que usamos en nuestros hogares, el agua que bebemos, el transporte que nos mueve, las tiendas en las que compramos y los

sistemas de comunicación de los que dependemos para mantenernos en contacto con amigos y familiares". [3]

Brasil: "instalaciones, servicios, bienes y sistemas cuya interrupción o destrucción, total o parcial, causa graves impactos sociales, ambientales, económicos, políticos, internacionales o la seguridad del Estado y de la sociedad". [4]

[1]DIRECTIVA 2008/114/CE DEL CONSEJO de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección
[2]Ley 8/2011, Medidas para la Protección de Infraestructuras Críticas.
[3]Directiva de la Política Presidencial PPD-21.
[4]DECRETO N° 11.200, DE 15 DE SEPTIEMBRE DE 2022 - Plan Nacional de Seguridad de Infraestructuras Críticas.

Sección 2

Conceptos y definiciones en el Ámbito Nacional

En año 2019, con la Resolución 1523/2019 de la Jefatura de Gabinetes de Ministro, se aprueba y publica en la República Argentina, la Estrategia Nacional de Ciberseguridad (ENCS) en la cual se establece:

- La definición de infraestructuras críticas y de infraestructuras críticas de información.
- La enumeración de los criterios de identificación y la determinación de los sectores alcanzados

Según lo establecido por la Estrategia Nacional de Ciberseguridad de la República Argentina, se define como infraestructura crítica:

*"**A 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**".*

Asimismo establece los siguientes parámetros o criterios para identificar las infraestructuras críticas y los sectores identificados:

A. Criterios para identificar las infraestructuras críticas:
   • IMPACTO EN LA VIDA HUMANA

Existe impacto para la vida humana, en aquellos casos en los cuales debido a la afectación de un sistema informático, se genere riesgo de pérdida de vida o grave amenaza a la salud e integridad física de las personas.

• IMPACTO ECONÓMICO

Existe impacto económico para el país, en aquellos casos en los cuales debido a la afectación de un sistema informático se genere daño o amenaza de daño, grave, a la estructura productiva y/o financiera del país

• IMPACTO EN EL MEDIO AMBIENTE

Existe impacto en el medio ambiente cuando debido a la afectación de un sistema informático se afecte negativamente o dañe gravemente el espacio en el que se desarrolla la vida de los seres vivos.

• IMPACTO EN EL EJERCICIO DE LOS DERECHOS HUMANOS Y DE LAS LIBERTADES INDIVIDUALES

Existe impacto en ejercicio de derechos humanos o de las libertades individuales en aquellos casos en que mediante cualquier acción desarrollada mediante un sistema informático, se restrinja o coarte indebidamente de manera colectiva, el pleno ejercicio de los derechos consagrados en los Tratados Internacionales, la Constitución Nacional o las leyes.

• IMPACTO PÚBLICO O SOCIAL

Existe impacto público o social, en aquellos casos en que debido a la afectación de un sistema informático se produzcan acontecimientos susceptibles de provocar grave conmoción en una parte significativa de la población.

• IMPACTO EN EL EJERCICIO DE LAS FUNCIONES DEL ESTADO

Existe impacto en el ejercicio de las funciones del Estado, cuando debido a la afectación de un sistema informático, se afecte de manera sustancial el normal desempeño de los órganos de los poderes Ejecutivo, Legislativo o JudiciaL

• IMPACTO EN LA SOBERANÍA NACIONAL

Existe impacto sobre la soberanía nacional, cuando mediante la afectación de un sistema informático se cuestione o restrinja el poder del Estado Nacional en el ámbito del territorio nacional.

• IMPACTO EN MANTENIMIENTO DE LA INTEGRIDAD TERRITORIAL NACIONAL:

Existe impacto en el mantenimiento de la integridad territorial nacional, cuando mediante la afectación de un sistema informático, se vulneren las fronteras territoriales, marítimas o espaciales de la nación.

B. Sectores identificados

- Energía
- Tecnologías de Información y Comunicaciones
- Transportes
- Hídrico
- Salud
- Alimentación
- Finanzas
- Nuclear
- Químico
- Espacio
- Estado

Sección 3
Aproximación a la clasificación de las Infraestructuras Críticas

El Ingeniero Aguirre Ponce en su tesis de maestría en Seguridad Informática del año 2017, realiza una clasificación de las IICC las que constituye un punto de partida a ser considerado.

Según él las infraestructuras críticas pueden clasificarse de la siguiente manera, de acuerdo a su prestación:

	TIPO	FUNCIÓN	DISPONIBILIDAD	EFECTOS	AMENAZAS	OBJETIVOS BUSCADOS
	De servicio	**Proveen servicios vitales a un país y para ellas**	**La disponibilidad constituye la condición especial.**	**La falta de disponibilidad genera un gran impacto en los ciudadanos**	**Los ataques de denegación de servicio distribuidos y el malware.**	**Alterar el funcionamiento de los sistemas principales.**

PRESTACIÓN	**De información**	**Almacenan, procesan o transfieren información de tipo confidencial o sensible para su propietario.**	**El propietario de la información puede ser una organización proveedora de servicios vitales, instituciones públicas o privadas o un ciudadano**	**La información es el activo crítico de estas infraestructuras y por lo tanto, se debe garantizar su confidencialidad, integridad y disponibilidad**	**Fraudes, robo de información confidencial y malware**	**Dedicado a secuestrar la información sensible.**

Sección 4

Amenazas a Infraestructuras Críticas

La adopción de nuevas tecnologías, sin considerar los debidos controles de ciberseguridad en las infraestructuras críticas, genera potencialmente nuevos vectores de amenazas, especialmente en los ambientes industriales porque se conectan redes seguras con entornos no seguros como Internet.

Las amenazas buscan aprovechar una debilidad o ausencia de controles en los sistemas para explotar una vulnerabilidad.

Una vulnerabilidad es una debilidad existente en un sistema que puede ser utilizada por un atacante para comprometer su seguridad.

Las vulnerabilidades pueden ser de varios tipos: software, hardware, procedimentales o humanas. Algunos ejemplos de sistemas vulnerables serían:

- Aplicaciones desactualizadas u obsoletas
- La utilización de un mecanismo de cifrado inseguro
- Un control de acceso insuficiente
- La inexistencia de una política de gestión de contraseñas
- Una persona, vulnerable a ingeniería social

A continuación podemos identificar algunas fuentes de amenazas:

- Estados extranjeros
- Crimen organizado
- Hacktivistas
- Delincuentes
- Organizaciones terroristas

Estas fuentes pueden originar, entre otros, los siguientes tipos de amenazas:

- Espionaje industrial
- Sabotaje
- Robo de datos
- Indisponibilidad del servicio
- Explotación de código malicioso
- Conflictos entre naciones

Conclusiones Parciales

En línea con la introducción del presente capítulo, se puede concluir que, en general, tanto en el ámbito internacional como nacional, los conceptos establecidos sobre infraestructuras críticas son similares.

Asimismo, se observa que la importancia de las IICC radica en su relación con los servicios esenciales, dando un amplio abanico de acción y medidas a considerar para brindar seguridad y funcionamiento.

En la República Argentina, este tipo de IICC se encuentra bajo gestión privada y sumado al vacío legal en la materia de protección de las mismas, dificulta el trabajo de carácter interagencial. Por lo que se debe pugnar por una legislación que nos permita trabajar en conjunto.

La realidad es que la mayoría de las IICC de servicios esenciales para la vida de las personas y para la economía, como la energía, el agua, el transporte, las comunicaciones y los servicios financieros, entre otros, tienen en la actualidad una fuerte dependencia de las redes informáticas y lo seguirá teniendo conforme siga avanzando la tecnología.

Su protección es extremadamente compleja, ya que implica la coordinación de esfuerzos de múltiples actores públicos y privados. El resguardo de dichas infraestructuras, transforma las condiciones del ambiente geográfico Nacional, siendo de interés tanto el nivel operacional, como en el nivel estratégico.

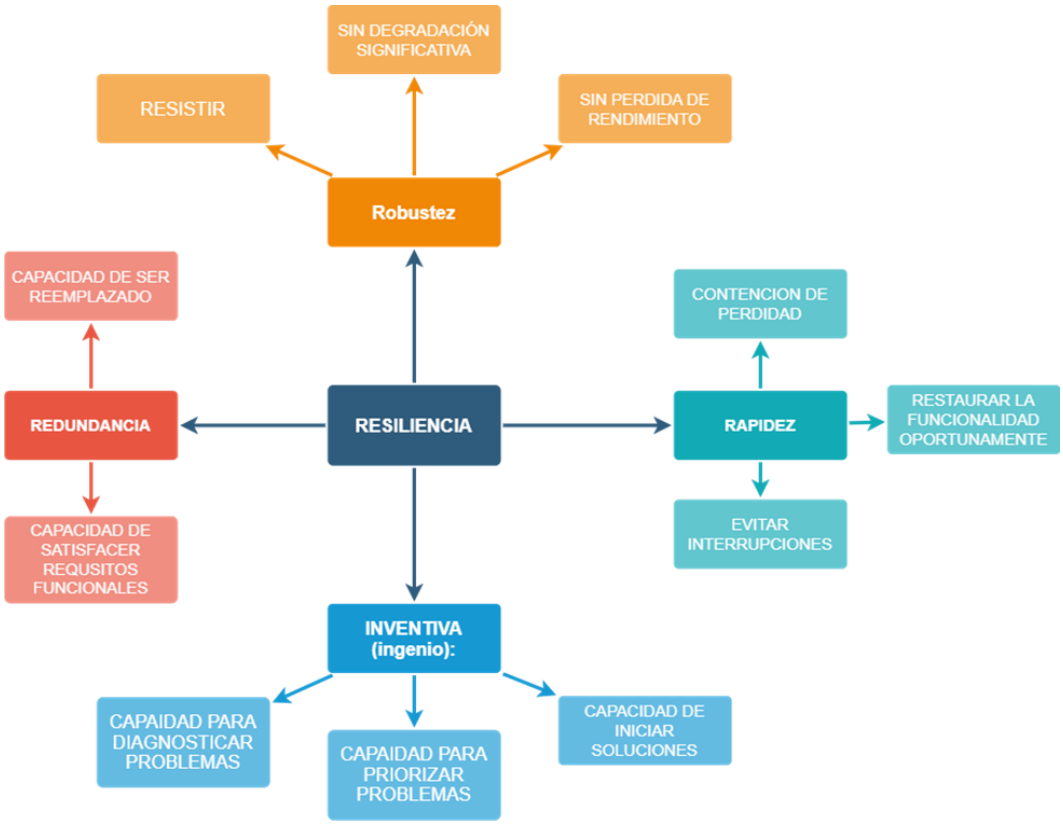
Capítulo II
La Resiliencia en las Infraestructuras Críticas

El presente capítulo tiene por finalidad establecer las bases conceptuales de la Resiliencia y su relación con las infraestructuras críticas.

Sección 1
La Resiliencia

La resiliencia de infraestructuras críticas se refiere a la capacidad de estas infraestructuras para anticiparse, resistir, recuperarse y adaptarse a situaciones adversas, como desastres naturales, ataques cibernéticos, fallos operativos o crisis sanitarias, minimizando el impacto en el funcionamiento de la infraestructura y en la sociedad.

Esto implica no sólo la robustez física de las infraestructuras, sino también la flexibilidad organizativa, la capacidad de respuesta y la planificación a largo plazo.



Fuente: elaboración propia en base a la información disponible en el Manual de Resiliencia - **Alejandro Corletti Estrada-** Madrid, octubre de 2020.

Otros autores, establecen que la resiliencia de se basa en varios componentes clave:

- **Prevención y Mitigación:** implementación de medidas que reduzcan la vulnerabilidad a eventos adversos.
- **Robustez:** capacidad de una infraestructura para resistir las disrupciones sin perder su funcionalidad esencial. Esto puede incluir la redundancia de sistemas y componentes críticos.
- **Redundancia:** existencia de sistemas y procesos alternativos que puedan tomar el relevo en caso de falla de los sistemas principales. Esto asegura que haya una capacidad de reserva disponible en todo momento.
- **Capacidad de respuesta:** habilidad para reaccionar de manera efectiva y rápida ante incidentes, minimizando el tiempo de inactividad y los impactos negativos. Esto incluye la disponibilidad de equipos de emergencia y la realización de ejercicios de simulación.
- **Capacidad de recuperación:** capacidad para restablecer la operatividad normal de las infraestructuras en el menor tiempo posible. Esto implica tener planes de recuperación bien definidos y recursos disponibles para su implementación.
- **Adaptabilidad:** capacidad de las infraestructuras y las organizaciones para aprender de los eventos pasados y mejorar continuamente sus estrategias de protección y resiliencia.

Sección 2

Gestión de las IICC basada en la estrategia de Resiliencia

Las estrategias de resiliencia para infraestructuras críticas abarcan un conjunto de acciones y enfoques que buscan mejorar la capacidad de estas infraestructuras para enfrentar y recuperarse de eventos adversos.

Las estrategias de resiliencia incluyen, pero no se limitan a:

- **Desarrollo de Infraestructuras flexibles y adaptables:** Diseñar infraestructuras que puedan adaptarse a cambios y resistir diversos tipos de amenazas.
- **Mejora continua:** Revisar y actualizar constantemente los planes de protección y recuperación basados en nuevas amenazas, tecnologías y lecciones aprendidas de eventos anteriores.
- **Colaboración y coordinación:** Fomentar la cooperación entre diferentes sectores y niveles de gobierno para compartir información y recursos, y coordinar respuestas ante emergencias.
- **Innovación tecnológica:** Implementar tecnologías avanzadas que mejoren la vigilancia, detección y respuesta ante incidentes. Esto incluye el uso de inteligencia artificial y análisis de big data para predecir y mitigar riesgos.

Asimismo, el Departamento de Seguridad Nacional de EE.UU proporciona a través del **"National Infrastructure Protection Plan"** (NIPP), un marco para la protección y resiliencia de las infraestructuras críticas.

Algunas de las estrategias más efectivas que propone incluyen:

- **Evaluación de Riesgos:** Realizar análisis detallados para identificar vulnerabilidades y riesgos potenciales, permitiendo priorizar acciones.
- **Diseño Robusto:** Implementar principios de diseño que aumenten la resistencia de las infraestructuras, como materiales más duraderos y estructuras redundantes.
- **Planificación y Preparación:** Desarrollar planes de emergencia y protocolos de respuesta que incluyan simulacros regulares y formación del personal.
- **Monitoreo y Mantenimiento:** Establecer sistemas de monitoreo en tiempo real para detectar fallos o anomalías y realizar un mantenimiento preventivo adecuado.
- **Diversificación de Recursos:** No depender de un solo recurso o sistema, lo que ayuda a mitigar el impacto de fallos en un componente específico.

- **Colaboración y Alianzas:** Fomentar la cooperación entre diferentes sectores, agencias gubernamentales y comunidades para compartir recursos y conocimientos.
- **Inversión en Tecnología:** Adoptar tecnologías avanzadas, como inteligencia artificial y análisis de datos, para mejorar la gestión de riesgos y la respuesta a emergencias.
- **Educación y Conciencia Pública:** Informar y educar a la población sobre los riesgos y las medidas de preparación, fomentando una cultura de resiliencia.
- **Adaptación Climática:** Integrar estrategias que consideren el cambio climático y sus efectos, asegurando que las infraestructuras sean adaptables a futuras condiciones.
- **Financiamiento Sostenible:** Asegurar recursos financieros para la implementación y mantenimiento de medidas de resiliencia a largo plazo.

Conclusiones Parciales

En conclusión, la resiliencia de las infraestructuras críticas es esencial para garantizar su funcionamiento ante situaciones adversas.Este concepto abarca no sólo la robustez física, sino también la flexibilidad organizativa y la capacidad de respuesta ante emergencias.

Las estrategias propuestas, que incluyen la evaluación de riesgos, el diseño robusto, la colaboración interinstitucional y la innovación tecnológica, son fundamentales para mejorar la capacidad de estas infraestructuras de anticiparse, resistir, recuperarse y adaptarse.

Al implementar un enfoque integral en estas áreas, se puede asegurar un sistema más robusto y preparado para enfrentar los desafíos del futuro, minimizando así el impacto en la sociedad y promoviendo una cultura de resiliencia.

Implementar estas estrategias de manera integral puede fortalecer significativamente la resiliencia de infraestructuras críticas, garantizando su funcionamiento continuo y su capacidad de recuperación ante crisis.

Conclusiones Finales

La resiliencia de los servicios críticos que abastecen la infraestructura en ningún tiempo ha sido tan significativa. Hay inmensidades de experiencias incuestionables de que la inversión en la resiliencia de las infraestructuras está económicamente justificada.

Una infraestructura flexible y vasta puede atenuar las interrupciones e ir más allá de los límites del sistema para garantizar la capacidad de recursos frente a alteraciones insospechadas. Seleccionar las medidas en función de las competencias, los recursos disponibles y el acomodamiento de la solución al entorno cambiante.

Se debe originar una capacidad de adaptación en los sistemas de infraestructura en todas las etapas del ciclo de vida para permitir la flexibilidad en la toma de decisiones, la transición y la resolución de problemas. Es necesario desarrollar estructuras de gestión y organizaciones dinámicas y flexibles que permitan a los trabajadores adecuarse en caso de perturbación.

Es ineludible insistir en el desarrollo de las competencias del personal operativo a todos los niveles, con una formación que permita tener autoridad para intervenir de forma autónoma. Los procesos que contienen sistemas humanos y digitales deben garantizar las operaciones en tiempo y forma de acuerdo a lo previsto.

La incorporación de la capacidad de control manual permite a los humanos responder a las sorpresas abriendo y cerrando vías para el flujo de servicios, permitiendo que la infraestructura funcione más allá de los umbrales diseñados, y encendiendo y apagando recursos de reserva. Esto puede permitir intervenciones rápidas en respuesta a perturbaciones inesperadas.

Los planes y proyectos de inversión en la infraestructura deben evaluarse antes de su puesta en marcha para garantizar el cumplimiento de la Ganancia neta de resiliencia. El estudio requiere la creación de capacidades y conocimientos de las distintas partes interesadas que participan en todas las fases de desarrollo, explotación y mantenimiento de las infraestructuras

Resiliencia, ciberseguridad y ciberresiliencia son términos afines, pero no idénticos que comparten fronteras difusas. La preocupación por prevenir los riesgos (ciberseguridad) se ha ampliado a la recuperación si se producen ciberataques (ciberresiliencia) o crisis complejas en las que entran componentes cibernéticos y no cibernéticos (resiliencia). La ciberresiliencia es un prerrequisito del ciberespacio y del ecosistema de ciberseguridad asociado a una economía digitalizada madura. Abarca todos los ámbitos de la ciberseguridad, incluida la recuperación, y tiene su

propia dinámica de adaptación. Se incluye por diseño en las políticas nacionales y corporativas de ciberseguridad y dispone de un creciente conjunto de instrumentos.

Por otra parte, la resiliencia ocupa un lugar destacado entre las prioridades de los responsables de las seguridades colectiva, nacional y corporativa. La resiliencia tiene vocación omnicomprensiva, gestionar todos los componentes relevantes y evitar rupturas sistémicas.

Que un Estado, organización o corporación sean resilientes significa que pueden resistir mejor los riesgos y amenazas que afectan a los servicios esenciales y también que pueden recuperar su funcionamiento si los ataques se producen en entornos degradados.

La ciberresiliencia, la resiliencia de la ciberseguridad, obliga a los CISO y autoridades responsables a gestionar los riesgos de ciberseguridad y a colaborar en la gestión de los riesgos no cibernéticos. Para lo primero, la ciberresiliencia ha evolucionado desde el cumplimiento de unas medidas de seguridad establecidas ex ante hacía la obligación de anticipar y evaluarlos riesgos individuales a los que se ve expuesto cada agente, proceso o producto crítico y adoptar por diseño una estrategia de gestión del riesgo embebida al mismo. Para los segundos, la ciberresiliencia debe formar parte de los mecanismos de gestión de crisis y continuidad de negocio para asegurar la resiliencia global/integral. Según el volumen y la vulnerabilidad de las empresas a la continuidad de negocio, los CISO continuarán ocupándose de la ciberseguridad, de la ciberresiliencia o de la resiliencia si participan en la gestión de los riesgos no cibernéticos.

Por todo lo expuesto podemos concluir que los principales desafíos encontrados al implementar una estrategia efectiva de resiliencia sobre un infraestructura crítica cualquiera, se basan en:

- La falta de una legislación acorde para permitir a quien corresponda accionar, controlar y/o monitorear las infraestructuras críticas de la información, lo cual considerando que no existen ICI definidas legalmente, dificulta entender sobre las capacidades resilientes de las mismas.

- El no tener conocimiento de las capacidades tanto de personal como material de las ICI dificulta, el planeamiento estratégico de los elementos de ciberdefensa para brindar apoyo cuando se lo solicite. Y con esto un adiestramiento muy amplio y general, cuando sería más eficiente realizarlo de manera particularizado.

- En un mundo interconectado, la poca o nula interacción entre entes estatales y/o privados, en la detección, análisis y respuesta ante amenazas, no permite la transmisión de experiencia o indicadores de

compromiso, en un ámbito en el que un par de minutos pueden hacer la diferencia entre que un malware ingrese o no a nuestras sistemas.

- Planificar la resiliencia en una Infraestructura crítica es esencial para lograr una recuperación acorde a las necesidades de los sectores críticos por toda la influencia que estos tienen en el normal desarrollo de nuestro país. Este término no es nuevo, pero se debe ir incorporando poco a poco en las IC para que se adapten a las nuevas tecnologías con sus riesgos y amenazas.

- Tener una IC resiliente no es nada fácil. Implica gran inversión no solo de herramientas, hardware y software sino también en personal calificado para su implementación. Pero los beneficios de lograrlo, se verán al momento de poder dar una respuesta ante un ataque del cual nadie está exento.

- Por último no hay que olvidarse del eslabón más débil, que en toda esta maraña de redes interconectadas es el ser humano. Por lo que un desafío presente y futuro es y será la formación, concientización y educación constante de las personas que día a día están más interconectadas y vulnerables a los ataques cada vez más innovadores.

Referencias

- Ciberdefensa, Ciberseguridad, Introducción a las infraestructuras críticas, protección y resiliencia. https://ciberprisma.org/2024/07/16/introduccion-a-las-infraestructuras-criticas-proteccion-y-resiliencia/

- Ciberdiplomacia y Ciberdefensa La ciberresiliencia: entre la ciberseguridad y la resiliencia Real Instituto Elcano. https://www.realinstitutoelcano.org/analisis/la-ciberresiliencia-entre-la-ciberseguridad-y-la-resiliencia/

- Corletti Estrada, Alejandro. Manual de la Resiliencia. Una guía práctica de Ciber Resiliencia en Redes y Sistemas de TI Con los especiales aportes de General de División Evergisto de Vergara Universidad Alfonso X el sabio. Madrid 2020.

- Correa, Gabriel. Yusta, José M. Planes de Protección de Infraestructuras Críticas. Critical Infrastructure Protection Plans https://www.researchgate.net/profile/Jose-Yusta/publication/265346933_Critical_Infrastructure_Protection_Plans/links/540999a10cf2187a6a700856/Critical-Infrastructure-Protection-Plans.pdf

- La Ciberresiliencia: entre la ciberseguridad y la resiliencia Real Instituto Elcano. https://www.realinstitutoelcano.org/analisis/la-ciberresiliencia-entre-la-cibersegurida -y-la-resiliencia/.

- Decreto n° 11.200, de 15 de septiembre de 2022 **-** Plan Nacional de Seguridad de Infraestructuras Críticas. https://www.planalto.gov.br/ccivil_03/Ato2019-2022/2022/Decreto/D11200.htm

- Directiva de política presidencial: seguridad y resiliencia de infraestructuras críticas. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

- Directiva 2008/114/CE. Consejo de la Unión Europea. Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. 8 de diciembre de 2008. https://www.ccncert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf

- Ley 08/2011, Medidas para la Protección de Infraestructuras Críticas. https://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630

- Principios para la Infraestructura resiliente. Oficina de Naciones Unidas para la reducción de riesgos de desastre/marco de Sendai/ODS. https://www.undrr.org/media/86825/download?startDownload=20241021