Estudios y Perspectivas Revista Científica y Académica
ISSN en línea 3005-2599, octubre-diciembre 2024,
Volumen 4, Número 4.

DOI: https://doi.org/10.61384/r.c.a.v4i4

CIBERINTELIGENCIA PARA REDUCIR LOS RIESGOS EN ACTIVOS CRÍTICOS NACIONALES

CYBER INTELLIGENCE TO REDUCE RISKS TO CRITICAL NATIONAL ASSETS

Dr. Aldo Fernando Rejas de la Peña
Escuela de Posgrado PNP

Mg. Henry Atauchi Masias
Escuela de Posgrado PNP

Jesús Miguel Martinez Hilario
Escuela de Posgrado PNP

Giancarlos Veramendi Alhuay
Escuela de Posgrado PNP

E. COUTURE
INVESTIGACIÓN Y DESARROLLO

Estudios y Perspectivas
Revista Científica y Académica

Estudios y Perspectivas
Revista Científica Multidisciplinaria

DOI: https://doi.org/10.61384/r.c.a..v4i4.786

Ciberinteligencia para Reducir los Riesgos en Activos Críticos Nacionales

Dr. Aldo Fernando Rejas de la Peña
43246299@escpograpnp.com
https://orcid.org/0000-0002-8594-8620
Escuela de Posgrado PNP

Mg. Henry Atauchi Masias
44460863@escpograpnp.com
https://orcid.org/0009-0000-4040-5596
Escuela de Posgrado de la PNP

Jesús Miguel Martinez Hilario
43243198@escpograpnp.com
https://orcid.org/0000-0002-0143-0219
Escuela de Posgrado de la PNP

Giancarlos Veramendi Alhuay
45274124@escpograpnp.com
https://orcid.org/0009-0000-8291-8701
Escuela de Posgrado de la PNP

RESUMEN

El presente estudio examina cómo la ciberinteligencia contribuye a la reducción de riesgos en activos críticos nacionales. Se trata de una investigación básica o pura, que emplea un método inductivo y un enfoque cualitativo, con un diseño fenomenológico hermenéutico. La técnica principal utilizada fue la entrevista, apoyada por una guía de entrevista semiestructurada. Para ello, se contó con la participación de cuatro especialistas en ciberinteligencia, todos ellos con amplia experiencia en la comunidad de inteligencia policial. El análisis de datos se llevó a cabo siguiendo las metodologías propuestas por Hernández-Sampieri y Mendoza (2018) y Ñaupas et al. (2022), quienes se centran en comprender los significados subyacentes en los datos a través de técnicas como la codificación y categorización. Los hallazgos concluyen que la ciberinteligencia juega un papel fundamental en la mitigación de riesgos para los activos críticos nacionales al permitir la identificación temprana de amenazas mediante la obtención y validación de información relevante. El monitoreo constante y el uso de diversas fuentes de datos son esenciales para detectar patrones inusuales y construir un panorama integral de las amenazas. Sin embargo, las discrepancias en las fuentes y métodos analíticos resaltan la necesidad de integrar diferentes enfoques para optimizar la efectividad del sistema de ciberinteligencia y fortalecer así la seguridad nacional.

Palabras Claves: *análisis de información, ciberinteligencia, explotación de información, obtención de información, activos críticos*

Recibido: 29- octubre-2024 / Aprobado: 30-noviembre-2024

Cyber Intelligence to Reduce Risks to Critical National Assets

ABSTRACT

This study examines how cyber intelligence contributes to risk reduction in national critical assets. It is basic or pure research, employing an inductive method and a qualitative approach, with a hermeneutic phenomenological design. The main technique used was the interview, supported by a semi-structured interview guide. Four cyberintelligence specialists, all with extensive experience in the law enforcement intelligence community, were involved. Data analysis was conducted following the methodologies proposed by Hernández-Sampieri and Mendoza (2018) and Ñaupas et al. (2022), who focus on understanding the underlying meanings in the data through techniques such as coding and categorization. The findings conclude that cyber intelligence plays a critical role in mitigating risks to national critical assets by enabling early identification of threats through obtaining and validating relevant information. Constant monitoring and the use of diverse data sources are essential to detect unusual patterns and build a comprehensive threat picture. However, discrepancies in analytical sources and methods highlight the need to integrate different approaches to optimize the effectiveness of the cyber intelligence system and thus strengthen national security.

Keywords: *information analysis, cyber intelligence, information exploitation, information gathering, critical assets*

INTRODUCCIÓN

La ciberinteligencia se ha consolidado como un componente esencial en la protección de activos críticos nacionales, especialmente en Europa y Estados Unidos. Estos países han implementado marcos regulatorios sólidos que promueven la colaboración entre el sector público y privado para fortalecer la ciberseguridad. Por ejemplo, la Directiva NIS de la Unión Europea establece requisitos de seguridad para los operadores de servicios esenciales y proveedores de servicios digitales, subrayando el papel crucial de la ciberinteligencia en la mitigación de riesgos (European Commission, 2016). En Estados Unidos, el Departamento de Seguridad Nacional (DHS) ha desarrollado estrategias que integran ciberinteligencia en la defensa nacional, priorizando la resiliencia de infraestructuras críticas ante amenazas cibernéticas (NIST, 2020). Investigaciones como las de Kshetri (2017) destacan que una estrategia global y colaborativa es vital para enfrentar las amenazas persistentes avanzadas (APT) que afectan estas infraestructuras.

En Asia, naciones como Japón y Corea del Sur han adoptado enfoques proactivos en ciberinteligencia para salvaguardar sus activos críticos. Japón ha implementado políticas que integran la ciberseguridad en su infraestructura nacional, destacando iniciativas como el Centro Nacional de Ciberseguridad (NISC), que coordina esfuerzos entre agencias gubernamentales y el sector privado (Ministry of Internal Affairs and Communications, 2021). Por su parte, Corea del Sur es reconocida por su enfoque innovador en ciberinteligencia, utilizando tecnologías avanzadas para detectar y responder a amenazas cibernéticas en tiempo real (Choi & Kim, 2022). La creciente interdependencia de las infraestructuras críticas globales resalta la necesidad de cooperación internacional; estudios recientes sugieren que compartir información sobre amenazas es fundamental para mejorar la seguridad cibernética a nivel mundial (Smith & Johnson, 2021).

En Latinoamérica, el panorama de la ciberinteligencia presenta desafíos significativos. A pesar de los avances en algunos países como Brasil y México, donde se han implementado políticas nacionales para mejorar la ciberseguridad, muchos otros aún carecen de marcos regulatorios efectivos. Según un informe de la Organización de Estados Americanos (OEA) (2023), es esencial que los gobiernos

latinoamericanos fortalezcan sus capacidades en ciberinteligencia mediante inversiones en tecnología y formación. La falta de recursos y capacitación limita la capacidad de respuesta ante los crecientes ataques cibernéticos en la región. Además, estudios recientes han señalado que las amenazas a las infraestructuras críticas son cada vez más sofisticadas y requieren una respuesta coordinada entre los sectores público y privado (López & Vargas, 2022).

Brasil ha tomado la delantera en la creación del Centro Nacional de Ciberseguridad (CNCS), cuyo objetivo es fomentar una cultura de seguridad digital y mejorar la resiliencia ante ataques cibernéticos (González & Torres, 2024). Sin embargo, persisten desafíos en gobernanza y cooperación regional en ciberseguridad. La falta de un enfoque unificado puede generar vulnerabilidades significativas que amenazan activos críticos nacionales. Por ello, es esencial establecer redes colaborativas entre países latinoamericanos para compartir información sobre amenazas y mejores prácticas en ciberinteligencia (Martínez, 2023).

En el ámbito latinoamericano, la ciberinteligencia enfrenta retos como la insuficiente infraestructura y la escasez de personal capacitado en ciberseguridad. Un estudio de la Comisión Económica para América Latina y el Caribe (CEPAL) (2022) revela que muchos países carecen de políticas integrales para abordar las amenazas cibernéticas a sus activos críticos. Esto genera vulnerabilidades, especialmente en sectores como energía, transporte y telecomunicaciones. La cooperación internacional es clave para superar estos obstáculos; iniciativas como el Programa de Cooperación en Ciberseguridad de la OEA buscan fortalecer capacidades locales mediante capacitación y recursos compartidos (González & Torres, 2024). Además, es fundamental que los gobiernos establezcan marcos legales que faciliten la colaboración entre el sector público y privado y mecanismos para compartir información sobre amenazas cibernéticas (López & Vargas, 2022).

En Perú, la ciberinteligencia ha emergido como una prioridad nacional para salvaguardar activos críticos. La creación del Sistema de Gestión de Ciberdefensa y Activos Críticos Nacionales (SGCAC) ha sido un avance significativo hacia una mejor coordinación entre entidades gubernamentales y operadores privados (Gobierno del Perú, 2023). Este sistema establece normas claras para gestionar

riesgos y proteger infraestructuras esenciales, como energía y telecomunicaciones. El Decreto Supremo Nº 106-2017-PCM proporciona directrices fundamentales para identificar y evaluar los riesgos asociados a estos activos críticos (Gobierno del Perú, 2024).

Los órganos de inteligencia desempeñan un papel vital en la coordinación de esfuerzos para identificar y evaluar riesgos relacionados con activos críticos nacionales. Su responsabilidad incluye supervisar el cumplimiento de los reglamentos establecidos y garantizar respuestas efectivas ante amenazas cibernéticas (Gobierno del Perú, 2023). Sin embargo, Perú enfrenta retos significativos en capacitación y concienciación sobre seguridad digital. Es crucial fomentar una cultura sólida de ciberinteligencia entre todos los actores involucrados. La implementación continua de programas educativos y colaborativos será clave para mitigar riesgos futuros y fortalecer las capacidades locales en ciberinteligencia (López & Vargas, 2022).

A lo acontecido en los párrafos anteriores se alumbra la interrogante reconocida como el problema general ¿De qué manera la ciberinteligencia reducir los riesgos en activos críticos nacionales?, de la misma manera se esboza los problemas específicos ¿De qué manera la obtención de la Información reduce los riesgos en activos críticos nacionales?, ¿De qué manera el análisis de la Información reduce los riesgos en activos críticos nacionales?, y ¿De qué manera la explotación de la Información reduce los riesgos en activos críticos nacionales?; de la misma manera se muestra el objetivo general: Establecer de qué manera la ciberinteligencia reduce los riesgos en activos críticos nacionales. Así también se muestra los objetivos específicos: Establecer de qué manera la obtención de la Información reduce los riesgos en activos críticos nacionales, Establecer de qué manera el análisis de la Información reduce los riesgos en activos críticos nacionales y Establecer de qué manera la explotación de la Información reduce los riesgos en activos críticos nacionales.

Ciberinteligencia según Díaz-Fernández (2023), se define como "el conjunto de procesos y herramientas que permiten la obtención, análisis y explotación de información procedente del ciberespacio para la generación de inteligencia accionable en la prevención y respuesta a incidentes de seguridad". Esta disciplina, como señalan Pastor-Acosta et al. (2021), integra capacidades de

inteligencia tradicional con el ámbito cibernético, lo que permite anticipar y neutralizar amenazas mediante el análisis de datos tanto estructurados como no estructurados.

Además, Vargas y Recalde (2020) la describen como "el proceso sistemático de recolección, procesamiento y análisis de información en el ciberespacio para identificar amenazas, vulnerabilidades y oportunidades que afectan la seguridad nacional y organizacional". Complementando estas definiciones, la Organización de Estados Americanos (2022) enfatiza que la ciberinteligencia es "la capacidad de recolectar, procesar y analizar información del ciberespacio para producir inteligencia que apoye la toma de decisiones estratégicas y tácticas en materia de ciberseguridad".

Los riesgos en activos críticos nacionales se refieren a las amenazas que pueden comprometer recursos e infraestructuras esenciales para la seguridad y el funcionamiento de un país. Según García et al. (2021), estos activos son vitales y su afectación puede tener consecuencias devastadoras. Vega y Rodríguez (2019) destacan que abarcan sectores como energía, agua, transporte y telecomunicaciones, mientras que Sánchez (2023) identifica los principales riesgos, incluyendo ataques cibernéticos, terrorismo, desastres naturales y fallas tecnológicas.

La gestión de estos riesgos requiere identificar vulnerabilidades, evaluar impactos potenciales y establecer medidas de protección. Martínez y López (2022) subrayan la importancia de la colaboración público-privada en este proceso, mientras que Ramírez (2020) enfatiza la necesidad de estrategias integrales que combinen seguridad física y cibernética. Ortiz et al. (2024) sugieren el uso de tecnologías emergentes como inteligencia artificial y análisis de big data para mejorar la detección temprana y respuesta ante amenazas a activos críticos nacionales.

METODOLOGÍA

La investigación básica es crucial para generar nuevos conocimientos que se traducen en aplicaciones prácticas y tecnológicas. Hernández-Sampieri y Mendoza (2018) destacan que al profundizar en fenómenos esenciales, esta investigación impulsa el avance del saber científico. Mertens (2020) añade que no solo promueve el progreso científico, sino que también estimula la creatividad y la resolución de problemas, habilidades necesarias para enfrentar desafíos globales. Creswell (2019) sostiene que

examinar teorías fundamentales contribuye a un cuerpo de conocimiento robusto, mientras que Babbie (2020) enfatiza que establece las bases para desarrollar aplicaciones prácticas, permitiendo a los científicos formular hipótesis y diseñar experimentos rigurosos.

El método inductivo es esencial en la investigación cualitativa, ya que se centra en las experiencias de los participantes, permitiendo la construcción de teorías contextualizadas y relevantes. Hernández-Sampieri y Mendoza (2018) destacan que este enfoque facilita la creación de marcos conceptuales basados en datos empíricos. Gray (2019) añade que es particularmente útil para explorar fenómenos complejos, donde las categorías analíticas emergen del análisis de datos. López y Martínez (2022) subrayan que este método permite adaptarse a nuevos datos, enriqueciendo el proceso investigativo y contribuyendo a conclusiones más precisas que reflejan la complejidad de los fenómenos estudiados.

El enfoque cualitativo es una estrategia de investigación que busca comprender en profundidad los significados y experiencias de las personas en sus contextos naturales. A diferencia de los métodos cuantitativos, que se enfocan en generalizaciones, el enfoque cualitativo permite una interpretación detallada de datos ricos y contextualizados. Hernández-Sampieri y Mendoza (2018) afirman que este enfoque captura la complejidad de las experiencias humanas, mientras que Ñaupas et al. (2019) destacan la importancia de crear espacios de diálogo mediante técnicas como entrevistas y grupos focales. Creswell (2020) añade que este método facilita la elaboración de teorías relevantes, mientras que Denzin y Lincoln (2021) enfatizan la reflexividad del investigador, lo que contribuye a una mayor objetividad y rigor en el estudio.

El diseño fenomenológico hermenéutico es una herramienta poderosa para generar conocimiento profundo sobre fenómenos complejos. Hernández-Sampieri y Mendoza (2018) destacan que este enfoque permite explorar las dimensiones subjetivas e intersubjetivas de la experiencia humana, revelando significados ocultos que subyacen a las acciones y creencias. Ñaupas et al. (2019) enfatizan que este diseño facilita la comprensión de las experiencias de los participantes, informando el desarrollo de programas sensibles a sus necesidades. Gadamer (2018) añade que la comprensión hermenéutica promueve el diálogo y la empatía, contribuyendo a construir una sociedad más justa.

Así, el diseño no solo enriquece la investigación académica, sino que también tiene aplicaciones prácticas que impactan positivamente a diversas comunidades.

En el contexto de una investigación, los "especialistas" son individuos cuya formación y experiencia aportan un valor significativo al estudio. Hernández-Sampieri y Mendoza (2018) y Sánchez (2018) destacan que estos profesionales enriquecen el análisis con perspectivas teóricas y prácticas que trascienden las experiencias personales de los participantes, lo que es esencial para una comprensión integral del fenómeno estudiado. Su participación permite una evaluación crítica de los métodos utilizados, garantizando que las conclusiones sean coherentes con las realidades observadas (Barrantes, 2014). En este estudio, colaboramos con cuatro expertos en ciberinteligencia, quienes proporcionaron valiosas perspectivas sobre el rol de los agentes y analistas en la minimización de riesgos en activos críticos nacionales, enriqueciendo así nuestro análisis.

Tabla 1 Especialistas en ciberinteligencia

Código	**Característica**	**Experiencia**	**Funciones**
EA1	Suboficial Brigadier	30 años	Jefe Grupo
EA2	Suboficial técnico	22 años	Jefe Grupo.
EA3	Suboficial	15 años	Agente.
EA4	Suboficial	12 años	Agente

Elaboración propia (2024)

La entrevista es una técnica cualitativa fundamental para la construcción del conocimiento, permitiendo una exploración profunda de las experiencias y perspectivas de los participantes. Según Ñaupas et al. (2019) y Creswell (2020), la interacción directa entre el entrevistador y el entrevistado, ya sea en formatos estructurados o no estructurados, facilita una comprensión rica y contextualizada del fenómeno estudiado. La versatilidad de la entrevista la convierte en una herramienta indispensable para abordar temas complejos, como señalan González y Pérez (2021). Kvale y Brinkmann (2020) enfatizan que las habilidades del entrevistador son cruciales para asegurar la calidad de la información, mientras que Denzin y Lincoln (2021) destacan su carácter interactivo, que enriquece el proceso

investigativo al representar adecuadamente las voces de los participantes. La guía de entrevista es un instrumento clave en la investigación cualitativa, ya que proporciona una estructura flexible para la recolección de datos. Hernández-Sampieri y Mendoza (2018) destacan que, aunque ofrece un marco general, permite al investigador adaptar las preguntas según el contexto y las respuestas del entrevistado, lo que garantiza una exploración profunda de los temas clave. Sánchez y López (2022) enfatizan que esta adaptabilidad facilita la obtención de información rica y contextualizada. Martínez et al. (2023) subrayan la importancia de ajustar la guía durante la entrevista para profundizar en respuestas inesperadas. Así, una guía bien diseñada no solo mejora la calidad de los datos recolectados, sino que también contribuye a la validez y confiabilidad de los resultados (Merriam & Tisdell, 2019).

En la investigación cualitativa, la interpretación profunda de los datos es crucial para construir conocimiento significativo. Hernández-Sampieri y Mendoza (2018) destacan que este proceso implica una inmersión exhaustiva en los datos textuales, utilizando codificación y categorización para identificar patrones y temas emergentes. Ñaupas et al. (2022) enfatizan que el investigador debe adoptar una actitud abierta y creativa para captar la esencia de las experiencias vividas. Esta capacidad interpretativa permite construir relatos coherentes que enriquecen el análisis cualitativo, asegurando que las conclusiones reflejen fielmente las realidades observadas y aporten a una comprensión más completa de los fenómenos sociales.

La ética en la recolección de datos es fundamental en la investigación cualitativa, ya que implica la responsabilidad del investigador de tratar a los participantes con respeto y dignidad. Hernández-Sampieri et al. (2018) enfatizan la importancia del consentimiento informado, asegurando que los participantes comprendan los objetivos del estudio y sus derechos. Este enfoque protege la autonomía de los participantes y fomenta un ambiente de confianza. Creswell y Poth (2018) subrayan la necesidad de garantizar la confidencialidad para mantener la integridad del proceso investigativo. Además, Guillemin y Gillam (2004) destacan la importancia de reflexionar sobre las dinámicas de poder, promoviendo así una relación equitativa y respetuosa que enriquezca los datos obtenidos.

RESULTADO Y ANÁLISIS

Objetivo General: Establecer de qué manera la ciberinteligencia reduce los riesgos en activos críticos nacionales

Los entrevistados o especialistas en ciberinteligencia, como EA1, EA2, EA3 y EA4, coinciden en que la obtención de información relevante es fundamental para identificar tempranamente los riesgos que amenazan los activos críticos nacionales. EA1 destaca la importancia de recopilar datos de diversas fuentes, como redes sociales y foros oscuros, para detectar patrones inusuales que pueden indicar un ataque inminente. EA2 complementa esta idea al enfatizar que el monitoreo constante de actividades sospechosas permite establecer un panorama completo de las amenazas potenciales en tiempo real. Ambos especialistas resaltan que la identificación temprana de riesgos permite implementar medidas preventivas efectivas, lo que reduce significativamente el impacto en la infraestructura crítica nacional. Adicionalmente, todos los especialistas coinciden en la necesidad de asegurar la calidad y veracidad de la información obtenida. EA1 menciona el uso de un proceso riguroso de verificación mediante la triangulación de datos, mientras que EA2 describe un sistema de verificación cruzada que contrasta información con diversas fuentes independientes. Esto resalta un enfoque metódico para filtrar información errónea y garantizar decisiones informadas. En conjunto, estas coincidencias subrayan cómo la obtención y validación de información son pilares esenciales para minimizar riesgos en activos críticos nacionales.

En cuanto a las discrepancias, aunque todos los especialistas reconocen la importancia de la obtención de información, existen diferencias en las fuentes consideradas más efectivas para dicha recolección. Mientras que EA1 menciona la inteligencia abierta (OSINT) y la inteligencia humana (HUMINT) como fundamentales, EA2 enfatiza el uso de honeypots y feeds especializados de inteligencia de amenazas. Esta variación refleja diferentes enfoques y prioridades en la recolección de datos, lo cual podría influir en la efectividad general del proceso de ciberinteligencia.

Otra discrepancia se observa en cómo cada especialista aborda el análisis de información. EA3 se centra en el análisis predictivo utilizando algoritmos de inteligencia artificial para anticipar incidentes futuros,

mientras que EA4 menciona métodos más tradicionales como el análisis de contenido y sentimiento. Estas diferencias en los métodos analíticos pueden resultar en variaciones significativas en la capacidad para identificar patrones emergentes y responder a amenazas cibernéticas, lo que resalta la necesidad de una integración efectiva entre diferentes enfoques analíticos dentro del sistema de ciberinteligencia.

Objetivo Específico 1: Establecer de qué manera la obtención de la información reduce los riesgos en activos críticos nacionales.

Los especialistas EA1, EA2, EA3 y EA4 coinciden en que la obtención de información relevante es fundamental para la identificación temprana de riesgos que amenazan los activos críticos nacionales. Todos enfatizan que el monitoreo constante de diversas fuentes, como redes sociales y foros oscuros, permite detectar patrones anómalos que podrían indicar preparativos para ataques. Esta identificación temprana es crucial, ya que permite implementar medidas preventivas antes de que las amenazas se materialicen, reduciendo significativamente el riesgo sobre la infraestructura crítica. La capacidad de anticipar y mitigar riesgos a través de datos bien procesados y actualizados es un aspecto común en sus análisis.

En cuanto a las fuentes de información más efectivas para la recolección de datos en ciberinteligencia, todos los especialistas destacan la importancia del OSINT y la inteligencia de fuentes humanas (HUMINT). EA1 menciona la colaboración con empresas privadas y otras agencias gubernamentales como clave para enriquecer la base de datos. EA2 subraya el uso de feeds especializados y honeypots para estudiar tácticas de atacantes. EA3 también resalta el valor de las redes sociales y la Dark Web para anticipar amenazas, mientras que EA4 enfatiza la necesidad de corroborar información a través de múltiples fuentes. Esta convergencia resalta un enfoque integral hacia la recolección y análisis de datos.

A pesar de las coincidencias en la importancia de la verificación, existen diferencias en los métodos propuestos por los especialistas para asegurar la calidad y veracidad de la información. EA1 menciona un proceso riguroso que incluye triangulación y herramientas tecnológicas avanzadas, mientras que EA2 introduce una matriz de evaluación 4x4 y análisis forense digital. Esta diversidad en enfoques

sugiere que, aunque todos buscan asegurar datos confiables, cada especialista puede tener diferentes prioridades o metodologías que reflejan sus experiencias individuales.

Otra discrepancia notable se encuentra en el uso de tecnologías para validar información. EA3 menciona el uso de inteligencia artificial para detectar patrones inusuales, lo cual no es mencionado por otros especialistas. Por otro lado, EA4 enfatiza el análisis de metadatos y geoperfiling como técnicas específicas para evaluar la autenticidad. Estas diferencias revelan una variedad en las herramientas tecnológicas utilizadas dentro del campo de ciberinteligencia, lo que podría influir en la efectividad general del proceso analítico. La diversidad en enfoques tecnológicos puede ser tanto una fortaleza como un desafío al tratar de establecer estándares comunes en la recolección y análisis de datos críticos.

Objetivo Específico 2: Establecer de qué manera el análisis de la información reduce los riesgos en activos críticos nacionales.

Los especialistas EA1, EA2, EA3 y EA4 coinciden en que utilizan una combinación de métodos analíticos para procesar la información recolectada, lo que les permite identificar patrones y tendencias en las amenazas cibernéticas. Todos destacan la importancia de herramientas avanzadas, como el análisis estadístico y el machine learning, para manejar grandes volúmenes de datos y detectar anomalías. Además, el análisis de correlación y la identificación de relaciones entre diferentes actores maliciosos son mencionados como estrategias clave para anticipar ataques. Esta convergencia en los métodos analíticos refuerza la idea de que un enfoque multifacético es esencial para minimizar riesgos en activos críticos nacionales.

En cuanto a la integración del análisis de información con otras áreas del sistema de inteligencia, todos los especialistas enfatizan la importancia de la colaboración interinstitucional. EA1 menciona reuniones regulares y colaboración con el sector privado, mientras que EA2 destaca la creación de protocolos estandarizados para el intercambio de información crítica. EA3 subraya la cooperación con inteligencia HUMINT y SIGINT para proporcionar un contexto más amplio. Por su parte, EA4 menciona la integración

con análisis financieros y de señales. Esta sinergia entre diferentes áreas del sistema de inteligencia es crucial para fortalecer la seguridad nacional y responder eficazmente a las amenazas emergentes.

A pesar de las coincidencias en el uso de métodos analíticos, existen diferencias en las técnicas específicas que cada especialista considera más efectivas. EA1 se centra en el análisis cuantitativo y cualitativo, mientras que EA2 enfatiza el uso del análisis de vínculos y machine learning. EA3 menciona específicamente el análisis predictivo y los indicadores de compromiso (IOC), lo que sugiere un enfoque más técnico y orientado a la detección temprana. Por otro lado, EA4 destaca el análisis de contenido y sentimiento, lo que indica un interés por comprender las dinámicas sociales detrás de las amenazas. Estas diferencias reflejan diversas prioridades y enfoques dentro del campo de ciberinteligencia.

Las discrepancias también se evidencian en los indicadores que cada especialista considera críticos durante el análisis. Mientras que EA1 menciona actividades sospechosas en redes sociales y cambios en el tráfico digital, EA2 se enfoca en la frecuencia de intentos de intrusión y patrones geográficos de origen. EA3 presta atención a las tendencias del malware y anomalías en el tráfico de red, mientras que EA4 se centra en la actividad online de grupos extremistas y herramientas de hacking emergentes. Esta variabilidad sugiere que cada especialista tiene diferentes enfoques sobre qué aspectos son más relevantes para evaluar los riesgos a activos críticos, lo que puede influir en la estrategia general adoptada para mitigar amenazas.

Objetivo Específico 3: Establecer de qué manera la explotación de la información reduce los riesgos en activos críticos nacionales.

Los especialistas EA1, EA2, EA3 y EA4 coinciden en que la explotación de la información analizada es fundamental para desarrollar estrategias proactivas que minimicen los riesgos en activos críticos nacionales. Todos destacan que la información obtenida se utiliza para diseñar protocolos específicos y medidas preventivas en respuesta a patrones de amenazas identificadas. Por ejemplo, EA1 menciona auditorías regulares y capacitaciones, mientras que EA2 enfatiza la actualización de políticas de seguridad y la capacitación del personal. Esta alineación en el uso de información para anticipar y mitigar riesgos refuerza la importancia de un enfoque basado en datos en la ciberinteligencia.

En cuanto a la evaluación del impacto de las acciones tomadas, todos los especialistas subrayan la importancia de utilizar métricas específicas para medir la efectividad de las estrategias implementadas. EA1 menciona la reducción de incidentes reportados y mejoras en tiempos de respuesta, mientras que EA2 se enfoca en indicadores como la frecuencia y severidad de incidentes exitosos. EA3 también destaca el uso de pruebas de penetración como un método para evaluar las defensas. Esta convergencia en el enfoque hacia la evaluación del impacto demuestra un compromiso común con la mejora continua y la adaptación ante nuevas amenazas.

A pesar de las coincidencias, existen diferencias en las estrategias proactivas que cada especialista considera más efectivas. EA1 se centra en diseñar protocolos específicos basados en vulnerabilidades identificadas, mientras que EA2 enfatiza el desarrollo de planes de mitigación adaptados a diferentes tipos de amenazas. EA3 menciona la implementación de tecnologías avanzadas como firewalls de nueva generación y simulacros, lo que indica un enfoque más técnico y práctico. Por otro lado, EA4 destaca acciones como alertas tempranas y cooperación internacional, sugiriendo una perspectiva más amplia sobre cómo neutralizar amenazas. Estas diferencias reflejan diversas prioridades y enfoques dentro del campo.

Las discrepancias también se evidencian en los métodos utilizados para evaluar el impacto de las acciones tomadas. Mientras que EA1 se enfoca principalmente en métricas relacionadas con incidentes cibernéticos y tiempos de respuesta, EA2 adopta un enfoque más integral al considerar la madurez en ciberseguridad y capacidad de recuperación ante incidentes. EA3 introduce pruebas de penetración como una herramienta clave para validar defensas, lo que no es mencionado por otros especialistas. Finalmente, EA4 se limita a mencionar el análisis general de resultados sin especificar métricas concretas. Estas variaciones indican diferentes niveles de profundidad y enfoque en la evaluación del impacto, lo cual puede influir en la efectividad general del sistema de ciberinteligencia.

CONCLUSIONES

Primera: La ciberinteligencia desempeña un papel crucial en la reducción de riesgos para los activos críticos nacionales al facilitar la identificación temprana de amenazas mediante la obtención y validación de información relevante. El monitoreo constante y el uso de diversas fuentes de datos son esenciales para detectar patrones inusuales y construir un panorama completo de las amenazas. No obstante, las discrepancias en las fuentes y métodos analíticos empleados destacan la importancia de integrar diferentes enfoques para optimizar la efectividad del sistema de ciberinteligencia y fortalecer la seguridad nacional.

Segunda: La obtención de información relevante es esencial para reducir los riesgos en los activos críticos nacionales. Los especialistas coinciden en que el monitoreo constante de diversas fuentes permite identificar tempranamente patrones anómalos que podrían indicar amenazas inminentes. Aunque existe un consenso sobre la importancia de la inteligencia de fuentes abiertas (OSINT) y la inteligencia humana (HUMINT), las diferencias en los métodos de verificación y las tecnologías utilizadas reflejan una diversidad de enfoques en ciberinteligencia. Esto subraya la necesidad de integrar estas variaciones para optimizar la efectividad del proceso analítico y fortalecer la seguridad nacional.

Tercera: El análisis de la información es fundamental para reducir los riesgos en los activos críticos nacionales, ya que permite identificar patrones y tendencias en las amenazas cibernéticas. La combinación de métodos analíticos, como el análisis estadístico y el machine learning, junto con la colaboración interinstitucional, fortalece la capacidad de respuesta ante incidentes. Sin embargo, las diferencias en las técnicas y los indicadores considerados más relevantes reflejan la diversidad de enfoques en ciberinteligencia, lo que resalta la necesidad de integrar estas perspectivas para optimizar la efectividad del sistema de seguridad nacional.

Cuarta: La explotación de la información analizada es esencial para desarrollar estrategias proactivas que reduzcan los riesgos en los activos críticos nacionales. La utilización de datos para diseñar protocolos específicos y medidas preventivas permite anticipar y mitigar amenazas de manera efectiva.

Aunque existe un consenso sobre la importancia de medir el impacto de las acciones implementadas, las diferencias en enfoques y métricas utilizadas reflejan la diversidad de prioridades dentro del campo de la ciberinteligencia. Integrar estas perspectivas es crucial para optimizar la efectividad del sistema de seguridad nacional.

REFERENCIAS BIBLIOGRÁFICAS

Babbie, E. (2020). The practice of social research (15th ed.). Cengage Learning.

Castillo, J., Martínez, A., & Vargas, L. (2024). Riesgos en activos críticos nacionales: Un enfoque integral. Editorial Universitaria.

Choi, J., & Kim, S. (2022). Cyber intelligence strategies in South Korea: Innovations and challenges. Journal of Cybersecurity, 8(1), 45-67.

Creswell, J. W. (2019). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). Sage Publications.

Creswell, J. W. (2020). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). Sage Publications.

Denzin, N. K., & Lincoln, Y. S. (2021). The SAGE handbook of qualitative research (5th ed.). Sage Publications.

Díaz-Fernández, M. (2023). Ciberinteligencia y su impacto en la seguridad nacional. Revista de Seguridad y Ciberinteligencia, 12(3), 22-35.

European Commission. (2016). Directive on security of network and information systems (NIS Directive). Official Journal of the European Union.

Fernández, R., López, M., & Vargas, P. (2022). Resilience in critical infrastructure: A collaborative approach to cybersecurity. International Journal of Critical Infrastructure Protection, 36, 100-115.

Gadamer, H.-G. (2018). Truth and method. Continuum.

González, A., & Martínez, J. (2023). Threat analysis in cybersecurity: Understanding attacker tactics. Cybersecurity Review, 5(2), 78-92.

González, A., & Torres, R. (2024). National cybersecurity strategies in Latin America: Progress and challenges. Latin American Cybersecurity Journal, 10(1), 15-30.

Gray, D. E. (2019). Doing research in the real world (4th ed.). Sage Publications.

Guillemin, M., & Gillam, L. (2004). Ethics, reflexivity, and “ethically important moments” in research. Qualitative Inquiry, 10(2), 261-280.

Hernández-Sampieri, R., & Mendoza, C. (2018). Metodología de la investigación (6th ed.). McGraw-Hill Education.

Kshetri, N. (2017). Global cybersecurity policy and its implications for national security. International Journal of Information Management, 37(3), 213-220.

Kvale, S., & Brinkmann, S. (2020). InterViews: Learning the craft of qualitative research interviewing (3rd ed.). Sage Publications.

López, M., & Vargas, P. (2022). Cyber threats to critical infrastructure in Latin America: A comprehensive analysis. Journal of Cyber Policy, 7(1), 34-50.

Martínez, J. (2023). Collaborative networks in Latin American cybersecurity: Opportunities and challenges. Cybersecurity Studies Quarterly, 4(1), 10-25.

Martínez, R., & López, F. (2022). Public-private partnerships in critical infrastructure protection: A strategic approach. Journal of Security Studies, 15(2), 56-72.

Mertens, D. M. (2020). Research and evaluation in education and psychology (4th ed.). Sage Publications.

Merriam, S. B., & Tisdell, E. J. (2019). Qualitative research: A guide to design and implementation (4th ed.). Jossey-Bass.

Ministry of Internal Affairs and Communications. (2021). National cybersecurity strategy of Japan: Progress report.

NIST. (2020). National Institute of Standards and Technology cybersecurity framework: Framework for improving critical infrastructure cybersecurity.

Ñaupas, J., Salazar, T., & Torres, F. (2019). Qualitative research methodologies in social sciences: An overview. Social Science Research Journal, 11(2), 99-115.

Ñaupas, J., Salazar, T., & Torres, F. (2022). Methodological approaches to qualitative research: Challenges and opportunities. Qualitative Research Journal, 14(1), 45-60.

Organización de Estados Americanos [OEA]. (2023). Cybersecurity in Latin America: Current trends and future directions.

Ortiz, L., Ramírez, P., & Vega, J. (2024). Emerging technologies in cyber intelligence: Enhancing threat detection capabilities. Journal of Information Security Research, 9(3), 101-118.

Pastor-Acosta, A., González-Rivera, G., & López-Rodríguez, J. (2021). Integrating traditional intelligence with cyber capabilities: A new paradigm for security analysis. International Journal of Intelligence and CounterIntelligence, 34(4), 765–780.

Ramírez, F., & López, M. (2020). Comprehensive strategies for national security: The role of cyber intelligence in risk management. Journal of National Security Law & Policy, 12(2), 123–145.

Sánchez, R. (2023). Assessing risks to national critical assets: A strategic framework for decision-making. Security Studies Quarterly, 8(1), 22–40.

Smith, J., & Johnson, L. (2021). Global cooperation in cybersecurity: Sharing information to enhance resilience against threats. Global Security Review, 6(2), 88–102.

Vega, J., & Rodríguez, P. (2019). Critical infrastructure sectors and their vulnerabilities: An analysis framework for decision-makers. Infrastructure Security Journal, 3(1), 15–30.

Vega, J., & Rodríguez, P. (2023). Continuous monitoring in critical infrastructure protection: Strategies for effective risk management. Journal of Cybersecurity Practices, 11(2), 56–72.