Universidad Siglo 21

Trabajo final de grado. Manuscrito científico

Carrera: Licenciatura en Criminología y Seguridad.

"Ciberataques contra Infraestructuras Críticas: Desafíos, Amenazas y Estrategias de Protección en la Era Digital"

"Cyberattacks against Critical Infrastructures: Challenges, Threats, and Protection Strategies in the Digital Age"

Autor: Diego Alejandro Sarmiento

Legajo Nro: VCYS002649

Tutor: Francisco Gabriel Bolzan

Buenos Aires, Capital Federal, noviembre 2023

Índice

Resumen

En esta tesis, se profundiza en el tema crucial de la ciberseguridad en infraestructuras críticas en el contexto del mundo digital contemporáneo. El estudio detallado examina las complejidades de las amenazas cibernéticas que afectan a sectores vitales como energía, transporte, salud y finanzas. Se revela la creciente sofisticación de los ciberataques, subrayando la urgencia de estrategias preventivas y planes de recuperación meticulosos para garantizar la continuidad operativa.

Además de exponer las vulnerabilidades que enfrentan estas infraestructuras, se destaca la necesidad imperante de colaboración público-privada, educación pública y tecnologías innovadoras para contrarrestar las amenazas. Se abordan las tendencias emergentes en ciberseguridad, desde la inteligencia artificial hasta el aprendizaje automático, y se proponen medidas concretas para fortalecer nuestra postura ante los desafíos futuros.

Palabras Claves:

Ciberseguridad, Infraestructuras Críticas, Amenazas Cibernéticas, Prevención de Ciberataques, Recuperación de Incidentes, Resiliencia Digital, Colaboración Público-Privada, Tendencias en Ciberseguridad, Concientización Pública, Innovación Tecnológica, Inteligencia Artificial, Aprendizaje Automático.

Abstract

This thesis delves into the critical topic of cybersecurity in critical infrastructures within the context of the contemporary digital world. The in-depth study examines the complexities of cyber threats affecting vital sectors such as energy, transportation, healthcare, and finance. It reveals the growing sophistication of cyber-attacks,

emphasizing the urgency of preventive strategies and meticulous recovery plans to ensure operational continuity.

In addition to exposing the vulnerabilities faced by these infrastructures, the pressing need for public-private collaboration, public education, and innovative technologies to counter threats is underscored. Emerging trends in cybersecurity, from artificial intelligence to machine learning, are addressed, and specific measures are proposed to strengthen our stance against future challenges.

Keywords:

Cybersecurity, Critical Infrastructures, Cyber Threats, Cyberattack Prevention, Incident Recovery, Digital Resilience, Public-Private Collaboration, Cybersecurity Trends, Public Awareness, Technological Innovation, Artificial Intelligence, Machine Learning.

Introducción

En nuestra Argentina actual, dependemos enormemente de las infraestructuras críticas que hacen posible nuestra vida cotidiana. Desde tener electricidad confiable hasta acceder a servicios médicos y utilizar el transporte público, estas estructuras son fundamentales para nuestra sociedad. Sin embargo, nuestra creciente dependencia de la tecnología y la conectividad digital también ha traído consigo una preocupación cada vez mayor: la amenaza constante de ataques dirigidos contra estas infraestructuras vitales. Es un tema que nos afecta a todos y del que debemos estar conscientes para proteger lo que valoramos en nuestra vida diaria.

El problema central que nos ocupa radica en la creciente vulnerabilidad de las infraestructuras críticas en Argentina ante las amenazas en línea. A medida que estas infraestructuras se tornan cada vez más interconectadas y dependientes de la tecnología, se exponen a un conjunto en constante crecimiento de actores maliciosos que buscan explotar las vulnerabilidades inherentes en su seguridad. Además, la naturaleza en perpetua evolución de las tácticas y técnicas utilizadas por estos delincuentes digitales complica aún más la detección y prevención efectivas de estos ataques, planteando un desafío continuo para la seguridad de nuestras infraestructuras críticas.

La necesidad de investigar y abordar con urgencia los ataques dirigidos contra las infraestructuras en Argentina se justifica por una serie de razones que están interrelacionadas y que resaltan la magnitud de este problema:

Primero, la amenaza de los ataques no hace más que crecer de manera constante, tanto en su frecuencia como en su sofisticación. Los incidentes recientes a nivel global y en el ámbito nacional demuestran que las amenazas en línea están dispuestas a aprovechar cualquier oportunidad para poner en peligro la integridad de nuestras infraestructuras críticas.

Segundo, estos ataques no solo impactan la funcionalidad de las infraestructuras críticas en sí, sino que también tienen efectos secundarios que se extienden a la economía, la seguridad pública y la confianza en las instituciones gubernamentales. Su alcance es tan amplio que puede poner en riesgo la vida de las personas y debilitar la resiliencia de una nación en su conjunto.

Tercero, los ataques conllevan consecuencias económicas significativas. La pérdida de ingresos, los costos de recuperación y la necesidad de inversiones considerables en seguridad tienen un impacto duradero en las finanzas de organizaciones y gobiernos.

Cuarto, la constante evolución de las tácticas de ataque exige un enfoque constante en la mejora de la seguridad digital. La investigación en este campo se convierte en esencial para desarrollar soluciones innovadoras que protejan de manera efectiva las infraestructuras contra las amenazas digitales en constante cambio.

Por último, en el contexto de la soberanía nacional, la integridad de nuestras infraestructuras críticas son un pilar fundamental para la autonomía y la seguridad de Argentina. Los ataques pueden representar una amenaza directa a la soberanía, lo que acentúa la necesidad de abordar este problema con un enfoque serio y comprometido.

La creciente amenaza de ataques contra las infraestructuras y las consecuencias significativas que entrañan hacen que la investigación en este campo sea esencial. Esta investigación se realiza con el fin de ampliar nuestro conocimiento de las amenazas actuales, y se espera poder contribuir a desarrollar estrategias y soluciones efectivas para proteger nuestras infraestructuras en un entorno digitalmente interconectado y en constante evolución.

Este trabajo de investigación se sumerge en el campo de la ciberseguridad en infraestructuras críticas. Está diseñado para proporcionar una visión integral de los

aspectos clave relacionados con la protección de estas infraestructuras vitales. A lo largo de los siguientes capítulos, exploraremos desde los fundamentos teóricos hasta las estrategias de prevención y las lecciones aprendidas de casos reales. Nuestro objetivo es analizar la naturaleza de las amenazas en línea, las vulnerabilidades inherentes en estas infraestructuras y el impacto potencial de los ciberataques.

En el primer capítulo de esta tesis, se establece su objetivo principal que es investigar los ciberataques a infraestructuras críticas en Argentina y comprender su impacto. Los antecedentes indican un aumento alarmante de estos ataques en el país. Los objetivos de investigación se centran en analizar vulnerabilidades, evaluar estrategias de ciberseguridad, identificar tendencias y proponer soluciones.

Para lograr esto, se plantean preguntas de investigación sobre la naturaleza de las amenazas, las vulnerabilidades específicas, las tendencias emergentes y las estrategias de fortalecimiento. La metodología incluye revisión bibliográfica, recopilación de datos, análisis de vulnerabilidades, evaluación de impacto, revisión de ciberseguridad actual y propuestas de soluciones.

El capítulo 2 establece una base teórica sólida para comprender las infraestructuras críticas, los ciberataques y las tecnologías involucradas en estas infraestructuras, proporcionando un marco esencial para la investigación en curso sobre la seguridad cibernética en Argentina.

El capítulo 3 explora las amenazas actuales y emergentes que enfrentan las infraestructuras críticas, así como las vulnerabilidades comunes que pueden comprometer su seguridad. Las amenazas incluyen ransomware y extorsión digital, ataques destructivos y sabotaje, amenazas a la Internet de las Cosas (IoT), ataques de ingeniería social, amenazas a la nube y la virtualización, y ciberespionaje y guerra cibernética. Estas

amenazas son impulsadas por actores estatales, grupos terroristas y ciberdelincuentes, y representan riesgos significativos para la economía y la seguridad pública.

Además, se identifican vulnerabilidades comunes en las infraestructuras críticas, como la falta de actualizaciones y parches, deficiencias en la seguridad de la red, vulnerabilidades en software y hardware, falta de conciencia y educación en ciberseguridad, amenazas tanto externas como internas, y la dependencia de tecnología obsoleta. Abordar estas vulnerabilidades requiere una estrategia integral de ciberseguridad y una colaboración efectiva entre sectores público y privado.

En el cuarto capítulo, se evalúan en detalle los efectos y consecuencias de los ciberataques en infraestructuras críticas. Se analizan los costos económicos y sociales de estos ataques, destacando su impacto en la sociedad y la economía. Se estudian casos emblemáticos de ciberataques que han dejado huellas profundas en la sociedad, resaltando la importancia de comprender las implicaciones reales de estos eventos.

El quinto capítulo se enfoca en las estrategias de protección y prevención utilizadas para resguardar las infraestructuras críticas. Se revisan las mejores prácticas y los estándares de seguridad aplicables, así como la relevancia de la colaboración entre los diferentes sectores en la protección de estas infraestructuras esenciales. La ciberseguridad se convierte en un componente crucial para mitigar las amenazas identificadas previamente, y se destaca la importancia de una estrategia integral que abarque aspectos técnicos, de capacitación y colaboración entre distintos actores para garantizar la seguridad y continuidad de las infraestructuras críticas.

En los siguientes capítulos, profundizaremos en aspectos fundamentales relacionados con la recuperación, resiliencia y el futuro de la ciberseguridad en infraestructuras críticas. En el capítulo 6, evaluaremos las estrategias de recuperación y resiliencia en infraestructuras críticas a través de tres dimensiones clave: planificación de

la recuperación, estrategias de resiliencia y la integración de la seguridad cibernética en estos procesos. El capítulo 7 se centrará en la discusión de la ciberseguridad en un contexto futuro, explorando tendencias y desafíos emergentes en el ámbito de las infraestructuras críticas. Además, presentaremos propuestas concretas para fortalecer la ciberseguridad en este contexto. Finalmente, en el capítulo 8 proporcionaremos conclusiones generales basadas en nuestro análisis y destacaremos recomendaciones específicas para futuras investigaciones, con el propósito de seguir mejorando la seguridad de nuestras infraestructuras críticas.

Capítulo 1:

1.1 Propósito de la Tesis

El propósito de esta tesis es llevar a cabo una investigación sobre los ciberataques dirigidos contra las infraestructuras críticas en Argentina. Esta investigación tiene como objetivo primordial comprender las múltiples dimensiones de este problema y estudiar su impacto y sus implicaciones.

Se explorarán sus diversas dimensiones, desde las técnicas empleadas por los atacantes hasta las consecuencias económicas y sociales que acarrean. Además, se prestará especial atención al contexto local, analizando cómo estas amenazas afectan la infraestructura en un país con características y desafíos particulares como el nuestro.

La importancia de esta tesis no solo reside en profundizar el conocimiento sobre los ciberataques a infraestructuras críticas, sino también en su aplicabilidad práctica. Las conclusiones y recomendaciones resultantes tendrán un valor agregado para las autoridades encargadas de la seguridad y la protección de las infraestructuras críticas en nuestro país.

1.2 Antecedentes

En las últimas décadas, el aumento notorio de los ataques dirigidos a infraestructuras críticas ha reconfigurado el panorama global de las amenazas en la era digital. Este fenómeno, que no distingue fronteras, ha alcanzado también a Argentina, generando una creciente preocupación tanto a nivel gubernamental como en el ámbito privado y académico.

Según datos recopilados por la Comisión Económica para América Latina y el Caribe (CEPAL) en su informe "Ciberataques a la logística y la infraestructura crítica en

América Latina y el Caribe"[1], Argentina ha experimentado un preocupante aumento en estos incidentes durante el periodo 2020-2022. Este análisis revela que se han registrado al menos 19 ataques significativos en el país durante este periodo. Entre las instituciones afectadas se encuentran la Cámara del Senado de la Nación, el Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) y el Poder Judicial de la Provincia de Córdoba. Estos ataques han involucrado diversas variantes de ransomware[2], mostrando la diversidad y sofisticación de las amenazas que enfrenta Argentina.

Un ejemplo particularmente alarmante ocurrió en 2020, cuando la Dirección Nacional de Migraciones (DNM)[3] fue víctima de un ataque que resultó en la difusión de información sensible en la deep web por parte de los atacantes. Además, en agosto del presente año, el Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (PAMI)[4] sufrió un ataque de ransomware que alteró el sistema informático, impactando a más de 5 millones de afiliados y resaltando la vulnerabilidad incluso de las instituciones de servicios sociales vitales.

Estos incidentes han generado un llamado de atención urgente, no solo en el ámbito gubernamental, sino también en la comunidad académica y profesional.

Por lo anteriormente expuesto, se hace evidente la necesidad de abordar estas amenazas de manera integral y proactiva.

---

[1] Comisión Económica para América Latina y el Caribe (CEPAL). (2023). Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe (No. LC/TS.2023/93). Documentos de Proyectos. Santiago. Naciones Unidas. (S.23-00614) Recuperado de: https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

[2] Secretaría de Innovación Tecnológica del Sector Público. (2022). El ransomware, el software malicioso usado para atacar organizaciones. Recuperado de: https://www.argentina.gob.ar/sites/default/files/2022/08/el_ransomware_el_software_malicioso_usado_para_atacar_a_las_organizaciones.pdf

[3] Davidovsky, S. (2020, 10 de septiembre). Migraciones: cómo fue ataque del ransomware Netwalker. La Nación. Recuperado de: https://www.lanacion.com.ar/tecnologia/migraciones-como-fue-ataque-del-ransomware-netwalker-nid2446451/

Ministerio del Interior. (2020, 27 de agosto). Migraciones contuvo un intento de ciberataque. Argentina.gob.ar. Recuperado de: https://www.argentina.gob.ar/noticias/migraciones-contuvo-un-intento-de-ciberataque

[4] EL CRONISTA. (11 de 08 de 2023). Recuperado de: https://www.cronista.com/infotechnology/actualidad/alerta-pami-hackearon-los-sistemas-y-amenazan-con-publicar-todos-los-datos-de-los-afiliados/

1.3 Objetivos de Investigación

Los objetivos de investigación están diseñados para abordar de manera exhaustiva los desafíos planteados por los ciberataques a las infraestructuras críticas en Argentina. Estos objetivos se desarrollan en detalle a continuación:

Objetivo General

Comprender las múltiples dimensiones de los ciberataques dirigidos contra las infraestructuras críticas en Argentina y estudiar su impacto e implicaciones.

Objetivos específicos

- Analizar las vulnerabilidades de las infraestructuras críticas en Argentina ante las amenazas digitales.
- Examinar las estrategias y medidas de ciberseguridad que actualmente se implementan en Argentina para proteger las infraestructuras.
- Identificar y comprender las tendencias emergentes en ciberataques.
- Proponer estrategias y soluciones innovadoras que puedan implementarse con éxito para mejorar la seguridad cibernética de las infraestructuras críticas en Argentina.

Los objetivos establecidos están diseñados para crear una estrategia integral que permita enfrentar los desafíos de seguridad cibernética que afectan a las infraestructuras críticas en Argentina. A través de esta investigación, se aspira a contribuir significativamente a la protección de estos activos vitales.

1.4 Metodología

La presente investigación adoptará un enfoque metodológico cualitativo estructurado para abordar el estudio de los ciberataques dirigidos contra infraestructuras críticas en Argentina. El diseño de la metodología se fundamenta en la necesidad de

comprender a profundidad las dimensiones, el impacto y las posibles soluciones a esta problemática crítica.

Las etapas que se seguirán son las detalladas a continuación:

Revisión Bibliográfica y Documental: Se llevará a cabo una revisión de la literatura científica, informes gubernamentales y documentos técnicos relacionados con ciberseguridad y ciberataques en el contexto de infraestructuras críticas, tanto a nivel nacional como internacional.

Se buscarán y analizarán las mejores prácticas y marcos regulatorios utilizados en otros países con el propósito de evaluar su aplicabilidad en el contexto argentino.

Recopilación de Datos Empíricos: Se recopilarán datos relevantes sobre incidentes de ciberseguridad en infraestructuras críticas, incluyendo detalles técnicos y el impacto económico y social de dichos incidentes.

Evaluación de Vulnerabilidades: Se examinarán casos de estudio específicos para comprender cómo estos incidentes afectaron la sociedad argentina y las organizaciones involucradas.

Evaluación de la Ciberseguridad Actual: Se analizarán en detalle las políticas y regulaciones de ciberseguridad en Argentina relacionadas con la protección de infraestructuras críticas.

Se evaluarán las estrategias y medidas de ciberseguridad implementadas por organizaciones públicas y privadas, identificando buenas prácticas y áreas de mejora.

Propuesta de Soluciones Innovadoras: Basándose en la revisión bibliográfica, los datos empíricos recopilados y los resultados de las evaluaciones de vulnerabilidad e impacto, se propondrán soluciones para fortalecer la seguridad cibernética de las infraestructuras críticas en Argentina.

Documentación y Presentación de Resultados: Se documentarán de manera exhaustiva todos los hallazgos, análisis y recomendaciones en un informe de investigación académica.

Esta metodología proporciona un enfoque riguroso y sistemático para llevar a cabo la investigación en un contexto académico y profesional, garantizando la calidad y la relevancia de los resultados obtenidos.

Capítulo 2: Fundamentos Teóricos

En este capítulo, estableceremos una base sólida al definir lo que entendemos por infraestructuras críticas y ciberataques. También exploraremos la historia de los ciberataques contra estas infraestructuras y analizaremos la relevancia de los diferentes tipos de infraestructuras críticas en la sociedad actual. Además, examinaremos las tecnologías clave que desempeñan un papel esencial en su funcionamiento.

2.1 Definiciones de infraestructuras críticas y ciberataques.

Infraestructuras críticas

La resolución 1523/2019 ANEXO 1 de la Jefatura de Gabinete de ministros de la República Argentina, define el término infraestructura crítica como:

> "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.
>
> Las Infraestructuras Críticas de Información 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 (Jefatura de Gabinete de ministros, 2019, Anexo1, párr.1-2)."[5]

[5] Boletín Oficial. (2019). Resolución 1523/2019, Anexo 1, párrafos 1-2. Recuperado de: https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

Ciberataques[6]

Ciberataque es un término que se refiere a la acción maliciosa o el conjunto de actividades emprendidas por individuos o grupos, con la intención de comprometer la integridad, confidencialidad o disponibilidad de sistemas informáticos, redes, datos o servicios en línea. Estas acciones suelen llevarse a cabo mediante la explotación de vulnerabilidades de seguridad, el uso de técnicas avanzadas de hacking, o la implementación de malware y software malicioso. Los ciberataques pueden tener diversas motivaciones, que van desde el robo de información sensible, el sabotaje de infraestructuras críticas, la extorsión a través de ransomware, hasta el espionaje cibernético o la interrupción de operaciones comerciales y gubernamentales. La constante evolución de las amenazas cibernéticas hace que la detección, prevención y mitigación de los ciberataques sean desafíos continuos en el ámbito de la seguridad digital.

2.2 Ciberataques contra Infraestructuras Críticas a nivel mundial

Breve Historia

En las últimas décadas, los ciberataques a infraestructuras críticas han evolucionado de manera alarmante, transformando el paisaje de la seguridad cibernética a nivel global. Este fenómeno no solo ha sido una amenaza técnica, sino también una realidad humana y económica, afectando a individuos, comunidades y naciones enteras.

Los primeros indicios significativos de ciberataques a infraestructuras críticas se remontan a principios de la década de 2000. Estos incidentes, aunque limitados en comparación con los ataques modernos, sentaron las bases para futuras amenazas. Con el

[6] Microsoft. (2023). ¿Qué es un ciberataque? Recuperado de https://www.microsoft.com/es-ar/security/business/security-101/what-is-a-cyberattack

Utsupra. (Fecha desconocida). Doctrina | Origen: Argentina. Citar como: Protocolo A00399486169 de Utsupra. Recuperado de http://server1.utsupra.com/doctrina1?ID=articulos_utsupra_02A00399486169

tiempo, la sofisticación de los ataques aumentó, alimentada por un submundo digital en constante crecimiento, donde hackers individuales, grupos criminales y actores respaldados por estados buscaban explotar vulnerabilidades en sistemas vitales.

En la última década, ataques notorios han sacudido a naciones de todo el mundo. Desde el gusano Stuxnet[7] en 2010, que apuntó a instalaciones nucleares en Irán, hasta el devastador ataque de ransomware WannaCry[8] en 2017, que afectó a organizaciones de salud y empresas en más de 150 países, los ciberataques han dejado su huella en la infraestructura crítica global.

Argentina, al igual que otras naciones, no ha escapado de esta tendencia. Desde intrusiones en redes eléctricas hasta ataques a sistemas de salud y transporte, el país ha enfrentado diversos desafíos de seguridad cibernética.[9] La interconexión digital de las infraestructuras críticas a amplificado las vulnerabilidades, haciendo que la protección de estos sistemas sea más crucial que nunca.

2.3 Momentos significativos a nivel global: Stuxnet, BlackEnergy 3 y Triton

Se pueden identificar tres momentos significativos que ejemplifican el peligro potencial en ciberataques dirigidos a infraestructuras críticas: [10]

---

[7] Mueller, P., & Yadegari, B. (2012). Stuxnet Worm. Universidad de Arizona. Recuperado de https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf

[8] Kaspersky. (2023). ¿Qué es el ransomware WannaCry? Recuperado de https://www.kaspersky.es/resource-center/threats/ransomware-wannacry

[9] Infobae. (2019, 17 de junio). Las redes eléctricas inteligentes a prueba por los hackeos. Recuperado de https://www.infobae.com/america/mundo/2019/06/17/las-redes-electricas-inteligentes-a-prueba-por-los-hackeos/

Stillman, A., & do Rosario, J. (2019, 17 de junio). El apagón masivo de Argentina se produjo por un "ataque cibernético"? El Perfil. Recuperado de https://www.perfil.com/noticias/bloomberg/bc-argentina-no-descarta-ataque-cibernetico-en-apagon.phtml

Harán, J. M. (2022, 6 de mayo). Ataque al sistema de tarjetas SUBE afecta la recarga. WeLiveSecurity by ESET. Recuperado de https://www.welivesecurity.com/la-es/2022/05/06/ataque-sistema-tarjetas-sube-afecta-recarga/

Infobae. (2022, 23 de octubre). Hackearon el sistema informático del Ministerio de Salud de la Nación. Recuperado de https://www.infobae.com/salud/ciencia/2022/10/23/hackearon-el-sistema-informatico-del-ministerio-de-salud-de-la-nacion/

[10] UNE. (2019). Ciberataques dirigidos a infraestructuras críticas. En Michael A. Mullane (Ed.), UNE, Nº 15, junio de 2019. Recuperado de https://revista.une.org/15/ciberataques-dirigidos-a-infraestructuras-criticas.html

Irán 2010 - Stuxnet y la Planta Nuclear de Natanz: En este incidente, se hizo público el software malicioso denominado Stuxnet, el cual tuvo un impacto significativo al detener la operación de la planta nuclear de Natanz. Stuxnet fue diseñado con el propósito de afectar los motores utilizados en centrifugadoras para el enriquecimiento de uranio, resultando en la pérdida de control de estas. Como resultado, se logró desactivar temporalmente cerca de 1.000 centrifugadoras.

Ucrania 2015 - Apagones Eléctricos y BlackEnergy 3: En este caso, los atacantes emplearon el malware BlackEnergy 3 para desencadenar apagones en tres subestaciones de la red eléctrica en Ucrania. Estos ciberdelincuentes lograron infiltrarse en tres empresas de energía y desconectar temporalmente la generación de electricidad en tres regiones del país, dejando a casi un cuarto de millón de personas sin electricidad durante hasta seis horas en pleno invierno. Se presume que este programa malicioso se distribuyó a través de correos electrónicos de phishing personalizados, ocultos en archivos adjuntos falsos de Microsoft Office.

Arabia Saudita 2017 - Ataque con Tritón y la Amenaza al Sistema de Seguridad Instrumentado (SIS): En este incidente, ciber terroristas lograron tomar el control remoto de una estación de trabajo ampliamente reconocida. Utilizaron una variante de malware llamada Tritón para asumir el control del Sistema de Seguridad Instrumentado (SIS), diseñado para prevenir accidentes industriales catastróficos. Los investigadores creen que este acto fue un intento de sabotaje destinado a provocar una explosión al desactivar los sistemas de seguridad. Este tipo de ataques, que se centran en sistemas de control industrial, también conocidos como tecnología operativa (TO), difieren de los ataques anteriores, que se enfocaban en la destrucción de datos o la interrupción de plantas de energía. Se ha señalado que un error de codificación evitó

consecuencias más graves. Las evidencias sugieren que este ataque también se basó en técnicas de phishing o phishing personalizado.

Estos eventos ilustran claramente la creciente amenaza que representan los ciberataques a las infraestructuras críticas, destacando la necesidad imperante de fortalecer la seguridad y la prevención en este ámbito.

2.4 Tipos de infraestructuras críticas y su relevancia.[11]

Los tipos de infraestructuras críticas y su relevancia en la sociedad contemporánea constituyen un tema de gran importancia desde diversas perspectivas. Estas infraestructuras, esenciales para el funcionamiento continuo y seguro de una nación, pueden clasificarse en varios grupos fundamentales, cada uno con su propia relevancia y rol dentro de la estructura socioeconómica y de seguridad.

Energía: Las infraestructuras energéticas, que engloban la generación, transmisión y distribución de electricidad, son vitales para mantener el bienestar y la operación de todos los sectores económicos y la vida cotidiana. Su relevancia radica en garantizar la disponibilidad de energía eléctrica constante para hogares, empresas, hospitales, sistemas de transporte y más.

Transporte: Las infraestructuras de transporte, que incluyen carreteras, ferrocarriles, puertos y aeropuertos, son cruciales para la conectividad nacional e internacional. Facilitan el comercio, el movimiento de personas, el abastecimiento de bienes y servicios, y tienen un impacto directo en la economía.

Agua y Saneamiento: Las infraestructuras hídricas son esenciales para garantizar el acceso a agua potable y el tratamiento adecuado de aguas residuales. Esto no solo afecta

[11] Boletín Oficial de la República Argentina. (2019, 18 de septiembre). Resolución 1523/2019, Anexo 1, párrafos 1-2. Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

la salud pública, sino que también respalda la producción agrícola, industrial y otros sectores clave.

Salud: Las infraestructuras de atención médica, como hospitales y clínicas, son de importancia crítica, especialmente en situaciones de emergencia y pandemias. Garantizan la capacidad de respuesta y el cuidado de la salud de la población.

Comunicaciones: Las redes de telecomunicaciones y tecnologías de la información son esenciales para la conectividad, la transmisión de datos y la comunicación global. Desempeñan un papel fundamental en la economía digital actual y en la gestión de emergencias.

Finanzas: Las infraestructuras financieras, como bancos y sistemas de pago, respaldan la economía al facilitar transacciones comerciales y financieras. La estabilidad en este sector es fundamental para evitar crisis económicas.

Alimentación: La cadena de suministro de alimentos depende de infraestructuras críticas, desde la producción agrícola hasta la distribución y el abastecimiento en supermercados y restaurantes. Garantizar la disponibilidad de alimentos es esencial para la seguridad alimentaria.

Químico y Nuclear: Las instalaciones químicas y nucleares son cruciales para la producción de energía, productos químicos y materiales estratégicos. Su relevancia radica en la seguridad y en evitar posibles amenazas nucleares o químicas.

Espacio: Las infraestructuras espaciales, como satélites y estaciones terrestres, son esenciales para la navegación, las comunicaciones, la observación terrestre y la exploración espacial.

Estado: Las infraestructuras gubernamentales y administrativas son vitales para la gobernabilidad, la seguridad nacional y la prestación de servicios públicos esenciales.

2.5 Descripción de las tecnologías involucradas en estas infraestructuras.[12]

La descripción de las tecnologías involucradas en las infraestructuras críticas es un componente esencial para comprender cómo estas operan y mantienen su funcionalidad en un mundo cada vez más interconectado y digitalizado. A continuación, exploraremos algunas de las principales tecnologías que desempeñan un papel fundamental en estas infraestructuras.

Tecnologías de Automatización y Control: En el corazón de muchas infraestructuras críticas se encuentran sistemas de automatización y control. Esto incluye el uso de Controladores Lógicos Programables (PLC), que permiten la supervisión y el control de procesos en tiempo real. Estas tecnologías son vitales para garantizar la eficiencia y la seguridad en sectores como la energía, el agua y la industria química.

Redes de Comunicación: Las redes de comunicación, tanto públicas como privadas, son esenciales para la transmisión de datos y la comunicación en tiempo real. Esto involucra tecnologías como las redes de fibra óptica, 5G y protocolos de comunicación seguros, que aseguran la conectividad y la transmisión segura de datos críticos.

Ciberseguridad: En un mundo cada vez más digital, la ciberseguridad desempeña un papel crucial en la protección de las infraestructuras críticas. Se utilizan tecnologías avanzadas de seguridad de la información, como cortafuegos (firewalls), sistemas de detección de intrusiones y autenticación de múltiples factores, para prevenir y responder a ciberataques.

---

[12] Kamlofsky, J., Abdel Masih, S., Colombo, H., Milio, C., & Hecht, P. (Sin fecha). Ciberseguridad en los Sistemas de Control Industrial: Clave para la Ciberdefensa de las Infraestructuras Críticas. Universidad Abierta Interamericana. Recuperado de http://sedici.unlp.edu.ar/bitstream/handle/10915/77258/Documento_completo.%20Clave%20para%20la%20Ciberdefensa%20de%20las%20Infraestructuras%20Cr%C3%ADticas.pdf-PDFA.pdf?sequence=1&isAllowed=y

Sistemas de Supervisión y Control (SCADA): Los sistemas SCADA son herramientas vitales en la monitorización y gestión de infraestructuras críticas. Estos sistemas permiten la visualización de datos en tiempo real y la toma de decisiones basada en información precisa. Utilizan interfaces humanas, software de control y sensores para supervisar y controlar procesos críticos.

Tecnologías de Energía Sostenible: En la búsqueda de una infraestructura más sostenible, las tecnologías relacionadas con la energía renovable, como paneles solares y turbinas eólicas, están desempeñando un papel creciente en la generación de energía limpia y en la reducción de la dependencia de fuentes de energía no renovables.

Inteligencia Artificial (IA): La IA se está incorporando cada vez más en la gestión de infraestructuras críticas. Los algoritmos de aprendizaje automático pueden predecir fallos en equipos, optimizar la distribución de recursos y ayudar en la toma de decisiones críticas para el funcionamiento seguro y eficiente.

Tecnologías de Control de Acceso: Para garantizar la seguridad física de las instalaciones, se utilizan tecnologías de control de acceso, como sistemas de reconocimiento facial, tarjetas de identificación electrónica y sistemas biométricos, para regular y supervisar quién tiene acceso a áreas sensibles.

Tecnología Satelital: La tecnología satelital desempeña un papel fundamental en la navegación, la comunicación y la recopilación de datos para una variedad de aplicaciones, incluyendo la gestión de flotas de transporte y la observación de la Tierra desde el espacio.

Estas tecnologías desempeñan un papel crítico en el funcionamiento y la seguridad de las infraestructuras críticas modernas.

Capítulo 3: Amenazas y Vulnerabilidades:

En este capítulo, nos adentraremos en las amenazas actuales y emergentes que enfrentan las infraestructuras críticas, identificando las vulnerabilidades comunes. Mediante el estudio de casos de ciberataques históricos, aprenderemos de la experiencia pasada para estar mejor preparados en el futuro.

La defensa contra estas amenazas requiere una combinación de tecnologías avanzadas, educación continua, colaboración internacional y políticas gubernamentales sólidas. La comunidad académica, en estrecha colaboración con las entidades gubernamentales y el sector privado, desempeña un papel crucial en la investigación y el desarrollo de soluciones innovadoras para proteger nuestras infraestructuras críticas de las amenazas cibernéticas en constante evolución.

3.1 Exploración de las amenazas actuales y emergentes contra infraestructuras críticas.

En el panorama actual de la seguridad cibernética, las amenazas contra las infraestructuras críticas se han vuelto más sofisticadas y diversificadas, representando un desafío constante para la seguridad global. Estas amenazas, impulsadas por actores estatales, ciberdelincuentes y grupos terroristas, han evolucionado para explotar las vulnerabilidades en sectores vitales como energía, salud, transporte y comunicaciones. Este escenario plantea riesgos significativos para la economía, la seguridad pública y la estabilidad política de las naciones.

Ransomware y Extorsión Digital[13]:

Los ataques de ransomware han proliferado, con grupos criminales que cifran datos y exigen rescates para su liberación. Las organizaciones de infraestructuras críticas son objetivos principales, afectando la prestación de servicios esenciales y generando consecuencias financieras graves.

Ataques Destructivos y Sabotaje:

Actores estatales y grupos terroristas han demostrado interés en ataques destructivos, como Stuxnet[14], que pueden dañar físicamente sistemas industriales. Estos ataques pueden desencadenar apagones, contaminaciones de agua o incluso accidentes en centrales nucleares.

Amenazas a la Internet de las Cosas (IoT):[15]

La creciente adopción de dispositivos IoT ha ampliado las superficies de ataque. Atacantes pueden comprometer dispositivos conectados para infiltrarse en redes de infraestructuras críticas y realizar acciones maliciosas.

Ataques de Ingeniería Social:[16]

Los ataques de ingeniería social siguen siendo una amenaza grave. Phishing, pretexting[17] y otras tácticas engañosas son utilizadas para obtener acceso no autorizado a sistemas y datos sensibles.

---

[13] Dirección Nacional de Ciberseguridad. (2022). El ransomware, el software malicioso usado para atacar a las organizaciones. Recuperado de https://www.argentina.gob.ar/sites/default/files/2022/08/el_ransomware_el_software_malicioso_usado_para_atacar_a_las_organizaciones.pdf

[14] Lipovsky, R. (2017, 20 de junio). Sistemas industriales en la mira. WeLiveSecurity by ESET. Recuperado de https://www.welivesecurity.com/la-es/2017/06/20/sistemas-industriales-en-la-mira/

[15] Téllez Tejada, N. (2023, 18 de enero). IoT y la infraestructura crítica, en el foco de la preocupación de la ciberseguridad industrial y de gobierno. TeleSemana. Recuperado de https://www.telesemana.com/blog/2023/01/18/iot-y-la-infraestructura-critica-en-el-foco-de-la-preocupacion-de-la-ciberseguridad-industrial-y-de-gobierno/

[16] Gómez, J. A. (Sin fecha). Ingeniería social: 6 consejos para proteger a tu empresa de su impacto. Delta Protect. Recuperado de https://www.deltaprotect.com/blog/ingenieria-social

[17] Common Attack Pattern Enumeration and Classification. (s.f.). CAPEC-407: Pretexting attack. Recuperado de https://capec.mitre.org/data/definitions/407.html

Amenazas a la Nube y la Virtualización:

Las infraestructuras críticas están migrando a entornos en la nube y sistemas virtualizados. Esto crea nuevas vulnerabilidades, incluyendo la posibilidad de ataques a nivel de hipervisores y manipulación de datos en la nube.

Ciberespionaje y Guerra Cibernética:[18]

Naciones y actores estatales se involucran en actividades de ciberespionaje para recopilar información sobre infraestructuras críticas y pueden desencadenar operaciones de guerra cibernética en conflictos internacionales.

3.2 Identificación de las vulnerabilidades comunes en estas infraestructuras.[19]

Dentro del complejo entorno de las infraestructuras críticas, es fundamental reconocer la existencia de vulnerabilidades que representan potenciales puntos de acceso para ciberataques. Estas vulnerabilidades pueden originarse a partir de diversas fuentes y tienen la capacidad de poner en peligro sistemas vitales en sectores tan fundamentales como la energía, el transporte, la salud y las comunicaciones.

Para abordar estas vulnerabilidades, es esencial una estrategia integral de ciberseguridad que incluya medidas técnicas, formación del personal y una cultura organizacional de seguridad.

---

[18] Mendoza, M. Á. (2022, 21 de diciembre). Ciberataques a infraestructuras críticas: tendencias en ciberseguridad. WeLiveSecurity by ESET. Recuperado de https://www.welivesecurity.com/la-es/2022/12/21/ciberataques-infraestructuras-criticas-tendencias-ciberseguridad/

Lisa Institute. (Fecha desconocida). Ciberguerra: tipos, armas, objetivos y ejemplos de la guerra tecnológica. Recuperado de https://www.lisainstitute.com/blogs/blog/ciberguerra-tipos-armas-objetivos-ejemplos

[19] Aguirre Ponce, A. A. (2017). Ciberseguridad en Infraestructuras Críticas de Información (Tesis de maestría). Universidad de Buenos Aires, Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería. Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1115_AguirrePonceAA.pdf

Kippeo. (Fecha desconocida). Ciberseguridad en la automatización industrial. Recuperado de https://kippeo.com/ciberseguridad-en-la-automatizacion-industrial/

ODS Open Data Security. (2020, 27 de agosto). Ciberseguridad en las infraestructuras críticas. Ciberseguridad para empresas, Noticias sobre ciberseguridad. Recuperado de https://opendatasecurity.io/ciberseguridad-en-las-infraestructuras-criticas/

Entre las vulnerabilidades más recurrentes y dignas de destacar, encontramos las siguientes:

Falta de Actualizaciones y Parches:

Las infraestructuras críticas a menudo utilizan sistemas heredados que no reciben actualizaciones regulares. Esto puede dejarlos expuestos a vulnerabilidades conocidas que podrían haberse solucionado con parches de seguridad.

Deficiencias en la Seguridad de la Red:

La falta de segmentación de red adecuada y el uso de contraseñas débiles pueden facilitar la entrada de intrusos en sistemas críticos, permitiendo el acceso no autorizado.

Vulnerabilidades en Software y Hardware:

Las debilidades en el diseño y la codificación del software, así como en el hardware utilizado en infraestructuras críticas, pueden ser explotadas por ciberatacantes para interrumpir operaciones y manipular sistemas.

Falta de Conciencia y Educación en Ciberseguridad:

La falta de conciencia sobre las amenazas cibernéticas y las mejores prácticas de seguridad puede llevar a errores humanos que permiten a los atacantes acceder a sistemas críticos.

Amenazas Externas e Internas:

Tanto las amenazas externas (ciberdelincuentes, grupos terroristas) como las internas (empleados descontentos, contratistas) pueden aprovechar las vulnerabilidades para realizar ataques.

Dependencia de Tecnología Obsoleta:

La dependencia continua de tecnologías obsoletas y sistemas no compatibles con estándares modernos puede dejar a las infraestructuras críticas expuestas a amenazas, ya que estos sistemas a menudo carecen de medidas de seguridad robustas.

Insuficiente Planificación para la Continuidad del Negocio:

La falta de planes de continuidad del negocio y de recuperación ante desastres puede aumentar el impacto de los ciberataques, prolongando el tiempo necesario para restaurar las operaciones normales.

3.3 Estudio de casos de ciberataques históricos contra infraestructuras críticas.

La comprensión de las amenazas y vulnerabilidades que enfrentan las infraestructuras críticas se ve reforzada por el análisis de casos históricos de ciberataques que han afectado a sistemas vitales en todo el mundo. Estos ejemplos ilustran la diversidad de amenazas y los impactos significativos que pueden tener en la sociedad y la economía. A continuación, se presentan algunos casos destacados:

3.3.1 Ataque a la Planta de Tratamiento de Aguas de Maroochy (2000) - Australia[20]

En 2000, un ingeniero descontento con la gestión local llevó a cabo un ciberataque contra la planta de tratamiento de aguas de Maroochy en Australia. El ataque consistió en manipular el sistema de control de las bombas de la planta, lo que resultó en el vertido de millones de litros de aguas sin tratar en ríos y parques cercanos. Este incidente ilustra cómo incluso un individuo con conocimientos técnicos limitados puede afectar gravemente las infraestructuras críticas.

[20] Hemsley, K. E., & Fisher, R. E. (2018, diciembre). History of Industrial Control System Cyber Incidents (p. 4). Recuperado de https://www.osti.gov/servlets/purl/1505628

3.3.2 Ataque al Sistema de Control Industrial en Ucrania (2016) - Industria Energética[21]

En diciembre de 2016, Ucrania fue nuevamente víctima de un ciberataque que afectó a su infraestructura energética. Los atacantes utilizaron malware para interrumpir los sistemas de control industrial en una central eléctrica, lo que provocó un apagón en la región de Ivano-Frankivsk. Este ataque subrayó la vulnerabilidad continua de las infraestructuras eléctricas a nivel mundial y la amenaza que representan los ciberataques dirigidos a sistemas de control industrial.

3.3.3 Ataque al Sistema de Salud del Reino Unido (2017) - NHS[22]

En mayo de 2017, el Servicio Nacional de Salud (NHS) del Reino Unido fue objeto de un ataque de ransomware conocido como WannaCry. El malware cifró los datos en los sistemas del NHS, lo que resultó en la cancelación de citas médicas, la interrupción de servicios de atención médica y la pérdida de datos médicos de pacientes. Este incidente destaca cómo los ciberataques pueden afectar gravemente los servicios de atención médica, que son parte integral de las infraestructuras críticas.

3.3.4 Ataque a la Central Nuclear de Gundremmingen (2016) - Alemania[23]

En 2016, se detectó un virus informático en una central nuclear en Gundremmingen, Alemania. Aunque el virus no afectó las operaciones nucleares, ilustró

---

[21] Hemsley, K. E., & Fisher, R. E. (2018, diciembre). History of Industrial Control System Cyber Incidents (p. 16). Recuperado de https://www.osti.gov/servlets/purl/1505628

[22] Diario El Mundo. (2017, mayo 12). Los hospitales de Reino Unido, en alerta por un ciberataque. El Mundo. Recuperado de https://www.elmundo.es/tecnologia/2017/05/12/5915cb15e5fdea24788b4658.html

House of Commons Committee of Public Accounts. (2018, abril). Cyber-attack on the NHS. Recuperado de https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/787/787.pdf

[23] CCN-CERT. (2016, abril 28). Encontrados dos virus informáticos en la mayor central nuclear de Alemania. Recuperado de https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/3752-encontrados-dos-virus-informaticos-en-la-mayor-central-nuclear-de-alemania.html

la capacidad de los ciberataques para infiltrarse en instalaciones críticas y suscitar preocupaciones sobre la seguridad nuclear.

3.3.5 Ataque al Sistema de Transporte Público de San Francisco (2016) - Estados Unidos[24]

En noviembre de 2016, el sistema de transporte público de San Francisco fue blanco de un ataque de ransomware que bloqueó los sistemas de pago y acceso de los pasajeros. Este incidente resaltó cómo los ciberataques pueden afectar la movilidad urbana y la infraestructura de transporte en las ciudades.

Estos ejemplos que ilustran la diversidad de amenazas y vulnerabilidades que pueden afectar a las infraestructuras críticas en diferentes partes del mundo y en diversos sectores. Cada caso presenta desafíos únicos y enfatiza la importancia de la ciberseguridad en la protección de estas infraestructuras.

[24] Cointelegraph. (2016, noviembre). Ransomware en sistema de transporte en San Francisco: nueva alerta de una creciente amenaza. Recuperado de https://es.cointelegraph.com/news/ransomware-en-sistema-de-transporte-de-san-francisco-nueva-alerta-de-una-creciente-amenaza

Capítulo 4: Impacto de los Ciberataques en Infraestructuras Críticas

En este capítulo, profundizaremos en la evaluación de los efectos y consecuencias de los ciberataques en las infraestructuras críticas, abordando los costos económicos y sociales que estos incidentes conllevan.

4.1 Análisis de los efectos y consecuencias de los ciberataques en infraestructuras críticas.

El análisis del impacto de los ciberataques en infraestructuras críticas nos sumerge en una realidad de gran complejidad y matices. Estos ataques, que pueden manifestarse de diversas formas y escalas, despliegan un alcance que trasciende la simple interrupción de servicios esenciales, repercutiendo en esferas fundamentales de nuestra sociedad. En este contexto, resulta crucial examinar este tema con un enfoque riguroso y profesional.

Uno de los aspectos más notorios es la capacidad de los ciberataques para perturbar servicios esenciales que son vitales para el bienestar y la calidad de vida de los ciudadanos. La interrupción de servicios como la generación de energía eléctrica, la atención médica y el transporte no solo causa inconvenientes inmediatos, sino que también tiene un impacto duradero en la vida cotidiana de las personas.

A su vez, las organizaciones y empresas que son blanco de estos ataques enfrentan consecuencias significativas que van más allá de lo puramente técnico. Los daños en la reputación empresarial son notorios, erosionando la confianza de los clientes y del público en general. Esta pérdida de confianza puede tener ramificaciones a largo plazo en la salud financiera y la continuidad operativa de las entidades afectadas.

Los ciberataques no deben ser considerados únicamente como amenazas aisladas; en muchos casos, pueden convertirse en una preocupante cuestión de seguridad nacional. Cuando actores estatales hostiles emplean tácticas de ciberataque como parte de una

estrategia de guerra cibernética, la amenaza adquiere dimensiones críticas. La seguridad de un país puede verse comprometida, poniendo en riesgo la integridad de sus sistemas y recursos más allá de las fronteras digitales.

En términos económicos, los ciberataques conllevan costos significativos. Estos costos abarcan desde los gastos directamente relacionados con la recuperación de los sistemas afectados, pasando por la pérdida de ingresos debido a la interrupción de operaciones comerciales, hasta las inversiones necesarias para reforzar las medidas de ciberseguridad y prevenir futuros ataques. El impacto económico puede ser devastador, afectando tanto a las empresas como a la economía nacional en su conjunto.

Para proporcionar una visión más concreta de este panorama, a continuación, se presenta un relevamiento de incidentes ocurridos en nuestro país durante el período comprendido entre 2020 y 2022, informado por la Comisión Económica para América Latina y el Caribe (CEPAL)[25]. Este registro ofrece un vistazo a la magnitud del impacto que los ciberataques pueden tener en diferentes infraestructuras y cómo estas amenazas han evolucionado en los últimos años. Este análisis nos brinda una valiosa perspectiva para comprender la importancia crítica de la ciberseguridad en la era digital actual.

[25] [25] CEPAL (Comisión Económica para América Latina y el Caribe). (2023). Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe. En R. M. Díaz y G. Núñez (Autores), Publicación de las Naciones Unidas LC/TS.2023/93. Copyright © Naciones Unidas, 2023. Todos los derechos reservados. Impreso en Naciones Unidas, Santiago. Número de documento: S.23-00614. https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

Imagen 1 – Fuente: CEPAL [26]

Tipo de actividad	Argentina	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días impacto	Impacto Costo en dólares	Resolución
	X	La Serenísima, como empresa reconocida, fue invocada como medio para realizar la estafa	Producción láctea y productos derivados		X	X	Suplantación de identidad-phishing-ingeniería social	1/4/2021	Mediante un link por WhatsApp y redes sociales donde se suplanta la identidad de la empresa láctea La Serenísima. El mensaje se presenta como "¡Celebración del 90 aniversario de La Serenísima!, prometiendo regalos con motivo de la celebración mencionada, solicitando a la vez datos personales del afectado	No identificado	No identificado			La empresa publicó comunicado en redes sociales advirtiendo sobre el engaño
Industria	X	Fábrica Argentina de Aviones-FADEA	La Fábrica Argentina de Aviones «Brigadier San Martín» S. A. es una empresa dedicada a la producción de aeronaves y la investigación aeroespacial, cuya planta está ubicada en la provincia de Córdoba		X	X	Malware/ 1estafa/ phishing/ suplantación de identidad	6/4/202	Transferencias internacionales que suman casi medio millón de dólares realizadas desde la FADEA a "personas aún no identificadas" que "simularon pertenecer" a *Advent Aircrfot Systems* (proveedor dedicado al diseño, fabricación y certificación de productos y componentes de aviones)	Autores desconocidos se hicieron pasar por ambas partes y concretaron la estafa	No aplica	300	500 000	No aplica
Estado	X	Instituto de Obra Social de las Fuerzas Armadas	El Instituto de Obra Social de las Fuerzas Armadas es una obra social que presta servicio a las Fuerzas Armadas, la Gendarmería Nacional Argentina y la Prefectura Naval Argentina	X	X		Robo y 1publicación de datos internos del organismo	29/9/202	Robo y publicación de datos internos del organismo correspondiente a 1.200.000 afiliados aproximadamente	Hay nombres completos, estado civil, sexo, dirección postal, números de teléfono, correo electrónico y rango de las personas afectadas	El instituto declara que la base de datos afectadas es obsoleta, por lo que los datos son desactualizados			El organismo no tomo ninguna medida, argumentando que se trata de información desactualizada
Estado	X	Registro Nacional de las Personas	Registro de la identidad de los ciudadanos de la República Argentina, conteniendo: las direcciones, teléfonos, fotos y número de trámite de DNI, entre otras cosas. Esta información es consultada por organismos públicos y la sociedad privada	X	X		Robo de datos internos del organismo	24/10/2021	Filtración de datos de una cantidad no confirmada depersonas registradas	En redes sociales, se publicó el robo de aproximadamente 60.000 registros personales y a modo de prueba confirmatoriade la filtración realizada, fue difundidainformación sensible deperiodistas, políticos, deportistas y artistas reconocidos, entre muchos otros	Considerando los resultados provisorios del Censo 2022 realizado en Argentina, la cantidad de registros sustraídos representa el 0,12% del total de las bases de datos de RENAPER		17 000	El organismo procedió a restringir, en distintos niveles de alcance, el acceso a las bases de datos

Fuente: Imagen 2 – Fuente: CEPAL [27]

Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días impacto	Impacto Costo en dólares	Resolución
Prominente S.A.	Compañía de soluciones tecnológicas, especializada en automatización de procesos de negocios, desarrollo de software, *big data* y servicios *cloud*	X	X		Ransomware	4/5/2022	Afectó el sistema de emisión de boletos electrónicos para viajes urbanos, corta y mediana distancia en la ciudad de Buenos Aires y aledaños	El hackeo contra los servidores de la empresa Prominente, que provee los servicios de alojamiento para Emova (subterráneos) y Metrovías (ferrocarril Urquiza)	No informado	3		Dada la reserva tomada por la empresa, se supone se procedió a recuperar la información secuestrada desde copias de respaldo
Aceitera General Deheza	Complejo agroindustrial dedicado a la producción de proteínas y aceites vegetales, biodiésel y glicerina refinada	X	X		Ransomware	10/8/2022	Fue detectada una intromisión en los sistemas informáticos. Es por este motivo que se activaron protocolos de seguridad, a fin de realizar un análisis exhaustivo de la situación y se efectuaron las denuncias correspondientes	La empresa declara haber continuado sus operaciones en forma manual	No se reveló el monto que solicitaron los delincuentes para devolver el acceso a los archivos se presume que la cifra fue grande. No obstante, la empresa declaró que no accederá al pago de rescate			La empresa procedió a recuperar la información secuestrada desde copias de respaldo
Poder Judicial de la Provincia de Córdoba	Administración de justicia a nivel provincial	X	X		Ransomware-PlayCrypt	13/8/2022	Cambia la extensión de todos los archivos afectados a "play"	Afectó la totalidad de los trámites judiciales como las constancias, libramientos de oficios y órdenes de pago peritos, abogados, cuota beneficiarios de alimentaria, entre otros)	Alcanzó a unos 8 mil usuarios del sistema interno y a los cerca de 25 mil abogados matriculados en la provincia			Se tomaron medidas de tipo administrativa: postergación de fechas de vencimiento y se pasó toda la gestión a documentación impresa

[26] CEPAL (Comisión Económica para América Latina y el Caribe). (2023). Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe (p. 40). En R. M. Díaz y G. Núñez (Autores), Publicación de las Naciones Unidas LC/TS.2023/93. Copyright © Naciones Unidas, 2023. Todos los derechos reservados. Impreso en Naciones Unidas, Santiago. Número de documento: S.23-00614. https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

[27] CEPAL (Comisión Económica para América Latina y el Caribe). (2023). Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe (p. 42). En R. M. Díaz y G. Núñez (Autores), Publicación de las Naciones Unidas LC/TS.2023/93. Copyright © Naciones Unidas, 2023. Todos los derechos reservados. Impreso en Naciones Unidas, Santiago. Número de documento: S.23-00614. https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

Fuente: Imagen 3 – Fuente: CEPAL [28]

Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Días impacto	Costo en dólares	Resolución
Cámara Senado de la Nación	Cuerpo legislativo que representa a las jurisdicciones provinciales de la Nación	X	X		Ransomware	12/1/2022	Secuescitro paral de información pública y de tipo sensible	No informado	No informado	2		Recuperación de la información desde copias de respaldo
Mercado Libre	Comercio electrónico		X		Robo de datos internos de la empresa	8/3/2022	Acceso no autorizado al repositorio de su código fuente	La empresa reconoció haber sido objeto de acceso no autorizado a información de sus usuarios, sin encontrar evidencia de acceso a otros datos sensibles de la misma	Filtración de datos de 300.000 de usuarios de la empresa (casi 140 millones de usuarios activos únicos)			La empresa declaró haber puesto en marcha los protocolos indicados para la situación
Transportadora de Gas del Sur	Transportadora de gas natural. Red 9231 km. Distribuye en siete provincias, siendo la operadora de la red más extensa de América Latina	X	X		Ransomware	1/4/2022	El incidente se detectó contra su sistema SPAC, plataforma de procesamiento de solicitudes, asignación y programación de los volúmenes de gas se cargan en la red de gasoductos	El ciberataque dejó fuera de servicio la página web de TGS, pero no hubo riesgo para la operación en si misma del sistema de gas	No especificada			La empresa declaró haber detectado el ataque lo que permitió minimizar el impacto del mismo, no obstante, reconoció haber operado la aplicación impactada "a ciegas" con un esquema de comunicación de solicitudes de contingencia
Grupo Ledesma	Compañía azucarera	X	X		Ransomware-Lockbit	1/4/2022	Encriptado de archivos y solicitando un rescate para devolver la información y no publicar lo sucedido	No informado	No se reveló el monto que solicitaron los delincuentes para devolver el acceso a los archivos se presume que la cifra fue grande			Dada la reserva tomada por la empresa, se supone se procedió a recuperar la información secuestrada desde copias de respaldo
Consejo Nacional de Investigaciones Científicas y Técnicas-CONICET	Organismo dedicado a la promoción de la ciencia y la tecnología en Argentina, dependiente del Ministerio de Ciencia, Tecnología e Innovación de la Nación	X	X		Ransomware	22/4/2022	Las oficinas de la Sede Central del CONICET fueron las únicas afectadas durante el ataque virtual. El mismo fue bajo la modalidad 'ransomware', donde los ciberdelincuentes secuestran información sensible para luego pedir rescate por los datos que robaron	No fueron afectados los servicios críticos	No declarado			Preventivamente se aislaron los servidores críticos y se procedió a recuperar la información secuestrada desde copias de respaldo

4.2 Evaluación de los costos económicos y sociales de estos ataques.[29]

En este apartado, se profundiza en la evaluación de los costos económicos y sociales asociados a los ciberataques contra infraestructuras críticas. Se presentan datos cualitativos para comprender mejor la magnitud de estas consecuencias.

El 16 de enero de 2023, Argentina anunció un importante paso hacia la mejora de su seguridad cibernética con el apoyo del Banco Interamericano de Desarrollo (BID). El BID aprobó un préstamo de US$30 millones para la implementación del Programa de Ciberseguridad para Infraestructuras Críticas de Información (ICI). Esta iniciativa tiene como objetivo principal reducir los costos que generan los ciberataques en el país.

[28] CEPAL (Comisión Económica para América Latina y el Caribe). (2023). Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe (p. 41). En R. M. Díaz y G. Núñez (Autores), Publicación de las Naciones Unidas LC/TS.2023/93. Copyright © Naciones Unidas, 2023. Todos los derechos reservados. Impreso en Naciones Unidas, Santiago. Número de documento: S.23-00614. https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

[29] BID (Banco Interamericano de Desarrollo). (2023, 16 de enero). Argentina busca reducir los costos de los ciberataques con apoyo del BID. Recuperado de https://www.iadb.org/es/noticias/argentina-busca-reducir-los-costos-de-los-ciberataques-con-apoyo-del-bid

El programa se enfocará en aumentar la seguridad cibernética en Argentina fortaleciendo la protección de la infraestructura tecnológica de sus instituciones públicas. Este enfoque beneficiará tanto a los ciudadanos como al sector privado y a la administración pública.

Para lograrlo, se llevarán a cabo las siguientes acciones:

- Fortalecimiento de las capacidades institucionales y tecnológicas de la Secretaría de Innovación Pública (SIP).
- Consolidación del talento humano en ciberseguridad.
- Mejora en la protección del ecosistema de Gestión Documental Electrónica (GDE).

Los ataques cibernéticos han ido en aumento, especialmente con la creciente adopción de tecnologías digitales durante la pandemia de COVID-19. Según el Foro Económico Mundial, los ciberataques son considerados uno de los riesgos más importantes que enfrentan las economías en la actualidad. La transformación digital se ha convertido en un elemento clave en la recuperación económica postpandemia, lo que hace que fortalecer la ciberseguridad sea una prioridad para los países de la región.

El Programa de Ciberseguridad para ICI se centra en la detección temprana de incidentes cibernéticos como estrategia para reducir los costos asociados con la respuesta y la recuperación frente a estos ataques. Además, busca abordar la escasez de profesionales en ciberseguridad y la baja representación de mujeres en este campo, desafíos que son comunes tanto en América Latina como a nivel global.

A continuación, se presentan algunos aspectos clave a considerar:

Costos Financieros Directos:

- Incluyen los gastos de recuperación necesarios para restaurar los sistemas y datos afectados por el ataque.
- Comprenden los rescates pagados en casos de ransomware a los ciberdelincuentes.
- Implican recursos invertidos en investigaciones forenses para identificar a los perpetradores y comprender la extensión del daño.

Costos Indirectos:

- Abordan la pérdida de productividad que resulta de la interrupción de las operaciones comerciales.
- Consideran los retrasos en la prestación de servicios esenciales, lo que puede afectar a la población y a las empresas.
- Incluyen las oportunidades perdidas, como contratos o transacciones comerciales que se cancelan debido al ataque.

Impacto en la Economía Nacional:

- Los ciberataques pueden tener un impacto significativo en la economía nacional.
- Pueden afectar el crecimiento económico al reducir la confianza de los inversionistas y la capacidad de las empresas para operar sin interrupciones.
- También pueden influir en la creación de empleo y en la inversión extranjera, lo que a largo plazo puede debilitar la economía de un país.

Costos Sociales y Humanos:

- A nivel social, los ciberataques pueden comprometer la seguridad de las personas.
- Pueden afectar la prestación de atención médica y la disponibilidad de servicios públicos esenciales, poniendo en riesgo la salud y el bienestar de la población.

La comprensión de estos costos económicos y sociales es fundamental para justificar inversiones en ciberseguridad y para promover la conciencia sobre la importancia de la protección de infraestructuras críticas en la sociedad. La reciente aprobación del préstamo del BID para el Programa de Ciberseguridad para ICI en Argentina es un paso significativo en esta dirección, ya que busca reducir los costos y fortalecer la capacidad del país para enfrentar los desafíos cibernéticos.

Resultados

Capítulo 5: Estrategias de Protección y Prevención

5.1 Revisión de las Estrategias y Tecnologías de Ciberseguridad utilizadas para Proteger Infraestructuras Críticas

En este capítulo, se llevará a cabo una revisión de las estrategias y tecnologías de ciberseguridad empleadas para resguardar las infraestructuras críticas del país. Esta revisión se fundamentará en el análisis de la situación actual de la ciberdelincuencia, considerando tanto datos nacionales como estándares internacionales. Los elementos clave que se abordarán en esta sección incluyen:

5.1.1 Panorama Actual de la Ciberdelincuencia - Evaluación y Análisis[30]

Para comprender adecuadamente la naturaleza de la ciberdelincuencia en el país y sus implicaciones en las infraestructuras críticas, se llevará a cabo una evaluación integral que incluirá:

Definiciones precisas de delitos cibernéticos y ciberseguridad, en línea con las mejores prácticas y estándares internacionales:

Para garantizar una estrategia efectiva contra la ciberdelincuencia, es fundamental establecer definiciones claras y precisas de los delitos cibernéticos y los conceptos relacionados con la ciberseguridad. Estas definiciones deben estar en consonancia con las mejores prácticas y estándares internacionales.

Esto implica:

- **Definición de Delitos Cibernéticos:** Es crucial definir los delitos cibernéticos de manera específica, abarcando una amplia gama de actividades delictivas que se

[30] Castillo, G. (2023, 19 de julio). Ciberseguridad en Argentina: situación actual, delitos más comunes y leyes. Innovación Digital 360. Recuperado de https://www.innovaciondigital360.com/cyber-security/ciberseguridad-en-argentina-situacion-actual-delitos-mas-comunes-y-leyes/

INTERPOL. (2020, 4 de agosto). Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19. Recuperado de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

llevan a cabo en el ciberespacio. Los delitos cibernéticos se refieren a actividades ilícitas que tienen lugar en el ámbito digital utilizando tecnologías de la información y las comunicaciones. Estos delitos abarcan una amplia variedad de acciones, como el acceso no autorizado a sistemas informáticos, la distribución de software malicioso, el engaño en línea (phishing), el robo de información personal o financiera, el fraude en línea y la interferencia intencionada en infraestructuras tecnológicas. Los perpetradores de delitos cibernéticos pueden ser individuos o grupos que persiguen diversos objetivos, como ganancias económicas, motivaciones políticas o simplemente gratificación personal.

- **Definición de Ciberseguridad:** La ciberseguridad debe definirse de manera completa, abarcando medidas técnicas, legales y organizativas para proteger los sistemas y datos de ataques cibernéticos. Esto incluye la prevención, detección, respuesta y recuperación de incidentes de seguridad cibernética.

  La ciberseguridad es la disciplina que se encarga de salvaguardar sistemas informáticos, redes y datos contra amenazas y ataques cibernéticos. En esencia, implica la implementación de medidas técnicas, políticas y procedimientos diseñados para garantizar la confidencialidad, integridad y disponibilidad de la información digital y los recursos tecnológicos. Esto engloba desde la prevención de accesos no autorizados y la detección de posibles amenazas hasta la respuesta ante incidentes de seguridad y la concienciación de los usuarios. Además, la ciberseguridad promueve la colaboración entre diferentes actores, incluyendo el sector privado y las entidades gubernamentales, con el fin de fortalecer la seguridad cibernética en general.

- **Alineación con Estándares Internacionales:** Las definiciones y conceptos relacionados deben alinearse con estándares internacionales ampliamente

aceptados, como los definidos por organizaciones como ISO (Organización Internacional de Normalización) y NIST (Instituto Nacional de Estándares y Tecnología de EE. UU.), para garantizar la coherencia y la interoperabilidad a nivel global.

En Argentina, la alineación con estándares internacionales es crucial para fortalecer la ciberseguridad y abordar los desafíos cibernéticos de manera efectiva en un mundo globalmente interconectado. Esto implica adoptar enfoques y marcos de trabajo reconocidos a nivel mundial. Algunos de los estándares y directrices ampliamente aceptados incluyen:

1. **ISO 27001:** Un estándar internacional que establece un marco para la gestión de la seguridad de la información, proporcionando pautas claras para la implementación de controles de seguridad.
2. **NIST Cybersecurity Framework:** Aunque originado en Estados Unidos, este marco es referente internacional y brinda orientación sobre cómo las organizaciones pueden mejorar su ciberseguridad.
3. **Directrices de la UE sobre ciberseguridad:** Aunque Argentina no es miembro de la Unión Europea, estas directrices pueden servir como referencia para el desarrollo de políticas y regulaciones relacionadas con la ciberseguridad.
4. **Cooperación internacional:** La colaboración con organizaciones internacionales, como INTERPOL y Europol, es fundamental para prevenir y combatir delitos cibernéticos a nivel global y puede influir en las estrategias de Argentina en este ámbito.

Análisis de datos estadísticos nacionales relacionados con la ciberdelincuencia, desglosados por tipo de delito, ubicación geográfica, demografía y otros factores relevantes:

La comprensión detallada de la ciberdelincuencia en el país es esencial para desarrollar estrategias efectivas. Esto implica:

- **Recopilación de Datos:** Recopilar datos estadísticos nacionales sobre ciberdelincuencia, que incluyan información sobre el tipo de delitos cibernéticos, su frecuencia, su ubicación geográfica y el perfil demográfico de las víctimas y los perpetradores.
- **Análisis Detallado:** Realizar un análisis minucioso de estos datos para identificar patrones, tendencias y áreas de mayor vulnerabilidad. Esto ayudará a comprender las amenazas cibernéticas específicas que enfrenta el país.
- **Identificación de Puntos Críticos:** Identificar las áreas geográficas o sectores demográficos que pueden ser más susceptibles a ciertos tipos de ciberdelitos, lo que permitirá una asignación más precisa de recursos y medidas de prevención.

En nuestro país: “El Equipo de Respuesta ante Emergencias Informáticas nacional (CERT.ar) de la Dirección Nacional de Ciberseguridad realiza tareas vinculadas con posibles ciberataques, que puedan afectar los sistemas y redes del Sector Público Nacional, para brindar mejoras en materia de prevención, protección y resiliencia. Además, hace el seguimiento y la evolución de los hechos detectados o reportados con el fin de brindar asistencia técnica y administrativa”[31]

[31] Dirección Nacional de Ciberseguridad. (2022). Informe de Gestión CERT.ar 2022. Recuperado de https://www.argentina.gob.ar/sites/default/files/2023/02/informe_cert_2022.docx.pdf

El Centro de Respuesta a Incidentes Cibernéticos de Argentina (CERT.ar) registró un total de 335 incidentes informáticos en el período de enero a diciembre de 2022, lo que representó una disminución del 43.3% en comparación con el año anterior, cuando se reportaron 591 incidentes. La principal fuente de reportes fue el correo electrónico, con 232 casos, seguida por repositorios de información específica (76 casos) y el formulario web (27 casos). Hasta finales de 2022, se resolvieron 323 incidentes, y los 12 restantes estaban en proceso de análisis o esperando respuestas.

En cuanto a la categorización de los incidentes, el indicio de fraude fue el más común, representando el 72.8% del total de incidentes, seguido por el compromiso de la información (63 casos) y otros tipos más específicos. El sector más afectado fue el de Finanzas, con 185 incidentes (55.2% del total), seguido por el Estado (71 incidentes) y Sectores no críticos (33 incidentes). El phishing fue el tipo de incidente más reportado en ambos sectores, con 182 casos en Finanzas y 13 en el Estado.

En términos de severidad, la mayoría de los incidentes (91.04%) se consideraron de alta severidad, seguidos por incidentes de severidad media (5.37%) y crítica (3.28%). La disminución en el número de incidentes puede atribuirse a la vuelta al trabajo presencial y a las medidas de seguridad cibernética implementadas, como la Decisión Administrativa 641/2021[32].

A pesar de la disminución general de incidentes, hubo un aumento en los incidentes críticos, particularmente dirigidos a los Ministerios y en el sector privado, lo que sugiere cambios en los vectores de ataque y motivaciones de los ciberatacantes. Además, se observó un aumento en los reportes a través del formulario web, indicando esfuerzos por mejorar la agilidad en la detección y respuesta a incidentes.

[32] Jefatura de Gabinete de Ministros. (2021, junio). Decisión Administrativa 641/2021 - Requisitos mínimos de Seguridad de la Información para Organismos. Boletín Oficial de la República Argentina. https://www.boletinoficial.gob.ar/detalleAviso/primera/246104/20210628

Identificación de las autoridades y agencias existentes encargadas de investigar y combatir la ciberdelincuencia, así como su alcance de jurisdicción y roles en el sistema de justicia penal:

Es fundamental conocer las instituciones y autoridades responsables de abordar la ciberdelincuencia:

- **Identificación de Autoridades:** Identificar las agencias gubernamentales y las unidades policiales encargadas de investigar y combatir los delitos cibernéticos.
- **Alcance de Jurisdicción:** Comprender la jurisdicción y el ámbito de actuación de estas autoridades, tanto a nivel nacional como regional o local, según corresponda.
- **Roles y Responsabilidades:** Definir claramente los roles y responsabilidades de estas autoridades en el sistema de justicia penal, incluyendo la coordinación con otras entidades gubernamentales y el sector privado.

En Argentina, la lucha contra la ciberdelincuencia involucra a varias autoridades y agencias gubernamentales a nivel nacional y provincial. Aquí hay una identificación general de las principales instituciones y su alcance de jurisdicción:

Policía Federal Argentina (PFA):[33]

Jurisdicción: Nacional.

Roles y Responsabilidades: La PFA, a través de su División de Delitos Tecnológicos, se encarga de investigar los delitos cibernéticos en todo el país. Esto

[33] División Delitos Tecnológicos de la Policía Federal Argentina. (Fecha desconocida). Recuperado de https://www.argentina.gob.ar/servicio/denunciar-un-delito-informatico

incluye la persecución de delitos como la pornografía infantil, el fraude cibernético y otros delitos relacionados con la tecnología.

Gendarmería Nacional:[34]

Jurisdicción: Nacional.

Roles y Responsabilidades: La Gendarmería Nacional también tiene una unidad especializada en delitos cibernéticos y colabora en investigaciones relacionadas con la seguridad digital, el cibercrimen y la ciberseguridad, participando como miembro de CSIRT del Ministerio de Seguridad de la Nación.

Policía de la Ciudad de Buenos Aires:[35]

Jurisdicción: Ciudad Autónoma de Buenos Aires.

Roles y Responsabilidades: La Policía de la Ciudad tiene una división dedicada a la ciberseguridad y combate de la ciberdelincuencia en el ámbito de la ciudad.

Ministerio Público Fiscal:[36]

Jurisdicción: Nacional y provincial.

Roles y Responsabilidades: El Ministerio Público Fiscal a nivel nacional y provincial es responsable de la investigación y enjuiciamiento de delitos, incluyendo los

[34] CSIRT del Ministerio de Seguridad de la Nación. (2023). Recuperado de https://csirt.minseg.gob.ar/

[35] Jefatura de Gabinete de la Ciudad de Buenos Aires. (2023). Centro de Ciberseguridad. Recuperado de https://buenosaires.gob.ar/jefaturadegabinete/centro-de-ciberseguridad

[36] Ministerio Público Fiscal. Unidad Fiscal Especializada en Ciberdelincuencia (UFECI). (2023). Recuperado de https://www.mpf.gob.ar/ufeci/

Ministerio Público Fiscal CABA. Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas (UFEDyCI). (2023). Recuperado de https://mpfciudad.gob.ar/tematicas/2020-03-09-18-42-38-delitos-informaticos

delitos cibernéticos. Trabaja en conjunto con las fuerzas de seguridad en la persecución de estos delitos.

Revisión de la legislación nacional vigente relacionada con la ciberdelincuencia y la ciberseguridad, con especial atención a leyes de ciberseguridad, delitos informáticos, derecho penal sustantivo y procesal, entre otros:

Una revisión completa de la legislación es esencial para garantizar que esté actualizada y sea efectiva:

- **Leyes de Ciberseguridad:** Evaluar las leyes y regulaciones relacionadas con la ciberseguridad para asegurar que proporcionen un marco legal sólido para la protección de infraestructuras críticas y la prevención de delitos cibernéticos.
- **Delitos Informáticos:** Examinar las leyes que tipifican y sancionan los delitos cibernéticos, asegurándose de que estén alineadas con las mejores prácticas y estándares internacionales.
- **Derecho Penal Sustantivo y Procesal:** Revisar el derecho penal sustantivo y procesal para garantizar que permita una persecución efectiva de los delitos cibernéticos y una respuesta adecuada ante incidentes de ciberseguridad.

La legislación en Argentina relacionada con la ciberdelincuencia y la ciberseguridad ha experimentado cambios significativos en los últimos años para abordar los desafíos emergentes en el ámbito digital. A continuación, una revisión general de algunas de las leyes y regulaciones más relevantes:

- **Ley de Delitos Informáticos (Ley 26.388)[37]:** Esta ley establece las penas para diversos delitos informáticos, como acceso ilegítimo a sistemas, daño a datos informáticos y la difusión de información personal sin consentimiento. Fue una de las primeras leyes en Argentina en abordar específicamente la ciberdelincuencia.
- **Ley de Protección de Datos Personales (Ley 25.326)[38]:** Aunque no está dirigida exclusivamente a la ciberseguridad, esta ley regula el tratamiento de datos personales, lo que es fundamental en la protección de la privacidad y la seguridad en línea.
- **Normativa de Firma Electrónica (Ley 25.506)[39]:** Regula la firma electrónica y su validez legal, promoviendo la confianza en las transacciones electrónicas y la seguridad en línea.
- Segunda Estrategia Nacional de Ciberseguridad (Resolución 44/2023)[40]
- Otras normativas relacionadas a la ciberseguridad:
    1. Decreto 577/2017. Creación del Comité de Ciberseguridad.[41]

[37] Justicia y Derechos Humanos de la República Argentina. Delitos informáticos. Los delitos informáticos ahora forman parte del Código Penal. Ley 26.388. Recuperado de https://www.argentina.gob.ar/justicia/derechofacil/leysimple/delitos-informaticos

[38] Justicia y Derechos Humanos de la República Argentina. Datos personales. Ley de protección de datos personales o hábeas data te protege si tus datos de identidad, de salud o de crédito son usados sin tu consentimiento. Ley 25326. Recuperado de https://www.argentina.gob.ar/justicia/derechofacil/leysimple/datos-personales

[39] Jefatura de Gabinete de Ministros de la República Argentina. Normativa de Firma Digital. Ley N° 25.506 de Firma Digital (Texto Actualizado). Reconoce y establece las condiciones para el empleo de la firma electrónica y de la firma digital y su eficacia jurídica, y crea la Infraestructura de Firma Digital de la República Argentina. Recuperado de https://www.argentina.gob.ar/jefatura/innovacion-publica/innovacion-administrativa/firma-digital/normativa-de-firma-digital

[40] Jefatura de Gabinete de Ministros, Secretaría de Innovación Pública. (2023, 4 de septiembre). Resolución 44/2023 (RESOL-2023-44-APN-SIP#JGM). Boletín Oficial de la República Argentina. Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904

[41] Poder Ejecutivo Nacional. (2017, 28 de julio). Decreto 577/2017. Comité de Ciberseguridad. Creación. Publicado en el Boletín Nacional del 31 de julio de 2017. Recuperado de https://www.argentina.gob.ar/normativa/nacional/decreto-577-2017-277518

2. Decreto 480/2019. Modificación del Decreto 577/2017.[42]
3. Resolución 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad.[43]
4. Resolución 141/2019. Presidencia del Comité de Ciberseguridad.[44]

- **Código Penal[45]:** El Código Penal de Argentina ha sido modificado para incluir disposiciones relacionadas con la ciberdelincuencia y la responsabilidad penal de los infractores digitales.
- **Ley de Acceso a la Información Pública (Ley 27.275)[46]:** Esta ley regula el acceso a la información pública y puede ser relevante en investigaciones de ciberdelincuencia que involucren la obtención de información gubernamental.
- **Ley de Grooming (26.904):** La Ley 26.904 fue promulgada en Argentina el 13 de noviembre de 2013 y establece la criminalización específica del grooming. Esta ley busca proteger a los menores de edad de posibles abusos sexuales y explotación en línea.

Evaluación de la cooperación internacional y los acuerdos de asistencia judicial recíproca, como los Tratados de Asistencia Judicial Recíproca (MLAT), para abordar la ciberdelincuencia a nivel internacional:

---

[42] Poder Ejecutivo Nacional. (2019, fecha desconocida). Decreto 480/2019. Modificación del Decreto N° 577/2017. Publicado en el Boletín Oficial. Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/211277/20190712

[43] Jefatura de Gabinete de Ministros de la República Argentina. (2019, 24 de mayo). Resolución 829/2019. Estrategia Nacional de Ciberseguridad - Aprobación. Publicada en el Boletín Nacional del 28 de mayo de 2019. Recuperado de https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-829-2019-323594

[44] Jefatura de Gabinete de Ministros de la República Argentina. (2019, 9 de mayo). Resolución 141/2019. Delegaciones - Comité de Ciberseguridad. Publicada en el Boletín Nacional del 13 de mayo de 2019. Recuperado de https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-141-2019-323038

[45] Congreso de la Nación Argentina. (2008). Código Penal. Ley 26.388. Modificación. Sancionada el 4 de junio de 2008. Promulgada de hecho el 24 de junio de 2008. Recuperado de https://www.oas.org/juridico/PDFs/arg_ley26388.pdf

[46] Justicia y Derechos Humanos de la República Argentina. (Fecha desconocida). Acceso a la información pública. Ley 27.275. Recuperado de https://www.argentina.gob.ar/justicia/derechofacil/leysimple/acceso-la-informacion-publica

La ciberdelincuencia es un problema transfronterizo que requiere cooperación internacional:

- **MLAT y Acuerdos Similares:** Evaluar la existencia y eficacia de los acuerdos de asistencia judicial recíproca, como los MLAT, para facilitar la colaboración entre países en investigaciones de ciberdelincuencia.
- **Colaboración Internacional:** Identificar oportunidades para mejorar la colaboración con otros países y organizaciones internacionales en la lucha contra la ciberdelincuencia, incluyendo el intercambio de información y la extradición de delincuentes.
- **Cumplimiento de Estándares Internacionales:** Asegurarse de que los acuerdos y la cooperación internacional estén en línea con los estándares y las mejores prácticas internacionales en la lucha contra la ciberdelincuencia.

La cooperación internacional en la lucha contra la ciberdelincuencia es fundamental debido a la naturaleza transnacional de los delitos cibernéticos. Argentina ha establecido acuerdos de asistencia judicial recíproca y colabora activamente con otros países y organizaciones internacionales en este ámbito.

Tratados de Asistencia Judicial Recíproca (MLAT):

Argentina ha firmado varios Tratados de Asistencia Judicial Recíproca (MLAT) con diferentes países para facilitar la cooperación en investigaciones y persecuciones de delitos cibernéticos. Estos tratados permiten el intercambio de evidencia digital, la extradición de delincuentes y la coordinación de esfuerzos en casos de ciberdelincuencia.

Los acuerdos más relevantes son:

1. **Convenio de Budapest sobre Ciberdelincuencia**[47]: Aunque no es un MLAT en sí, Argentina es parte de este tratado internacional, también conocido como el Convenio de Budapest. Este tratado se centra en la armonización de leyes nacionales para combatir la ciberdelincuencia y facilitar la cooperación internacional en este ámbito.
2. **MLAT con Estados Unidos**[48]: Argentina tiene un Tratado de Asistencia Legal Mutua (MLAT) con los Estados Unidos que abarca una variedad de áreas, incluida la ciberseguridad y la lucha contra el cibercrimen. Este acuerdo permite la cooperación en investigaciones y el intercambio de información en casos de delitos cibernéticos.
3. **Acuerdos Bilaterales**: Argentina ha establecido acuerdos bilaterales con varios países, incluyendo tratados específicos de asistencia judicial que pueden incluir disposiciones relacionadas con la ciberseguridad y el cibercrimen. Estos acuerdos pueden variar en contenido y alcance según el país con el que se hayan firmado.

Interpol y Europol:

Argentina es miembro de Interpol y colabora con esta organización para combatir la ciberdelincuencia a nivel internacional. También coopera con Europol en investigaciones relacionadas con la ciberseguridad y la ciberdelincuencia que afectan a la Unión Europea y otros países asociados.

Foros y Organizaciones Internacionales:

[47] Argentina.gob.ar. (2023, 16 de febrero). Argentina y la Unión Europea unen esfuerzos para combatir el ciberdelito. Recuperado de https://www.argentina.gob.ar/noticias/argentina-y-la-union-europea-unen-esfuerzos-para-combatir-el-ciberdelito

[48] Justicia y Derechos Humanos de la República Argentina. (Fecha desconocida). Tratado de Asistencia Jurídica Mutua en Asuntos Penales, suscripto con el Gobierno de los Estados Unidos de América, aprobado por ley 24.034. Recuperado de https://www.argentina.gob.ar/justicia/asuntosinternacionales/juridica-internacional-en-material-penal

Argentina participa en foros y organizaciones internacionales relacionados con la ciberseguridad y la ciberdelincuencia, como la ONU, la OEA y la UIT. Estos foros proporcionan un marco para la cooperación y el intercambio de información sobre amenazas cibernéticas y buenas prácticas.

5.2 Análisis de las Mejores Prácticas y Estándares de Seguridad

La seguridad de las infraestructuras críticas es un tema de vital importancia tanto en Argentina como en el ámbito internacional. Para resguardar la integridad y el funcionamiento de estas infraestructuras, es esencial implementar las mejores prácticas y estándares de seguridad cibernética. En este contexto, el análisis de estas prácticas y estándares se convierte en un componente crucial para la formulación de estrategias efectivas de protección.

El siguiente análisis detallado revela una panorámica completa de las medidas necesarias para proteger las infraestructuras críticas en Argentina y en todo el mundo. Además, destaca la importancia de adaptar estas prácticas a las necesidades y regulaciones locales, así como la necesidad de una revisión continua para enfrentar las cambiantes amenazas de seguridad cibernética.

ISO 27001[49]:

La norma ISO 27001 establece un marco de trabajo para la gestión de la seguridad de la información. Esta norma internacional es aplicable a cualquier tipo de organización, incluyendo las encargadas de infraestructuras críticas, y se centra en la identificación, evaluación y mitigación de riesgos de seguridad. La implementación de ISO 27001

[49] International Organization for Standardization. ISO 27001: Gestión de la seguridad de la información. Recuperado de https://www.normas-iso.com/iso-27001/

implica la definición de políticas de seguridad, la realización de evaluaciones de riesgos y la implementación de controles de seguridad adecuados para proteger la información y los sistemas críticos. En Argentina, las organizaciones que gestionan infraestructuras críticas pueden utilizar ISO 27001 como una guía valiosa para establecer un marco de seguridad sólido.

NIST Cybersecurity Framework[50]:

El Marco de Ciberseguridad del NIST es una herramienta ampliamente aceptada para evaluar y mejorar la ciberseguridad en infraestructuras críticas. Está compuesto por cinco funciones clave: Identificar, Proteger, Detectar, Responder y Recuperar. En Argentina, este marco puede servir como una guía estructurada para abordar los desafíos de seguridad cibernética en las infraestructuras críticas. Ayuda a las organizaciones a entender sus riesgos, establecer medidas de seguridad adecuadas y responder de manera eficiente a incidentes.

Ciberseguridad Industrial (IEC 62443)[51]:

La norma IEC 62443 es esencial para las infraestructuras críticas que gestionan sistemas de control industrial (ICS). Ofrece directrices específicas para la protección de estos sistemas, que son vitales en sectores como la energía, el transporte y la manufactura. En Argentina, donde la industria y la infraestructura crítica son fundamentales para la economía, la adopción de la norma IEC 62443 puede ayudar a fortalecer la ciberseguridad en sectores clave.

[50] National Institute of Standards and Technology. (Fecha desconocida). Cybersecurity Framework. Recuperado de https://www.nist.gov/cyberframework
[51] Ingertec. (Fecha desconocida). Norma IEC 62443. Recuperado de https://ingertec.com/norma-iec-62443/

Evaluación de riesgos[52]:

La evaluación de riesgos es un paso crítico para identificar amenazas y vulnerabilidades específicas en las infraestructuras críticas. Esto implica realizar un análisis exhaustivo de los activos, amenazas potenciales y el impacto que podrían tener los incidentes de seguridad. En Argentina, un enfoque basado en la evaluación de riesgos puede ayudar a priorizar las inversiones en seguridad y garantizar que los recursos se asignen de manera efectiva para proteger lo más importante.

Capacitación y concienciación:

La capacitación del personal es esencial en la protección de infraestructuras críticas. La concienciación sobre la ciberseguridad debe ser una parte integral de la cultura organizacional. En Argentina, promover una mayor comprensión de los riesgos de seguridad cibernética entre los empleados y las partes interesadas es fundamental para prevenir ataques y garantizar un entorno seguro.

Cumplimiento normativo:

Cumplir con las regulaciones y estándares de seguridad aplicables en Argentina es esencial. Las organizaciones deben asegurarse de que están al día con las leyes y requisitos específicos de su sector.

Colaboración y compartir información:

La cooperación entre organizaciones y la compartición de información sobre amenazas y ataques cibernéticos son prácticas cruciales para mantenerse al tanto de las tendencias de seguridad y responder de manera más efectiva a las amenazas.

---

[52] Blog Ciberseguridad. (2023). Metodologías de evaluación de riesgos cibernéticos. Recuperado de https://ciberseguridad.com/herramientas/metodologias-evaluacion-riesgos-ciberneticos/

Resiliencia y redundancia:

Diseñar infraestructuras críticas con resiliencia y redundancia significa asegurarse de que puedan seguir funcionando incluso en situaciones adversas o después de un ataque cibernético.

En este capítulo hemos proporcionado una visión completa de las estrategias de protección y prevención en el campo de la ciberseguridad de las infraestructuras críticas en Argentina. Hemos explorado aspectos cruciales como la definición precisa de delitos cibernéticos y ciberseguridad, la evaluación de la ciberdelincuencia en el país, la identificación de las autoridades competentes, la revisión de la legislación nacional, la cooperación internacional y el análisis de las mejores prácticas y estándares de seguridad.

Nuestra revisión revela la importancia crítica de alinear las estrategias de ciberseguridad con estándares internacionales ampliamente aceptados, como ISO 27001, el Marco de Ciberseguridad del NIST y la norma IEC 62443, para garantizar la robustez y la eficacia de las medidas de protección. Además, destacamos la necesidad de una evaluación continua de los riesgos, la capacitación y concienciación del personal, y la promoción de una cultura de ciberseguridad en las organizaciones.

La colaboración y la compartición de información tanto a nivel nacional como internacional son ejes fundamentales en la lucha contra la ciberdelincuencia, y Argentina ha establecido acuerdos y tratados para facilitar esta cooperación.

Por último, el capítulo 5 establece una base para la formulación de estrategias efectivas de ciberseguridad que protejan las infraestructuras críticas de Argentina en un entorno digital en constante evolución. El siguiente capítulo se centrará en la

implementación de estas estrategias y la evaluación de su efectividad en la protección de nuestras infraestructuras más vitales contra las amenazas cibernéticas.

Capítulo 6: Evaluación de Estrategias de Recuperación y Resiliencia en Infraestructuras Críticas.[53]

La preparación y respuesta ante eventos adversos que puedan afectar a las infraestructuras críticas son elementos cruciales en la protección de la seguridad nacional y la continuidad de operaciones. Sin embargo, la mera anticipación de amenazas no es suficiente; la capacidad de recuperación y resiliencia ante desafíos imprevistos se ha convertido en algo imperativo en un entorno cada vez más globalizado y tecnológico. Este capítulo está enfocado en la evaluación de las estrategias de recuperación y resiliencia aplicadas a las infraestructuras críticas de Argentina.

En el marco de este análisis, exploraremos cómo se planifica la recuperación en situaciones de crisis, qué estrategias de resiliencia se implementan para mitigar los impactos de eventos adversos y cómo se integra la seguridad cibernética en este contexto. Argentina, como muchas otras naciones, se enfrenta a desafíos constantes que amenazan la seguridad de sus infraestructuras críticas, desde eventos naturales hasta ciberataques sofisticados. Por lo tanto, comprender y evaluar las estrategias que respaldan la recuperación y resiliencia se convierte en una tarea ineludible.

En el transcurso de este capítulo, investigaremos los elementos clave de la planificación de la recuperación, desde la identificación de riesgos y vulnerabilidades específicas. Del mismo modo, exploraremos cómo se construyen infraestructuras críticas resilientes, cómo se diversifican los recursos y se establece la redundancia para asegurar la continuidad de las operaciones. Además, destacaremos la importancia de la integración de la seguridad cibernética en todas estas estrategias, reconociendo la creciente amenaza que representan los ataques en el ciberespacio.

---

[53] UNDRR. (Fecha desconocida). Principios para la Infraestructura Resiliente. Recuperado de https://www.undrr.org/media/86825/download?startDownload=true

6.1 Planificación de la Recuperación en Infraestructuras Críticas. [54]

La planificación de la recuperación en infraestructuras críticas es un proceso esencial para garantizar la continuidad de las operaciones en situaciones de crisis. En este apartado, se abordará en detalle cómo se lleva a cabo este proceso, desde la identificación de riesgos hasta la implementación de planes de recuperación sólidos.

6.1.1 Identificación de Riesgos y Vulnerabilidades[55]

La identificación de riesgos y vulnerabilidades es el punto de partida fundamental en la planificación de la recuperación de infraestructuras críticas. Este proceso implica la evaluación exhaustiva de amenazas potenciales y la determinación de las áreas más vulnerables de las infraestructuras críticas en Argentina. A continuación, se detallan los elementos clave a considerar:

- **Evaluación de Amenazas Naturales y Humanas:** La identificación de riesgos debe abarcar amenazas tanto naturales como humanas. Las amenazas naturales pueden incluir terremotos, inundaciones, incendios forestales y eventos climáticos extremos. Por otro lado, las amenazas humanas pueden abarcar actos de terrorismo, sabotaje, ciberataques y otras actividades maliciosas.
- **Sector Específico:** Diferentes sectores de infraestructuras críticas pueden enfrentar amenazas específicas. Por ejemplo, el sector de energía puede verse afectado por ataques cibernéticos en la red eléctrica, mientras que el

[54] Agrupación Empresarial Innovadora para la Seguridad de las Redes y los Sistemas de Información. (2012). Protección de Infraestructuras Críticas (p. 203). Recuperado de https://www.aeiciberseguridad.es/GuiaPIC.pdf

Ciberseguridad.com. (Fecha desconocida). Metodologías de Evaluación de Riesgos Cibernéticos. Recuperado de https://ciberseguridad.com/herramientas/metodologias-evaluacion-riesgos-ciberneticos/

[55] United Nations Office of Counter-Terrorism. (2018). The protection of critical infrastructures against terrorist attacks: Compendium of good practices. Recuperado de https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf

sector de transporte puede estar expuesto a desastres naturales que afecten la infraestructura de carreteras y ferrocarriles. Es importante considerar las particularidades de cada sector al identificar riesgos.

- **Evaluación de Impacto:** Junto con la identificación de amenazas, es esencial evaluar el impacto potencial de estas amenazas en la infraestructura crítica. Esto implica analizar cómo un evento adverso podría interrumpir las operaciones, causar daños materiales, afectar la seguridad pública y tener repercusiones económicas.
- **Análisis de Vulnerabilidades:** Para comprender completamente la exposición a riesgos, es necesario llevar a cabo un análisis de vulnerabilidades. Esto implica examinar las debilidades existentes en la infraestructura, como sistemas obsoletos, falta de medidas de seguridad cibernética o inadecuada planificación de la contingencia.
- **Fuentes de Información:** La identificación de riesgos se basa en una variedad de fuentes de información, que van desde datos históricos de eventos adversos hasta informes de inteligencia sobre amenazas actuales. Además, se puede obtener información valiosa de organismos gubernamentales, organizaciones internacionales y la colaboración con expertos en seguridad.
- **Consideración de Escenarios:** Al identificar riesgos, es útil considerar diversos escenarios posibles, desde los más probables hasta los menos probables, pero altamente impactantes. Esta metodología ayuda a prepararse para una amplia gama de situaciones de crisis.
- **Localización Geográfica:** La ubicación geográfica de las infraestructuras críticas desempeña un papel crucial en la identificación de riesgos. Las

áreas propensas a ciertos tipos de desastres naturales deben ser evaluadas de manera más detenida para comprender la vulnerabilidad de la infraestructura en esas ubicaciones específicas.

6.1.2 Desarrollo de Planes de Recuperación[56]

Una vez que se han identificado los riesgos y vulnerabilidades en las infraestructuras críticas, es esencial desarrollar planes de recuperación sólidos y efectivos. Estos planes son la columna vertebral de la capacidad de una organización para responder eficazmente a incidentes y desastres, minimizando el tiempo de inactividad y reduciendo al mínimo los impactos negativos.

Algunos aspectos clave a considerar en el desarrollo de planes de recuperación:

- **Objetivos de Recuperación:** Es fundamental establecer objetivos de recuperación claros y medibles. Esto implica definir cuánto tiempo puede tolerar una infraestructura crítica estar inactiva y cuántos recursos están disponibles para la recuperación. Los objetivos deben ser realistas y adaptados a las necesidades específicas de cada sector.
- **Estrategias de Recuperación:** Se deben definir estrategias específicas para cada tipo de evento adverso identificado. Por ejemplo, un plan de recuperación para un ciberataque puede incluir la restauración de sistemas desde copias de seguridad, la revisión de la seguridad cibernética y la comunicación con partes interesadas clave.

---

[56] Instituto Nacional de Estándares y Tecnología (NIST). (2018, abril). Marco para la mejora de la seguridad cibernética en infraestructuras críticas (v1.1). Recuperado de https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

Organización de los Estados Americanos. (2019). Ciberseguridad Marco NIST: Un abordaje integral de la Ciberseguridad. Recuperado de https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Kyndryl. (s.f.). What is a disaster recovery plan and how does it work? Recuperado de https://www.kyndryl.com/es/es/learn/disaster-recovery-plan

- **Roles y Responsabilidades:** Es necesario establecer roles y responsabilidades claros para todas las partes involucradas en la recuperación. Esto incluye a los equipos internos de la organización, agencias gubernamentales, proveedores de servicios y otros actores relevantes.
- **Recursos y Capacidades:** Se deben identificar y asegurar los recursos necesarios para la recuperación, como personal capacitado, equipos de respuesta de emergencia y herramientas tecnológicas. Además, es esencial evaluar la capacidad de recuperación de proveedores y socios comerciales.
- **Comunicación y Coordinación:** La comunicación efectiva y la coordinación son fundamentales durante la recuperación. Se deben establecer canales de comunicación claros y protocolos de coordinación con todas las partes interesadas, incluidos los organismos gubernamentales pertinentes.
- **Pruebas y Ejercicios:** Los planes de recuperación deben ser probados y evaluados regularmente a través de ejercicios y simulacros. Esto permite identificar debilidades en el plan y mejorar la capacidad de respuesta de la organización.
- **Actualización Continua:** Los planes de recuperación no son estáticos; deben ser revisados y actualizados regularmente para reflejar cambios en las amenazas, la infraestructura y las capacidades de respuesta. La retroalimentación de incidentes anteriores también debe ser incorporada en las actualizaciones.
- **Cumplimiento Normativo:** Los planes de recuperación deben cumplir con las regulaciones y estándares de seguridad aplicables en Argentina. Esto incluye la alineación con leyes de ciberseguridad, regulaciones de salud y seguridad, y otras normativas sectoriales.

- **Documentación Detallada:** Todos los aspectos del plan de recuperación deben estar documentados de manera clara y accesible. Esto facilita la implementación efectiva del plan durante una crisis.

6.1.3 Pruebas y Simulaciones de Recuperación[57]

Una vez que se han desarrollado los planes de recuperación para las infraestructuras, es necesario llevar a cabo pruebas y simulaciones de recuperación para garantizar que estos planes sean efectivos y puedan implementarse con éxito en situaciones de crisis.

A continuación, se detallan los aspectos clave de las pruebas y simulaciones de recuperación:

- **Propósito de las Pruebas:** El propósito principal de las pruebas y simulaciones de recuperación es evaluar la eficacia de los planes de recuperación y garantizar que sean capaces de cumplir con los objetivos de recuperación establecidos. Las pruebas pueden revelar debilidades en los planes y proporcionar la oportunidad de corregirlas antes de un evento real.
- **Escenarios de Prueba:** Es esencial definir escenarios de prueba realistas y variados que aborden diferentes tipos de eventos adversos que podrían afectar a las infraestructuras críticas. Esto puede incluir ciberataques, desastres naturales, interrupciones en la cadena de suministro y otros eventos relevantes.
- **Planificación Detallada:** Antes de llevar a cabo las pruebas, se debe realizar una planificación detallada que incluya la identificación de los participantes, la asignación de roles y responsabilidades, la definición de objetivos y la

[57] INCIBE. (Fecha desconocida). Plan de contingencia y continuidad de negocio. Recuperado de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

Rogers, C. (2021, diciembre). Pruebas de recuperación ante desastres: puede salvar su negocio. Zerto. Recuperado de https://www.zerto.com/blog/disaster-recovery/disaster-recovery-testing-it-may-just-save-your-business/

documentación de los procedimientos de prueba. La planificación debe ser meticulosa para garantizar la efectividad de las pruebas.

- **Evaluación de Rendimiento:** Durante las pruebas, se debe evaluar el rendimiento de los equipos de respuesta, la eficacia de las estrategias de recuperación y la capacidad de cumplir con los objetivos de recuperación. Esto incluye la medición del tiempo de recuperación, la identificación de posibles cuellos de botella y la evaluación de la comunicación y coordinación.
- **Identificación de Mejoras:** Las pruebas pueden revelar áreas que requieren mejoras en los planes de recuperación, los procedimientos o la infraestructura. Es importante documentar todas las observaciones y desarrollar planes de acción para abordar las deficiencias identificadas.
- **Simulaciones de Escritorio:** Además de pruebas prácticas en el terreno, las simulaciones de escritorio son una herramienta valiosa. Estas simulaciones permiten a los equipos revisar los planes y procedimientos en un entorno controlado, discutir estrategias y evaluar la toma de decisiones.
- **Documentación y Retroalimentación:** Cada prueba y simulación debe ser documentada de manera detallada, incluyendo los resultados, las lecciones aprendidas y las recomendaciones de mejora. La retroalimentación de los participantes y observadores también es esencial para la mejora continua.
- **Ciclo de Mejora Continua:** Basándose en los resultados de las pruebas y simulaciones, se debe implementar un ciclo de mejora continua en los planes de recuperación. Esto implica revisar y actualizar regularmente los planes en función de la retroalimentación y los cambios en el entorno de amenazas.
- **Cumplimiento Normativo:** Es importante asegurarse de que las pruebas y simulaciones cumplan con las regulaciones y estándares de seguridad

aplicables en Argentina. Esto puede incluir la alineación con leyes de ciberseguridad, regulaciones de salud y seguridad, y otras normativas sectoriales.

Las pruebas y simulaciones proporcionan la oportunidad de identificar y abordar debilidades en los planes de recuperación antes de que ocurra un evento adverso real, fortaleciendo así la resiliencia y la capacidad de respuesta ante amenazas potenciales.

6.1.4 Monitoreo y Actualización Continua[58]

La planificación de la recuperación en infraestructuras críticas no se limita a la creación de planes y protocolos, sino que también incluye un proceso de monitoreo y actualización continua para asegurar su eficacia y relevancia a lo largo del tiempo. La dinámica naturaleza de las amenazas cibernéticas y los cambios en el entorno operativo de las infraestructuras críticas requiere una adaptación constante de las estrategias de recuperación. A continuación, se destacan aspectos clave:

Supervisión de Indicadores de Rendimiento: Establecer indicadores clave de rendimiento (KPIs) y métricas específicas para evaluar la eficacia de los planes de recuperación. Estos indicadores pueden incluir tiempos de recuperación, costo de la recuperación, nivel de impacto en las operaciones y otros factores relevantes.

Monitoreo de Amenazas Emergentes: Mantenerse al tanto de las amenazas emergentes es esencial para adaptar los planes de recuperación. El monitoreo constante

[58] Centro Nacional de Protección de Infraestructuras Críticas. (2022). Guía de buenas prácticas Plan de Protección Específico (PPE). Recuperado de https://cnpic.interior.gob.es/opencms/pdf/publicaciones/guias-y-metodologias/2.GUIA-BUENAS-PRATICAS-PPE.pdf

Global Forum of Cyber Expertise. (2016, noviembre). Guía de buenas prácticas de GFCE-MERIDIAN sobre protección de infraestructuras críticas de la información para responsables de políticas gubernamentales. Recuperado de https://www.meridianprocess.org/siteassets/web_106011_tno_brochure-good-practice-guide---spaans-def.pdf

de nuevas amenazas cibernéticas y tendencias en el ciberespacio permite a las organizaciones estar preparadas para los desafíos futuros.

Evaluación de Ejercicios y Eventos Previos: Después de cada ejercicio de recuperación o evento adverso real, realizar una revisión exhaustiva para identificar áreas de mejora. Estos aprendizajes deben incorporarse en los planes de recuperación para futuras iteraciones.

Actualización de Protocolos y Procedimientos: Los planes de recuperación deben actualizarse regularmente para reflejar cambios en la infraestructura crítica, tecnología, regulaciones y amenazas. Esto garantiza que los procedimientos estén alineados con la realidad operativa.

Formación Continua: Proporcionar formación continua al personal involucrado en la recuperación. La capacitación constante asegura que los equipos estén al tanto de los últimos protocolos y tecnologías de recuperación.

Revisión Legal y Normativa: Evaluar si los planes de recuperación cumplen con las leyes y regulaciones vigentes en Argentina. Las actualizaciones normativas pueden requerir modificaciones en los procedimientos de recuperación.

Colaboración con la Comunidad de Ciberseguridad: Mantener una colaboración activa con la comunidad de ciberseguridad en Argentina y participar en grupos de trabajo y foros donde se compartan las mejores prácticas y lecciones aprendidas.

Simulaciones de Actualización: Realizar simulaciones periódicas para probar la eficacia de las actualizaciones en los planes de recuperación. Esto ayuda a identificar posibles deficiencias antes de enfrentar una crisis real.

Auditorías de Terceros: Considerar la realización de auditorías de terceros para evaluar la efectividad de los planes de recuperación y garantizar la objetividad en la revisión.

Estos procesos aseguran que los planes se mantengan relevantes y efectivos en un entorno que evoluciona constantemente.

6.1.5 Evaluación de Resultados

Una vez que se han implementado planes de recuperación y se han realizado pruebas y simulaciones, es fundamental evaluar la efectividad de estas medidas, para esto es importante definir indicadores de rendimiento clave (KPIs)[59] que permitan medir el éxito de las estrategias de recuperación. Estos KPIs pueden incluir tiempos de recuperación, capacidad de respuesta a incidentes, minimización de pérdidas económicas y otros factores relevantes.

Recopilar datos y métricas durante y después de la implementación de los planes de recuperación. Esto puede incluir información sobre el tiempo de recuperación real, el costo de la recuperación y la eficacia de las estrategias implementadas.

Comparar los resultados obtenidos con los objetivos establecidos en la planificación de la recuperación. Evaluar si se lograron los objetivos y, en caso contrario, identificar las áreas que requieren mejoras.

Realizar un análisis post-incidente en casos en los que se haya producido un evento adverso. Esto implica evaluar cómo se manejó el incidente, si se cumplieron los plazos de recuperación y si se implementaron medidas correctivas eficaces.

---

[59] Roncancio, G. (s.f.). ¿Qué son indicadores de gestión o desempeño (KPI) y para qué sirven? Recuperado de https://gestion.pensemos.com/que-son-indicadores-de-gestion-o-desempeno-kpi-y-para-que-sirven

Obtener feedback de las partes interesadas involucradas en la recuperación, como el personal interno, las autoridades gubernamentales y las organizaciones asociadas. Sus comentarios pueden proporcionar información valiosa sobre áreas de mejora.

Utilizar los resultados de la evaluación para el aprendizaje continuo. Identificar lecciones aprendidas y áreas de mejora y aplicar estas lecciones a la revisión y mejora de los planes de recuperación existentes.

Evaluar la eficiencia en el uso de recursos durante la recuperación. Esto incluye la gestión de costos y la asignación eficaz de recursos humanos y técnicos.

Considerar cómo los resultados de la evaluación afectan la adaptación de los planes de recuperación a escenarios cambiantes. Las amenazas y riesgos cibernéticos evolucionan constantemente, por lo que la planificación debe ser ágil y adaptable.

Documentar los resultados de la evaluación en informes detallados. Estos informes deben incluir hallazgos clave, recomendaciones y planes de acción para la mejora continua.

Comunicar los resultados de la evaluación a todas las partes interesadas pertinentes. Esto incluye a la alta dirección de la organización, el personal involucrado en la recuperación y las agencias gubernamentales relevantes.

Al medir y analizar el rendimiento, las organizaciones pueden adaptarse a desafíos cambiantes, fortalecer su resiliencia y garantizar la continuidad de operaciones.

En este capítulo, hemos explorado en detalle la planificación de la recuperación en infraestructuras críticas. Comenzamos identificando riesgos y vulnerabilidades, evaluando amenazas naturales y humanas, y analizando el impacto potencial en diversas industrias.

Luego, destacamos la importancia de desarrollar planes de recuperación sólidos, estableciendo objetivos claros y estrategias específicas. También resaltamos la necesidad de asignar roles y recursos, mantener una comunicación efectiva y realizar pruebas regulares para garantizar la eficacia de estos planes.

La sección de monitoreo y actualización continua subraya la importancia de adaptarse a un entorno de amenazas en constante cambio, actualizando protocolos y capacidades de manera regular y basándose en lecciones aprendidas.

Finalmente, abordamos la evaluación de resultados, utilizando indicadores clave de rendimiento y datos recopilados para mejorar constantemente la capacidad de recuperación.

Las estrategias presentadas en este capítulo proporcionan un marco sólido para abordar estos desafíos y garantizar la resiliencia en infraestructuras críticas.

Discusión

Capítulo 7: Futuro de la Ciberseguridad en Infraestructuras Críticas.

En la constante evolución del panorama tecnológico, las infraestructuras críticas se han vuelto el núcleo vital de nuestras sociedades modernas. Estas redes complejas e interconectadas, que sustentan sectores cruciales como energía, transporte, salud y finanzas, están intrínsecamente ligadas a nuestra seguridad y bienestar. Sin embargo, su vulnerabilidad ante amenazas cibernéticas representa un desafío significativo que exige una reflexión profunda y estratégica sobre el futuro de la ciberseguridad en infraestructuras críticas.

7.1 Recapitulación de Hallazgos y Discusión Académica

A lo largo de este estudio, se han explorado detenidamente los desafíos y estrategias en la ciberseguridad de las infraestructuras críticas. En la investigación, se identificaron varios hallazgos significativos que arrojan luz sobre la complejidad y la importancia de este tema. Estos hallazgos han sido fundamentales para construir una comprensión profunda del panorama actual de la ciberseguridad en infraestructuras críticas y han proporcionado valiosas perspectivas para el futuro de esta área vital. La discusión académica se ha enriquecido con los siguientes puntos clave:

Vulnerabilidades Multidimensionales

Las infraestructuras críticas son vulnerables a una variedad de amenazas, desde ataques cibernéticos sofisticados hasta desastres naturales. Estas amenazas multidimensionales resaltan la necesidad de un enfoque integral que combine medidas tecnológicas, colaboración intersectorial y resiliencia operativa.

Interconexión y Dependencia

La interconexión de las infraestructuras críticas significa que un ataque dirigido a un sector puede tener efectos de cascada en otros sectores. Esta interdependencia subraya la importancia de la colaboración público-privada y la necesidad de estrategias de respuesta y recuperación ágiles y coordinadas.

Tecnologías Emergentes y Amenazas Avanzadas

La adopción de tecnologías emergentes, como la inteligencia artificial y la computación cuántica, ofrece oportunidades para fortalecer la ciberseguridad. Sin embargo, también presenta desafíos en forma de amenazas cibernéticas avanzadas que requieren soluciones igualmente sofisticadas y adaptativas.

Rol Crítico de la Educación y Concienciación

La educación continua y la concienciación son fundamentales para fortalecer la ciberseguridad en todos los niveles. La capacitación del personal y la sensibilización sobre las prácticas seguras en línea son esenciales para mitigar el factor humano, que a menudo es aprovechado por los ciberdelincuentes.

Colaboración Público-Privada y Regulaciones Éticas

La colaboración entre el sector público y privado es esencial para compartir inteligencia sobre amenazas y desarrollar estrategias de ciberseguridad efectivas. Además, las regulaciones éticas y legales son necesarias para garantizar la protección de los derechos individuales y la privacidad en un mundo cada vez más conectado.

7.2 Exploración de Tendencias y Desafíos Futuros en el Ámbito de la Ciberseguridad para Infraestructuras Críticas.

En la exploración de tendencias y desafíos futuros en el ámbito de la ciberseguridad para infraestructuras críticas, es crucial mirar hacia adelante para anticipar y prepararse para las amenazas y tecnologías que marcarán el panorama de la ciberseguridad en el futuro. Esta sección se centra en las proyecciones y desafíos que se vislumbran en el horizonte, delineando el curso que deben seguir las estrategias de seguridad.

Amenazas Cibernéticas Avanzadas:

Las amenazas cibernéticas están evolucionando hacia formas más sofisticadas y sigilosas. Los atacantes utilizan técnicas de inteligencia artificial y aprendizaje automático para eludir las defensas tradicionales. Las técnicas de intrusión se vuelven cada vez más sutiles y difíciles de detectar. Se prevé un aumento en los ataques impulsados por algoritmos que pueden adaptarse en tiempo real a las medidas de seguridad, lo que demandará soluciones de inteligencia artificial igualmente avanzadas para contrarrestarlos, enfocándose en técnicas de analisis de patrones de comportamiento, identificando anomalías y previendo posibles ataques antes de que ocurran.

Internet de las Cosas (IoT) y 5G:

La proliferación de dispositivos IoT y la implementación de tecnología 5G ampliarán el alcance de las infraestructuras críticas. Si bien estas tecnologías ofrecen innovaciones significativas, también introducen nuevos puntos de vulnerabilidad. Los dispositivos IoT mal protegidos y las redes 5G, aunque más rápidas, pueden ser

explotados por ciberdelincuentes para infiltrarse en sistemas críticos. La seguridad integrada en estas tecnologías será esencial para mitigar riesgos.

Amenazas Cibernéticas Nacionales y Ciberterrorismo:

Las amenazas cibernéticas patrocinadas por estados y el ciberterrorismo son riesgos en constante aumento. Los ataques que tienen como objetivo desestabilizar economías, servicios públicos o incluso la seguridad nacional son preocupaciones reales. La detección temprana y la respuesta rápida serán esenciales para minimizar el impacto de tales ataques.

Regulaciones y Normativas Evolutivas:

Las regulaciones en torno a la ciberseguridad seguirán evolucionando para abordar los desafíos emergentes. Se esperan leyes más estrictas y normativas específicas para diferentes sectores de infraestructuras críticas. Las organizaciones deberán estar al tanto de estos cambios y ajustar sus estrategias de seguridad en consecuencia para garantizar el cumplimiento.

Integración de Tecnologías Emergentes:

La adopción generalizada de tecnologías emergentes, como la computación cuántica y la inteligencia artificial, será inevitable en el ámbito de la ciberseguridad. Estas tecnologías, inteligencia artificial, el aprendizaje automático y la computación cuántica no solo serán parte de las defensas contra ataques cibernéticos, sino que también serán aprovechadas por los atacantes. La ciberseguridad deberá avanzar de la mano con estas tecnologías, integrándolas de manera efectiva en las estrategias de defensa.

Educación y Concienciación Continuas:

La educación y concienciación en torno a la ciberseguridad serán una defensa fundamental contra las amenazas. A medida que las tácticas de los ciberdelincuentes evolucionan, también lo deben hacer las habilidades y el conocimiento de los profesionales de la ciberseguridad. Programas de formación continuos y campañas de concienciación serán esenciales para mantenerse al día con las últimas amenazas y mejores prácticas. Las organizaciones invertirán en programas educativos continuos para asegurar que cada individuo sea un eslabón fuerte en la cadena de seguridad.

Desafíos Éticos en la Seguridad Cibernética:

Con el aumento de la vigilancia cibernética y la recopilación masiva de datos para la seguridad, surgirán desafíos éticos y legales relacionados con la privacidad y la supervisión. La sociedad deberá abordar estas cuestiones éticas para encontrar un equilibrio entre la seguridad y los derechos individuales. Las regulaciones y estándares éticos se fortalecerán para garantizar que las prácticas de ciberseguridad sean tanto efectivas como respetuosas con los derechos y libertades fundamentales de las personas.

Resiliencia y Recuperación Continuas:

La resiliencia se convertirá en un componente central de las estrategias de ciberseguridad. Las infraestructuras críticas no solo deben centrarse en la prevención, sino también en la capacidad de recuperación. La capacidad de responder rápidamente, aprender de los incidentes y adaptarse será crucial para mantener la integridad de las infraestructuras críticas en el futuro. La planificación de la recuperación se volverá aún más ágil y dinámica, adaptándose a los incidentes en tiempo real y aprendiendo de cada experiencia para fortalecer futuras defensas.

Colaboración Público-Privada: La colaboración entre entidades públicas y privadas será fundamental. La cooperación internacional en el intercambio de información sobre amenazas permitirá un entendimiento global de las tácticas y estrategias de los ciberdelincuentes. Las alianzas estratégicas entre gobiernos, organizaciones privadas y organismos internacionales conducirán a un enfoque más efectivo y coordinado contra las amenazas cibernéticas.

7.3 Propuestas para el Fortalecimiento de la Ciberseguridad en el Futuro.

Ante el panorama desafiante que se vislumbra en el futuro de la ciberseguridad en infraestructuras críticas, es imperativo formular estrategias sólidas y adaptativas. Estas propuestas están diseñadas para fortalecer la ciberseguridad en un entorno tecnológico en constante evolución y enfrentar las amenazas emergentes con determinación y eficacia.

El futuro de la ciberseguridad en infraestructuras críticas depende de la preparación, la colaboración y la innovación continua. Al invertir en tecnologías avanzadas, fomentar la colaboración público-privada, fortalecer la educación en ciberseguridad y mantener una mentalidad de mejora continua, las organizaciones pueden estar mejor equipadas para enfrentar las amenazas del futuro y salvaguardar las infraestructuras esenciales de nuestras sociedades. Estas propuestas proporcionan un camino hacia un futuro más seguro y resistente en el ámbito de la ciberseguridad.

Inversión Continua en Investigación y Desarrollo:

Es fundamental invertir en investigación y desarrollo para crear tecnologías de seguridad más avanzadas. Financiar programas de investigación que se centren en la

inteligencia artificial, el aprendizaje automático y la criptografía cuántica para anticipar y neutralizar amenazas cibernéticas sofisticadas.

Fomento de la Colaboración Público-Privada:

Establecer y fortalecer asociaciones entre el sector público y privado es esencial. La colaboración permite compartir inteligencia sobre amenazas, mejores prácticas y recursos. Las alianzas público-privadas facilitan una respuesta coordinada y efectiva ante ataques cibernéticos, aprovechando la experiencia y los recursos de ambos sectores.

Desarrollo de Estrategias de Resiliencia:

Las estrategias de resiliencia deben ser una prioridad. Esto implica no solo enfocarse en la prevención, sino también en la capacidad de recuperación. Desarrollar planes de respuesta efectivos, realizar simulacros regulares y aprender de los incidentes pasados para mejorar continuamente las respuestas a futuros ataques.

Promoción de la Educación en Ciberseguridad:

Fomentar la educación en ciberseguridad desde edades tempranas es esencial para formar la próxima generación de expertos en seguridad. Programas educativos sólidos, becas y oportunidades de formación continua deben estar disponibles para garantizar un flujo constante de profesionales capacitados en ciberseguridad.

Implementación de Estándares de Seguridad:

Establecer estándares de seguridad robustos y exigir su cumplimiento en todas las infraestructuras críticas es fundamental. Los estándares deben ser dinámicos, capaces de

adaptarse a las nuevas amenazas y tecnologías emergentes. La implementación debe ser rigurosa, con auditorías periódicas para garantizar el cumplimiento continuo.

Desarrollo de Capacidades de Gestión de Crisis:

Fortalecer las capacidades de gestión de crisis es esencial para una respuesta efectiva a eventos cibernéticos. Esto implica entrenar a equipos de respuesta, establecer canales de comunicación claros y coordinar con las autoridades gubernamentales. La capacidad de tomar decisiones rápidas y precisas durante un ataque es crucial para minimizar el impacto.

Fomento de la Concientización Pública:

Crear conciencia pública sobre las amenazas cibernéticas y las mejores prácticas de seguridad es fundamental. Campañas de concientización a nivel nacional pueden educar a las personas sobre las señales de phishing, la importancia de las contraseñas seguras y cómo proteger sus dispositivos, reduciendo así los vectores de ataque.

Evaluación y Mejora Continua:

Establecer un ciclo continuo de evaluación y mejora es esencial. Después de cada incidente, realizar evaluaciones exhaustivas para identificar áreas de mejora. Esta retroalimentación debe incorporarse en los planes de seguridad. La adaptabilidad y la capacidad de aprendizaje continuo son esenciales para enfrentar las amenazas en constante evolución.

Capítulo 8: Conclusiones.

En el transcurso de esta investigación exhaustiva sobre la ciberseguridad en las infraestructuras críticas, se han desentrañado las complejidades y desafíos que enfrentan las sociedades modernas en un entorno digitalmente interconectado. A través del análisis detallado de los diversos aspectos de la ciberseguridad y su aplicación específica en sectores vitales como energía, transporte, salud y finanzas, se han revelado valiosas perspectivas que arrojan luz sobre el camino a seguir para garantizar la integridad y la continuidad de nuestras infraestructuras cruciales.

Uno de los puntos centrales que emerge de esta exploración es la creciente sofisticación y diversificación de los ciberataques. Desde el phishing ingenioso hasta los ataques de denegación de servicio distribuido (DDoS) que pueden paralizar sistemas enteros, la amplitud de las amenazas exige respuestas igualmente variadas y adaptables. La comprensión profunda de las motivaciones detrás de estos ataques, ya sea el espionaje industrial, el cibercrimen o el activismo cibernético, se revela como un pilar esencial para anticipar y mitigar futuras intrusiones.

La prevención y la preparación también emergen como elementos cruciales en esta narrativa de seguridad digital. La implementación de tecnologías avanzadas, como firewalls y sistemas de detección de intrusiones, combinada con políticas de acceso y control de privilegios rigurosas, se presenta como una estrategia preventiva robusta. Sin embargo, el desarrollo de planes de contingencia meticulosamente elaborados y la capacidad de recuperación son igualmente esenciales. La planificación cuidadosa desde la identificación de riesgos hasta la realización de pruebas y simulaciones detalladas es un imperativo ineludible para garantizar la continuidad operativa en momentos de crisis.

Mirando hacia el futuro, esta investigación no solo ha delineado las tendencias emergentes, como el auge de la inteligencia artificial y la creciente sofisticación de los ataques, sino que también ha propuesto medidas concretas para fortalecer la ciberseguridad en las infraestructuras críticas. La inversión continuada en investigación y desarrollo, la promoción de la colaboración entre el sector público y privado, y la concientización pública son componentes vitales de una estrategia prospectiva.

En última instancia, este estudio subraya la urgencia de un enfoque integrado y proactivo hacia la ciberseguridad. En un mundo cada vez más digitalizado y amenazado, la colaboración intersectorial, la educación continua y la innovación tecnológica no son simplemente opciones, sino imperativos para salvaguardar nuestras infraestructuras críticas y garantizar la seguridad y la continuidad de nuestras sociedades. En este viaje hacia una seguridad digital resiliente, estas conclusiones sirven como faro, iluminando el camino hacia un futuro más seguro y resistente.

Referencias

Agrupación Empresarial Innovadora para la Seguridad de las Redes y los Sistemas de Información. (2012). *Protección de Infraestructuras Críticas* (p. 203). Recuperado de https://www.aeiciberseguridad.es/GuiaPIC.pdf

Aguirre Ponce, A. A. (2017). *Ciberseguridad en Infraestructuras Críticas de Información* (Tesis de maestría). Universidad de Buenos Aires, Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería. Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1115_AguirrePonceAA.pdf

argentina.gob.ar. (08 de 2022). *El ransomware, el software malicioso usado para atacar a las organizaciones*. Recuperado de https://www.argentina.gob.ar/sites/default/files/2022/08/el_ransomware_el_software_malicioso_usado_para_atacar_a_las_organizaciones.pdf

argentina.gob.ar. (2022). *Informe CERT.ar 2022*. Recuperado de https://www.argentina.gob.ar/sites/default/files/2023/02/informe_cert_2022.docx.pdf

Argentina.gob.ar. (2023, 16 de febrero). *Argentina y la Unión Europea unen esfuerzos para combatir el ciberdelito*. Recuperado de https://www.argentina.gob.ar/noticias/argentina-y-la-union-europea-unen-esfuerzos-para-combatir-el-ciberdelito

BID (Banco Interamericano de Desarrollo). (2023, 16 de enero). *Argentina busca reducir los costos de los ciberataques con apoyo del BID*. Recuperado de https://www.iadb.org/es/noticias/argentina-busca-reducir-los-costos-de-los-ciberataques-con-apoyo-del-bid

Blog Ciberseguridad. (2023). *Metodologías de evaluación de riesgos cibernéticos*. Recuperado de https://ciberseguridad.com/herramientas/metodologias-evaluacion-riesgos-ciberneticos/

Boletín Oficial de la República Argentina. (2019, 18 de septiembre). *Resolución 1523/2019, Anexo 1, párrafos 1-2*. Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

Boletín Oficial. (2019). *Resolución 1523/2019, Anexo 1, párrafos 1-2*. Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

Carlos GARAU PÉREZ-CRESPO. (2015). Recuperado de https://armada.defensa.gob.es/: https://armada.defensa.gob.es/archivo/rgm/2015/01/cap09.pdf

Castillo, G. (2023, 19 de julio). *Ciberseguridad en Argentina: situación actual, delitos más comunes y leyes*. Innovación Digital 360. Recuperado de https://www.innovaciondigital360.com/cyber-security/ciberseguridad-en-argentina-situacion-actual-delitos-mas-comunes-y-leyes/

CCN-CERT. (2016, abril 28). *Encontrados dos virus informáticos en la mayor central nuclear de Alemania*. Recuperado de https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/3752-encontrados-dos-virus-informaticos-en-la-mayor-central-nuclear-de-alemania.html

Centro Nacional de Protección de Infraestructuras Críticas. (2022). *Guía de buenas prácticas Plan de Protección Específico (PPE)*. Recuperado de https://cnpic.interior.gob.es/opencms/pdf/publicaciones/guias-y-metodologias/2.GUIA-BUENAS-PRATICAS-PPE.pdf

CEPAL (Comisión Económica para América Latina y el Caribe). (2023). *Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe* (p. 40). En R. M. Díaz y G. Núñez (Autores), Publicación de las Naciones Unidas LC/TS.2023/93. Copyright © Naciones Unidas, 2023. Todos los derechos reservados. Impreso en Naciones Unidas, Santiago. Número de documento: S.23-00614. Recuperado de https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

CEPAL (Comisión Económica para América Latina y el Caribe). (2023). *Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe* (p. 41). En R. M. Díaz y G. Núñez (Autores), Publicación de las Naciones Unidas LC/TS.2023/93. Copyright © Naciones Unidas, 2023. Todos los derechos reservados. Impreso en Naciones Unidas, Santiago. Número de documento: S.23-00614. Recuperado de https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

CEPAL (Comisión Económica para América Latina y el Caribe). (2023). *Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe* (p. 42). En R. M. Díaz y G. Núñez (Autores), Publicación de las Naciones Unidas LC/TS.2023/93. Copyright © Naciones Unidas, 2023. Todos los derechos reservados. Impreso en Naciones Unidas, Santiago. Número de documento: S.23-00614. Recuperado de https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

Ciberseguridad.com. (Fecha desconocida). *Metodologías de Evaluación de Riesgos Cibernéticos*. Recuperado de https://ciberseguridad.com/herramientas/metodologias-evaluacion-riesgos-ciberneticos/

Cointelegraph. (2016, noviembre). *Ransomware en sistema de transporte en San Francisco: nueva alerta de una creciente amenaza*. Recuperado de https://es.cointelegraph.com/news/ransomware-en-sistema-de-transporte-de-san-francisco-nueva-alerta-de-una-creciente-amenaza

Comisión Económica para América Latina (CEPAL). (2023). Obtenido de https://www.cepal.org/es: https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

Comisión Económica para América Latina y el Caribe (CEPAL). (2023). *Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe* (No. LC/TS.2023/93). Documentos de Proyectos. Santiago. Naciones Unidas. (S.23-00614) Recuperado de: https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

Common Attack Pattern Enumeration and Classification. (s.f.). *CAPEC-407: Pretexting attack*. Recuperado de https://capec.mitre.org/data/definitions/407.html

Congreso de la Nación Argentina. (2008). *Código Penal*. Ley 26.388. Modificación. Sancionada el 4 de junio de 2008. Promulgada de hecho el 24 de junio de 2008. Recuperado de https://www.oas.org/juridico/PDFs/arg_ley26388.pdf

CSIRT del Ministerio de Seguridad de la Nación. (2023). Recuperado de https://csirt.minseg.gob.ar/

Davidovsky, S. (2020, 10 de septiembre). Migraciones: cómo fue ataque del ransomware Netwalker. *La Nación*. Recuperado de https://www.lanacion.com.ar/tecnologia/migraciones-como-fue-ataque-del-ransomware-netwalker-nid2446451/

Diario El Mundo. (2017, mayo 12). Los hospitales de Reino Unido, en alerta por un ciberataque. *El Mundo*. Recuperado de https://www.elmundo.es/tecnologia/2017/05/12/5915cb15e5fdea24788b4658.html

Dirección Nacional de Ciberseguridad. (2022). *El ransomware, el software malicioso usado para atacar a las organizaciones*. Recuperado de https://www.argentina.gob.ar/sites/default/files/2022/08/el_ransomware_el_software_malicioso_usado_para_atacar_a_las_organizaciones.pdf

Dirección Nacional de Ciberseguridad. (2022). *Informe de Gestión CERT.ar 2022*. Recuperado de https://www.argentina.gob.ar/sites/default/files/2023/02/informe_cert_2022.docx.pdf

División Delitos Tecnológicos de la Policía Federal Argentina. (Fecha desconocida). Recuperado de https://www.argentina.gob.ar/servicio/denunciar-un-delito-informatico

EL CRONISTA. (11 de 08 de 2023). Recuperado de https://www.cronista.com/infotechnology/actualidad/alerta-pami-hackearon-los-sistemas-y-amenazan-con-publicar-todos-los-datos-de-los-afiliados/

Global Forum of Cyber Expertise. (2016, noviembre). *Guía de buenas prácticas de GFCE-MERIDIAN sobre protección de infraestructuras críticas de la información para responsables de políticas gubernamentales*. Recuperado de https://www.meridianprocess.org/siteassets/web_106011_tno_brochure-good-practice-guide---spaans-def.pdf

Gómez, J. A. (Sin fecha). *Ingeniería social: 6 consejos para proteger a tu empresa de su impacto*. *Delta Protect*. Recuperado de https://www.deltaprotect.com/blog/ingenieria-social

Harán, J. M. (2022, 6 de mayo). Ataque al sistema de tarjetas SUBE afecta la recarga. *WeLiveSecurity by ESET*. Recuperado de https://www.welivesecurity.com/la-es/2022/05/06/ataque-sistema-tarjetas-sube-afecta-recarga/

Hemsley, K. E., & Fisher, R. E. (2018, diciembre). *History of Industrial Control System Cyber Incidents* (p. 16). Recuperado de https://www.osti.gov/servlets/purl/1505628

Hemsley, K. E., & Fisher, R. E. (2018, diciembre). *History of Industrial Control System Cyber Incidents* (p. 4). Recuperado de https://www.osti.gov/servlets/purl/1505628

House of Commons Committee of Public Accounts. (2018, abril). *Cyber-attack on the NHS*. Recuperado de https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/787/787.pdf

Idaho National Laboratory. (12 de 2018). Recuperado de https://www.osti.gov: https://www.osti.gov/servlets/purl/1505628

INCIBE. (Fecha desconocida). *Plan de contingencia y continuidad de negocio*. Recuperado de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

Infobae. (2019, 17 de junio). Las redes eléctricas inteligentes a prueba por los hackeos. Recuperado de https://www.infobae.com/america/mundo/2019/06/17/las-redes-electricas-inteligentes-a-prueba-por-los-hackeos/

Infobae. (2022, 23 de octubre). Hackearon el sistema informático del Ministerio de Salud de la Nación. Recuperado de https://www.infobae.com/salud/ciencia/2022/10/23/hackearon-el-sistema-informatico-del-ministerio-de-salud-de-la-nacion/

Ingertec. (Fecha desconocida). *Norma IEC 62443*. Recuperado de https://ingertec.com/norma-iec-62443/

Instituto Nacional de Estándares y Tecnología (NIST). (2018, abril). *Marco para la mejora de la seguridad cibernética en infraestructuras críticas* (v1.1). Recuperado de https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

International Organization for Standardization. *ISO 27001: Gestión de la seguridad de la información*. Recuperado de https://www.normas-iso.com/iso-27001/

INTERPOL. (2020, 4 de agosto). *Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19*. Recuperado de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

Jefatura de Gabinete de la Ciudad de Buenos Aires. (2023). *Centro de Ciberseguridad*. Recuperado de https://buenosaires.gob.ar/jefaturadegabinete/centro-de-ciberseguridad

Jefatura de Gabinete de Ministros de la República Argentina. (2019, 24 de mayo). *Resolución 829/2019. Estrategia Nacional de Ciberseguridad - Aprobación*. Publicada en el Boletín Nacional del 28 de mayo de 2019. Recuperado de https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-829-2019-323594

Jefatura de Gabinete de Ministros de la República Argentina. (2019, 9 de mayo). *Resolución 141/2019. Delegaciones - Comité de Ciberseguridad*. Publicada en el Boletín Nacional del 13 de mayo de 2019. Recuperado de https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-141-2019-323038

Jefatura de Gabinete de Ministros de la República Argentina. *Normativa de Firma Digital*. Ley N° 25.506 de Firma Digital (Texto Actualizado). Reconoce y establece las condiciones para el empleo de la firma electrónica y de la firma digital y su eficacia jurídica, y crea la Infraestructura de Firma Digital de la República Argentina. Recuperado de https://www.argentina.gob.ar/jefatura/innovacion-publica/innovacion-administrativa/firma-digital/normativa-de-firma-digital

Jefatura de Gabinete de Ministros, Secretaría de Innovación Pública. (2023, 4 de septiembre). *Resolución 44/2023 (RESOL-2023-44-APN-SIP#JGM)*. *Boletín Oficial de la República Argentina*. Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904

JEFATURA DE GABINETE DE MINISTROS. (18 de 09 de 2019). *Boletín Oficial*. Obtenido de https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

Jefatura de Gabinete de Ministros. (2021, junio). Decisión Administrativa 641/2021 - Requisitos mínimos de Seguridad de la Información para Organismos. Boletín Oficial de la República Argentina. https://www.boletinoficial.gob.ar/detalleAviso/primera/246104/20210628

Justicia y Derechos Humanos de la República Argentina. (Fecha desconocida). *Acceso a la información pública*. Ley 27.275. Recuperado de https://www.argentina.gob.ar/justicia/derechofacil/leysimple/acceso-la-informacion-publica

Justicia y Derechos Humanos de la República Argentina. (Fecha desconocida). *Tratado de Asistencia Jurídica Mutua en Asuntos Penales, suscripto con el Gobierno de los Estados Unidos de América, aprobado por ley 24.034*. Recuperado de https://www.argentina.gob.ar/justicia/asuntosinternacionales/juridica-internacional-en-material-penal

Justicia y Derechos Humanos de la República Argentina. *Datos personales*. Ley de protección de datos personales o hábeas data te protege si tus datos de identidad, de salud o de crédito son usados sin tu consentimiento. Ley 25326. Recuperado de https://www.argentina.gob.ar/justicia/derechofacil/leysimple/datos-personales

Justicia y Derechos Humanos de la República Argentina. *Delitos informáticos*. Los delitos informáticos ahora forman parte del Código Penal. Ley 26.388. Recuperado de https://www.argentina.gob.ar/justicia/derechofacil/leysimple/delitos-informaticos

Kamlofsky, J., Abdel Masih, S., Colombo, H., Milio, C., & Hecht, P. (Sin fecha). Ciberseguridad en los Sistemas de Control Industrial: Clave para la Ciberdefensa de las Infraestructuras Críticas. Universidad Abierta Interamericana. Recuperado de http://sedici.unlp.edu.ar/bitstream/handle/10915/77258/Documento_completo.%20Clave%20para%20la%20Ciberdefensa%20de%20las%20Infraestructuras%20Cr%C3%ADticas.pdf-PDFA.pdf?sequence=1&isAllowed=y

Kaspersky. (2023). ¿Qué es el ransomware WannaCry? Recuperado de https://www.kaspersky.es/resource-center/threats/ransomware-wannacry

Kippeo. (Fecha desconocida). Ciberseguridad en la automatización industrial. Recuperado de https://kippeo.com/ciberseguridad-en-la-automatizacion-industrial/

Kyndryl. (s.f.). What is a disaster recovery plan and how does it work? Recuperado de https://www.kyndryl.com/es/es/learn/disaster-recovery-plan

LA NACION. (10 de 09 de 2020). Recuperado de https://www.lanacion.com.ar/tecnologia/migraciones-como-fue-ataque-del-ransomware-netwalker-nid2446451/

Lipovsky, R. (2017, 20 de junio). Sistemas industriales en la mira. *WeLiveSecurity by ESET*. Recuperado de https://www.welivesecurity.com/la-es/2017/06/20/sistemas-industriales-en-la-mira/

Lisa Institute. (Fecha desconocida). Ciberguerra: tipos, armas, objetivos y ejemplos de la guerra tecnológica. Recuperado de https://www.lisainstitute.com/blogs/blog/ciberguerra-tipos-armas-objetivos-ejemplos

Mendoza, M. Á. (2022, 21 de diciembre). Ciberataques a infraestructuras críticas: tendencias en ciberseguridad. *WeLiveSecurity by ESET*. Recuperado de https://www.welivesecurity.com/la-es/2022/12/21/ciberataques-infraestructuras-criticas-tendencias-ciberseguridad/

Microsoft. (2023). ¿Qué es un ciberataque? Recuperado de https://www.microsoft.com/es-ar/security/business/security-101/what-is-a-cyberattack

Ministerio del Interior. (2020, 27 de agosto). Migraciones contuvo un intento de ciberataque. *Argentina.gob.ar*. Recuperado de: https://www.argentina.gob.ar/noticias/migraciones-contuvo-un-intento-de-ciberataque

Ministerio Público Fiscal CABA. Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas (UFEDyCI). (2023). Recuperado de https://mpfciudad.gob.ar/tematicas/2020-03-09-18-42-38-delitos-informaticos

Ministerio Público Fiscal. Unidad Fiscal Especializada en Ciberdelincuencia (UFECI). (2023). Recuperado de https://www.mpf.gob.ar/ufeci/

Mueller, P., & Yadegari, B. (2012). *Stuxnet Worm*. Universidad de Arizona. Recuperado de https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf

National Institute of Standards and Technology. (Fecha desconocida). *Cybersecurity Framework*. Recuperado de https://www.nist.gov/cyberframework

ODS Open Data Security. (2020, 27 de agosto). Ciberseguridad en las infraestructuras críticas. *Ciberseguridad para empresas, Noticias sobre ciberseguridad*. Recuperado de https://opendatasecurity.io/ciberseguridad-en-las-infraestructuras-criticas/

Organización de los Estados Americanos. (2019). *Ciberseguridad Marco NIST: Un abordaje integral de la Ciberseguridad*. Recuperado de https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Poder Ejecutivo Nacional. (2017, 28 de julio). *Decreto 577/2017. Comité de Ciberseguridad. Creación*. Publicado en el Boletín Nacional del 31 de julio de 2017. Recuperado de https://www.argentina.gob.ar/normativa/nacional/decreto-577-2017-277518

Poder Ejecutivo Nacional. (2019, fecha desconocida). *Decreto 480/2019. Modificación del Decreto N° 577/2017*. Publicado en el Boletín Oficial. Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/211277/20190712

Revista UNE. (06 de 2019). Recuperado de https://revista.une.org/15/ciberataques-dirigidos-a-infraestructuras-criticas.html

Rogers, C. (2021, diciembre). Pruebas de recuperación ante desastres: puede salvar su negocio. *Zerto*. Recuperado de https://www.zerto.com/blog/disaster-recovery/disaster-recovery-testing-it-may-just-save-your-business/

Roncancio, G. (s.f.). ¿Qué son indicadores de gestión o desempeño (KPI) y para qué sirven? Recuperado de https://gestion.pensemos.com/que-son-indicadores-de-gestion-o-desempeno-kpi-y-para-que-sirven

Secretaría de Innovación Tecnológica del Sector Público. (2022). *El ransomware, el software malicioso usado para atacar organizaciones*. Recuperado de: https://www.argentina.gob.ar/sites/default/files/2022/08/el_ransomware_el_software_malicioso_usado_para_atacar_a_las_organizaciones.pdf

Stillman, A., & do Rosario, J. (2019, 17 de junio). El apagón masivo de Argentina se produjo por un "ataque cibernético"? *El Perfil*. Recuperado de https://www.perfil.com/noticias/bloomberg/bc-argentina-no-descarta-ataque-cibernetico-en-apagon.phtml

Téllez Tejada, N. (2023, 18 de enero). IoT y la infraestructura crítica, en el foco de la preocupación de la ciberseguridad industrial y de gobierno. *TeleSemana*. Recuperado de https://www.telesemana.com/blog/2023/01/18/iot-y-la-infraestructura-critica-en-el-foco-de-la-preocupacion-de-la-ciberseguridad-industrial-y-de-gobierno/

UNDRR. (Fecha desconocida). *Principios para la Infraestructura Resiliente*. Recuperado de https://www.undrr.org/media/86825/download?startDownload=true

UNE. (2019). Ciberataques dirigidos a infraestructuras críticas. En Michael A. Mullane (Ed.), *UNE, Nº 15, junio de 2019*. Recuperado de https://revista.une.org/15/ciberataques-dirigidos-a-infraestructuras-criticas.html

United Nations Office of Counter-Terrorism. (2018). *The protection of critical infrastructures against terrorist attacks: Compendium of good practices*. Recuperado de https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf

University of Arizona. (2012). Obtenido de https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf

Utsupra. (Fecha desconocida). *Doctrina | Origen: Argentina*. Citar como: Protocolo A00399486169 de Utsupra. Recuperado de http://server1.utsupra.com/doctrina1?ID=articulos_utsupra_02A00399486169