FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

ANALISIS DE LA PERCEPCION EN LA INTEGRACION DE VISION E INTELIGENCIA ARTIFICIAL EN EL MONITOREO DE SEGURIDAD FISICA Y CIBERNETICA: CASO SERVICIO AEROPORTUARIO NACIONAL, HONDURAS, 2024

SUSTENTADO POR:

MARCIO JAVIER PAZ CARDONA

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN
GESTION DE TECNOLOGIAS DE LA INFORMACION

SAN PEDRO SULA, CORTES, HONDURAS, C.A.

ENERO, 2026

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTORA

ROSALPINA RODRíGUEZ

VICERRECTOR ACADÉMICO NACIONAL

JAVIER ABRAHAM SALGADO LEZAMA

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

DECANA FACULTAD DE POSTGRADO

ANA DEL CARMEN RETTALLY VARGAS

EVALUACION DE LA EFICACIA EN LA INTEGRACION DE VISION E INTELIGENCIA ARTIFICIAL EN EL MONITOREO DE SEGURIDAD FISICA Y CIBERNETICA: CASO SERVICIO AEROPORTUARIO NACIONAL, HONDURAS, 2024

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN

GESTION DE TECNOLOGIAS DE LA INFORMACION

ASESOR

JESÚS RICARDO RODRÍGUEZ RIVERA

MIEMBROS DE LA TERNA:

ALBA GABRIELA GARAY ROMERO
JUAN CARLOS ALMENDAREZ FLORES
CARLOS ROBERTO AMADOR

FACULTAD DE POSTGRADO

ANALISIS DE LA PERCEPCION EN LA INTEGRACION DE VISION E INTELIGENCIA ARTIFICIAL EN EL MONITOREO DE SEGURIDAD FISICA Y CIBERNETICA: CASO SERVICIO AEROPORTUARIO NACIONAL, HONDURAS, 2024

Marcio Javier Paz Cardona

Resumen

Este estudio examinó la percepción del personal del Servicio Aeroportuario Nacional (SAN) acerca de la integración de sistemas de visión e inteligencia artificial en el monitoreo de la seguridad cibernética y física en infraestructuras aeroportuarias de Honduras comprendidos en el año 2024. La investigación se ejecutó frente al aumento de amenazas hibridas que combinan riesgos físicos y digitales, así como las limitaciones de los sistemas tradicionales de vigilancia operados de una manera fragmentada. Por medio del diseño de estudio de caso, se recopilaron datos por medio de entrevistas semiestructuradas, triangulación de fuentes, y análisis documental con el fin de evaluar la eficacia percibida de los sistemas integrados ante la gestión de alertas manuales. Los resultados evidenciaron que la integración de estas tecnologías contribuye a una mejor detección oportuna de amenazas, mayor rapidez en la toma de decisiones operativas y reducción de falsos positivos. Sin embargo, se identificaron desafíos asociados por la falta de personal especializado, resistencia al cambio, limitaciones presupuestarias, y ausencia de protocolos estandarizados. El estudio concluyó que la adopción de soluciones integradas asentadas en inteligencia y visión artificial blinda la resiliencia operativa y la gestión integral del riesgo en el entorno aeroportuario.

Palabras claves: (Ciberseguridad, inteligencia artificial, monitoreo integrado, seguridad aeroportuaria, visión computacional)

GRADUATE SCHOOL

ANALYSIS OF PERCEPTION IN THE INTEGRATION OF VISION AND ARTIFICIAL INTELLIGENCE IN PHYSICAL AND CYBER SECURITY MONITORING: CASE STUDY OF THE NATIONAL AIRPORT SERVICE, HONDURAS, 2024

Marcio Javier Paz Cardona

Abstract

This study examined the perception of National Airport Service (SAN) personnel regarding the integration of vision and artificial intelligence systems in monitoring cybersecurity and physical security in Honduran airport infrastructure in 2024. The research was conducted in response to the increase in hybrid threats that combine physical and digital risks, as well as the limitations of traditional surveillance systems operated in a fragmented manner. Using a case study design, data was collected through semi-structured interviews, triangulation of sources, and document analysis to assess the perceived effectiveness of integrated systems in managing manual alerts. The results showed that the integration of these technologies contributes to better timely detection of threats, faster operational decision-making, and a reduction in false positives. However, challenges were identified due to a lack of specialized personnel, resistance to change, budgetary constraints, and the absence of standardized protocols. The study concluded that the adoption of integrated solutions based on intelligence and artificial vision strengthens operational resilience and comprehensive risk management in the airport environment.

Palabras claves: (Cybersecurity, artificial intelligence, integrated monitoring, airport security, computer vision)

DEDICATORIA

A Dios por darme la oportunidad de llegar hasta esta etapa de mi vida guiando cada día los pasos junto a las acciones que realizo con gran salud y bienestar.

A mis padres, Marcio Javier Paz y Dilcia Lizeth Cardona el cual han sido el motivo de seguir día a día mostrándome su apoyo incondicional desde el primer día de mi vida hasta la actualidad en el punto donde estoy ahora dándome ánimos y fuerzas para poder culminar esta etapa con éxito y orgullo.

A mi novia Yaileny Dayana Avelar López, por su apoyo incondicional en el transcurso de este proceso académico su motivación, paciencia y comprensión el cual fue un pilar importante en los momentos de mayor reto, gracias por creer en mí y alentarme a continuar inclusive en las dificultades.

A mi familia, el cual siempre estuvo en todo momento dándome consejos, orientándome con su apoyo en cada una de mis metas propuestas.

AGRADECIMIENTO

Primeramente, quiero dar gracias a mi Dios porque siempre estuvo a mi lado, guiándome por el buen camino, llenándome de bendiciones en mi vida universitaria. Gracias a él se ha logrado culminar esta gran etapa en mi vida, teniendo la certeza de que el siempre estará con nosotros en todos nuestros proyectos y metas.

A mis padres, hermanos por darme su apoyo incondicional durante todo el proceso de la maestría nunca dejando de creer en mi en ningún momento.

A mi novia agradezco profundamente, por mostrarme su constante comprensión y apoyo. Su motivación y compañía el cual fueron esenciales para culminar con éxito este trabajo académico.

A todos mis catedráticos por iluminar y compartir todo su conocimiento a lo largo de las diferentes clases correspondientes en mi vida universitaria.

Al ing. Jesús Ricardo Rodríguez Rivera por toda su ayuda, tiempo dedicado, consejos y asesoramiento en todo momento durante el desarrollo de este proyecto de investigación.

Gracias a todos.

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 INTRODUCCIÓN

> En el primer semestre de 2023, el malware de IoT a nivel mundial aumentó un 37 %, lo que resultó en un total de 77,9 millones de ataques, en comparación con los 57 millones de ataques del primer semestre de 2022. En promedio, cada semana el 54 % de las organizaciones sufren intentos de ciberataques dirigidos a dispositivos IoT. (Moore, 2022)

Las amenazas a la seguridad de las infraestructuras vitales se han encontrado en una evolución constante en una forma acelerada, por medio del cual se comparte más complejas y persistentes tanto en el ámbito cibernético y físico. En este contexto, los aeropuertos, describen instalaciones de alto valor por el papel estratégico en la movilidad de las personas, la conectividad y mercancías, en conjunto con el impacto directo en la seguridad y economía nacional. Esto lo convierte en el centro de atención ante amenazas o actos maliciosos que pueden comprometer la estabilidad y la continuidad operativa del país. Ante esta situación, las soluciones convencionales de monitoreo tienen como resultado insuficiente ante respuestas y detección con eficacia a situaciones de riesgo en tiempo real.

Chaki et al. (2010) hace la mención que la visión artificial es utilizada en el sector automotriz, farmacéutico y electrónico, caracterizado por su tolerancia donde es cero ante los defectos. Por lo tanto, a su vez reduce la dependencia de la visión humana, que es propensa a cometer diversos errores en diversas áreas que requieren de los más altos niveles de precisión.

La fusión de sistemas de inteligencia y visión artificial representan una innovación tecnológica clave en la robustez de los sistemas de respuesta y monitoreo ante amenazas. Estas tecnologías abren la posibilidad de hacer un análisis en tiempo real e identificar patrones con anomalías y por el cual pueden generar alertas automáticas mejorando de una manera significativa la capacidad de reaccionar al estar frente a eventos críticos.

Ramírez Pascual (2023) nos menciona que la inteligencia artificial existe hace más de 50 años, donde el termino de inteligencia artificial fue nombrado por primera vez al desarrollarse una conferencia de Dormouth en 1956. El cual empiezan a desarrollarse hasta finales de los 50 e inicios de los 60 con conceptos de chatbots o heurística los avances en el potencial de la informática han permitido que se presenten grandes avances respecto a la inteligencia artificial a través de los

últimos años.

En esa relación, la presente investigación tiene como determinación la evaluación y el análisis del impacto de la integración de visión e inteligencia artificiales en los procesos de monitoreo cibernético y físico del Servicio Aeroportuario Nacional (SAN). El estudio se centra en identificar como la aplicación de estas tecnologías salientes pueden fortalecer la protección de las instalaciones aeroportuarias, reduciendo vulnerabilidades y optimizando recursos proporcionando evidencias y fundamentos técnicos de una manera dinámica en la forma que sustenten sus beneficios y viabilidad.

Este documento se estructura en cinco capítulos, de tal manera el capítulo uno introduce el contexto, justificación, objetivos y el problema de la investigación. El capítulo dos se desenvuelve el marco teórico teniendo en consideración conceptos primordiales sobre visión, inteligencia artificial, ciberseguridad y protección física sobre infraestructuras aeroportuarias de alto valor, el capítulo tres hace referencia a la descripción de la metodología de investigación que se estará realizando, en el cual se incluyen las técnicas y diseños sobre recolección y análisis de los datos, el capítulo cuatro se analizan y presentan los resultados que se obtienen realizando la evaluación del impacto potencial de la integración tecnológica propuesta en el Servicio Aeroportuario Nacional y finalmente, el capítulo cinco argumenta las conclusiones y recomendaciones derivadas de la investigación, de igual manera probables líneas de investigación futuras.

1.2 ANTECEDENTES DEL PROBLEMA

Shaqwi et al. (2021) nos argumenta que la visión por computadora hace referencia al campo de la informática que se centra en las teorías y algoritmos para el procesamiento automático de la percepción visual, la visión por computadora implica diferentes niveles de tareas, como lo es la visión de nivel bajo el cual involucra numerosas tareas como ser el suavizado, la eliminación de ruido y el aumento del contraste. Y la visión de nivel intermedio tiene la implicación sobre la segmentación de imágenes con el objeto de tener la separación de los objetos y regiones mediante reconocimientos y descripción de regiones segmentadas, por lo tanto, un sistema de visión computacional debe de contar con todos los mecanismos necesarios que permitan una representación robusta.

Sin embargo, a pesar de que existe un desarrollo solido en estas técnicas existe una brecha en su aplicación integrada a los sistemas de monitoreo que hacen la combinación de un análisis

cibernético y físico en entornos de infraestructuras esenciales, como lo es los aeropuertos.

J. Li et al. (2020) hace la mención que la seguridad en las operaciones aéreas y los aeropuertos dominado gran interés, estableciendo la seguridad en un tema importante. Diversas personas resultan afectados al suscitarse un accidente y numerosos vuelos sufren retrasos o hasta incluso son cancelados.

No obstante, existe una abertura muy estrecha en el desarrollo de estrategias tecnológicas avanzadas que tengan la integración del monitoreo cibernético y físico para poder mitigar y prevenir los impactos que conllevan, principalmente en instalaciones como lo son los aeropuertos.

Z.-H. Chen & Juang (2018) nos explica que la inteligencia artificial reconoce automáticamente e identifica la ubicación del área y otras imágenes específicas de una manera independiente y ayudar a la torre del aeropuerto a planificar la ruta de manera que se reduzca la carga de trabajo humano, proporcionando un juicio apropiado para la reducción de la ocurrencia de errores y reducir eficazmente el número de accidentes en áreas críticas.

A pesar, de que los accidentes en aeropuertos suelen originarse por accesos no autorizados a áreas restringidas, de esa misma manera por la ejecución de tareas sin cumplir con los requisitos del equipo adecuado o seguridad, esto da la evidencia de una brecha fina en la ejecución de sistemas integrales de control y monitoreo que tengan la habilidad de detectar y prever incumplimientos operativos en tiempo real.

Zhang (2019) nos dice que más aeropuertos alrededor del mundo están usando el camino convencional para la seguridad de los aeropuertos, donde incluyen verificación de documentación y control de los pasajeros junto a su equipaje de carga. Ante las amenazas la aviación en constante evolución, algunas universidades y gigantes tecnológicos tienen la concentración en el desarrollo de la próxima generación de tecnología de inteligencia artificial esto en base para la elevación de la línea base para la seguridad en la aviación. Las técnicas de visión artificial se han visto limitadas debido a la funcionalidad cuando tiene su relación con el análisis de las imágenes, a pesar de eso los recientes avances en las redes neuronales y los chips informáticos de una alta capacidad san el acceso a que los sistemas de inteligencia artificial se fortalezcan.

Esto, aunque numerosos investigadores han explorado el uso de la inteligencia artificial para optimizar la automatización en diferentes sectores, aún perdura una exigencia por integrar

estas tecnologías con sistemas de monitoreo cibernético y físico para garantizar una supervisión preventiva y completa en infraestructuras esenciales, como lo son los aeropuertos.

1.3 DEFINICIÓN DEL PROBLEMA

Rakas et al. (2020) nos menciona que, de manera ordinaria, un sistema informático empresarial seguro debe de brindar lo siguiente, de acuerdo con un orden preferente: disponibilidad, confidencialidad e integridad. En el control de procesos un periférico puede llegar a tener la misma importancia un servidor en base de datos central.

Sin embargo, las plataformas relacionadas al monitoreo de ciberseguridad suelen operar de manera aislada, sin tener relación con el entorno físico, lo que impide una respuesta coordinada ante las amenazas que están presentes donde dan la combinación de elementos digitales como físicos. Erkek & Irmak (2025) nos hacen la mención de que la tecnología digital se ha venido convirtiendo en una herramienta poderosa para la diversidad, gestión de opciones y expansión de oportunidades, ofreciendo diversas innovaciones en el cambio de productos en los últimos años. Uniendo virtualmente sistemas internacionales, siendo utilizada en una amplia área de aplicaciones, como lo es la monitorización en tiempo real, la simulación, el análisis y el mantenimiento predictivo por el cual, en el presente, existe una línea importante en la integración de tecnologías avanzadas como la visión e inteligencia artificial.

La literatura existente contempla el papel de los sistemas de control automatizado en el área de los aeropuertos. Liu & Guan, (2010) nos dice que el papel de la gestión de la capacidad aeroportuaria (ACM) es significativamente especial. Existiendo diversos artículos que hacen estudios sobre el problema del ACM en un entorno estático. Incluso las herramientas desarrolladas en estos trabajos pueden emplearse para la planificación fuera de línea. Tomando en cuenta, en un ambiente real las condiciones y las demandas de tráfico del aeropuerto pueden presentar variación con el tiempo teniendo así dificultad de hacer una predicción con precisión.

Aunque advierten limitaciones en cuanto a capacidad y frecuencia de registro, lo que ocasiona brechas en la eficiencia de detección de incidentes vigorosos. Liu & Guan (2010) tienen una perspectiva de una manera diferente donde muestran tres formas intuitivas de explorar una estrategia de asignación sobre la capacidad aeroportuaria relacionada en un entorno dinámico. Donde la primera tiene su consistencia en la optimización de la asignación de capacidad mediante las herramientas, el segundo método basado en la optimización dinámica convencional para la

optimización del perfil de capacidad en un periodo comprendido y el tercero es el control retrospectivo. Esto rinde en las diferentes condiciones que llegan a centrarse los sistemas para monitoreo por medio de las soluciones inteligentes correlacionando los eventos del mundo digital en conjunto con el físico.

El grupo de hackers conocido como China 1937CN Team comprometió los sistemas de pantallas de anuncios de muchos aeropuertos importantes de Vietnam. Algunos expertos locales en seguridad también publicaron en sus páginas de Facebook algunas fotos que mostraban que la sección de pasajeros VIP del sitio web de Vietnam Airlines también había sido pirateada y desfigurada. No es la primera vez que China 1937CN Team ataca Vietnam. En mayo de 2015, el mismo grupo pirateó aproximadamente 1000 sitios web vietnamitas, incluidos 15 portales gubernamentales y 50 sitios educativos. En el mismo período, alrededor de 200 sitios web de Filipinas fueron atacados por los piratas informáticos de China 1937CN Team. (CYBER DEFENSE, 2016) No abordar esta problemática implica tener la presencia de vulnerabilidades latentes que pueden ser explotadas en cualquier instante.

Los sistemas que antes eran independientes y tenían sus propias redes se han integrado más con otros sistemas y los recursos de comunicación se comparten más. Lo que ha ocurrido es que, cuando se implementan nuevos sistemas para alcanzar un nivel de seguridad, a menudo se ha dado menos prioridad a los aspectos de seguridad. (Nystad et al., 2021) En particular, no existe un acondicionamiento de un framework que permita correlacionar de manera confiable y efectiva las alertas provenientes de los sistemas físicos como lo es la vigilancia por visión artificial en conjunto con alertas lógicas que provienen de monitoreo cibernético.

No todo el mundo habla de maravillas de estas nuevas tecnologías. Algunos citan implicaciones siniestras en las tecnologías que pueden espiar discretamente lo que está sucediendo sin nuestro permiso. Otros señalan que con el rápido aumento de las tecnologías biométricas y de imágenes, los días están contados. (Zhang, 2019) esta ausencia da limitación sobre la capacidad de detección temprana y la respuesta coordinada frente amenazas complejas que involucran ambos dominios.

Según la OACI, en la primera mitad de 2023 se produjo un aumento del 24 % en los ciberataques a la aviación en todo el mundo. Además, la tasa de ataques de malware únicos aumentó un 50 % entre octubre de 2022 y enero de 2023. Esto refleja la tendencia general en todos

los sectores, ya que los sistemas informáticos están cada vez más interconectados y las nuevas tecnologías, como el Internet de las cosas (IoT), presentan nuevos riesgos. (Zafire, 2024)

De este modo, el problema central de la investigación se arraiga en la insuficiencia de evidencia académica y empírica sobre la eficacia de integrar sistemas de inteligencia y visión artificial en el monitoreo conjunto de la seguridad física y cibernética en los aeropuertos. Esta grieta en la literatura sustenta la necesidad de un estudio crítico y sistemático con orientación a evaluar dicha combinación desde una perspectiva investigativa.

1.3 PREGUNTAS DE INVESTIGACION

PREGUNTA GENERAL

En el monitoreo de seguridad del aeropuerto (P), ¿La percepción de los sistemas de visión artificial en conjunto con plataformas de seguridad cibernética (I), en semejanza con la gestión manual de alertas (C), tiene reducción de manera significativa el tiempo de detección y respuesta ante las amenazas presentes (O)?

PREGUNTAS ESPECIFICAS

En entornos de escenarios sobre intrusión simulados en un aeropuerto (P), ¿La percepción del personal acerca de la implementación de un panel concentrado mediante la integración de alertas físicas y lógicas (I), en comparación con el uso de sistemas independientes (C), mejora la precisión y rapidez al momento de tomar decisiones en el periodo de incidentes de seguridad (O)?

En ambientes operativos de un aeropuerto (P), ¿La adaptación de inteligencia artificial aplicada al monitoreo de visión artificial y cibernético (I), en semejanza con los sistemas convencionales (C), contribuye a una rebaja percibida de falsos positivos en alertas de seguridad (O)?

En la infraestructura aeroportuaria (P), ¿La adquisición de sistemas integrados de monitoreo lógico y físico (I), en relación con sistemas fragmentados (C), el impacto es positivamente en la prolongación operativa y la mitigación de riesgos ambientales, económicos y sociales que están asociados a incidentes de seguridad (O)?

1.5 OBJETIVOS DE LA INVESTIGACION.

OBJETIVO GENERAL

Analizar (S) las percepciones del personal del Servicio Aeroportuario Nacional acerca de

la integración de sistemas de inteligencia y visión artificial en el monitoreo de seguridad cibernética y física, en comparación con la gestión manual de alertas, (M) identificando tendencias y patrones relacionados con la eficacia percibida en las respuestas y detección de amenazas, (A) por medio de análisis de contenido y aplicación de entrevistas, (R) con el fin de comprender el potencial de estas tecnologías en la mejora de procesos de seguridad aeroportuaria, (T) comprendido en el periodo de investigación 2024.

OBJETIVOS ESPECIFICOS

Explorar (S) la percepción del personal acerca de la efectividad de un panel integrado de alertas lógicas y físicas ante sistemas independientes, (M) por medio de las identificaciones de experiencias y opiniones recurrentes, (A) adhiriendo técnicas cualitativas de entrevista, (R) con el propósito de comprender su relación con la rapidez en la toma de decisiones, (T) en el entorno del año 2024.

Comprender (S) la percepción del uso de inteligencia artificial en el monitoreo de ciber seguridad y visión relacionado a la reducción de falsos positivos, (M) analizando las narrativas logradas en las entrevistas, (A) por medio de la interpretación de resultados, (R) para estipular la precisión de alertas de seguridad, (T) comprendido en el año 2024.

Describir (S) cómo el personal percibe el impacto de los sistemas integrados de monitoreo lógico y físico, (M) determinando temas claves enlazados con la mitigación de la continuidad y riesgos operativos, (A) por medio del análisis y recopilación de la testificación, (R) para reconocer su importancia en la gestión integral de seguridad aeroportuaria, (T) en el lapso de investigación 2024.

1.6 JUSTIFICACIÓN

La presente investigación es notable en términos prácticos al ser próximo a un sistema critico dentro del aeropuerto, la limitada capacidad de respuesta ante amenazas cibernéticas y físicas debido a sistemas de monitoreo fragmentados. En ese ámbito, resulta necesario examinar como la incorporación de inteligencia y visión artificial en plataformas de seguridad cibernética podría contribuir a la optimización sobre la detección temprana y la reducción de tiempos de respuesta ante incidentes, por el cual abre un campo de análisis sobre su potencial de impacto en la mitigación de riesgos económicos, ambientales y operativos, de la misma manera en la continuidad de los servicios aeroportuarios y la protección de la infraestructura y los pasajeros.

Desde una perspectiva teórica, esta investigación asistirá un marco metodológico validado para evaluar la eficacia de la integración de sistemas lógicos y físicos de seguridad, rellenando un vacío en la literatura académica sobre la interrelación de alertas hibridas en entornos críticos. Los resultados ayudaran como base para posteriores investigaciones en sistemas inteligentes de monitoreo y seguridad industrial.

Una revisión de los retos de ciberseguridad en la industria de la aviación a partir de 2022 reveló que el 71 % de los piratas informáticos se centraban en robar datos de inicio de sesión para acceder a los sistemas informáticos. De esos ataques, el 25 % eran ataques DDoS y el 4 % de los ciberdelincuentes tenían como objetivo corromper la integridad de los archivos.(Traynor, 2025)

En el ámbito social y empresarial, el análisis de modelos integrados de seguridad permitirá generar evidencia sobre el potencial para fortalecer la resiliencia del sector aeroportuario aumentando la confianza de los actores claves, comunidades y pasajeros en la seguridad de las operaciones aeroportuarias. De tal manera podría aportar evidencia útil para que las empresas aumenten su compromiso con la protección de infraestructuras de alto valor, por lo cual en estudios posteriores podría relacionarse con su confianza social y reputación. De forma adicional, incentivar el cumplimiento de los estándares internacionales en el área de seguridad informática industrial, alzando la competitividad del sector mediante la adopción de tecnologías de vanguardia con orientación a la mitigación y prevención de riesgos.

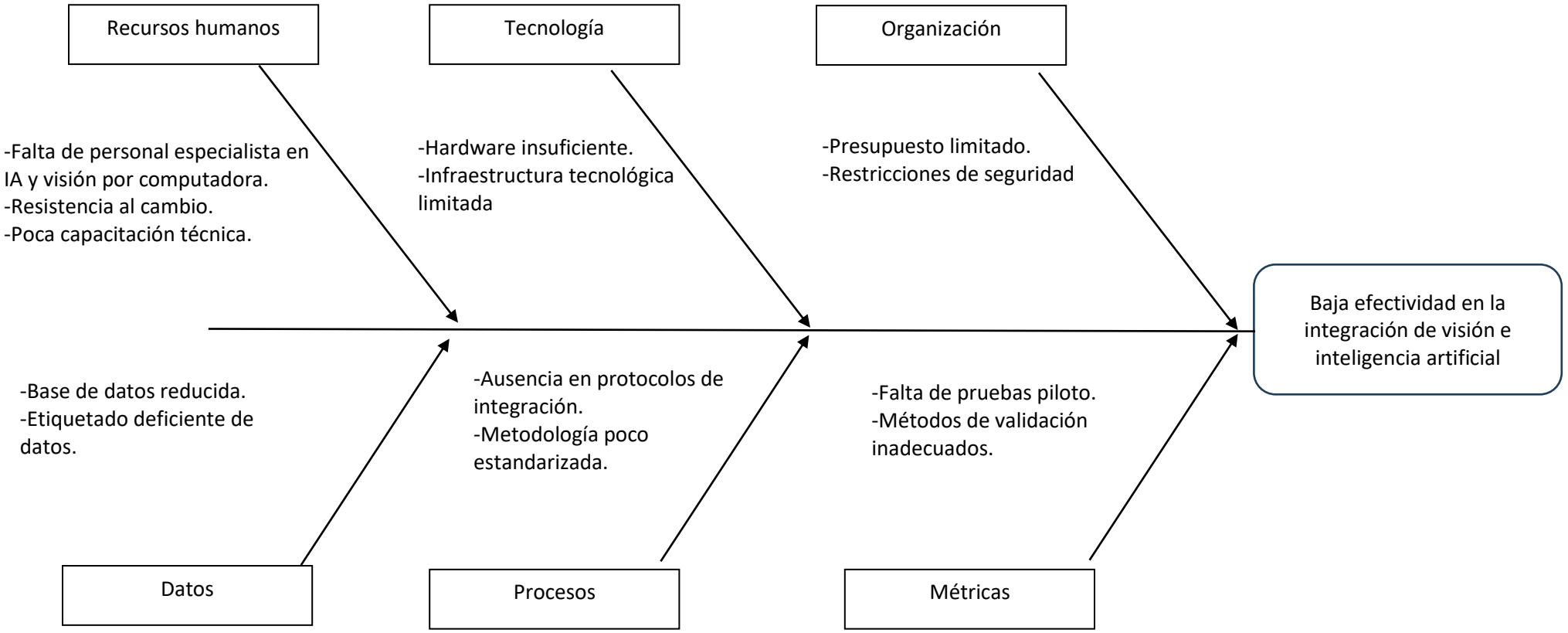


Figura 1. ACR

Fuente: Elaboración propia.

El diagrama causa raíz demostrado muestra los factores que contribuyen a la baja efectividad en la integración de inteligencia y visión artificial en el monitoreo de seguridad. Se contempla que los recursos humanos, como la falta de especialistas en visión por computadora e inteligencia artificial, la escasa capacitación técnica y la resistencia al cambio delimitan la correcta implementación de los sistemas. A esto se agrega la tecnología, identificada por el hardware insuficiente e infraestructura tecnológica limitadas, que estrecha la operatividad de soluciones. Por otro lado, la organización enfrenta restricciones de presupuesto y seguridad que complica la ejecución de proyectos piloto en conjunto con la validación de los sistemas.

Los datos con base de datos etiquetado y reducido de manera deficiente influyen directamente la calidad de los modelos de inteligencia artificial, mientras que los procesos, identificados por metodologías poco estandarizados y en ausencia de protocolos de integración, que impiden la correcta coordinación entre los sistemas. Por último, las métricas inapropiadas limitan la valoración objetiva del desempeño de la integración. Estas causas interactúan entre sí, debido a la deficiencia en un área que repercute en los demás, con la falta de personal capacitado que agrava los problemas de procesos y tecnológicos, mientras que los datos inconclusos dificultan la medición y validación de resultados.

En conjunto, este análisis denota la necesidad de la investigación, orientada a proyectar estrategias que optimicen la inclusión de inteligencia y visión artificial, aventajando las limitaciones señaladas y mejorando la efectividad del monitoreo de seguridad en el aeropuerto.

CAPÍTULO II. MARCO TEÓRICO

2.1 ANALISIS DEL MACROENTORNO

Honduras es un país en desarrollo, en base a estos retos de infraestructura tecnológica, pero con una progresiva adopción de la inteligencia artificial, innovación digital y visión por computadora en sectores como lo es el aeroportuario, tomando en cuenta eso se puede optar lo siguiente

América Latina tomando en cuenta a Colombia por contar con una geopolítica similar, y un nivel de desarrollo tecnológico en la región.

Sudeste asiático con filipinas con economías en un completo auge y un alto impulso encaminado a la digitalización y uso de la inteligencia artificial en seguridad.

África con Nigeria ya que tienen una adopción innovadora de inteligencia artificial en áreas con recursos limitados, similar a Honduras.

2.1.1 AMERICA LATINA (COLOMBIA)

Político: En el 2022, 34 empresas fueron atacadas, lo que representa un 133% más que el 2021. En septiembre de 2020, el gobierno publicó la primera edición de la Estrategia Nacional de Ciberdefensa y Ciberseguridad (ECDCS) para los siguientes diez años. Esta estrategia se destaca por su transversalidad, ya que busca integrar las políticas, planes e instituciones creadas hasta la fecha, con el objetivo de optimizar los resultados. (Acevedo & Guisado, 2024) Con esto el gobierno colombiano busca promover la digitalización y la seguridad nacional ante amenazas que buscan establecer marcos regulatorios aun débiles en relación con la inteligencia artificial.

Económico: Las empresas privadas, las universidades y los ciudadanos cuentan con capacidades para contribuir a la ciberseguridad del país. Por ejemplo, en colaboración con entidades estatales que gestionan temas económicos, como el Ministerio de Hacienda, el Ministerio de Industria y Comercio y el Banco de la República, podría crearse y ponerse en marcha una entidad que aborde exclusivamente cuestiones de inteligencia económica. (Acevedo & Guisado, 2024) con esto se denota una inversión moderada en innovación con dependencia en exportaciones y servicios.

Social: En el caso de Colombia, se reconoce que, aunque la Ciberseguridad y Ciberdefensa son responsabilidad de todos, cada uno de los trece sectores debe contar con un delegado visible,

en ese sentido se plantea que el líder de cada sector sea el oficial de seguridad o el jefe de la oficina de TI. (Molina Gomez et al., 2025) La alta percepción de inseguridad, es lo que impulsa la aceptación de tecnologías.

Tecnológico: Muchas entidades públicas ni siquiera son conscientes de su vulnerabilidad informática, lo cual constituye una alarma sobre lo que podría suceder en el país si se enfrenta a ciberataques exitosos. Colombia tiene mucho por hacer para mejorar sus capacidades y garantizar que el Estado. (Acevedo & Guisado, 2024) La creciente adopción de software de monitoreo, aunque son dependientes de proveedores externos.

Ecológico: Uno de los requisitos fundamentales para aprovechar el potencial de la energía osmótica es encontrar una zona en la que exista un fuerte gradiente de salinidad en una distancia geográfica corta y que dicho gradiente sea aproximadamente constante durante todo el año. (Álvarez-Silva et al., 2011)

Legal: Con el paso de los años, el país ha concentrado esfuerzos en el desarrollo de estrategias orientadas a reforzar la ciberseguridad. Desde 2011, en el documento CONPES 3701 se destacan las definiciones que se otorgan a los conceptos de ciberseguridad y ciberdefensa. El gobierno colombiano publicó en 2016 el documento CONPES 3854, titulado Política Nacional de Seguridad Digital. Este documento tiene como objetivo general fortalecer las capacidades para identificar, gestionar y mitigar los riesgos de seguridad digital. (Acevedo & Guisado, 2024) legislaciones en protección de datos que se encuentran en desarrollo, pero no son específicas para la inteligencia artificial.

2.1.2 SUDESTE ASIATICO (FILIPINAS)

Económico: Según la Autoridad Filipina de Estadísticas (PSA), la economía digital del país se disparó hasta alcanzar aproximadamente 36.500 millones de dólares en 2022, contribuyendo con el 9,4 % al Producto Interno Bruto (PIB). Esto representó un aumento del 11 % con respecto a los 33.000 millones de dólares registrados en 2021. (International Trade Administration, 2024) Cuentan con un crecimiento rápido del PIB con inversiones en tecnología en el área de seguridad pública.

Social: El Gobierno de Filipinas, la industria de externalización de procesos empresariales (BPO), el sector educativo, el sector financiero, el sector sanitario y la industria de las telecomunicaciones son mercados verticales clave para las TIC. Asimismo, se observa un

crecimiento en las plataformas de pagos electrónicos. (International Trade Administration, 2024) Cuenta con una población joven de alto consumo digital, y con una creciente preocupación por el tema de los delitos cibernéticos.

Tecnológico: Filipinas ocupó el puesto 61 entre 182 países en el Índice Global de Ciberseguridad de 2020, elaborado por la Unión Internacional de Telecomunicaciones. La adopción de medidas legales y de cooperación se identificó como una de las fortalezas del país en materia de ciberseguridad. (International Trade Administration, 2024) Avances en inteligencia artificial con control de tráfico, ciberseguridades presentes.

Ecológico: Desastres como el tifón Odette en 2021 y el tifón Paeng en 2022 pusieron de relieve la importancia de las soluciones TIC para los programas de respuesta ante desastres y gestión de la resiliencia. Los funcionarios de los gobiernos locales han impulsado la transformación digital de sus ciudades. (International Trade Administration, 2024) El uso de la inteligencia artificial para la gestión de riesgos naturales en conjunto a la protección de infraestructuras críticas.

Legal: Las leyes sobre ciberseguridad y protección de infraestructuras críticas de información se encuentran entre las principales propuestas políticas del PNCS. El Gobierno filipino continúa ampliando la Ley de Privacidad de Datos (RA 10173), estableciendo estándares de protección de datos y recomendando que todas las entidades se registren en su portal en línea. (International Trade Administration, 2024) Con marcos regulatorios incipientes sobre el tratamiento de datos y la seguridad informática.

2.1.3 AFRICA (NIGERIA)

Político: La teoría del estructural-funcionalismo sostiene que, para controlar la delincuencia, el gobierno debe promulgar leyes y crear marcos institucionales para hacer cumplir dichas leyes. En relación con Nigeria, el gobierno requiere la promulgación de una ley cibernética para abordar la naturaleza dinámica de la ciberdelincuencia y las amenazas a la ciberseguridad.(Odumesi, 2014) con el impulso a la economía digital por medio de programas de seguridad inteligente mediante el apoyo internacional.

Económico: La Comisión de Delitos Económicos y Financieros (EFCC) informa de resultados positivos en la lucha contra los delitos informáticos gracias a las redadas periódicas en cibercafés públicos, las detenciones y el enjuiciamiento de sospechosos. la falta de conocimientos

adecuados en materia de tecnologías de la información, la falta de financiación adecuada y la falta de la motivación necesaria para combatir adecuadamente a los delincuentes informáticos. (Odumesi, 2014) con las limitaciones presupuestarias, pero con un alto crecimiento en soluciones digitales de bajo costo.

Social: La teoría del funcionalismo estructural considera que las normas y valores compartidos son la base de la sociedad, se centra en el orden social basado en acuerdos tácitos entre grupos y organizaciones, y considera que el cambio social se produce de forma lenta y ordenada. (Odumesi, 2014) con la alta inseguridad física en zonas urbanas hace generar aperturas hacia los sistemas de vigilancia con inteligencia artificial.

Tecnológico: La agencia gubernamental de ciberseguridad garantiza la ciberseguridad mediante el desarrollo de capacidades, talleres sobre ciberdelincuencia, programas de concienciación pública, sesiones interactivas con el Comité Bancario y las fuerzas del orden, el patrocinio del proyecto de ley sobre ciberdelincuencia, la colaboración con la Comisión de Reforma Legislativa. (Odumesi, 2014). Cuentan con la adopción de la inteligencia artificial en el monitoreo de la seguridad informática y urbano.

Ecológico: Establecimiento de un marco para la implementación de la garantía de la información en sectores críticos de la economía, como los servicios públicos, las telecomunicaciones, el transporte, el turismo, los servicios financieros, el sector público, la industria manufacturera y la agricultura, y desarrollo de un marco para la gestión de los riesgos de seguridad de la información a todos los niveles. (Odumesi, 2014) Con la aplicación de la inteligencia artificial en infraestructuras criticas energéticas y ambientales de la nación.

Legal: La Ley contra el Fraude por Anticipo de 2006, la Ley contra el Blanqueo de Capitales de 2004, sección 12(1) (c) - (d), la Ley de la Comisión de Delitos Económicos y Financieros de 2005 y la Ley de Pruebas de 1948 son las únicas disposiciones disponibles en el derecho penal de Nigeria que pueden utilizarse para condenar a los autores de delitos cibernéticos. (Odumesi, 2014) con la regulación insuficiente, pero con una tendencia a seguir los estándares internacionales de protección de datos.

2.2 ANALISIS DEL MICROENTORNO

El presente análisis del microentorno se desenvuelve por medio de la aplicación del modelo

de las cinco fuerzas de Porter, una herramienta ampliamente utilizada para la evaluación de la dinámica competitiva de un sector industrial. La metodología se basa en analizar, comenzando con los factores que determinan la rivalidad competitiva, y el poder de negociaciones de proveedores y clientes, en conjunto con la amenaza de nuevas cavidades y productos sustituto, tomando en consideración ejemplos de tres países la región centroamericana seleccionados que son: Guatemala, Costa Rica y el Salvador. Donde luego, se realiza una comparación regional que permite identificar tendencias diferentes y comunes con relevancia en la integración de tecnologías relacionadas con la inteligencia y visión artificial para el monitoreo de seguridad informática y física. Finalmente, en base a estos modelos de referencia centroamericanos, se aplica el mismo marco analítico al caso de Honduras, con la intención de hacer resalte de los desafíos competitivos y las particularidades del contexto nacional, precisamente en el sector aeroportuario y en la seguridad relacionado a la infraestructura y operaciones del Servicio Aeroportuario Nacional.

2.2.1 COMPARACION REGIONAL

2.2.1.1 GUATEMALA

Rivalidad entre competidores existentes con una alta competencia entre empresas privadas de seguridad y una baja penetración de soluciones con inteligencia artificial, a pesar de que se empieza a tener crecimiento en la banca.

Amenazas de nuevos entrantes con una moderada afluencia, debido a que la industria de seguridad física está dividida y los costos de entrada son bajos. Por lo tanto, la inteligencia artificial aplicada a seguridad, la entrada requiere de una inversión en el área de manera significativa.

El poder de negociación de los proveedores es alto, debido a que la mayoría de soluciones tecnológicos provienen de proveedores extranjeros como ser los de software, servidores, etc.…

Con un alto poder de negociación de los clientes con empresas grandes a nivel bancario e industrial que exigen precios bajos y servicios integrales.

La amenaza de productos sustitutos es moderada con un uso de seguridad cotidiana con un cctv básico o incluso guardias al estar frente a una inteligencia artificial avanzada.

2.2.1.2 COSTA RICA

Cuenta con una rivalidad entre competidores existentes fuerte con relación a seguridad privada y seguridad cibernética siendo el país más avanzado en la adopción de tecnologías digitales en la región.

Con la amenaza de nuevos entrantes es moderada-alta ya que atrae muchas empresas emergentes por su ecosistema digital muy ponderado.

Al tener un poder de negociación con los proveedores con un nivel medio ya que existen multinacionales tecnológicas y proveedores locales que reducen la dependencia de este.

El poder de negociación de los clientes es alto ya que los clientes institucionales como las zonas energéticas tienen capacidad de exigir soluciones avanzadas.

La amenaza de productos sustitutos es baja ya que la sofisticación del crimen los obliga a realizar migración hacia soluciones con la inteligencia artificial en conjunto con el monitoreo inteligente.

2.2.1.3 EL SALVADOR

Al existir rivalidad entre competidores existentes el mercado de seguridad física es muy competitivo y la inteligencia artificial aplicada aun naciente, con un impulso en ciberseguridad por los programas de digitalización.

La amenaza de nuevos entrantes es baja-moderada que cuenta con regulaciones implícitas en seguridad que tienen la limitación de la entrada de nuevas firmas.

Cuentan con poder de negociación de los proveedores alto con una fuerte dependencia de importación tecnológica.

La negociación de los clientes es medio ya que es un sector gubernamental y corporativo en creciente demanda sobre la seguridad digital.

Al tener una amenaza de productos sustitutos moderada la seguridad tradicional sigue predominando sobre soluciones relacionadas con la inteligencia artificial.

2.2.1.4 CASO HONDURAS

Teniendo en cuenta las referencias centroamericanas:

La rivalidad entre competidores existentes el mercado de seguridad está saturado con empresas privadas tradicionales y con poca competencia en soluciones avanzadas con inteligencia artificial hace que se vea limitada la innovación, pero también abre consigo oportunidades.

Con la amenaza de nuevos entrantes al ser baja por la falta de infraestructura tecnológica y teniendo en cuenta el bajo presupuesto presentan limitación en la entrada de tecnologías

emergentes o incluso de proveedores internacionales especializados en el área.

El poder de negociación de los proveedores es muy alto ya que cuentan con la dependencia absoluta de proveedores externos tanto en el hardware y software como ser cámaras y los algoritmos de inteligencia artificial.

Tomando en cuenta el poder de negociación de los clientes el cual es bajo donde las instituciones públicas y grandes empresas demandan de una seguridad avanzada, pero teniendo presupuestos limitados.

La fuerte dependencia de proveedores externos para software y hardware de seguridad, sumada a la alta amenaza de sustitutos basados en esquemas tradicionales de videovigilancia y vigilancia física, lo que genera un entorno de vulnerabilidad para la protección de infraestructuras de alto valor en Honduras. En este ambiente se impone por la baja presión de los clientes en exigencia de innovación, lo que limita la introducción de soluciones avanzadas. En efecto, se justifica la necesidad de una investigación que evalué la integración de tecnologías de visión e inteligencia artificial en el sector aeroportuario, considerando como caso de estudio el Servicio Aeroportuario Nacional (SAN), con el fin de menguar estos riesgos de mercado y fortalecer la seguridad nacional.

De acuerdo con CONATEL (2024) la alta penetración de servicios digitales y conectividad evidenciada por la Comisión Nacional de Telecomunicaciones (CONATEL) con aproximadamente 495,760 suscriptores de internet fijo al cierre del 2024 y con una densidad de acceso de cerca de 68 suscriptores por cada 100 habitantes nos indica una creciente dependencia de sistemas conectados en la operación diaria, lo que lo vuelve considerablemente critico en la seguridad física y cibernética de estas plataformas.

Tabla 1. ANALISIS APLICADO A HONDURAS EN EL SECTOR AEROPORTUARIO.

	Descripción en el contexto hondureño	Nivel de impacto
Rivalidad entre competidores existentes	El mercado de seguridad cargado con empresas tradicionales, pero con una baja adopción de soluciones fundamentado en inteligencia artificial, lo que condiciona la diferenciación e innovación.	Alta
Amenaza de nuevos entrantes	La entrada de nuevas empresas tecnológicas es baja adecuada a la limitada infraestructura digital, escaso presupuesto institucional y elevados costos de inversión.	Baja

	Descripción en el contexto hondureño	Nivel de impacto
Poder de negociación de los proveedores	Alta supeditación de proveedores extranjeros de software y hardware, lo que aumenta los costos y reduce la autonomía tecnológica nacional.	Muy alta
Poder de negociación de los clientes	Grandes empresas e instituciones públicas demandan soluciones avanzadas de seguridad, pero con reducidos presupuestos, lo que delimita su capacidad de exigir innovación.	Baja
Amenazas de productos sustitutos	Persistencia de esquemas tradicionales de vigilancia física y CCTV básico ante sistemas con inteligencia artificial, lo que demora la adopción tecnológica.	Alta

Fuente: Elaboración propia.

El entorno competitivo hondureño en materia de seguridad cibernética y física presenta altos niveles de dependencia y rivalidad externa, con un bajo poder de negociación de los clientes y barreras significativas para la entrada de nuevos competidores tecnológicos. Esta perspectiva evidencia una brecha en la adopción e innovación de tecnologías inteligentes, argumentando la pertinencia del presente estudio acerca de la integración de inteligencia y visión artificial en el monitoreo de seguridad aeroportuaria del Servicio Aeroportuario Nacional (SAN).

2.3 CONCEPTUALIZACIÓN

En el marco de esta investigación, es fundamental demarcar conceptualmente las variables centrales que dan la orientación al estudio. El detalle terminológico permite la garantía de la coherencia entre los objetivos planteados en esta investigación y el análisis de los resultados.

2.3.1 VISION COMPUTACIONAL

Los sistemas de visión industrial desempeñan un papel importante a la hora de hacer que la producción sea más fiable y estable, más eficiente y rápida, más económica y sostenible en la fábrica del futuro de la industria 4.0. Las aplicaciones de la visión artificial en el ámbito industrial han sido un tema de investigación constante en el ámbito académico. (Demir et al., 2020)

En el contexto de la investigación, la visión computacional se entenderá como la tecnología que cedera el comportamiento anómalo por medio de análisis automatizado de videos o imágenes. Su comprensión será abordada partiendo de las percepciones del personal acerca de su confiabilidad, aporte y utilidad a la seguridad física en instalaciones aeroportuarias del Servicio Aeroportuario Nacional.

2.3.2 INTELIGENCIA ARTIFICIAL

La introducción de herramientas de economía digital e inteligencia artificial (IA) en la sociedad ha centrado cada vez más los debates en cuestiones como la sustitución de personas por máquinas, la distorsión de la ética, la degradación de la inteligencia natural, el uso malicioso de la IA, etc. (Raikov & Pirani, 2022)

Para el estudio, la inteligencia artificial se concibe como la capacidad de los sistemas tecnológicos para tomar y aprender decisiones de manera autónoma dentro de los procesos de seguridad aeroportuaria. Serán explorados a partir de las percepciones de los entrevistados sobre su grado de confiabilidad, la reducción de la intervención humana y su aporte a la automatización de tareas en la detección de amenazas.

2.3.4 EFECTIVIDAD

El análisis de rentabilidad es un estudio exhaustivo del coste y la eficiencia de los equipos, y también es una compensación entre el coste y la eficiencia del sistema. Su objetivo es proporcionar a los responsables de la toma de decisiones información sobre la rentabilidad de los equipos, para que puedan tomar decisiones basadas en los resultados del análisis. (Y.-H. Chen & Hu, 2020)

En esta investigación, la efectividad se operacionalizará por medio de tres métricas cualitativas:

a) La percepción del personal ante la frecuencia de falsos positivos en los reportes de incidentes de seguridad.

b) La percepción del personal ante la rapidez con la que los sistemas conceden la detección de amenazas.

c) La percepción del personal frente a la precisión de sus decisiones ante incidentes de seguridad al emplear los sistemas integrados de inteligencia y visión artificial.

2.3.5 INTEGRACION TECNOLOGICA

Características visuales del sistema integrado de herramientas digitales de sostenibilidad y moralidad cívica en la tecnología educativa de la nueva era, utilizando algoritmos para construir la percepción de fusión del sistema integrado de herramientas digitales de sostenibilidad y moralidad cívica en la tecnología educativa de la nueva era. (Song, 2025)

La variable se medirá en función del grado de interoperabilidad alcanzado entre la compatibilidad del software/hardware, el impacto en la continuidad operativa y la facilidad de adopción por parte del personal. En el estudio, será interpretado desde el punto de las percepciones del personal técnico acerca de la facilidad de adopción, impacto de dicha integración y compatibilidad en la integración de la continuidad operativa.

2.3.6 ENTORNO REGULATORIO

A medida que las tecnologías de inteligencia artificial (IA) configuran cada vez más los entornos digitales, garantizar la seguridad y los derechos de los niños se ha convertido en una preocupación normativa fundamental. (Spatari, 2025)

En el marco de este estudio, su análisis concederá la identificación de las limitaciones legales, oportunidades de adaptación de la inteligencia artificial y requisitos de cumplimiento en el sector aeroportuario.

2.4 TEORÍAS DE SUSTENTO

Para comprender de una manera más integral el fenómeno investigado, resulta necesario apoyarse en marcos teóricos que permitan analizar el impacto sobre la gestión organizacional y en la capacidad de las instituciones para enfrentar riesgos. De acuerdo con eso, se han seleccionado teorías fundamentales que apoyaran como una base analítica como lo son a continuación:

2.4.1 TEORIA DE RESILIENCIA ORGANIZACIONAL

En la actualidad, el estudio de la resiliencia ha cobrado cada vez más importancia, ya que el concepto crítico para la supervivencia de las organizaciones en entornos turbulentos, caóticos e impredecibles se ha convertido en un tema candente de interés académico. (Chen et al., 2021)

El estudio de la resiliencia se originó a finales de la década de 1960 y principios de la de 1970 en los campos de la ecología, la ingeniería y la psicología positiva, y se refiere a la capacidad del sistema para hacer frente al cambio. El concepto de resiliencia fue introducido por primera vez en el estudio del medio ambiente ecológico por Holling (1973) en el artículo resiliencia y estabilidad de los sistemas ecológico. (Chen et al., 2021)

En el contexto aeroportuario, la continuidad operativa es crítica y evaluar la eficacia de la Visión computacional e inteligencia artificial se conecta con la mejora de la recuperación después de un evento.

2.4.2 TEORIA DE LA GESTION DEL RIESGO

Los autores demostraron que la utilidad de la teoría general difiere en función de la naturaleza del fenómeno estudiado y, por lo tanto, también entre los distintos campos de estudio. Para Knight, de esta perspectiva surgió una idea importante. En el centro de los mercados se encuentran las empresas y los empresarios que coordinan el intercambio de servicios para los individuos. (Audretsch & Belitski, 2021)

Los individuos no intercambian entre sí directamente, sino a través de intermediarios. Por lo tanto, el capitalismo moderno incluye una variedad de empresarios que reconocen las oportunidades del mercado y crean empresas, así como negocios como organizaciones gestionadas profesionalmente y distintas de sus fundadores. (Audretsch & Belitski, 2021)

El estudio analiza como la inteligencia artificial y la visión por computadora mejora el monitoreo ante amenazas. Esta teoría proporciona la base para evaluar si la tecnología disminuye el nivel de riesgo en el sistema critico que se está evaluando donde permitirá interpretar los resultados bajo la lógica de aumentar la capacidad de respuesta.

2.4.3 TEORIA DEL CONTROL Y SUPERVISION

Según la teoría, Jensen y Meckling no solo diagnosticaron los graves problemas de la empresa que cotizaba en bolsa, sino que también presionaron para que se implementaran ajustes en la gobernanza como solución. La "Teoría de la Firma" supuestamente exigía que juntas directivas independientes y comprometidas se hicieran cargo de supervisar y disciplinar a los altos ejecutivos. (Cheffins, 2021)

La seguridad cibernética y física se delega en tecnología y humanos. La visión por computadora y la inteligencia artificial funcionan como agentes tecnológicos que monitorean en nombre de las organizaciones.

Tabla 2. COMPARACION DE TEORIAS DE SUSTENTO Y APLICACION AL CASO SAN.

Teoría	Supuestos principales	Variables clave	Aportes al análisis	Limitaciones	Conexión con hallazgos y propuesta.
Resiliencia organizacional	Las organizaciones deben resistir, adaptarse y anticipara eventos disruptivos	Adaptación, Continuidad operativa y capacidad de respuesta.	Permite interpretar como la integración tecnológica fortalece la recuperación y continuidad operativa.	No evalúa desempeño técnico del sistema.	Explica los hallazgos acerca de la mejora en continuidad operativa y sustenta la propuesta de monitoreo integrado.
Gestión del riesgo	El riesgo puede mitigarse por medio de la detección temprana y reducción de la incertidumbre.	Capacidad de respuesta, Amenaza.	Brinda un marco para analizar la reducción percibida de riesgo.	Enfoque conceptual.	Justifica los hallazgos acerca de la reducción de falsos positivos y respalda la integración de visión e inteligencia artificial.
Control y supervisión	La delegación requiere mecanismos de monitoreo para reducir errores.	Agentes tecnológicos, supervisión, toma de decisiones.	Explica el rol de inteligencia artificial como un agente de supervisión.	No profundiza en factores humanos.	Sustenta la propuesta de inteligencia artificial como apoyo a la supervisión continua.

Fuente: Elaboración propia.

2.5 ANALISIS DE METODOLOGIAS

En el aeropuerto Ramón Villeda Morales administrado por el Servicio Aeroportuario Nacional (SAN) no se ha demostrado empíricamente la eficacia de adherir sistemas de monitoreo lógico y físico por medio de plataformas de seguridad cibernética y visión artificial. Esta situación bosqueja la necesidad de investigar si dicha integración impacta de manera significativa en los tiempos de detección de amenazas, la reducción de falsos positivos, la precisión de la toma de decisiones y la continuidad operativa, en semejanza con la gestión de sistemas independientes o manuales.

Tabla 3. ESTRATEGIA METODOLOGICA.

Elemento	Formulación en caso de estudio	Relación con diseño metodológico
Problema	En el aeropuerto Ramon Villeda Morales (SAP) no se ha demostrado empíricamente la eficacia de integrar sistemas de monitoreo lógico y físico mediante plataformas de seguridad cibernética y sistemas de monitoreo físico. Esta posición limita el descubrimiento oportuno y la respuesta ante amenazas.	Justifica un estudio de caso evaluativo con un enfoque cualitativo, donde se pueden obtener datos cualitativos por medio de la percepción del personal sobre indicadores como ser precisión, falsos positivos, tiempos de detección y continuidad operativa y desempeño de los operadores para analizar el impacto de la combinación ante la gestión de sistemas independientes o manual.

Elemento	Formulación en caso de estudio	Relación con diseño metodológico
Pregunta de investigación	1. ¿Cómo percibe el personal el impacto de la integración de sistemas en el tiempo de detección y respuesta ante amenazas? 2. ¿Cómo perciben los operadores la precisión y rapidez en la toma de decisiones ante alertas de sistemas integrados vs independientes? 3. ¿Cómo percibe el personal el impacto de la integración tecnológica en la reducción de falsos positivos? 4. ¿Cómo perciben los operadores el fomento de la mitigación de riesgos sociales, la continuidad operativa, ambientales y económicos?	Se aborda con un diseño cualitativo: Cualitativo: observaciones y entrevistas de operadores para evaluar compresión y percepción.
Objetivo general	Analizar las percepciones del personal del Servicio Aeroportuario Nacional acerca de la integración de sistemas de inteligencia artificial, plataformas de seguridad cibernética y visión artificial en el monitoreo de la seguridad lógica y cibernética, en comparación con la gestión manual o por medio de sistemas independientes de alertas partiendo de entrevistas semiestructuradas y análisis de contenido ejecutados durante un periodo aproximado de cinco semanas, con el fin de comprender su impacto percibido en la detección de amenazas y toma de decisiones, en la seguridad aeroportuaria.	Determina un estudio de caso de corte transversal orientado a la comprensión de las percepciones del personal operativo, fundamentándose en entrevistas semiestructuradas y análisis de contenido temático.

Elemento	Formulación en caso de estudio	Relación con diseño metodológico
Objetivos específicos	1. Explorar la percepción del personal acerca de la efectividad de un panel integrado de alertas ante sistemas independientes en la toma de decisiones. 2. Comprender la percepción del personal acerca del impacto de la inteligencia y visión artificial en la precisión de las alertas de seguridad. 3. Describir la percepción del impacto de los sistemas integrados en la continuidad operativa y la mitigación de riesgos operativos.	Cada objetivo se hace efectivo en: Cualitativo: observación de desempeño percibido y la percepción de operadores por medio de entrevistas semiestructuradas y análisis cualitativo de los datos.

Fuente: Elaboración propia

2.5.2 DECLARACION DE REFLEXIVILIDAD.

Como investigador, reconozco que mi rol, mis percepciones y formación académica en ingeniería en mecatrónica y mi inclinación a las tecnologías emergentes podrían llevarme a valorar positivamente la combinación de la visión por computadora e inteligencia artificial donde pueden influir en la interpretación de los datos, generando un sesgo de favorabilidad inclinada a la integración de inteligencia y visión artificiales en sistemas de monitoreo. Por lo tanto, mi experiencia precia en entornos tecnológicos podría afectar la manera en que percibo la efectividad de las soluciones propuestas, influenciándome a valorar más los aspectos que los contextos organizacionales y humanos.

En un estudio de caso único, los principales riesgos de sesgos identificados son:

Sesgo de contexto: generalizando los resultados del aeropuerto Ramon Villeda Morales del Servicio Aeroportuario Nacional a todo el sector aeroportuario.

Sesgo del investigador: influir en la interpretación de entrevistas y observaciones.

Sesgo de confirmación: sobrevalorar los beneficios de la integración.

Para mitigar estos riesgos, serán aplicadas las siguientes estrategias:

Protocolos experimentales repetibles y estandarizados para la recolección de datos cualitativo.

Recolección de evidencia cualitativa como ser observación y entrevistas para validar la interpretación de resultados y contrastar hallazgos.

Estas medidas aseguran una postura sistemática, critica y reflexiva, incrementando la confiabilidad y validez de los resultados.

2.5.3 ESTRATEGIA DE TRIANGULACION.

Para este estudio de caso con un enfoque cualitativo-experimental, será aplicado una triangulación metodóloga y de fuentes como estrategia óptima para él aseguramiento de la confiabilidad y validez de los hallazgos.

Triangulación metodológica: Se realizará un enfoque cualitativo, enfocado en las experiencias y percepciones de los participantes. Los datos serán obtenidos por medio de análisis documental, entrevistas a operadores y revisión bibliografía, lo que brindara un contrates de las

percepciones profesionales con la existente información y brindad un contexto más específico. Esta combinación posibilita una interpretación más amplia de los descubrimientos evadiendo conclusiones sesgadas y enriqueciendo el entendimiento de los fenómenos estudiados.

Triangulación de fuentes: se contrastará la información del aeropuerto Ramon Villeda Morales con literatura académica, experiencias en casos similares en otras infraestructuras aeroportuaria sensible y reportes institucionales, con esto se fortalecerá la confiabilidad de los hallazgos, debido a que permite la validación de los resultados del estudio ante evidencia externa.

La aplicación de esta estrategia es fundamental para el diseño de estudio de caso, debido a que:

1. Permite comprobar empíricamente la eficacia de la integración de sistemas.
2. Garantiza que los resultados reflejen tanto la realidad operativa cuantificable como el desempeño y percepción de los operadores.
3. Minimiza los sesgos de interpretación al contrastar múltiples tipos de fuentes y datos, fortaleciendo la robustez y consistencia de los hallazgos.

La estrategia metodológica y de fuentes más adecuada para el diseño asegura que los resultados sean validos pertinentes y fiables para la evaluación del impacto de la integración de visión artificial con ciberseguridad en el aeropuerto Ramon Villeda Morales del Servicio Aeroportuario Nacional.

2.5.4 HERRAMIENTAS DE ANALISIS METODOLOGICO.

Para traslucir la arquitectura del análisis serán utilizado:

Mapas conceptuales, para la representación sobre la interacción entre la inteligencia artificial, visión artificial y procesos de monitoreo de seguridad.

Matrices comparativas, de manera que permitan evaluar diferencias entre los sistemas de inteligencia artificial y los métodos tradicionales.

Análisis temáticos, para categorizar y organizar la información cualitativa adquirida de las fuentes documentales.

Estadística descriptiva, para sintetizar los datos cualitativos alcanzados de investigaciones o estudios previos.

Estas herramientas permitirán reflejar de una manera transparente la fusión entre los componentes estudiados asegurando de esa manera un análisis transparente e integral.

2.6 ANTECEDENTES DE LAS METODOLIGIAS

En el área de la gestión de tecnologías de la información y comunicación (GTIC), los métodos habituales se han distinguido por un enfoque escolástico, ajustado en la aplicación rígida de marcos normativos y en la observancia estricta de modelos teóricos como lo son ITIL, ISO 27001 o COBIT. metodologías, aunque robustas, tienden a predisponer el cumplimiento normativo y la estandarización sobre la reflexión crítica y la adaptabilidad, limitando su eficacia en infraestructuras criticas como el sistema aeroportuario.

Los debates paradigmáticos en investigación destacan los enfoques principales:

Cualitativos: analizando experiencias, contextos y percepciones, proporcionando profundidad interpretativa, aunque con dificultad para generalizar resultados.

La metodología adaptada en este estudio tiene un enfoque cualitativo-experimental, que representa una adaptación innovadora ante los modelos tradicionales de GTIC:

Evaluando cualitativamente el impacto de la integración de visión artificial con ciberseguridad ante variables sensibles como lo son la precisión en la toma de decisiones, tiempos de detección, continuidad operativa.

Complementando los resultados con evidencia cualitativa, por medio de entrevistas, análisis documental y observaciones, percibiendo la experiencia de los operadores y lo distintivo del entorno del Aeropuerto Ramon Villeda Morales.

Superar las limitaciones de los enfoques escolásticos al integrar reflexión crítica, soluciones adaptadas a desafíos tecnológicos emergentes y el análisis situacional, como la gestión de sistemas interdependientes y complejos en entornos cruciales.

En consecuencia, la propuesta metodológica de este estudio responde de manera innovadora a los desafíos actuales en GTIC, haciendo una combinación rigurosa científica y con relevancia práctica, asegurando que los hallazgos sean confiables, contextualizados y aplicables para la gestión de infraestructura prioritaria en entornos tecnológicos avanzados.

2.7 METODOLOGIAS, ENFOQUES, METODOS Y DISEÑOS

Esta investigación se adopta un enfoque cualitativo, entendido como la integración de técnicas cualitativas en un mismo estudio Hamui-Sutton (2013) lo relaciona como la combinación mediante la perspectiva cualitativa en un mismo estudio. Cuando las preguntas de investigación son engorrosas, la combinación de estos métodos da la posibilidad de brindarle profundidad al análisis y entender de mejor manera los procesos de aprendizaje y enseñanza, los métodos cualitativos se sirven de diversas fuentes de información que relacionan de diversas maneras para sustentar un análisis más tolerante, sobre la problemática proyectada. Este enfoque se deriva pertinente debido a que la problemática entorno a la gestión de tecnologías de la información y comunicación demanda el análisis numérico de datos como ser el impacto, desempeño y eficiencia como una exploración demostrativa de prácticas organizacionales y de percepciones.

El enfoque cualitativo se justifica porque la problemática alrededor de la gestión de tecnologías de la información (GTIC) en infraestructuras sensibles, como lo es el sector aeroportuario, tiene la exigencia tanto del análisis numérico de indicadores de objetivo como ser la tasa de falsos positivos, tiempos de detección y la continuidad operativa. De igual manera la interpretación de percepciones operativas organizacionales de los actores involucrados. Únicamente por medio de la combinación de ambas perspectivas es posible obtener una compresión integral del impacto de integrar sistemas de Ciber seguridad y visión artificial.

El método optado es el estudio de caso, Al referirse a las diferentes finalidades del estudio de caso y a las distintas disciplinas que lo utilizan, STAKE recuerda dos puntos relevantes. Primero, la importancia de que quien decida emplear el estudio de caso en su investigación reconozca la tradición de la que parte. Segundo, que estudio de caso no es sinónimo de método cualitativo. (Simons, 2013. p. 41) En este caso se centra el aeropuerto Ramon Villeda Morales del Servicio Aeroportuario Nacional. Como un sistema sociotécnico de alto valor, en la que confluyen riesgos tanto lógicos como físicos, de esta manera el estudio de caso posibilita integrar distintas fuentes de información, experimentos controlados, observaciones y entrevistas, para poder comprender la interacción entre procesos organizacionales, tecnología, desempeño operativo. La elección se justifica porque el problema planteado no puede ser embebido sin tener consideración de la especificidad del contexto.

En particular, el diseño compete a un estudio de caso cualitativo secuencial explicativo, dado que se consideran diversas unidades de análisis como ser instituciones o proyectos vinculados

a GTIC. El estudio de caso es una investigación exhaustiva y desde múltiples perspectivas de la complejidad y unicidad de un determinado proyecto, política, institución, programa o sistema en un contexto "real". Se basa en la investigación, integra diferentes métodos y se guía por las pruebas. La finalidad primordial es generar una comprensión exhaustiva de un tema determinado. (Simons, 2013. p. 43)

En la primera fase se analizarán y recolectarán datos cualitativos basados en la percepción de los operadores sobre escenarios simulados de intrusión, abarcando su consideración sobre la precisión y tiempos de respuesta que permitirán establecer patrones objetivos sobre la eficacia del sistema integrado, posteriormente se desarrollara una fase cualitativa mediante observaciones con operadores y entrevistas, orientada a la explicación de los resultados numéricos, identificando las causas y significados detrás de los patrones encontrados. Este diseño resulta oportuno porque asegura que los hallazgos cualitativos no se limiten a percepciones aisladas, caso contrario sean comprometidos en relación con las practicas, desafíos y percepciones propias de la gestión de seguridad en infraestructuras de alto valor.

Desde la perspectiva epistemológica, la combinación de un estudio de caso, enfoque cualitativo y un diseño secuencial explicativo garantiza un abordaje holístico y riguroso que integra evidencias subjetivas y objetivas, permitiendo superar las limitaciones de un enfoque exclusivamente empírico o puramente teórico, que aporta al campo de la GTIC una aproximación reflexiva y practica respondiendo a los desafíos actuales de resiliencia y seguridad en sistemas estratégicos.

2.8 ANALISIS CRITICO DE LAS METODOLOGIAS

La elección de un enfoque cualitativo con énfasis en el diseño cualitativo-descriptivo dentro de un estudio de caso responde a la necesidad de captar tanto la dimensión objetiva de los fenómenos observados como la percepción contextual de sus dinámicas. Un inspector llega a cuestionar si el uso de un único caso tiene la limitación de la generalización de resultados. Es por ello por lo que es importante subrayar que la fortaleza de un estudio de caso radica en el detalle y profundidad con lo que se analiza en una situación decisiva, generando aprendizajes transferibles a contextos similares, aun sin aspirar a la universalidad estadística.

Otra critica eventual es sobre la combinación de técnicas cualitativas el cual podría generar dispersión analítica. La respuesta es que, en este caso, la triangulación metodológica se convierte

en un mecanismo de refuerzo con los datos cualitativos experimentales que permiten medir efectos y cambios de manera objetiva, mientras que los insumos cualitativos contribuyen a la compresión de las experiencias y percepciones de los actores involucrados. Esta unificación asegura no solo la validez interna, sino que también una interpretación más completa de los hallazgos.

Respecto a las limitaciones, se reconoce que los indicadores objetivos exigen condiciones controladas que, en un entorno real de infraestructura critica, pueden llegar a verse restringidas por factores externos como lo son la disponibilidad de recursos, resistencias organizacionales y tiempo de implementación. No obstante, estas limitaciones serán amortiguadas por medio de la definición de unidades de observación claras, el uso de herramientas digitales y protocolos estandarizados de recolección de datos que puedan garantizar la trazabilidad.

En términos de rigor metodológico, serán aplicados criterios diferenciados:

Cualitativo:

Transferibilidad: será ofrecido una descripción densa del contexto para que otros investigadores puedan valorar la aplicabilidad en escenarios semejantes.

Credibilidad: se validarán los hallazgos mediante la triangulación con diversas fuentes como lo son entrevistas, registros técnicos y documentos.

Confiabilidad: los instrumentos serán aplicados en condiciones semejantes y se documentarán los procedimientos para permitir la reproducibilidad

Validez interna: se diseñarán indicadores, y serán utilizados pruebas simuladas para verificar que las variables midan lo que se pretende.

Finalmente, en lo que respecta al rigor técnico y ético en GTIC, se custodiará el cumplimiento de normas de seguridad de la información y confidencialidad, de esta manera garantizando que los datos obtenidos no comprometan la operación de la infraestructura critica ni la privacidad de los participantes. Para que el estudio se aportara conocimiento sin perjudicar la integridad de los sistemas ni de las personas que son involucradas. El cual serán adoptados estándares y marcos de referencia:

ISO/IEC 27001 para la gestión de la seguridad de la información, garantizando el control de acceso y resguardo de datos sensibles.

ITIL v4 para asegurar que el manejo de datos se alinee con buenas prácticas en la gestión de los servicios de TI.

COBIT 2019 para garantizar la trazabilidad, alineación con los objetivos de gobernanza y control de riesgos en infraestructuras críticas.

Principio de minimización de datos donde solo serán recopilados aquellos estrictamente útiles, asegurando de esa manera consentimiento y anonimizarían informado de los participantes.

Gestión de incidentes técnicos/éticos que implementaran un protocolo de mitigación y notificación frente a cualquier vulneración de seguridad que sea detectada durante el estudio.

Este diseño metodológico no es una aplicación mecánica de recetas, sino una elección consistente que busca el equilibrio del control experimental, responsabilidad ética y profundidad analítica.

2.9 HERRAMIENTAS

Para garantizar la relevancia y validez de los datos recolectados, se seleccionaron herramientas metodológicos acordes al contexto del aeropuerto Ramon Villeda Morales. La elección de indicadores como lo es la percepción de rapidez de precisión, detección, falsos, continuidad operativa y falsos positivos actúa ante la necesidad de evaluar la eficacia del monitoreo de seguridad física y cibernética desde la experiencia de los operadores. Suplementariamente, se consideraron entrevistas semiestructuradas dirigidas a personal operador para obtener captación directa sobre la confiabilidad y la usabilidad de estas soluciones.

Seguidamente, se expone una descripción de las principales herramientas empleadas y una comparativa con las utilizadas en investigaciones similares guiadas a la evaluación de sistemas de seguridad cruciales.

Tabla 4. COMPARATIVA DE HERRAMIENTAS

Herramienta	Tipo	Ventaja	Desventaja
Entrevistas	Cualitativa	Conceden la obtención de información detallada, contextualizada y profunda de los operadores y personal.	Requieren planificación y tiempo además pueden generar sesgo por la subjetividad del entrevistado.

Herramienta	Tipo	Ventaja	Desventaja
Observación estructurada	Cualitativa	Concede evaluación sobre la interacción real entre sistemas y humanos, identificando brechas prácticas.	Puede estar influenciada por la presencia del observador y requiere estandarización en criterios.

Fuente: Elaboración propia.

Entre las herramientas analizadas, la "entrevista semiestructurada" se selecciona como instrumento principal de investigación, en relación de su potencial para la recopilación de datos de una manera, sistemática y amplia. Su pertinencia radica en que concede la obtención del aeropuerto Ramon Villeda Morales del Servicio Aeroportuario Nacional, Agilizando la identificación de patrones, tendencias y percepciones ante la eficacia de los sistemas de inteligencia y visión artificial. En diferencia con las entrevistas o la observación, que aportan información más limitada y cualitativa en alcance, la entrevista ofrece resultados comparables y estandarizados, fortaleciendo el rigor estadístico del estudio.

2.9.1 ANALISIS DE PERCEPCION EN LA EFICACIA DE LA INTEGRACION DE INTELIGENCIA Y VISION ARTIFICIAL

En este análisis se emplearán herramientas clave como Python con librerías statsmodels para la evaluación de la eficacia de la integración de sistemas de visión e inteligencia artificial en la detección de amenazas cibernéticas y físicas en el aeropuerto Ramon Villeda Morales (SAP). Y TensorFlow, OpenCV, camara, Wireshark para la solución. Estas herramientas permiten realizar pruebas absolutas para la detección de configuraciones inseguras y la simulación de ataques, contribuyendo a la mitigación e identificación de riesgos.

Python: Python es un lenguaje interpretado que se ha vuelto más común en aplicaciones de HPC. Python se beneficia de la capacidad de escribir módulos de extensión en C, que pueden utilizar bibliotecas optimizadas que han sido escritas en otros, Es posible escribir un núcleo computacional completo en un lenguaje compilado y luego compilar ese núcleo en un módulo de extensión. (Smith, 2016)

OpenCV: La biblioteca OpenCV está escrita en C, lo que garantiza un código rápido y cómodo, y está compilada para muchas plataformas integradas. La biblioteca OpenCV incluye las tareas elementales de imagen, que son operaciones lógicas y aritméticas. Esto también consiste en operaciones complejas, detección de objetos y seguimiento de objetos. (Deepthi & Sankaraiah,

2011)

Camara: Esta tecnología que se utiliza para el registro, la grabación, el procesamiento, el almacenamiento y la transmisión de imágenes y sonidos, tuvo su nacimiento subordinado a la televisión, a la cual, estaba destinada a servir y complementar. Hoy, el Vídeo, se ha alejado de aquella servidumbre, para obtener su propia autonomía. (Perona, 2010)

TensorFlow: Es un marco informático de código abierto de Google. Este marco informático puede implementar diversos algoritmos de aprendizaje profundo y ofrece un buen soporte para redes neuronales convolucionales. En el proceso de uso del marco TensorFlow, con el fin de debilitar los factores no relacionados con el reconocimiento de imágenes. (Ju et al., 2019)

Wireshark: es un analizador de paquetes gratuito y de código abierto. Se utiliza para la resolución de problemas de red, el análisis, el desarrollo de software y protocolos de comunicaciones, y la educación. Originalmente llamado Ethereal, en mayo de 2006 el proyecto pasó a llamarse Wireshark debido a problemas con la marca registrada. (Wang et al., 2010)

2.9.2 ANALISIS ESTADISTICO

Tabla 5.COMPARACION DE HERRAMIENTAS.

Herramienta	Tipo	Funcionalidades claves	Ventajas	Desventajas	Costo	URL de descarga
OpenCV	Librería de visión artificial.	Procesamiento de video e imágenes, detección de objetos y análisis de escenarios simulados.	Amplia comunidad, compatible con Python y flexible para pruebas.	Requiere de conocimientos de programación y curva de aprendizaje.	Gratuito	https://opencv.org/releases/
TensorFlow	Framework de aprendizaje automático.	Entrenamiento de modelos de IA, reconocimiento de patrones y detección de objetos.	Escalable, documentación extensa y compatible con Python.	Consumo de recurso elevado y una curva de aprendizaje para modelos engorrosos.	Gratuito	https://www.tensorflow.org/?hl=es-419
Cámara	Hardware	Captura de video en tiempo real.	Evidencia visual real e integración con sistemas de monitoreo.	Requiere de instalación física y puede ser costoso según modelo.	Variable según modelo	Depende de fabricante
Wireshark	Herramienta de análisis de red.	Detección de anomalías, monitoreo de tráfico y análisis de paquetes.	Análisis detallado de red y útil para seguridad cibernética.	Alto volumen de datos a procesar y una curva de aprendizaje.	Gratuito	https://www.wireshark.org/download.html
Python / Statsmodels	Librería de análisis estadístico.	Modelado estadístico, análisis de tendencias, regresión y patrones.	De alto valor para el análisis de datos e integración con librerías	Requiere conocimiento de programación y estadística.	Gratuito	https://www.python.org/downloads/

Fuente: elaboración propia.

Se opto por Python con librerías Statsmodels debido a su capacidad de procesar e integrar diversas fuentes de datos y su flexibilidad para análisis de modelado y estadístico de escenarios simulados, en conjunto con su compatibilidad con sistemas de inteligencia y visión artificial. Estas herramientas acceden a la aplicación del análisis cualitativo sin requerir de una programación excesiva, lo que facilita su uso dentro de la investigación. Por lo tanto, abren la posibilidad de evaluar la eficacia de los sistemas de una manera controlada y en tiempo real, aportando a una compresión integral de la detección de amenazas cibernéticas y físicas.

2.9.3 VIABILIDAD

La investigación es viable en ambos sentidos principalmente operativamente, las herramientas escogidas, donde incluyen Python con statsmodels, TensorFlow, OpenCV, Wireshark y cámara, son compatibles con los sistemas del Aeropuerto Ramon Villeda Morales, los datos suficientes para el análisis pueden ser obtenidos sin afectar la operación normal de la planta. Por lo tanto, el uso de entornos de simulaciones y pruebas da la accesibilidad de evaluar la eficacia de los sistemas de manera controlada, de esa manera asegurando los resultados replicables y confiables.

2.10 MARCO LEGAL

En el marco legal, la comparación de herramientas tecnológicas debe de realizarse considerando las normativas vigentes en materia de protección de datos, uso adecuado de software y seguridad de la información. Este apartado permite identificar como cada herramienta se ajusta a los lineamientos regulatorios aplicables, asegurando su implementación en conformidad con los estándares nacionales e internacionales basado con principios legales. De esta manera, se garantizará no solo la funcionalidad de la investigación, sino que también la pertinencia ética y legal de su uso abarcando el contexto de la investigación.

2.10.1 MARCO LEGAL NACIONAL

En el ámbito nacional, la comparación de herramientas tecnológicas debe de enmarcarse dentro de las regulaciones y leyes vigentes que rigen la protección de datos, uso responsable de la información y ciberseguridad en Honduras. Estas disposiciones establecen las pautas legales mínimas de manera que garanticen la integridad, confidencialidad y disponibilidad de los datos, asegurando que las soluciones adoptadas sean ajustadas al marco jurídico del país.

2.10.1.1 LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACION

PUBLICA (DECRETO LEGISLATIVO N. 170-2006)

Esta Ley es de orden público e interés social. Tiene por finalidad el desarrollo y ejecución de la política nacional de transparencia, así como el ejercicio del derecho de toda persona al acceso a la información pública para el fortalecimiento del Estado de Derecho y consolidación de la democracia mediante la participación ciudadana. (ARSA, 2006)

2.10.1.2 CODIGO PENAL DE HONDURAS (DECRETO N.130-2017)

La ley penal se aplica de forma retroactiva en las disposiciones más favorables al imputado o reo, así como al penado. No obstante, y a no ser que se disponga expresamente lo contrario, los hechos cometidos bajo la vigencia de una ley temporal deben ser juzgados conforme a ella. (Diario oficial la gaceta, 2019)

2.10.1.3 LEY DE COMERCIO ELECTRONICO (DECRETO N. 149-2014)

La presente ley regula todo tipo de información en forma de mensaje de datos, utilizada en el contexto de actividades comerciales, con excepción de las obligaciones asumidas por el estado en virtud de convenios o tratados internacionales y sin perjuicio de lo dispuesto en otras normas que tengan como finalidad la protección de la salud y seguridad pública, incluida la salvaguarda de la defensa nacional. (Diario oficial la gaceta, 2015)

2.10.1.4 CONATEL

Es un organismo estatal desconcentrado que ejecuta, mediante la regulación y coordinación, la política de Telecomunicaciones en la República de Honduras. Conatel fue fundada el 5 de diciembre de 1995, mediante Decreto 185/95. El ente técnico especializado del Estado de Honduras que regula los servicios en el sector de telecomunicaciones administra el Espectro Radioeléctrico e impulsa el desarrollo de las Tecnologías de la Información y la Comunicación (TIC). (Conatel, 2025)

2.10.1.5 LEY MARCO DEL SECTOR TELECOMUNICACIONES (DECRETO 32-2013)

La presente ley establece las normas para regular en el territorio nacional los servicios de telecomunicaciones en el territorio nacional los servicios de telecomunicaciones, comprendiéndose entre estos toda transmisión, emisión o recepción de signos, señales, escritos, imágenes fijas, imágenes en movimiento, sonidos o informaciones de cualquier naturaleza por medio de transmisión eléctrica por hilos, radioelectricidad. (Diario oficial la gaceta, 2014)

2.10.1.6 LEY ESPECIAL SOBRE INTERVENCION DE LAS COMUNICACIONES PRIVADAS (2011)

Esta ley tiene por finalidad establecer el marco legal de regulación procedimental de la intervención de las comunicaciones, como mecanismo excepcional de investigación contra la criminalidad tradicional y sobre todo contra la criminalidad organizada o no convencional garantizando el derecho humano de las personas a la comunicación. (Diario oficial la gaceta, 2011)

2.10.2 MARCO LEGAL INTERNACIONAL

En el caso de Honduras, la relación con este marco internacional es reflejado en un nivel de participación parcial, en donde se reconocen los principios universales de derechos fundamentales y privacidad. Los estándares internacionales generan un efecto indirecto en los países que no cuentan con una legislación robusta, dado que las organizaciones locales que interactúan en entornos globales se ven obligadas a inclinarse a medidas de cumplimiento más estricta para garantizar la protección de los datos.

2.10.2.1 CONVENIO DE BUDAPEST SOBRE CIBERDELINCUENCIA (2001)

Teniendo en cuenta los convenios existentes del consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre los estados miembros del consejo de Europa y otros estados, y subrayando que el objeto del presente convenio es completar dichos convenios con el fin de incrementar la eficacia de las investigaciones y procedimientos penales relacionados con sistemas y datos informáticos. (Consejo de Europa, 2001)

2.10.2.2 REGLAMENTO GENERAL DE PROTECCION DE DATOS (GDPR, UNION EUROPEA 2018).

El Reglamento General de Protección de Datos es la normativa más reciente y una de las más estrictas en materia de protección de datos aprobada por la Unión Europea. Las áreas clave que se tratan son: • Principios y derechos del RGPD • Seguridad de la información, protección de datos desde el diseño y por defecto, procedimientos de implementación, métodos de cifrado respuesta y gestión de incidentes, violaciones de datos. (Gobeo et al., 2020)

2.10.2.3 NORMA ISO/IEC 27001-SEGURIDAD DE LA INFORMACION

La norma ISO/IEC 27000 describe la visión general y el vocabulario de los sistemas de gestión de la seguridad de la información, haciendo referencia a la familia de normas sobre sistemas de gestión de la seguridad de la información (incluidas las normas ISO/IEC 27003[2], ISO/IEC 27004[3] e ISO/IEC 27005[4]), con términos y definiciones relacionados. (ISO, 2022a)

2.10.2.4 COBIT

COBIT proporciona un conjunto de herramientas para salvar la brecha entre los requisitos de control, las cuestiones técnicas y los riesgos empresariales. La tecnología de la información se ha convertido en una unidad indispensable de la vida empresarial en la era actual. Su aparición ha cambiado la forma en que se hacen negocios hoy en día en un entorno competitivo. (Noor & Ghazanfar, 2016)

2.10.2.5 ITIL

La Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) es el marco de mejores prácticas más popular para la gestión de servicios de tecnologías de la información (TI). Sin embargo, la implementación de ITIL no solo es muy difícil, sino que tampoco existen mejores prácticas para llevarla a cabo. Como resultado, las implementaciones de ITIL suelen ser largas, costosas y arriesgadas. (Pereira & da Silva, 2010)

2.10.2.6 PROTOCOLO ADICIONAL DEL CONVENIO DE BUDAPETS SOBRE EVIDENCIA ELECTRONICA (2022)

Conscientes de la necesidad de garantizar que las medidas efectivas de la justicia penal en materia de ciberdelincuencia y la recogida de pruebas en forma electrónica estén sujetas a condiciones y salvaguardias que prevean la adecuada protección de los derechos humanos y las libertades fundamentales. (Consejo de Europa, 2022)

2.10.2.7 RESOLUCION 70/237 DE LA ASAMBLEA GENERAL DE LA ONU SOBRE CIBERSEGURIDAD Y CIBERCRIMEN.

El 12 de diciembre de 2019, la Asamblea General aprobó la resolución 74/28, titulada "Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional", en relación con el tema 93 del programa, relativo a los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. (Naciones unidas, 2020)

2.10.2.8 ANEXO 17- SEGURIDAD DE LA AVIACION (OACI)

Cada Estado contratante asegurará que todos los programas de instrucción en seguridad de la aviación para el personal que desempeñe funciones en el marco del programa nacional de seguridad de la aviación civil comprendan la evaluación de las competencias que deban adquirirse y mantenerse en la instrucción inicial y de repaso. (OACI, 2022)

CAPÍTULO III. METODOLOGÍA

3.1 CONGRUENCIA METODOLOGICA

Este capítulo describe el enfoque metodológico adoptado para la evaluación de la eficacia de la integración de visión e inteligencia artificiales en el monitoreo de seguridad física y cibernética en el Servicio Aeroportuario Nacional, Honduras, durante el año 2024. La investigación parte de la necesidad de contar con mecanismos innovadores que tonifican la seguridad de infraestructuras críticas, donde las amenazas no solo provienen del ámbito físico como ser los sabotajes o intrusiones, sino que, también relacionados con el entorno digital, por medio de ciberataques dirigidos a sistemas de redes de comunicación y de control.

La metodología se construye como un sistema interconectado, por el cual cada decisión contesta de una manera coherente a los objetivos planteados y al problema de investigación. En este contexto, la elección del enfoque no es arbitrario, caso contrario una consecuencia lógica sobre el tipo de información requerido para el análisis de la eficacia de los sistemas basados en visión e inteligencia artificial en un entorno operativo real.

De igual modo, el diseño considera las condiciones específicas del sector aeroportuario, distinguido por el alto grado de criticidad en sus operadores, la exigencia de continuidad del servicio aeronáutico, y la exposición a riesgos tanto humanos como tecnológicos. Estas circunstancias forzan a integrar herramientas cuantitativas para la precisión y el rendimiento de los sistemas implementados, en conjunto de técnicas cualitativas que permitan la captación sobre la percepción de los actores implicados en la gestión y operación de la seguridad.

3.1.1 MATRIZ DE CONGRUENCIA

Tabla 6.MATRIZ DE CONCRUENCIA.

Nombre de la investigación	Problema	Preguntas de investigación.	Objetivos de la investigación	Metodología	Instrumentos	Variables	Indicadores
Evaluación de la eficacia en la integración de visión e inteligencia artificial en el monitoreo de seguridad física y cibernética: Caso Servicio Aeroportuario Nacional, Honduras, 2024.	La ausencia de integración entre los sistemas de monitoreo físico y cibernético en el SAN condiciona la eficacia en la detección temprana y la respuesta a incidentes de seguridad, exhibiendo a los aeropuertos a vulnerabilidades que afectan la continuidad operativa.	En el monitoreo de seguridad del aeropuerto, ¿La percepción de los sistemas de visión artificial en conjunto con plataformas de seguridad cibernética, en semejanza con la gestión manual de alertas, tiene reducción de manera significativa el tiempo de detección y respuesta ante las amenazas presentes? En entornos de escenarios sobre intrusión simulados en un aeropuerto, ¿La percepción del personal acerca de la implementación de un panel concentrado mediante la integración de alertas físicas y lógicas, en comparación con el uso de sistemas independientes, mejora la precisión y rapidez al momento de tomar decisiones en el periodo de incidentes de seguridad? En ambientes operativos de un aeropuerto, ¿La adaptación de inteligencia artificial aplicada al monitoreo de visión artificial y cibernético, en semejanza con los sistemas convencionales, contribuye a una rebaja percibida de falsos positivos en alertas de seguridad? En ambientes operativos de un aeropuerto, ¿La adaptación de inteligencia artificial aplicada al monitoreo de visión artificial y cibernético, en semejanza con los sistemas convencionales, contribuye a una rebaja percibida de falsos positivos en alertas de seguridad?	**GENERAL**: Analizar las percepciones del personal del Servicio Aeroportuario Nacional acerca de la integración de sistemas de inteligencia y visión artificial en el monitoreo de seguridad cibernética y física, en comparación con la gestión manual de alertas, identificando tendencias y patrones relacionados con la eficacia percibida en las respuestas y detección de amenazas, por medio de análisis de contenido y aplicación de entrevistas, con el fin de comprender el potencial de estas tecnologías en la mejora de procesos de seguridad aeroportuaria, comprendido en el periodo de investigación 2024. **ESPECIFICO**: Explorar la percepción del personal acerca de la efectividad de un panel integrado de alertas lógicas y físicas ante sistemas independientes, por medio de las identificaciones de experiencias y opiniones recurrentes, adhiriendo técnicas de entrevista, con el propósito de comprender su relación con la rapidez en la toma de decisiones, en el entorno del año 2024 Comprender la percepción del uso de inteligencia artificial en el monitoreo de ciber seguridad y visión relacionado a la reducción de falsos positivos, analizando las narrativas logradas en las entrevistas, por medio de la interpretación de resultados, para estipular la precisión de alertas de seguridad, comprendido en el año 2024. Describir cómo el personal percibe el impacto de los sistemas integrados de monitoreo lógico y físico, determinando temas claves enlazados con la mitigación de la continuidad y riesgos operativos, por medio del análisis y recopilación de la testificación, para reconocer su importancia en la gestión integral de seguridad aeroportuaria, en el lapso de investigación 2024.	Enfoque cualitativo. Diseño: No experimental. Alcance: Descriptivo y exploratorio, se integran técnicas cualitativas mediante análisis y entrevistas documentales permitiendo la triangulación de resultados.	Guías de entrevistas.	Independientes Integración de visión e inteligencia artificial. Dependientes: Eficacia de monitoreo de seguridad física y cibernética.	Nivel de satisfacción percibido en el monitoreo de seguridad. Percepción de automatización en la detección y toma de decisiones. Nivel de satisfacción del personal frente al desempeño del sistema. Identificación de barreras y limitaciones en la adopción tecnológica.

Fuente: Elaboración propia

3.1.2 ESQUEMA DE VARIABLES

3.1.2.1 IDENTIFICACION DE VARIABLES

A partir del tema de investigación, preguntas de investigación y objetivos se puede estructurar:

3.1.2.2 VARIABLES INDEPENDIENTES

Integración de visión e inteligencia artificial en el monitoreo de seguridad (Precisión en la detección de anomalías, tiempo de correlación de eventos, número de incidentes detectados y porcentaje de alertas manuales vs automáticas por medio de las percepciones).

3.1.2.3 VARIABLES DEPENDIENTES

Eficacia en el monitoreo de seguridad física (Control de acceso, reducción de falsos positivos, detección de intrusos y tiempos de respuesta).

Eficacia en el monitoreo de seguridad cibernética (Capacidad de respuesta ante ataques, reducción de incidentes cibernéticos, detección de anomalías en la red).

3.1.2.4 VARIABLES MEDIDORAS

Integración y compatibilidad con sistemas existentes, debido a que, si la IA no se ensambla correctamente con los sistemas de monitoreo actuales o con el sistema SCADA, su eficacia se ve reducida.

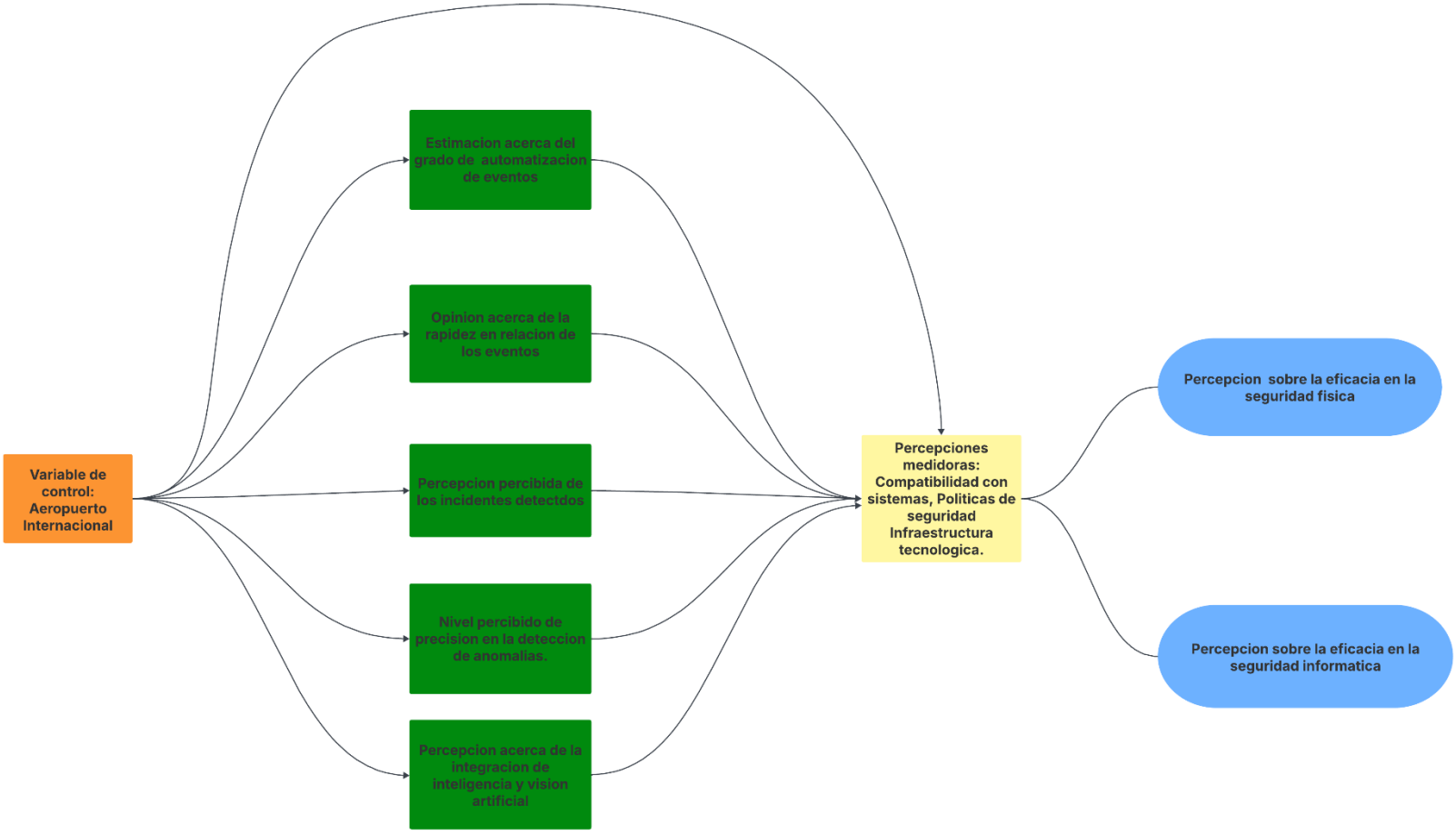
Calidad de la infraestructura tecnológica como ser servidores, redes y cámaras.

Nivel de políticas de seguridad existentes en el aeropuerto.

3.1.2.5 VARIABLES DE CONTROL

Contexto específico del aeropuerto internacional Ramon Villeda Morales (SAP) como lo es la infraestructura de alto valor, los protocolos actuales de seguridad, tiempo promedio de vigilancia efectiva.

Figura 2. VARIABLES DE ESTUDIO.



Fuente: Elaboración propia.

En el presente estudio seguidamente de las variables dependientes e independientes, se identifican factores medidores que pueden coincidir en la relación basada entre la integración de la inteligencia y visión artificial en conjunto de la eficacia del monitoreo de seguridad. Entre estos se resaltan la calidad de los datos utilizados para alimentar y entrenar los sistemas de inteligencia artificial, por la manera que un conjunto de datos sesgado o insuficiente puede engravecer significativamente la capacidad de análisis y detección. La conectividad disponible y la infraestructura tecnológica, donde un ancho de nada limitado o una inestabilidad en la red podrían interrumpir o retrasar el flujo continuo de la información en tiempo real, seguidamente las políticas institucionales de seguridad, el cual determinan los protocolos de acción y el marco normativo par la aplicación de estas tecnologías. Estos medidores no componen el objeto central de la investigación, pero son variables claves que tienen coincidencia con los resultados, de tal manera deben de ser considerados para la comprensión integral de la eficacia del sistema en el contexto

aeroportuario.

3.1.3 OPERAZIONALIZACION DE VARIABLES DE ESTUDIO

En la presente investigación se llevará a cabo la operacionalización de las variables principales, esto con el fin de analizar como la inclusión de sistemas de visión artificial y plataformas de seguridad cibernética influencian en la eficacia de la respuesta y detección frente amenazas en el sistema aeroportuario. Este proceso consta en la transformación de conceptos teóricos en indicadores medibles y concretos, lo que permite la recopilación de información de una manera objetiva que posibilita el análisis de los resultados.

Las principales variables que son seleccionadas incluyen: integración de visión e inteligencia artificial, eficacia en el monitoreo de seguridad física, eficacia en el monitoreo de seguridad cibernética, integración y compatibilidad con sistemas existentes, calidad de la infraestructura tecnológica, nivel de políticas existentes, contexto del aeropuerto y el tiempo promedio de vigilancia efectiva. Estas variables son esenciales para la evaluación tanto de la efectividad de los sistemas automatizados como la capacidad del personal para mantener prácticas de seguridad efectiva.

La variable integración de visión e inteligencia artificial será medida por medio de indicadores específicos que van relacionados con la detección automatizada de eventos y la generación de alertas, como ser:

Percepción del personal acerca de la capacidad del sistema para la detección de incidentes automáticamente.

Opinión acerca del tiempo de correlación de eventos.

Percepción de precisión en la detección de anomalías.

Porcentaje de alertas manuales vs automáticas.

La variable eficacia en el monitoreo de seguridad física se operacionalizará por medio de indicadores relacionados con la protección de respuestas e instalación frente amenazas:

Percepción sobre los intrusos detectados.

Evaluación de la rapidez captados de respuesta ante incidentes físicos.

Opinión acerca del control de acceso efectivo.

Percepción de la reducción de falsos positivos en alertas de seguridad.

La variable eficacia en el monitoreo de seguridad cibernética será evaluada por medio de indicadores que reflejen la capacidad del aeropuerto para responder e identificar las amenazas digitales:

Percepción de educción de incidentes cibernéticos.

Opinión sobre Capacidad de respuesta frente ataques cibernéticos.

Percepción acerca de la Detección de anomalías en los sistemas de control industrial y la red.

Las variables medidoras se operacionalizarán por medio de preguntas sobre:

Calidad de la infraestructura tecnológica, teniendo en consideración redes, servidores, y cámaras utilizadas.

Integración y compatibilidad con sistemas existentes, evaluando la correcta implementación de la inteligencia artificial con los sistemas de monitoreo actuales y sistemas SCADA.

Nivel de políticas de seguridad existentes, evaluando el cumplimiento e implementación de normas internas.

Las variables de control se medirán por medio de:

Percepción del tiempo de vigilancia efectiva, desde la percepción del personal ante la supervisión activa diaria.

Contexto específico del aeropuerto, incluyendo infraestructura crítica y protocolos de seguridad vigente, según el conocimiento y experiencia del personal.

Tabla 7.OPERACIONALIZACION.

Variable	Tipo	Definición Conceptual	Definición Operativa	Indicadores	Instrumento	Escala
Integración de visión e inteligencia artificial	Independiente	Uso de sistemas inteligentes para la detección supervisión de eventos en el aeropuerto	Evaluación de cómo la IA se implementa y funciona con los sistemas existentes	Precisión percibida en detección, percepción sobre tiempo de correlación, percepción del número de incidentes detectados automáticamente, porcentaje percibido de alertas manuales vs automáticas	Entrevista semiestructurada	Intervalo / Narrativa
Eficacia en el monitoreo de seguridad física	Dependiente	Capacidad del aeropuerto para proteger instalaciones y detectar intrusos	Opinión del personal sobre el control de acceso, reducción de falsos positivos y detección de intrusos	Control de acceso percibido, reducción percibida de falsos positivos, intrusos percibidos detectados, percepción de tiempos de respuesta	Entrevista semiestructurada	Intervalo / Narrativa
Eficacia en el monitoreo de seguridad cibernética	Dependiente	Capacidad del aeropuerto para identificar y responder ante incidentes digitales	Opinión del personal sobre la protección y detección de anomalías en la red	Capacidad de respuesta percibidas, percepción de reducción de incidentes cibernéticos, detección de anomalías	Entrevista semiestructurada	Intervalo / Narrativa
Integración y compatibilidad con sistemas existentes	Medidora	Grado de adaptación de la IA a sistemas de monitoreo y SCADA	Percepción del personal sobre el funcionamiento de la IA con los sistemas existentes	Número de fallos de integración percibidos, porcentaje percibido de funcionalidades operativas.	Entrevista semiestructurada	Intervalo / Narrativa
Calidad de la infraestructura tecnológica	Medidora	Estado y capacidad de servidores, redes y cámaras	Opinión del personal sobre la disponibilidad y rendimiento de los equipos	Estado percibido de servidores, rendimiento de redes, operatividad de cámaras	Entrevista semiestructurada	Intervalo / Narrativa
Nivel de políticas de seguridad existentes	Medidora	Cumplimiento de protocolos de seguridad internos	Opinión del personal sobre la implementación y cumplimiento de políticas	Número percibido de políticas implementadas, grado de cumplimiento	Entrevista semiestructurada	Intervalo / Narrativa

Variable	Tipo	Definición Conceptual	Definición Operativa	Indicadores	Instrumento	Escala
Contexto del aeropuerto	Control	Características específicas del aeropuerto que pueden afectar resultados	Percepción del personal sobre la infraestructura y protocolos existentes	Nivel percibido de protección física, número de protocolos vigentes	Entrevista semiestructurada	Intervalo / Narrativa
Tiempo promedio de vigilancia efectiva	Control	Tiempo percibido dedicado por el personal a supervisión continua	Opinión del personal sobre sus turnos y cobertura de vigilancia	Horas de vigilancia diarias, cobertura percibida de turnos	Entrevista semiestructurada	Intervalo / Narrativa

Fuente: Elaboración propia.

3.1.4 HIPOTESIS

Debido al carácter interpretativo y no experimental de la presente investigación, la formulación de hipótesis estadísticas no es metodológicamente adecuada. Las hipótesis no se establecen como supuestos formales a comprobar, sino que pueden modificarse conforme avanzan los razonamientos del investigador y las circunstancias del entorno. Las hipótesis se modifican sobre la base de los razonamientos del investigador y las circunstancias. Desde luego, no se prueban estadísticamente. adquieren un papel distinto al que tienen en la investigación cuantitativa. En primer término, en raras ocasiones se establecen antes de ingresar en el ambiente o contexto y comenzar la recolección de los datos. (Hernandez Sampieri et al., 2014)

En consecuencia, la incorporación de hipótesis alternativas y nulas propias del paradigma cuantitativo no resulta metodológicamente coherente con el objetivo interpretativo de este estudio. Su permanencia implicara asumir procedimientos de contraste estadístico que no forman parte del diseño adoptado. Por este motivo, se prescinde de dichas hipótesis manteniéndose y conservándose un enfoque inductivo y analítico acorde con la naturaleza de la investigación.

3.2 ENFOQUE

En esta investigación se empleará un enfoque cualitativo, El cual se guía en la comprensión y análisis en profundidad de las percepciones y experiencias de los participantes, por medio del cual este enfoque permite la interpretación de los fenómenos en su contexto natural, dando la prioridad del entendimiento y la riqueza descriptiva relativo acerca de la mera ponderación de los datos de acuerdo con Hernández-Sampieri & Mendoza Torres (2018) nos mencionan que el enfoque cualitativo hace su guía por temas o áreas significativos de la investigación, con periodicidad estas actividades sirven en primer lugar para el descubrimiento de cuáles son las preguntas de investigación con mayor relevancia y posteriormente a obtener su respuestas, la acción escrutada se traslada de manera dinámica por ambos sentidos basado en sus hechos e interpretaciones.

La recolección de información será llevada a cabo por medio de las entrevistas semiestructuradas con personal en seguridad informática y el personal del centro de operaciones, con la finalidad de comprender sus opiniones, percepciones y valoraciones acerca del impacto de las tecnologías en la gestión y detección de incidentes. El cual ayudara a construir una comprensión más contextualizada y amplia del como estas herramientas tributan en el fortalecimiento de la seguridad aeroportuaria.

Este enfoque cualitativo es el más adecuado para la investigación por diversas razones:

Profundidad y amplitud: El análisis cualitativo aportara a comprender los factores organizacionales y humanos que influyen en su funcionamiento.

Este enfoque cualitativo es el más adecuado para la investigación por diversas razones:

Profundidad y amplitud: El análisis cualitativo aportara a comprender los factores organizacionales y humanos que influyen en su funcionamiento.

Relevancia para la seguridad: Dada la importancia estratégica del Aeropuerto Internacional Ramon Villeda Morales (SAP), es requerido un enfoque general que abarque tanto la experiencia de los usuarios como la técnica de las herramientas responsables de su operación.

Triangulación de datos: La combinación de las métricas objetivas con percepciones y testimonios incrementan la confiabilidad y validez de los hallazgos.

ALCANCE

Este estudio adopta un alcance descriptivo, el cual esta alineado con la metodología propuesta. De acuerdo con Hernández Sampieri et al. (2014) nos indican que un estudio con alcance descriptivo se basaría en aquel que únicamente tiene la intención de medir el índice donde solo se formulan hipótesis cuando se da la pronosticación de un dato o hecho, de esa manera de forma tentativa se da una pronosticación por medio de una hipótesis, porción o cierta cifra. Esta combinación es eficaz debido a que no solo da la posibilidad de describir las prácticas de seguridad que están en la actualizad, sino que dan la posibilidad de analizar las causas que influyen en la aparición de vulnerabilidades especificas con recursos limitados.

El alcance de esta investigación es principalmente descriptivo, debido a que se orienta a examinar el caso del Aeropuerto Internacional Ramon Villeda Morales (SAP) del Servicio Aeroportuario Nacional con el fin de caracterizar la integración de tecnologías de inteligencia y visión artificial en los sistemas de monitoreo sobre la seguridad cibernética y física. El propósito es documentar de manera explícita el estado actual de estas herramientas con la identificación de los recursos tecnológicos disponibles y el análisis como se aplican en los procesos de prevención, detección y respuesta ante los incidentes. Sin embargo. El estudio también incorpora un alcance explicativo, en tanto busca la comprensión de qué manera la integración de estas tecnologías influye en el nivel de eficacia del sistema de seguridad, subrayando los factores que limitan o favorecen su funcionamiento. Con relación a ese sentido, la investigación no solo describe la situación presente durante el año 2024, además que aporta elementos que permiten la explicación de la relación entre la aplicación de inteligencia y visión artificial, en conjunto con el fortalecimiento de la seguridad integral de la organización, generando un insumo valioso para la toma de decisiones estratégicas y futuros estudios.

3.3 DISEÑO

El diseño de la investigación corresponde a un diseño no experimental, transversal descriptivo de estudio de caso. Siendo no experimental debido a que no se manipulan deliberadamente las variables, caso contrario son analizados en su contexto natural. Es considerado transversal debido a que la recolección de los datos será llevada a cabo en un único momento del tiempo, lo que permitirá la obtención de una visión clara de la situación actual sin extender el análisis a distintos periodos. Por lo que a su vez es descriptivo ya que busca caracterizar de manera

sistemática las practicas, fenómenos y condiciones presentes en la unidad de estudio, además es pretende analizar e identificar los factores que influyen en dichas condiciones, brindando una comprensión más profunda de las relaciones existentes. La elección del estudio de caso facilita el análisis detallado y contextualizado de la problemática en una unidad específica, aportando evidencia que puede apoyar de base para reflexiones más amplias.

3.4.1 POBLACION

Esta investigación se desarrolla bajo la modalidad de un análisis en profundidad de la Servicio Aeroportuario Nacional, Honduras. Como una unidad de estudio. De igual manera Yin (2017) menciona que los estudios de caso son pertinentes cuando se busca la comprensión de fenómenos contemporáneos en un contexto real, particularmente cuando la frontera entre el contexto y el fenómeno no está claramente delimitada.

Para la determinación del tamaño exacto de la población, se consultaron las fuentes oficiales del servicio aeroportuario nacional mediante organigramas, verificando la relación del personal descrito atribuido a la Unidad de Tecnologías de la información. Por medio de este proceso se identificaron las unidades de análisis pertinentes para la investigación, cumpliendo con los criterios de inclusión previamente definidos.

Tabla 8. POBLACION DE ESTUDIO EN LA UNIDAD DE TECNOLOGIAS DE LA INFORMACION DEL SAN.

Área	Total de personal operativo
Unidad de tecnologías de la información	7

Fuente: (Dirección de despacho, 2025)

Esta población es clara para la evaluación de la eficacia de los sistemas de inteligencia y visión artificial, debido a que desde el centro de operaciones se determina el funcionamiento real de la seguridad y monitoreo del Servicio Aeroportuario Nacional.

3.4.2 MUESTRA

En esta investigación, la muestra coincide con la totalidad de la población, conformada por siete personas que desempeñan funciones desde el centro de operaciones en la Unidad de Tecnologías de la información. Debido a que se trata de una población pequeña y directamente relacionada al objeto de estudio, se trabajara con la totalidad de los sujetos, por lo cual permite la máxima saturación teórica y la captura de la totalidad de perspectivas disponibles. De esta forma

se asegura que los descubrimientos sean reflejados de una manera integral las valoraciones y experiencias del personal involucrado en el uso y gestión de los sistemas de visión e inteligencia artificial. Asegurando de esa manera la relevancia y aplicabilidad de los resultados en el contexto preciso de la seguridad física y cibernética del aeropuerto.

De esa manera Hernández-Sampieri & Mendoza Torres (2018) nos explican que cuando la población es estrecha y accesible en su cabalidad, resulta no indispensable realizar técnica de muestreo, por lo tanto se puede trabajar con todos los elementos que estén disponibles. Por la manera en que están diseñadas para la selección de una parte representativa de amplios conjuntos, eliminando la eventualidad de un error muestral.

3.4.3 TECNICAS DE MUESTREO

La técnica de muestreo utilizada es esta investigación corresponde a un muestreo no probabilístico de tipo intencional. Debido a que la muestra está compuesta exclusivamente por el personal operativo del Servicio Aeroportuario Nacional, quienes cumplen un papel directo en la gestión y operación de los sistemas de inteligencia y visión artificial para el monitoreo de seguridad cibernética y física. No es aplicado un muestreo probabilístico, debido a que la selección no se realizó al azar y todos los sujetos fueron incluidos por su relevancia para los objetos de estudio. A pesar de que la muestra coincide con la totalidad de la población, se mantiene dentro del enfoque no probabilístico intencional, porque la inserción se rige en criterios de experiencia y pertinencia, afirmando la validez del análisis y saturación lógica.

Este método abarca las recomendaciones de Otzen & Manterola (2017) donde mencionan que la técnica de muestreo no probabilístico intencional permite la selección de casos característicos de una población limitándose la muestra a solo estos casos, donde es utilizada en escenarios en la que la población es altamente variable y por consiguiente la muestra es pequeña.

Los estudios de casos tienen un lugar distintivo en la investigación de evaluación en la que hay al menos cuatro aplicaciones diferentes. Lo más importante es explicar los presuntos vínculos causales en las intervenciones de la vida real que son demasiado complejas para la encuesta o las estrategias experimentales. (Yin, 2009, p.19)

3.4.4 CRITERIOS DE SELECCIÓN DE LA MUESTRA

Durante la selección de la muestra para esta investigación, se definieron criterios de exclusión e inclusión minuciosos para el aseguramiento de los participantes elegidos de manera

que aporten información relevante al estudio, centrado en la efectividad de los sistemas de inteligencia y visión artificial en el monitoreo de seguridad cibernética y física del Servicio Aeroportuario Nacional. Estos principios acuerdan específicamente que integrantes del personal operativo sean considerados, certificando que los datos obtenidos reflejen de manera fiel las actividades reales de control y operación de los sistemas, concediendo un análisis pertinente sobre su eficacia y desempeño en la seguridad de la planta.

3.4.4.1 CRITERIOS DE INCLUSION Y CRITERIOS DE EXCLUSION

Tabla 9.CRITERIOS DE INCLUSION Y CRITERIOS DE EXCLUSION

Criterio	Inclusión	Exclusión
Experiencia en sistemas de monitoreo.	Serán incluidos el personal que tenga experiencia comprobable en la supervisión u operación de los sistemas de inteligencia y visión artificial del aeropuerto.	Se excluirá al personal sin interacción o experiencia con los sistemas de monitoreo.
Disponibilidad para participar.	Se incluirá al personal disponible para participar en la recolección de datos durante el periodo del estudio.	Sera excluido el personal que no pueda participar por restricciones de tiempo o funciones asignadas fuera del área de monitoreo.
Personal operativo.	Se incluirá únicamente al personal operativo que interactué directamente con los sistemas de inteligencia y visión artificial.	Se excluirá al personal técnico externo, administrativo o cualquier empleado que no utilice o supervisé los sistemas de monitoreo.

Fuente: Elaboración Propia.

3.4.4 TÉCNICAS, INSTRUMENTOS Y PROCEDIMIENTOS APLICADOS

En este estudio será adoptado un enfoque cualitativo con el objetivo de explorar de una manera más profunda las percepciones del personal de la unidad de tecnologías de la información del servicio Aeroportuario Nacional acerca de la visión e integración artificial en los procesos de seguridad física y cibernética.

La principal técnica de recolección de información estará basada en la entrevista semiestructurada y preguntas abiertas, delineada para profundizar en las opiniones y experiencias del personal. Este planeamiento permitirá abordar de manera directa la percepción de los participantes con relación al funcionamiento e implementación de los sistemas inteligentes.

Basado en esta manera, se asegura que los datos se reflejen en la interpretación subjetiva del personal y se refleje una compresión integral acerca de la eficacia de la inteligencia artificial en los procesos de seguridad física y cibernética del Servicio Aeroportuario Nacional.

3.5.1 TECNICAS

Se emplearán técnicas cualitativas, por medio de la aplicación de la entrevista semiestructurada, por lo que permitirán la exploración en profundidad de las valoraciones y experiencias de los participantes con relación a la integración de visión computacional e inteligencia artificial en la ciber seguridad. Por lo que esta técnica posibilitara la obtención de información flexible pero guiada, amparando la riqueza de los datos y la identificación de patrones significativos. De esa misma manera, será complementado con la revisión de literatura especializada, que ayudará como referente para enriquecer y contrastar los hallazgos.

Las entrevistas semiestructuradas permiten a los investigadores explorar en profundidad las perspectivas, experiencias y percepciones de los participantes. Pueden sacar a la luz relatos ricos, percepciones personales y detalles contextuales que quizá no surjan en formatos de entrevista más estandarizados. (Salomão, 2023)

3.5.2 INSTRUMENTOS ELABORADOS.

El instrumento principal será una guía de entrevistas semiestructuradas, aplicada en línea por medio de herramientas digitales seguras. La guía será organizada en bloques temáticos como ser formación y conocimiento en ciberseguridad, característicos generales del personal, recursos y condiciones operativas, opiniones abiertas acerca de oportunidades de mejora y desafíos, percepción acerca de la integración de inteligencia y visión artificial.

Las técnicas de recolección de los datos pueden ser múltiples. Por ejemplo: En los estudios cualitativos: entrevistas exhaustivas, pruebas proyectivas, cuestionarios abiertos, sesiones de grupos, biografías, revisión de archivos, observación, entre otros. Debemos insistir en que tanto en el proceso cualitativo es posible regresar a una etapa previa. (Hernández Sampieri et al., 2014, p. 14)

Además, se incorporará un apartado inicial con el consentimiento informado, por el cual se explicará la finalidad de la investigación, el carácter voluntario de la participación, resguardo de la investigación y el uso académico de los datos.

3.5.3 PROCEDIMIENTOS

El proceso de aplicación de los instrumentos proseguirá varias fases:

Elaboración y validación de los instrumentos: Las guías de entrevistas fueron revisado por especialistas en metodología y ciberseguridad para el aseguramiento de la pertinencia y

claridad de cada ítem.

Aunque ciertamente hay una revisión inicial de la literatura, ésta puede complementarse en cualquier etapa del estudio y apoyar desde el planteamiento del problema hasta la elaboración del reporte de resultados (la vinculación entre la teoría y las etapas del proceso se representa mediante flechas curvadas). (Hernández Sampieri et al., 2014, p. 8)

Realización de entrevistas: Las entrevistas semiestructuradas serán realizadas de manera virtual con el personal seleccionado, con la utilización de herramientas digitales seguras, donde cada entrevista tendrá una duración aproximadamente de 20 a 30 min, siendo grabada únicamente con el consentimiento informado de los participantes.

A veces la experiencia y la observación constante ofrecen materia potencial para el establecimiento importante, y lo mismo se dice de la intuición. Desde luego, cuanto menor apoyo empírico previo tenga, se deberá tener mayor cuidado en su elaboración y evaluación. (Hernández Sampieri et al., 2014, p. 106)

Gestión y análisis de datos: Las grabaciones de las entrevistas serán transcritas de una manera literal y analizadas por medio de técnicas de análisis temático cualitativo, temas emergentes, identificación de patrones, percepciones destacadas acerca de la integración de visión e inteligencia artificial en el monitoreo de la seguridad aeroportuaria. Los datos permanecerán almacenados en un lugar de restringido acceso garantizando la confidencialidad.

El análisis de datos es un proceso crucial que implica la exploración y la interpretación de conjuntos de datos para extraer información significativa, la calidad del análisis de datos depende en gran medida de la precisión y la integridad de los datos recopilados. (Rodríguez, 2024)

3.5 FUENTES DE INFORMACIÓN

En esta sección se presentan las fuentes de información empleadas para el desarrollo de la investigación, por medio del cual ceden el sustento y análisis de los hallazgos obtenidos. Las fuentes primarias abarcan los datos recopilados directamente por medio de entrevistas al personal encargado del monitoreo de seguridad del Servicio Aeroportuario Nacional. Seguidamente, las fuentes secundarias centran estudios previos, manuales técnicos, artículos científicos y documentos institucionales que armonizan el soporte técnico y metodológico para tener comprensión sobre la integración de sistemas de inteligencia y visión artificial en la seguridad

cibernética y física.

3.6.1 FUENTES PRIMARIAS

Las fuentes primarias se obtendrán por medio de la recolección de datos directos a través de entrevistas semiestructuradas. Estas herramientas ceden la recopilación de información detallada y actualizada acerca de la integración de sistemas de inteligencia y visión artificial en el monitoreo de seguridad cibernética y física, sosteniendo un análisis característico del contexto del Servicio Aeroportuario Nacional.

Entrevistas semiestructuradas: Serán realizadas a expertos en Ciber seguridad y seguridad industrial con conocimiento sobre sistemas de monitoreo inteligente. Estas entrevistas rastrearan temas como la efectividad de la inteligencia artificial en la detección de incidentes, vulnerabilidades en el aeropuerto, estrategias recomendadas para la optimización de la seguridad integral.

La guía de los temas (al igual que en el caso de las entrevistas) puede ser estructurada, semiestructurada o abierta. En la estructurada los temas son específicos y el margen para salirse de éstos es mínimo; en la semiestructurada se presentan temas que deben tratarse, aunque el moderador tiene libertad para incorporar nuevos que surjan durante la sesión, e incluso alterar parte del orden en que se tratan; finalmente, en la abierta se plantean puntos generales para cubrirse con libertad durante la sesión. (Hernández Sampieri et al., 2014)

La información recolectada por medio de las entrevistas será comprobada con las fuentes secundarias, el cual permitirá la verificación en qué medida las percepciones del recinto tienen coincidencia o dilatan sobre las recomendaciones técnicas internacionales. Por lo cual, se da aseguramiento que las conclusiones no tengan dependencia precisamente de opiniones individuales, caso contrario que tengan respaldo en evidencia de estándares reputados.

3.6.2 FUENTES SECUNDARIAS

Las fuentes secundarias proporcionarán el marco teórico y conceptual junto a los datos primarios para la contextualización de los hallazgos donde se incluirán:

Estudios e informes de organismos internacionales: Se consultarán documentos de referencia de la Organización de Aviación Civil Internacional (OACI), el Airports Council International (ACI). Donde estos informes brindan estadísticas y lineamientos globales acerca de

la ciberseguridad en aeropuertos, brindando una visión comparativa que permitirá el contraste de la situación del Servicio Aeroportuario Nacional con las mejores prácticas internacionales.

El sector de la aviación civil depende cada vez más de la disponibilidad de los sistemas de tecnología de la información y las comunicaciones, así como de la integridad y confidencialidad de los datos. La amenaza que representan los posibles incidentes cibernéticos para la aviación civil está en constante evolución, y los autores de las amenazas se centran en las intenciones maliciosas, las interrupciones de la continuidad de las actividades y el robo de información por motivos políticos, financieros o de otro tipo. (ICAO, 2019)

Análisis y estudios especializados: Se explorarán reportes técnicos en revistas registradas y publicaciones académicas en conjunto a centros de investigación como IEEE Xplore que se acometan en la integración de la visión e inteligencia artificial en la seguridad de infraestructuras de alto valor. Estos estudios aportan análisis actualizados y evidencia empírica acerca de la aplicación de dichas tecnologías en el sector aeroportuario.

Una fuente muy valiosa de datos cualitativos son los documentos, materiales y artefactos diversos. Nos pueden ayudar a entender el fenómeno central de estudio. Prácticamente la mayoría de las personas, grupos, organizaciones, comunidades y sociedades los producen y narran, o delinean sus historias y estatus actuales. Le sirven al investigador para conocer los antecedentes de un ambiente, así como las vivencias o situaciones que se producen en él y su funcionamiento cotidiano y anormal. (Hernández Sampieri et al., 2014, p. 415)

Literatura metodológica: Serán empleados obras de referencia como lo son las de Hernández Sampieri y otros autores reconocidos en metodología de la investigación, con el fin de sustentar la confiabilidad y validez del diseño metodológico empleado.

Una característica única de la literatura metodológica reside en el tipo de fuentes. Si bien los artículos académicos son las fuentes esperadas para una revisión bibliográfica sobre el problema de investigación, necesitamos un conjunto diferente de materiales para comprender los fundamentos metodológicos del estudio. (Salmons, 2024)

3.6 PLAN DE ANALISIS

El análisis de datos en esta investigación será estructurado en fases sucesivas que integra el enfoque cualitativo, con el propósito de evaluar de manera integral la eficacia en la integración

de inteligencia y visión artificial en el monitoreo de la seguridad cibernética y física en el Servicio Aeroportuario Nacional. Este diseño metodológico cualitativo admitirá la obtención tanto una comprensión profunda de las percepciones y experiencias de los actores, una caracterización del panorama que respalde la formulación de conclusiones recomendaciones solidas.

3.7.1 ANALISIS CUALITATIVO

Fase 1: Transcripción y organización de datos.

Transcripción literal de las entrevistas semiestructuradas efectuadas a expertos, regulando la información de acuerdo con los criterios intuidos en el guion de entrevista.

Fase 2: Codificación temática.

Por medio de un proceso de codificación inicial, se distinguirán subcategorías y categorías vinculadas con los objetivos de la investigación, como ser la percepción de eficacia, barreras de implementación, propuestas de mejora y vulnerabilidades.

Fase 3: Análisis de contenido.

Se efectuará un análisis de contenido para la interpretación de los patrones, significados y vinculaciones emergentes en la testificación de los participantes, cediendo la generación de una compresión profunda acerca de los fenómenos contemplados.

Fase 4: Triangulación cualitativa.

Los resultados obtenidos de las entrevistas serán triangulados con las fuentes secundarias como ser literatura científica, e informes de la OACI con el fin de hacer validación y enriquecimiento de la interpretación basado desde un marco comparativo internacional.

Fase 5: Presentación y síntesis de resultados.

Los descubrimientos serán descritos en narrativas temáticas, remarcando contrastes y coincidencias entre las charlas de los participantes y la documentación examinada, lo que permitirá la formulación de conclusiones sólidas y recomendaciones adaptables al contexto aeroportuario.

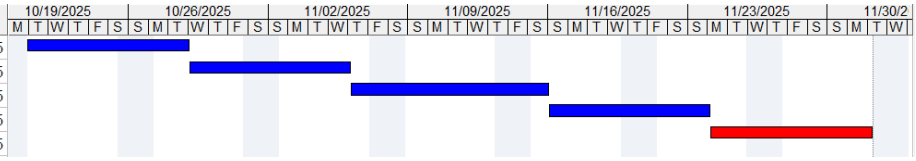
3.7.2 INTEGRACION DE RESULTADOS.

La fase final estará dedicada a la integración de los resultados cualitativos, por medio de la triangulación basados entre los hallazgos recabados de las entrevistas, las fuentes primarias corroboradas y el análisis de contenido. Este proceso brindara enriquecimiento y contraste en la

interpretación, haciendo un fortalecimiento de las conclusiones.

Figura 3. PLAN DE ACCION PARA IMPLEMENTACION.

	WBS	Name	Duration	Start	Finish
1	1	Transcripcion y organizacion de datos.	7d	10/20/2025	10/28/2025
2	2	Codificacion tematica Codificación temática	7d	10/29/2025	11/06/2025
3	3	Análisis de contenido	7d	11/07/2025	11/17/2025
4	4	Triangulacion cualitativa	7d	11/18/2025	11/26/2025
5	5	Presentación y síntesis de resultados.	7d	11/27/2025	12/05/2025



Fuente: Elaboración propia.

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

Este capítulo presenta los resultados obtenidos del análisis cualitativo realizado en el Servicio Aeroportuario Nacional (SAN), Honduras, orientado a la evaluación de la eficacia en la integración de sistemas de visión e inteligencia artificial dentro del monitoreo de seguridad cibernética y física. El estudio se centró en la comprensión de las experiencias, valoraciones y percepciones del personal técnico y de seguridad dentro del contexto aeroportuario, teniendo en consideración la experiencia del personal técnico, los factores organizacionales y las condiciones operativas que influyen en su funcionamiento.

Por medio del análisis exploratorio de datos (EDA) asistido por la herramienta Python, se sistematizaron y organizaron las categorías emergentes y respuestas, agilizando la identificación de percepciones claves, patrones de eficacia y temas recurrentes en el uso combinado de inteligencia y visión artificial. El análisis facilito establecer una comprensión profunda acerca de cómo los sistemas integrados contribuyen a la detección temprana de incidentes, la mejora en la coordinación entre las áreas de seguridad cibernética y física, y la optimización de los recursos tecnológicos. De esa misma manera, se evidenciaron desafíos y limitaciones presentes en su aplicación dentro del entorno aeroportuario nacional.

Los resultados aquí expuestos ceden la valoración acerca de la pertinencia y relevancia de la integración tecnológica como una herramienta de apoyo a la seguridad operativa de SAN, brindando evidencia practica para futuras decisiones estratégicas en materia de gestión de riesgos e infraestructura. A lo largo del capítulo, se expone en primer lugar a descripción de los datos recolectados y el proceso de codificación de las respuestas obtenidas. Seguidamente se detallan los principales hallazgos derivados de los análisis y las categorías emergentes, complementados de representaciones visuales que facilitan su interpretación. Posteriormente, se discuten los resultados en función y los marcos teóricos revisados. Por último, se expone las bases para la discusión final del trabajo.

4.1 ANALISIS EXPLORATORIO DE DATOS

4.1.1 DESCRIPCION GENERAL DEL CONJUNTO DE DATOS

El presente análisis se basa en un conjunto de datos logrados por medio de entrevistas semiestructuradas aplicadas al personal operativo del Servicio Aeroportuario Nacional (SAN),

Honduras. Estuvo adecuada a 7 participantes quienes representan el personal directo correlacionado con las operaciones de gestión y monitoreo de seguridad cibernética y física en el entorno aeroportuario.

Las variables de análisis no se definieron en términos numéricos, si no temáticos, agremiando la información en categorías emergentes.

De esta manera, el conjunto de datos se constituye una base interpretativa acaudalada en contenido descriptico, permitiendo comprender como los miembros del personal operativo experimentan y perciben la integración de inteligencia y visión artificial en la seguridad aeroportuaria.

4.1.2 LIMPIEZA Y PREPARACION DE LOS DATOS.

Se analizaron aspectos claves presentes en las entrevistas, tales como la percepción acerca de la eficacia de los sistemas de monitoreo de seguridad, la rapidez en la detección de incidentes, la integración de visión artificial con plataformas de seguridad informática y la experiencia del personal en la gestión de alertas.

Seguidamente, se evaluaron temas recurrentes relacionados con la seguridad digital y física, el nivel de coordinación entre los sistemas humanos y tecnológicos, la percepción de los sistemas utilizados y la implementación de procedimientos de respuesta ante incidentes.

```
Exploración inicial del conjunto de datos:
                          Hablante  Edad  ... Longitud                                        Texto_Puro
0     Lennyn Orlando Bonilla Garcia    25  ...     1501  Transcript november 4, 2025, 12:02am marcio ja...
1               Cristian Chinchilla    31  ...     1525  Transcript october 26, 2025, 8:14pm marcio jav...
2                  Carlos Hernandez    34  ...     2154  Transcript november 3, 2025, 9:30pm marcio jav...
3                      Julio Rivera    27  ...     1451  Transcript november 5, 2025, 12:45am marcio ja...
4  Roberto Carlos Serrano Velasquez    45  ...     1991  Transcript october 26, 2025, 8:37pm marcio jav...
5                  Sileny Hernandez    24  ...     3273  Transcript november 3, 2025, 6:33pm marcio jav...
6                    Yasser Bonilla    39  ...     2734  Transcript october 25, 2025, 12:34am marcio ja...

[7 rows x 8 columns]
```

Figura 4. EXPLORACION DE LOS DATOS.

Fuente: Elaboración propia.

El análisis presentado en la exploración de datos muestra una visualización estructurada de datos categóricos, permitiendo la comprensión de la frecuencia y distribución de diferentes variables a través de grafico de barras y tablas, facilitando la interpretación de los datos al ser mostrados de una manera clara las categorías de respuesta y su recurrencia dentro del conjunto de

información.

Cada variable contiene un número determinado de valores únicos, lo que facilita la identificación de patrones y tendencias relevantes. Por lo tanto, la ausencia de datos faltantes prioriza una representación precisa y completa. Los gráficos de barras brindan una vista rápida de la distribución de las respuestas brindadas. Brindando una detección sobre la concentración de datos y posiblemente discrepancia dentro del análisis.

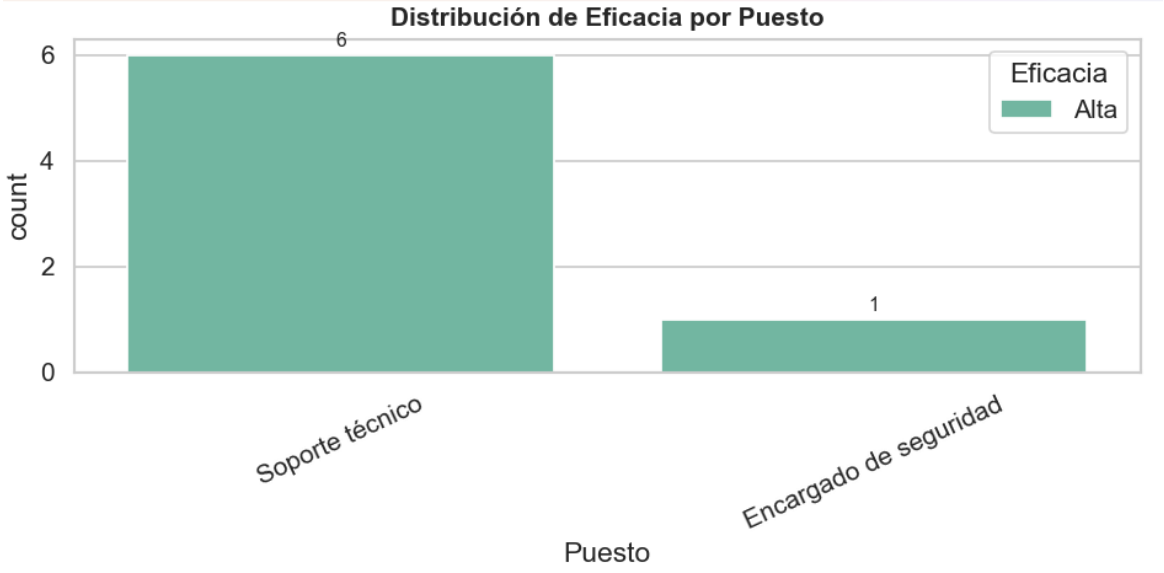


Figura 5. DATA EXPLORER 1.

Elaboración propia

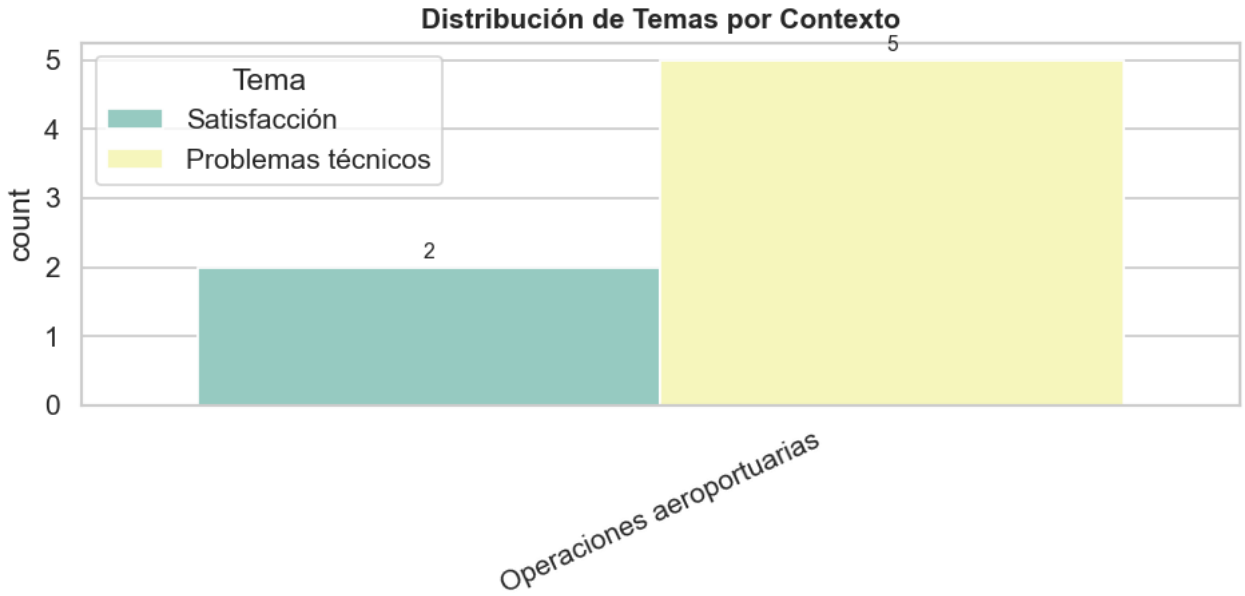


Figura 6. DATA EXPLORER 2.

Fuente: Elaboración propia.

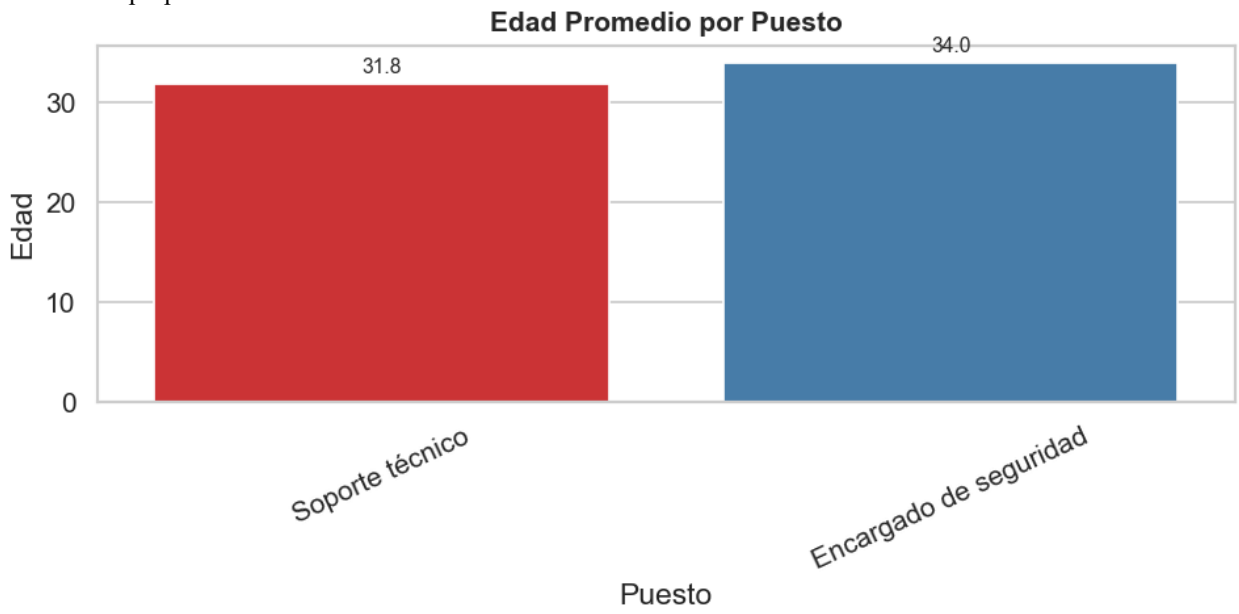


Figura 7. DATA EXPLORER 3.

Fuente: Elaboración propia.

Los entrevistados con puesto de soporte técnico tienden a asociar alta eficacia con contextos técnicos.

Los supervisores mencionan más temas de sugerencias y operaciones aeroportuarias, mostrando visión macro.

A mayor edad, las respuestas son más extensas, lo que indica experiencia o mayor profundidad en la reflexión.

Contextos técnicos están relacionados con percepciones positivas hacia la IA, mientras que los operativos con retos prácticos.

Para la etapa de preparación y limpieza textual, se ejecutó por medio de Python que integro distintas librerías de análisis de texto y procesamiento. Se empleo NLTK para la eliminación de stop words en idioma español, el manejo de lenguaje natural y la normalización de texto, RE para expresiones regulares para suprimir signos, espacios innecesarios y caracteres no alfabéticos, PANDAS para la estructuración y organización del conjunto de datos. Este proceso incluyo la tokenizacion, la depuración de nombres propios sin relevancia analítica, la conversación del texto

a minúsculas y la eliminación de palabras carentes de contenido semántico significativo.

4.1.3 VARIABLES ANALIZADAS

El conjunto de datos incluye variables que reflejan las experiencias y percepciones del personal operativo con relación de la eficacia de los sistemas de inteligencia y visión artificial implementados en el Servicio Aeroportuario Nacional.

Las variables analizadas se clasifican en:

Percepción de eficacia del sistema integrado.

Experiencia del personal con la integración tecnológica.

Percepción acerca de la reducción de incidentes.

Coordinación entre seguridad cibernética y física.

Identificación de desafíos operativos y técnicos.

Satisfacción general con el desempeño del sistema.

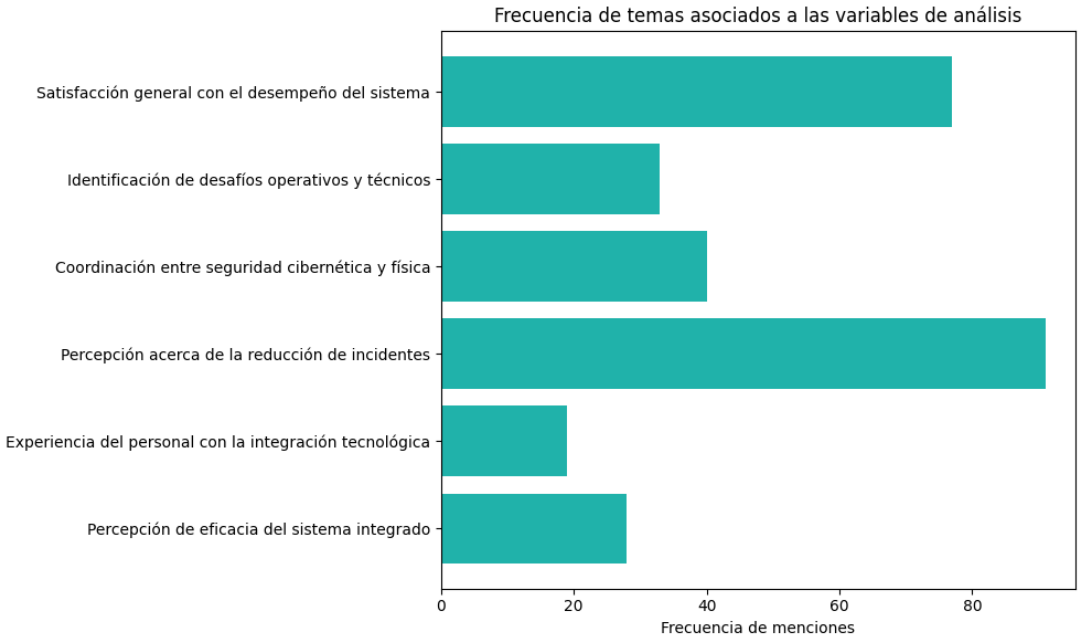


Figura 8. FRECUENCIA DE TEMAS POR VARIABLE

Fuente: Elaboración propia.

La figura 8 muestra la frecuencia de menciones asociadas a las variables del análisis, obtenidas a partir de las entrevistas aplicadas al personal operativo del Servicio Aeroportuario

Nacional. El propósito de esta visualización es identificar las tendencias temáticas y patrones discursivos que manifiestan la percepción del personal ante la integración de sistemas de visión e inteligencia artificial en el monitoreo de seguridad cibernético y física.

Los resultados evidencian que la variable con mayor frecuencia de menciones retribuye a la satisfacción general con el desempeño del sistema, lo que sugiere una valoración positiva por parte del personal acerca de la precisión, funcionamiento y utilidad de las tecnologías implementadas.

Además, sobresale la percepción acerca de la reducción de incidentes, denotando que los entrevistados asocian la integración tecnológica con una disminución de eventos de riesgo y una mejora en la capacidad de respuesta frente a incidentes tanto cibernéticos como físicos. De igual forma, las variables identificación de desafíos operativos y técnicos exponen una frecuencia media, evidenciando que, aunque el sistema es percibido como eficaz, aunque aún existen retos de mantenimiento y limitaciones técnicas que deben ser abordados para la optimización de su funcionamiento. Por último, las variables de experiencia del personal con la integración tecnológica y la percepción de eficacia del sistema integrado presentan una menor frecuencia, por el cual podría asociarse a que el proceso de aprendizaje y de adaptación se encuentra en desarrollo dentro del personal operativo.

En términos globales, el análisis muestra una tendencia positiva en la percepción del personal hacia la integración tecnológica, complementada de reconocimiento de mejoras operativas y una aceptación creciente del sistema, aunque con la presencia de retos técnicos que requieren consolidación continua.

En conjunto, estas tendencias demuestran una relación preliminar entre la satisfacción del personal, la reducción de incidentes, la eficacia percibida del sistema, lo que propone que la integración de inteligencia y visión artificial está contribuyendo al fortalecimiento de la seguridad cibernética y física en el entorno aeroportuario.

4.1.3.1 VALORES FALTANTES

```
 Valores nulos detectados:
Hablante      0
Edad          0
Puesto        0
Tema          0
Eficacia      0
Contexto      0
Longitud      0
Texto_Puro    0
dtype: int64
```

Figura 9. DATOS FALTANTES.

Fuente: Elaboración propia.

En relación con los datos faltantes, se empleó la librería pandas de Python, para el análisis de la presencia de valores nulos en el conjunto de datos. Esta función permite la identificación de una forma precisa las columnas que contienen datos ausentes de los valores afectados, Al ejecutar el análisis, se observó que todas las variables presentan un valor cero en la columna correspondiente, lo que confirma que no existen datos faltantes en ellas, de manera que se concluye que el conjunto de datos esta completo y no es necesario la aplicación de técnicas de sustitución o eliminación de valores.

4.1.3.2 VALORES ATIPICOS

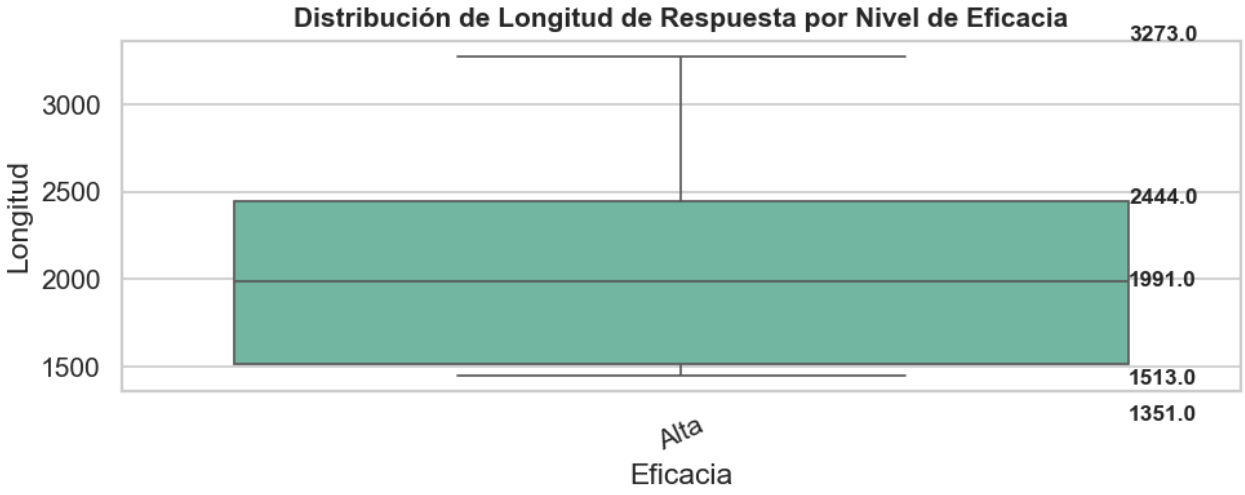


Figura 10.DIAGRAMA DE CAJA.

Fuente: Elaboración propia

Los bigotes muestran la distribución de la longitud de las respuestas asociadas al nivel de

eficacia. La mediana se sitúa aproximadamente en 1991 caracteres, demostrando que la mitad de las respuestas se concentran alrededor de ese valor. Los cuartiles reflejan que el 50% central de los datos rondan entre 1513 y 2444 caracteres lo que sugiere una variabilidad moderada en la cantidad de información brindada por los participantes. Los valores extremos más altos y más bajos 3273 y 1351 caracteres evidencian que, a pesar de que existen respuestas más extensas o breves, estas no distorsionan el patrón general. Por lo tanto, la distribución muestra que las respuestas con nivel de eficacia alta tienden a ser amplias de manera relativa y consistentes en su extensión.

4.1.4 CONCLUSION DEL EDA

El análisis exploratorio de datos ejecutado a partir de las entrevistas aplicadas al personal operativo del Servicio Aeroportuario Nacional posibilito la identificación de los principales patrones, tendencias y temas discursivas relacionadas con la integración de sistemas de inteligencia y visión artificial en el monitoreo de seguridad cibernética y física.

Los hallazgos más relevantes:

Eficacia del sistema integrado: Las menciones más frecuentes se enlazan con la percepción de que la incorporación de inteligencia y visión artificial ha mejorado la capacidad de respuesta y detección ante incidentes, brindando una vigilancia más oportuna. El personal reconoce una mayor eficacia en las operaciones de monitoreo físico, principalmente en el control de acceso.

Mejoras operativas y reducción de incidentes: Los entrevistados asocian la integración tecnológica con una disminución en la cantidad de alertas o eventos tanto en el ámbito cibernético como físico. Se percibe que la automatización en la detección de irregularidades ha contribuido a minimizar la intervención manual.

Satisfacción general del personal: La variable con mayor frecuencia de menciones ha sido la satisfacción con el desempeño del sistema, destacando la confianza del personal en la funcionalidad y estabilidad de las herramientas basadas en inteligencia artificial. Esta tendencia refleja una aceptación positiva del cambio tecnológico abarcando el entrono aeroportuario.

Coordinación entre seguridad cibernética y física: El análisis temático evidencio una mejora en la colaboración y comunicación entre ambas áreas, lo cual propone que la inteligencia artificial está sirviendo como un elemento integrador dentro de la estructura de seguridad

institucional.

Adaptación del personal y desafíos técnicos: Aun con la percepción positivos general, se identifican retos técnicos y operativos, principalmente relacionados con la compatibilidad de algunos componentes, la necesidad de capacitación continua del personal e infraestructura tecnológica existente.

4.2 INFORME DE PROCESO DE RECOLECCIÓN DE DATOS

4.2.1 DESCRIPCION DEL PROCESO

La recolección de datos se llevó a cabo por medio de la aplicación de entrevistas semiestructuradas mediante la plataforma de Microsoft Teams al personal operativo y técnico del área y seguridad del Servicio Aeroportuario Nacional (SAN), en las instalaciones del Aeropuerto Ramon Villeda Morales, San Pedro Sula, Honduras.

El proceso se desarrolló en tres etapas:

Diseño y validación del instrumento:

Se elaboro una guía de entrevista con base a los objetivos específicos de la investigación, centrándose en explorar la percepción de los colaboradores acerca de la eficacia, desempeño y desempeño de los sistemas de visión e inteligencia artificial implementados. La guía fue validada por un especialista en seguridad tecnológica.

Aplicación de entrevistas:

Las entrevistas se realizaron de manera virtual entre el 21 de octubre y el 7 de noviembre del 2025, cada sesión tuvo una duración promedio de 15-30 min, y fueron registradas por medio de grabaciones de audio con previo consentimiento y notas de campo.

Procesamiento y transcripción:

Las entrevistas fueron transcritas de manera automática y procesadas utilizando Python con librerías de análisis, con el fin de identificar patrones de frecuencia, temas recurrentes y relaciones entre categorías.

Recursos y tiempos utilizados:

Duración total: 3 semanas

Recursos:

Equipos portátiles.

Software: Microsoft Teams, Python.

4.2.2 CONTINUIDAD DEL PROCESO

Para realizar el análisis acerca de la eficacia del sistema integrado de monitoreo basado en visión e inteligencia artificial, se definió un proceso de recolección de datos basado en criterios operáticos y técnicos que permitieran obtener información representativa, contextual y relevante.

Tamaño de la muestra:

El estudio incluyo 7 ~~8~~ entrevistas semiestructuradas aplicadas al personal del área de seguridad e infraestructura tecnológica del aeropuerto, centrándose tanto en la seguridad cibernética como física.

Criterios de selección:

1. Participación directa en operación de monitoreo: Se seleccionaron colaboradores que trabajan de forma activa con los sistemas de cámaras, sensores, vigilancia y plataforma de inteligencia artificial.
2. Conocimiento sobre la integración tecnológica: Los participantes debían tener conocimiento o interacción acerca de la implementación de herramientas basadas en inteligencia y visión artificial.
3. Experiencia mínima de un ano: Se incluyo personal con experiencia comprobada en la supervisión u operación de sistemas de monitoreo aeroportuario.

Perfil de los participantes:

Los entrevistados correspondieron a soporte técnico y analistas tecnológicos, correspondiente al Servicio Aeroportuario Nacional.

4.2.3 INSTRUMENTOS UTILIZADOS

El instrumento principal de recolección de datos fue la entrevista semiestructurada, trazada con preguntas abiertas que facilitaron la exploración de experiencias, opiniones y percepciones acerca de la eficacia de la integración tecnológica.

Características del instrumento:

Conformada por 10 preguntas guía distribuidas en seis dimensiones:

1. Percepción de eficacia del sistema integrado.
2. Coordinación entre seguridad cibernética y física.
3. Experiencia del personal con la integración tecnológica.
4. Percepción sobre la reducción de incidentes.
5. Satisfacción general con el desempeño del sistema.
6. Identificación de desafíos operativos y técnicos.

- Se garantizo la validación del instrumento por medio de la revisión de experto y la aplicación piloto con un miembro del área técnica.
- Las entrevistas fueron grabadas y transcritas textualmente.

4.2.4 DIFICULTADES ENCONTRADAS

En el transcurso de la recolección de datos se presentaron algunas dificultades de logística y técnicas, las cuales fueron abordadas por medio de estrategias de mitigación adecuadas.

Problemas durante las estrategias y recolección aplicadas:

Condiciones del entorno físico:

- El ruido ambiental en el área de monitoreo afecto parcialmente la calidad del audio grabado.
- Estrategia aplicada: Complementación con validación posterior con los entrevistados y notas de campo.

Disponibilidad limitada del personal:

- Debido a la naturaleza operativa del aeropuerto, varios participantes se encontraban en turnos rotativos o incluso en atención directa de incidentes.
- Estrategia aplicada: Entrevistas realizadas y reprogramación flexible en diferentes horarios, incluyendo fines de semana.

Limitaciones en el tiempo de respuesta:

Algunos participantes ofrecieron respuestas breves por carga laboral.

Estrategia aplicada: Aplicación de ejemplos y reformulación de preguntas practicas durante la entrevista.

4.2.5 CONSIDERACIONES ETICAS

El proceso de recolección de datos se realizó bajo los principios éticos de respeto, consentimiento y confidencialidad, basándose en los lineamientos institucionales del Servicio Aeroportuario Nacional.

4.2.5.1 CONSENTIMIENTO INFORMADO

Los participantes autorizaron el uso de la información únicamente para fines investigativos, sin divulgación individual de datos personales.

Antes de cada entrevista, se explicó el propósito académico del estudio, asegurando que la participación se basara totalmente de manera confidencial y voluntaria.

4.2.5.2 CONDIDENCIALIDAD Y PROTECCION DE DATOS

Los archivos digitales (texto y audio) se almacenaron de una forma segura en carpetas protegidas y de acceso restringidos.

Las entrevistas fueron codificadas con identificadores anónimos, sin vincular cargos específicos o nombres.

4.2.5.3 ASPECTOS ETICOS ADICIONALES

Se mantuvo la neutralidad del investigador durante el análisis y la recopilación.

Los resultados fueron tratados de manera agregada, reverenciando la privacidad de los colaboradores.

Se evito cualquier tipo de presión o de imposición institucional.

4.3 TEMAS EMERGENTES

4.3.1 CAPACIDADES POTENCIADAS POR LA INTEGRACION TECNOLOGICA.

Esta categoría conceptual agrupa los elementos admiten la comprensión de igual manera la integración de tecnologías como la inteligencia artificial, sistemas automatizados y visión artificial para fortalecer las capacidades operativas del aeropuerto. Partiendo del análisis computacional de frecuencias léxicas se identificaron dos subcategorías precisión y credibilidad

seguidamente eficacia operativa, identificadas directamente con la mejora del desempeño operativo y la reducción del error humano percibido en el personal operativo.

Tabla 10.EFICACIA OPERATIVA

Palabra	Frecuencia
tiempo	27
rapidez	9
ágil	0
centralizado	3
automatizado	5
automatización	0
respuesta	17

Fuente: Elaboración propia.

La tabla 10. Demuestra que los términos tiempo (27 menciones) y respuesta (17 menciones) destacan como los elementos más vinculados sobre la percepción de la eficiencia operativa por parte del personal. Por lo tanto, los entrevistados relacionan altamente la integración tecnológica con una reducción significativa de los tiempos de reacción y con una mayor agilidad en la atención de incidentes operativos. A pesar de que las palabras automatizado (5 menciones) y centralizado (3 menciones) presentan valores moderados, su presencia reafirma que los participantes distinguen beneficios en la automatización y simplificación de procesos antes fragmentados.

Tabla 11.PRECISION Y CREDIBILIDAD

Palabra	Frecuencia
preciso	2
precisión	3
errores	6
falsos	17
patrones	5
detección	0
alerta	13

Fuente: Elaboración propia.

En la Tabla 11. Destacan falsos (17 menciones), alerta (13 menciones), errores (6 menciones) lo que marca la precisión del sistema es una preocupación central para el personal. Los entrevistados reconocen que la integración tecnológica reduce falsos positivos y mejora la confiabilidad de las alertas. Términos como patrones (5 menciones) demuestran que se valora la capacidad del sistema para identificar comportamientos relevantes. A pesar de que precisión (3 menciones) y preciso (2 menciones) aparezcan menos, refuerzan la percepción de un monitoreo riguroso.

4.3.2 DESAFIOS PARA LA EFECTIVIDAD DEL SISTEMA

Tabla 12.HABILITADORES TECNICOS.

Palabra	Frecuencia
hardware	1
infraestructura	1
potencia	1
equipos	3
costo	2
mantenimiento	1
tecnología	1
limitante	1

Fuente: Elaboración propia.

La tabla 12. Demuestra frecuencias bajas, pero reveladoras, en términos como equipos (3 menciones) y costo (2menciones), lo que indica que los entrevistados reconocen que la efectividad del sistema tiene dependencia de contar con la inversión necesaria y tecnología adecuada para sostenerla y palabras como hardware (1 mención), infraestructura (1 mención) y potencia (1 mención) muestran la necesidad de recursos técnicos robustos para operar sistemas avanzados. En general, los datos demuestran que la capacidad técnica sigue siendo un desafío clave para la integración tecnológica.

Tabla 13.FACTORES ORGANIZACIONALES.

Palabra	Frecuencia
capacitación	5
capacitacion	0
usuario	3
resistencia	1
aprendizaje	1
adaptacion	0
entrenamiento	1

Fuente: Elaboración propia.

En la Tabla 13. Capacitación (5 menciones) y usuario (3 menciones) destacan como los principales desafíos organizacionales, resaltando que el personal requiere mayor formación para utilizar adecuadamente las nuevas herramientas tecnológicas. La comparecencia de aprendizaje (1 mención), entrenamiento (1 mención) y resistencia (1 mención) confirma que la adaptación humana continúa siendo un elemento esencial en la efectividad del sistema.

4.3.3 IMPACTO ESTRATEGICO EN EL ECOSISTEMA AEROPORTUARIO

Tabla 14.IMPACTO ECONOMICO

Palabra	Frecuencia
económico	0
costos	2
inversion	0
operativo	1
perdidas	0

Fuente: Elaboración propia.

La tabla 14 demuestra frecuencias bajas en términos relacionados al impacto económico, el cual contiene costos (2 menciones) y operativo (1 mención) por lo que sugiere que a pesar que los entrevistados reconocen que la integración tecnológica puede influir en los costos operativos y en la eficiencia financiera, este aspecto no aparece como un tema que domine y la ausencia como inversión (0 menciones), perdidas (0 menciones), económico (0 menciones) relaciona que la dimensión económica es percibida más como un defecto indirecto que como una preocupación central.

Tabla 15. SEGURIDAD INTEGRAL

Palabra	Frecuencia
riesgo	8
amenaza	0
seguridad	111
protección	0
continuidad	10

Fuente: Elaboración propia.

La tabla 15. Da la constancia de un fuerte énfasis en la palabra seguridad (111 menciones), por lo cual confirma que este impacto estratégico más importante para los entrevistados, por lo tanto, continuidad (10 menciones) y riesgo (8 menciones) resaltan la percepción de que la tecnología fortalece la protección operativa y reduce vulnerabilidades. La ausencia de protección (0 menciones) y amenaza (0 menciones) no reduce la importancia, caso contrario demuestra que el personal concentra su vocabulario en términos más directos como seguridad (111 menciones) reflejando la integración tecnológica es vista fundamentalmente como un mecanismo para elevar la seguridad aeroportuaria.

Tabla 16. COMPETITIVIDAD Y MODERNIZACION

Palabra	Frecuencia
moderno	0
actualizacion	0
estandar	0
competitivo	0
avanzado	1
categoria	0
nivel	14

Fuente: Elaboración propia.

En la Tabla 16. Los términos nivel (14 menciones) y avanzado (1 mención) demuestran la percepción de que el uso de tecnologías inteligente aporta a posicionar el aeropuerto en un estándar más alto de operación a pesar de que las palabras como moderno, competitivo, actualización tienen cero menciones no aparecen con frecuencia, esto se debe a que los entrevistados tienden a expresar la idea de modernización por medio de conceptos como nivel (14 menciones) o avanzado (1 mención) la evidencia indica que la modernización es comprendida como un efecto estratégico y positivo de la transformación tecnológica.

4.3.1 TEMAS RECURRENTES

- Inteligencia artificial
- Visión artificial
- Artificial monitoreo
- Monitoreo seguridad
- Inteligencia visión
- Integración sistemas
- Seguridad aeropuerto
- Sistemas integrados
- Falsos positivos
- Vez dicho

El análisis realizado permite la visualización de manera estructurada la frecuencia de conceptos claves y los patrones de respuesta. Lo que facilita la comprensión de la distribución de ideas y la identificación de temas recurrentes dentro del conjunto de información.

Figura 11. EXPLORACION DE LOS DATOS

Fuente: Elaboración propia.

Como resultado, se obtuvo un conjunto de datos coherente y limpio utilizando la librería WordCloud en conjunto con matplotlib para la representación visual de las frecuencias léxicas., por el cual se generaron la tabla 10. A la 16. Principales conceptos y temas emergentes del análisis textual y nube de palabras como se muestra en la figura 11. Exploración de los datos. Que reflejan los principales temas y conceptos emergentes en el discurso del personal operativo entrevistado.

Cada categoría temática se identificó partiendo de las expresiones y palabras más mencionadas en las entrevistas, lo que ayuda a detectar tendencias y concentraciones de opinión acerca de aspectos críticos del monitoreo de seguridad. La preparación de los datos incluyendo la eliminación de valores atípicos y el tratamiento de valores faltantes, garantizando la representación de los hallazgos sea consistente y precisa.

La visualización de temas recurrentes y palabras permite extraer conclusiones relevantes, comparando la percepción del personal sobre diversos aspectos del sistema y respaldar la toma de decisiones para mejorar la eficacia e implementación de los sistemas de seguridad.

4.3.2 ANALISIS DE ENTREVISTA A PERSONAL DEL CENTRO DE OPERACIONES DEL SERVICIO AEROPORTUARIO NACIONAL

Con el propósito de obtener una perspectiva acerca de la eficacia de la integración de inteligencia y visión artificial en el monitoreo de seguridad cibernética y física en entornos

aeroportuarios, se realizaron entrevistas a siete profesionales del área de tecnología que laboran en el Servicio Aeroportuario Nacional. Los participantes con experiencia en soporte técnico, monitoreo infraestructura y gestión de sistemas brindaron sus percepciones acerca del funcionamiento de los sistemas tradicionales, los beneficios potenciales relacionados a la automatización inteligente y los desafíos asociados a su implementación.

4.3.2.1 EXPERIENCIA CON SISTEMAS TRADICIONALES DE MONITOREO.

Los entrevistados coinciden en que los sistemas tradicionales exhiben limitaciones significativas debido a su fuerte dependencia del factor humano. Un oficial de soporte técnico señaló que estos sistemas requieren procedimientos manuales que entorpecen la seguridad, mientras que otro afirmo que el monitoreo manual exige alta observación, análisis constante y respuesta rápida esta percepción se refuerza con la idea de que el usuario debe de estar al 100% pendiente para evitar intrusiones o ataques, evidenciando que la carga operativa recae casi exclusivamente ante la vigilancia humana. En conjunto, las citas revelan que el modelo tradicional es visto como demandante, vulnerable, ineficiente al error humano.

4.3.2.2 PERCEPCION ACERCA DE LA INTEGRACION DE VISION ARTIFICIAL E INTELIGENCIA ARTIFICIAL

La integración de inteligencia y visión artificial es percibida como un cambio transformador en la operación. Para diversos participantes, esta tecnología permite monitoreo y reconocimiento en tiempo real, liberando la carga humana, lo que demuestra un desplazamiento de las tareas más pesadas hacia sistemas automatizados. Un agente de soporte técnico la describió como una mejora grande, capaz de analizar puntos ciegos que nosotros no vemos indicando una capacidad superior a la percepción humana. Por lo tanto, otro oficial de soporte técnico resalto que la inteligencia artificial reduce errores humanos y mejora la precisión ante amenazas estas opiniones reflejan una percepción generalizada de que la integración tecnológica incrementa fiabilidad, precisión y alcance en el monitoreo.

4.3.2.3 REDUCCION DE TIEMPOS DE DETECCION Y RESPUESTA.

Uno de los temas más recurrentes es la rapidez operativa que aportaría la inteligencia artificial. Un oficial de soporte técnico señaló que la inteligencia artificial permitirá alertas automáticas en fracciones de segundo, lo que contrasta drásticamente con la velocidad humana. Para un desarrollador del área de IT, esta integración definitivamente reducirá los tiempos de

reacción ante emergencias, mientras que otro entrevistado destaco que también corrige el error humano y reduce los tiempos de detección. Esta dualidad de corrección y rapidez demuestra que el valor percibido no se limita al tiempo, sino a la fiabilidad integral del proceso de respuesta.

4.3.2.4 VISUALIZACION CENTRALIZADA DE ALERTAS.

Los participantes valoran extraordinariamente la centralización del monitoreo como un avance estratégico. Un agente de soporte describió este beneficio al afirmar que la integración es lo mejor, porque ya no hay que saltar de sistema en sistema, lo que reduce confusiones y pérdidas de tiempo. Otro oficial menciono que esta centralización permite reaccionar más rápido y bloquear intrusiones de forma inmediata, mostrando una percepción de mayor control operativo. Asimismo, se destacó que transforma la seguridad en un sistema más inteligente y predictivo, lo cual evidencia una visión de modernización y mejora continua del ecosistema de monitoreo.

4.3.2.5 EFICACIA DE MONITOREO Y FALSOS POSITIVOS.

La capacidad de disminuir falsos positivos surge como uno de los beneficios más destacados. Un oficial de soporte afirmo que el sistema inteligente, evita falsos positivos y mejora el desempeño, por otro lado, mencionan que la tecnología reduce los errores y mejora la eficacia en las respuestas. Estas declaraciones se complementan con la percepción de que la IA disminuye la saturación de alertas y aprovecha mejor los recursos, indicando que el monitoreo automatizado no solo reduce ruido operativo, sino que optimiza la interpretación de eventos. En general, la percepción compartida es que la tecnología reduce cargas innecesarias y eleva la precisión operativa.

4.3.2.6 IMPACTO SOCIAL, ECONOMICO Y AMBIENTAL.

Varios entrevistados señalaron efectos secundarios positivos más allá de lo operativo. Un desarrollador de IT resalto que la reducción de personal operativo disminuye desplazamientos y mejora la calidad de vida del personal especializado, evocando beneficios positivos. A nivel económico, un oficial comento que, aunque costoso, el sistema incrementa la competitividad aeroportuaria, reflejando una relación entre inversión y posicionamiento institucional. De la misma manera, se mencionó que la tecnología aumenta la protección al personal, reduce consumo energético y previene incidentes ambientales reforzando dimensiones del ecosistema aeroportuario.

4.3.2.7 LIMITACIONES Y DESAFIOS

Los entrevistados también identificaron barreras importantes para la adopción plena del sistema. Para un oficial de soporte técnico, las búsquedas en sistemas tradicionales son engorrosas propensas a errores humanos, lo que resalta la necesidad de modernización. Un agente de soporte enfatizo que el mayor desafío es la potencia necesaria y la capacitación del personal, evidenciando que la formación y recursos técnicos siguen siendo limitantes. Por consiguiente, se mencionaron desafíos éticos y resistencia al cambio, especialmente vinculados al reconocimiento facial. Simultáneamente estos elementos muestran que la adopción tecnológica requiere formación, infraestructura y estrategia organizacionales de adaptación.

4.3.3 INTERPRETACION.

Los resultados obtenidos a partir de las entrevistas permiten una comprensión como el personal técnico del Servicio Aeroportuario Nacional percibe la integración de inteligencia y visión artificial del servicio aeroportuario en los procesos de monitoreo de seguridad cibernética y física. En consonancia, los hallazgos evidencian que las percepciones de los participantes se articulan por medio de tres dimensiones principales como ser, integración tecnológica, efectividad operativa y gestión de riesgo, elementos que coinciden con las teorías de resiliencia de control, organizacional y de supervisión.

En primer lugar, los participantes describen que los sistemas actuales presentan limitaciones de precisión y generan un volumen significativo de alertas manuales.

En segundo lugar, las apreciaciones acerca de la integración entre sistemas físicos y lógicos reflejan que la interoperabilidad todavía representa un reto.

De esa manera, las opiniones del personal coinciden con la teoría de gestión del riesgo, al indicar que la visión computacional e inteligencia artificial pueden fortalecer la capacidad del aeropuerto para responder y anticipar eventos anómalos. La idea de estas tecnologías permite detectar antes y responder más rápido, se relaciona con los modelos de afrontacion y anticipación descritos en la teoría de resiliencia organizacional, donde la capacidad de reacción tiene dependencia de la automatización, la disponibilidad de datos en tiempo real y la reducción de errores humanos.

Por último, los relatos de los entrevistados demuestran un consenso acerca de la necesidad de fortalecer la capacidad técnica, superar la resistencia al cambio y mejorar la infraestructura tecnológica. Estas percepciones coinciden directamente con el análisis causa-raíz, el cual identifica

factores como disponibilidad de hardware, habilidades del personal, madurez organizacional como elementos críticos para incrementar la efectividad de la integración tecnológica.

Aunque los hallazgos demuestran una clara correspondencia con los marcos teóricos revisados, también ponen en evidencia dimensiones que dichas teorías abordan de manera insuficiente o parcial. A pesar de que la teoría de resiliencia organizacional explica adecuadamente la capacidad de anticipación y respuesta, los resultados sugieren que subestima el rol critico de la infraestructura tecnológica preexistente y de la madurez operativa como factores condicionantes de dicha resiliencia. Consecutivamente, la teoría de gestión de riesgo tiende a centrarse en la capacidad de evaluar, mitigar e identificar amenazas, pero los datos empíricos muestran que esta capacidad depende, en gran medida, de la disponibilidad de sistemas avanzados, la reducción del error humano y la automatización. En consecuencia, los hallazgos abren la posibilidad de ampliar estos marcos teóricos hacia una perspectiva más integral que incorpore explícitamente los limites técnicos, estructurales y organizacionales que influyen en la efectividad real de la gestión de riesgo y la resiliencia.

La interpretación de los datos demuestra que las percepciones del personal validad los supuestos teóricos correlacionados con la integración de tecnologías avanzadas en entornos de infraestructura critica. Los hallazgos revelan que la inteligencia y visión artificial son consideradas herramientas con un alto potencial para mejorar la precisión operativa, fortalecer la resiliencia del aeropuerto y reducir errores, siempre que se aborden los desafíos estructurales, tecnológicos y organizacionales identificados.

4.3.4 TRIANGULACION.

Para fortalecer la validez y credibilidad de los hallazgos, en este estudio se llevó a cabo una triangulación de fuentes y una triangulación metodológica, tal como fue establecido en el diseño de investigación. En esta etapa, los resultados recabados por medio de las entrevistas se contrastaron con documentación institucional del Servicio Aeroportuario Nacional, lineamientos internacionales emitidos por organismos como la ACI y la OACI, literatura académica especializada. Este proceso permitió validad la coherencia de las percepciones de los participantes con la evidencia técnica disponible.

Las entrevistas señalaron deficiencias en la precisión de los sistemas tradicionales, estas percepciones coinciden con reportes internacionales que destacan la necesidad de fortalecer la

detección temprana ante infraestructuras de alto impacto con relación a el creciente refinamiento de las amenazas. De esa manera, la preocupación de los participantes por el exceso de carga operativa asociada al monitoreo manual el cual se ve reflejada en estudios especializados que documentan las limitaciones de los centros de control basados principalmente en supervisión humana.

Por otro lado, los entrevistados manifestaron que la integración de inteligencia y visión artificial podría mejorar significativamente los tiempos de respuesta, centralizar la información y reducir los errores humanos. Este planteamiento es consistente con la literatura que respalda el uso de algoritmos inteligentes en la gestión de incidentes y el análisis en tiempo real como efectivas estrategias para la incrementación de la eficacia operativa en aeropuertos e infraestructuras de alto impacto.

De igual manera se permitió evidenciar que diversos desafíos mencionados por los participantes como ser la falta de interoperabilidad entre sistemas, la resistencia organizacional y la necesidad de capacitación hacen relación con las limitaciones identificadas en el análisis documental y en estudios posteriores con relación al GTIC, donde se advierte que la integración tecnológica requiere madurez organizacional, recursos adecuados y marcos normativos entendibles para su implementación eficiente.

En conjunto, La validez de los hallazgos se fortaleció al demostrar que las percepciones del personal entrevistado no constituyen apreciaciones aisladas, si no que se alinean con evidencia técnica, tendencias internacionales y estudios especializados. Este contraste aporto una robustez mayor interpretativa permitiendo situar los resultados dentro de un marco comparativo más amplio, tal como se definió en el diseño metodológico del estudio.

4.4 ANÁLISIS INFERENCIAL Y MODELOS APLICADOS

4.4.1 ANALISIS INFERENCIAL

A partir del análisis temático y de la frecuencia de menciones asociadas a las variables de estudio, es posible realizar inferencias interpretativas que permiten la comprensión de como el personal percibe el desempeño del sistema integrado de seguridad y cuáles son los patrones subyacentes que orientan su experiencia operativa.

Los datos se muestran que las categorías de la imagen 8. “Percepción acerca de la

reducción de incidentes (92 menciones) y satisfacción general con el desempeño del sistema (78 menciones) concentran la mayor proporción de referencias. Este patrón sugiere que, para el personal involucrado, el valor as tangible del sistema no reside solo en su capacidad tecnológica, caso contrario en su impacto directo acerca de la disminución de eventos operativos, lo cual refuerza una cultura institucional orientada a la eficiencia operativa y control del riesgo.

En contraste, temas como experiencia del personal con la integración tecnológica (20 menciones) y percepción de eficacia del sistema integrado (28 menciones) presentan frecuencias considerablemente menores. Este desfase brinda la inferencia que, a pesar de que el sistema es percibido como funcional y útil, existe una asimetría entre el desempeño técnico y la aprobación tecnológica por parte del personal, lo que indica posibles brechas en capacitación, acompañamiento o comprensión del sistema.

De esa misma manera, la categoría identificación de desafíos operativos y técnicos (33 menciones) reflejan que, a pesar de tener una valoración positiva del sistema, el personal continúa experimentando limitaciones operativas que condicionan la percepción de integración plena. Esto evidencia una fase de transición donde la modernización tecnológica aun convive con prácticas de monitoreo tradicionales.

Desde una perspectiva inferencial cualitativa, estos patrones ceden concluir que la aceptación del sistema está fuertemente anclada en resultados prácticos relacionados con la reducción de incidentes, por lo tanto, los aspectos relacionados con la transformación digital, experiencia de usuario e integración tecnológica aun no alcanzan el mismo nivel de internalización en la cultura organizacional. Esta inferencia coincide con marcos teóricos de adopción tecnológica que establecen el cual los beneficios percibidos a nivel operativo suelen anteceder a la apropiación cultural de la innovación.

En correspondencia con lo expuesto por Hernández Sampieri et al. (2014) no se necesita reducirlos a números ni analizarlos estadísticamente, la investigación se fundamenta en una perspectiva interpretativa centrada en el entendimiento del significado además el proceso cualitativo es inductivo por lo que procede dato por dato y caso por caso, por lo que la inferencia no es matemática caso contrario analítica, interpretativa e inductiva.

En síntesis, la inferencia permite que el sistema integrado es valorado principalmente como un mecanismo de fortalecimiento de la seguridad operativa, y solo en segunda instancia como un

instrumento de modernización tecnológica, lo que tendrá implicaciones directas para futuros procesos de escalabilidad, implementación y capacitación dentro del entorno aeroportuario.

4.4.2 MODELOS APLICADOS

Para el tratamiento sistemático de la información se implementó un modelo de procesamiento de lenguaje natural (NLP) en Python, guiado a la analítica de texto descriptiva. El objetivo de este modelo fue transformar las entrevistas en datos textuales estructurados que permitieran identificar patrones léxicos, su relación con las variables de análisis definidas en el estudio y temas recurrentes. El modelo se basa en ser descriptivo automatizado, configurado por medio de un script de Python que integro las librerías NLTK, pandas, collections y wordcloud. Este enfoque permitió reducir el sesgo del análisis exclusivamente manual, estandarizando el procesamiento del corpus y generando salidas reproducibles.

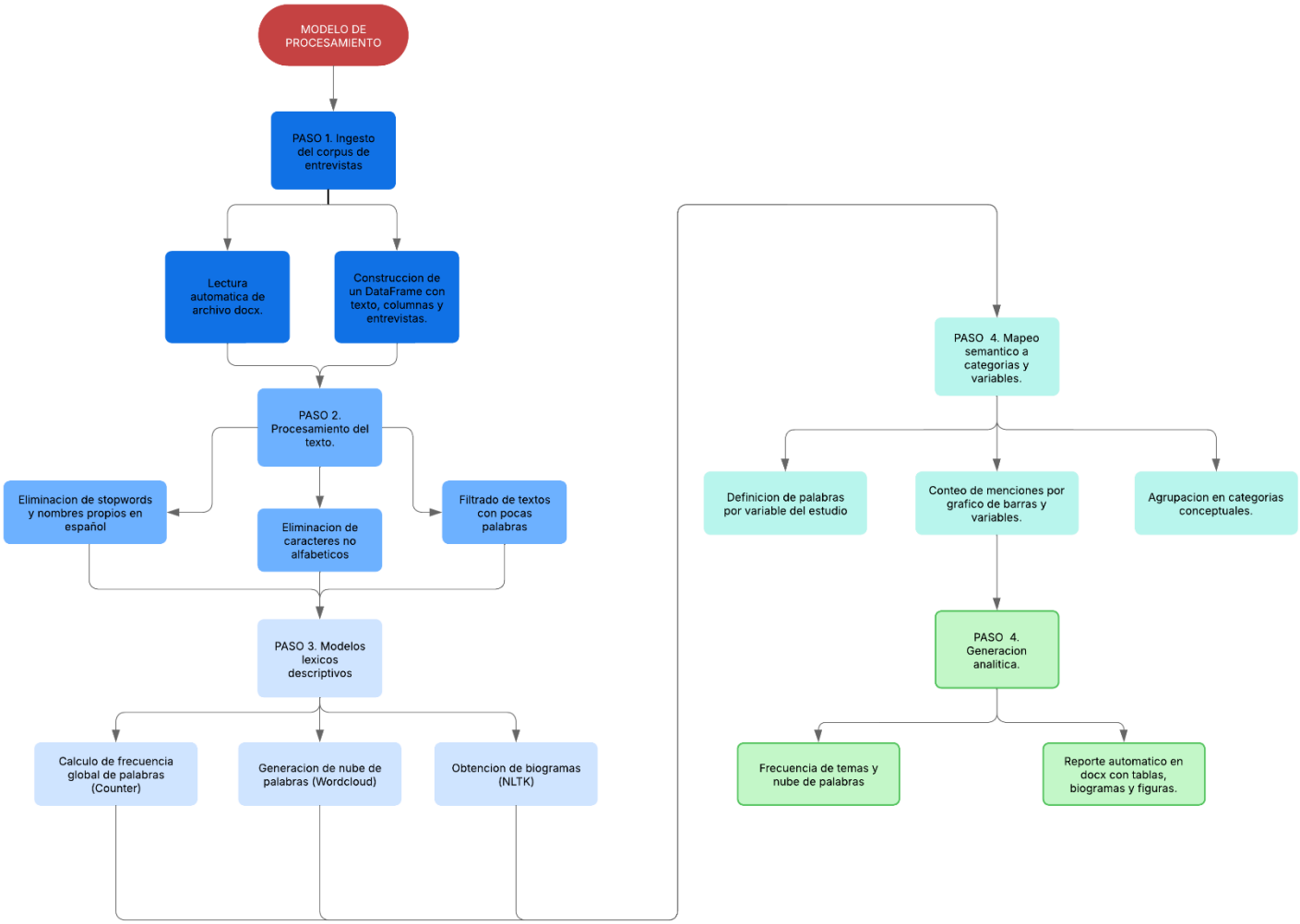


Figura 12.ARQUITECTURA DE ALTO NIVEL DE PROCESAMIENTO DE LENGUAJE NATURAL.

Fuente: Elaboración propia.

El diagrama del modelo aplicado resume las etapas principales del procesamiento del corpus documental. En el paso 1, el modelo realiza la ingesta automática de las entrevistas en formato .docx consolidando su contenido en un DataFrame estructurado que constituye la base del análisis. Seguidamente el paso 2 ejecuta el preprocesamiento del texto, que incluye la conversión a minúsculas, la remoción de stopwprds y nombres propios, y la eliminación de caracteres, de la misma manera como el filtrado de textos con escaso contenido. Esta depuración brinda la depuración de ruido semántico y conservación únicamente de elementos destacados para el análisis.

En el paso 3, el modelo ejecuta los procesos léxicos descriptivos, el cálculo de frecuencias globales por medio Counter, la identificación de biogramas por medio de NLTK y la generación de una nube de palabras para la visualización de prominencia de términos. Por lo cual brindan la detección de asociaciones frecuentes abarcados en el discurso del personal entrevistado. Estos procedimientos generas patrones que ayudan como una base para el análisis desarrollado en la sección anterior.

Consecutivamente, en el Paso 4. Se lleva a cabo el mapeo semántico direccionado a las categorías y variables conceptuales del estudio. Esta fase engloba la definición de palabras clave por variable, la elaboración de grafico de barras y el conteo de menciones, de la misma manera como la organización de los hallazgos dentro de categorías superiores (Impacto estratégico, capacidades potenciadas y desafíos técnicos). Esta etapa integra el análisis léxico con el marco teórico, concediendo la vinculación de los resultados con las dimensiones analíticas del estudio.

Por último, en el paso 5 el modelo brinda la generación analítica procedente del procesamiento de visualizaciones como nube de palabras y gráficos temáticos, y un reporte automatizado que integra figuras, tablas y biogramas. Este conjunto de salidas brinda una base analítica sistemática, trazable y reproducible, fortaleciendo la rigurosidad del análisis.

Tales procedimientos se alinean con los lineamientos metodológicos propuestos por Creswell (2013) quien destaca que los modelos en la investigaciones cualitativas no son de naturaleza numérica, caso contrario esquemas interpretativas el cual permiten comprender la complejidad del fenómeno estudiado. De esa manera la modelación expresada se alinea al generar clústeres temáticos, asociaciones conceptuales y frecuencias léxicas que profundizan en la

comprensión del fenómeno, constituyendo un modelo descriptivo y explicativo adecuado para este tipo de análisis.

4.4.3 DISCUSION DE LOS HALLAZGOS.

Los resultados obtenidos en esta investigación revelan percepciones y patrones que guardan una relación estrecha con los planteamientos teóricos y antecedentes revisados en el marco conceptual acerca del uso de tecnologías de inteligencia y visión artificial en contexto de seguridad aeroportuaria, los hallazgos reflejan que el personal operativo reconoce el valor de la analítica de video, la automatización de procesos y la integración de sistemas inteligentes como una herramienta que fortalece la eficiencia del monitoreo y la capacidad de respuesta, en concordancia con los expuesto por autores que resaltan la relevancia de la reducción y detección temprana de la carga operativa por medio de tecnologías basadas en inteligencia artificial.

De la misma manera, se observó una coincidencia significativa entre las percepciones del personal entrevistado y los estudios previos que trazan la importancia de la interoperabilidad entre sistemas, la modernización de la infraestructura tecnológica y la estandarización de los procedimientos. Estos resultados de igual manera dialogan con teorías de gestión del riesgo y los modelos de vigilancia inteligente, por lo cual argumentan que la eficacia de los sistemas depende tanto de la calidad tecnológica como de la capacidad del personal y su adaptación a nuevas herramientas.

En cuanto a las aportaciones originales, la investigación ofrece una perspectiva aplicativa desde el contexto operativo especifico de los aeropuertos administrados por el Servicio Aeroportuario Nacional de Honduras, un ámbito poco documentado en la literatura regional. Los hallazgos brindan la comprensión, partiendo la voz de los propios autores, los desafíos percibidos, las necesidades reales y las oportunidades de mejora en la integración de sistemas de visión e inteligencia artificial. Esta contribución empírica resulta relevante debido a que proporciona insumos contextualizados que pueden orientar actualizaciones tecnológicas, fortalecimiento de capacidades institucionales y decisiones de inversión.

De esta manera, la discusión no solo confirma elementos presentes en estudios previos, sino que también amplia el conocimiento disponible al aportar evidencia situadas que permiten la comprensión de cómo se configuran las dinámicas operativas, las expectativas del personal ante la adopción de tecnologías emergentes y los requerimientos técnicos en el ámbito aeroportuario

hondureño.

4.4.3.1 VINCULACION DE TEORIAS CON LOS HALLAZGOS Y LA PROPUESTA.

Los hallazgos del estudio se interpretan a la luz de las teorías de sustento,

La teoría de la resiliencia organizacional nos dice como la integración de inteligencia artificial blinda la continuidad operativa y la capacidad de respuesta del Servicio Aeroportuario Nacional, Hallazgo evidenciado en la percepción del personal sobre mejor detección oportuna de amenazas.

La teoría de la gestión del riesgo brinda la comprensión acerca de la reducción percibida de los falsos positivos y la mejora en la identificación de amenazas, sustentando la propuesta de integración tecnológica como mecanismo de mitigación del riesgo.

Por último, la teoría del control y supervisión fundamenta el uso de sistemas inteligentes como agentes tecnológicos que apoyan la supervisión humana y la toma de decisiones, justificando la arquitectura propuesta de monitoreo integrado.

4.4.4 LIMITACIONES

Esta investigación reconoce limitaciones propias y del contexto especifico en que se desarrolló, al tratarse de un estudio interpretativo enfocado en las percepciones del personal del Servicio Aeroportuario Nacional, los resultados brindan compresiones construidas en un entorno particular y no buscan ser generalizados a otros espacios aeroportuarios. Si bien esta característica metodológica acota el alcance de los hallazgos, con comprometer la consistencia ni la validez interpretativa del estudio.

De igual manera, la accesibilidad y disponibilidad del personal operativo y técnico constituyo una limitación relevante. Los tiempos de operación aeroportuaria, la dinámica propia de los turnos y las responsabilidades del personal propia de los turnos restringieron la posibilidad de obtener una mayor diversidad de opiniones de los participantes contemplados inicialmente. En consecuencia, algunos puntos de vista complementarios podrían no haber sido capturados mediante la recolección de datos.

Otra limitación se relaciona con la sensibilidad de la información vinculada a los sistemas de vigilancia, procesos de seguridad aeroportuaria e infraestructura critica. Debido a protocolos institucionales ciertos detalles operativos y técnicos no pudieron ser explorados a profundidad, por

lo cual restringió el nivel de detalle alcanzado en algunos apartados del análisis. No obstante, se enfatizó en mantener un equilibrio entre el cumplimiento de las normas de seguridad establecidas y el rigor metodológico.

Por último, se reconoce que el proceso de interpretación puede estar influenciado en la perspectiva del investigador, dado que en estudios cualitativos la subjetividad constituye un elemento inevitable del análisis. Para minimizar este efecto, se emplearon procedimientos de triangulación conceptual y sistemático de conceptualización, orientados a asegurar coherencia, fidelidad y transparencia en la interpretación de los datos.

A pesar de estas limitaciones, el estudio conserva solidez metodológica y brinda información valiosa que contribuye a la comprensión del estado actual y las necesidades de mejora en la integración de tecnologías de inteligencia y visión artificial en los aeropuertos del país.

4.5 SINTESIS DE LOS HALLAZGOS

4.5.1 PRINCIPALES HALLAZGOS

Los hallazgos derivados del análisis se organizan en cuatro ejes centrales que reflejan la percepción del personal del centro de operaciones del Servicio Aeroportuario Nacional acerca de la integración del sistema de visión e inteligencia artificial en el monitoreo de seguridad cibernética y física.

Hallazgo 1. PERCEPCION DE MAYOR EFICACIA OPERATIVA.

Percepciones recurrentes:

El personal percibe que la integración tecnológica agiliza la detección de incidentes.

Se resalta la reducción del esfuerzo manual requerido para el monitoreo de múltiples plataformas.

Se reconoce una mayor claridad en la lectura de eventos y alertas.

Significado para los participantes:

La tecnología es entendida como un apoyo que facilita el trabajo, disminuye la carga cognitiva y mejoramiento del ritmo de respuesta en situaciones críticas.

Hallazgo 2. VALORACIONES POSITIVAS DE LA CENTRALIZACION DEL MONITOREO.

Percepciones recurrentes:

Los participantes consideran que un panel único facilita la correlación entre eventos lógicos y físicos.

Expresan que la centralización reduce retrasos y confusiones.

Señalan que sistemas fragmentados generan posibles errores e incertidumbres.

Manifiestan que la centralización reduce retrasos y confusiones.

Significado para los participantes:

Centralizar la información es percibido como un elemento clave para el fortalecimiento de la operación y el evitamiento de fallas derivadas de la dispersión tecnológicas.

Hallazgo 3. RECONOCIMIENTO DE LIMITACIONES TECNICAS Y ORGANIZACIONALES.

Percepciones recurrentes:

Se percibe una insuficiencia de infraestructura tecnológica en el aeropuerto.

Reconocen que hay una falta de capacitación técnica en visión e inteligencia artificial.

Los entrevistados revelan inquietud por la limitada disponibilidad de hardware moderno.

Significado para los participantes:

Estas limitaciones se comprenden como barreras reales que podrían afectar la adopción plena de tecnologías avanzadas.

Hallazgo 4. PERCEPCION DEL IMPACTO ESTRATEGICO PARA LA SEGURIDAD.

Percepciones recurrentes:

La tecnología es vista como un mecanismo que fortalece la capacidad para la identificación de amenazas tempranamente.

Diversos participantes relacionan esta integración con estándares internacionales.

Se percibe una mejora general en el control operativo y la seguridad.

Significado para los participantes:

Existe una percepción generalizada de que estas tecnologías aportan modernización,

alineamiento y mayor control con prácticas de infraestructura de alto valor.

4.5.2 IMPLICACIONES

Las implicaciones que derivan de estas percepciones brindan la comprensión de oportunidades de mejora y líneas de acción institucional.

4.5.2.1 IMPLICACION OPERATIVA

La tecnología es vista como un apoyo directo para el desempeño diario del personal.

Favorece la interpretación más clara de eventos en tiempo real.

Puede contribuir a la disminución del estrés operativo y mejoramiento de la fluidez del monitoreo.

4.5.2.2 IMPLICACION TECNOLOGICA.

La percepción de falta de infraestructura sugiere la necesidad de fortalecer la plataforma y equipamiento.

El reconocimiento de debilidades técnicas indica áreas prioritarias de inversión.

La centralización es vista como un beneficio, por lo cual se orienta a futuras decisiones de integración tecnológica.

4.5.2.3 IMPLICACION INSTITUCIONAL

Los participantes exteriorizan la necesidad de actualización y formación en herramientas emergentes.

La adopción tecnológica debe acompañarse de desarrollo de capacidades humanas.

Sus percepciones aportan insumos para decisiones estratégicas en presupuestos y modernización.

Tabla 17.MAPA DE HALLAZGOS DERIVADOS DEL ANALISIS DE ENTREVISTAS.

Hallazgo	Evidencia	Implicación
Mayor eficacia operativa	La tecnología reduce carga manual y agiliza detecciones.	Menor carga cognitiva y apoyo operativo directo.
Centralización valorada positivamente.	Facilita correlación y un panel único reduce confusión.	Foco institucional hacia plataformas integradas.

Hallazgo	Evidencia	Implicación
Limitaciones percibidas.	Falta de hardware, capacitación e infraestructura.	Necesidad de fortalecimiento técnico e inversión.
Impacto estratégico reconocido.	Percepción de mayor modernización y seguridad.	Orienta decisiones hacia estándares y modernización.

Fuente: Elaboración propia.

Esta investigación aporta una perspectiva contextualizada acerca de la seguridad en aeropuertos hondureños, un campo con escaza documentación especializada en la región. Las implicaciones derivadas de los hallazgos no solo enriquecen la literatura existente, sino que brindan insumos concretos para la toma de decisiones, la priorización de inversiones y la formulación de políticas internas orientadas al fortalecimiento de la infraestructura critica aeroportuaria.

4.5.3 MATRIZ DE TRAZABILIDAD

Tabla 18. MATRIZ DE VINCULACION.

Objetivo de la investigación	Hallazgo clave	Evidencia	Conclusión	Acción en la propuesta.
Analizar la percepción sobre la integración de inteligencia y visión artificial en el monitoreo de seguridad.	El personal percibe una detección más oportuna de amenazas con sistemas integrados.	Tabla 9 (Eficacia operativa), Tabla 16 (Mapa de hallazgos), entrevistas centro de operaciones SAN.	La integración tecnológica mejora la detección temprana de amenazas.	Implementación de un panel integrado de monitoreo físico y lógico.
Explorar a percepción acerca de paneles integrados vs sistemas independientes.	Los operadores reportan mayor rapidez en la toma de decisiones.	Tabla 10 (Precisión y credibilidad, Figura 8(Frecuencia de temas)	Los sistemas integrados agilizan la toma de decisiones operativas.	Arquitectura de correlación de alertas.
Comprender la percepción del impacto de IA en los falsos positivos.	Se percibe una reducción de falsos positivos en alertas.	Tabla 9, tabla 16, análisis temático de las entrevistas.	La Inteligencia artificial contribuye a mejorar la precisión de las alertas.	Uso de inteligencia artificial para el filtrado y priorización de alertas.
Describir el impacto de la integración de sistemas inteligentes en la continuidad operativa y la mitigación de riesgos, considerando las limitaciones técnicas y organizacionales.	Mejora percibida en continuidad operativa y resiliencia: se identifica limitaciones asociadas a la falta de personal especializado y protocolos estandarizados.	Tabla 13(Impacto económico), Tabla 14 (Seguridad integral), figura 1 (ACR), Tabla 12 (Factores organizacionales)	La integración fortalece la resiliencia operativa del aeropuerto, sin embargo, las barreras organizacionales pueden limitar su efectividad.	Plan de monitoreo continuo y gestión integral del riesgo, acompañado de un programa de capacitación y estandarización de procesos.

Fuente: Elaboración propia.

La tabla 18. Sintetiza de forma estructurada el proceso analítico detallado en la investigación, articulando los objetivos planteados con los hallazgos empíricos y la evidencia obtenida partiendo del análisis cualitativo. Por medio de esta matriz se establece una correspondencia explicita entre los resultados del estudio, las conclusiones formuladas y las acciones propuestas, accediendo a demostrar que las decisiones planteadas en la propuesta se derivan directamente de la evidencia analizada y no de apreciaciones subjetivas, fortaleciendo así el rigor y la validez metodológica del estudio.

4.5.4 TRANCISION AL CAPITULO V

El análisis ejecutado brindo la obtención integral del estado actual de los sistemas de monitoreo y de las percepciones del personal acerca de la posible integración de tecnologías de inteligencia y visión artificial en los aeropuertos del Servicio Aeroportuario Nacional. Para apoyar en el proceso analítico, se emplearon herramientas computacionales en Python orientadas exclusivamente a la organización y exploración preliminar de la información, sin que ello implicara la aplicación de modelos predictivos o estadísticos.

Los hallazgos sintetizados en este capítulo constituyen la base para la elaboración de las recomendaciones estratégicas y conclusiones generales que se presentan en el capítulo V. Dichas conclusiones se derivan del análisis interpretativo de los datos, mientas que las recomendaciones se orientan al fortalecimiento de la seguridad aeroportuaria, optimización de los procesos operativos y guiar la toma de decisiones institucionales relacionadas con la modernización tecnológica.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.2 CONCLUSIONES

Los participantes coinciden en que un panel centralizado mejora la rapidez con la que pueden tomar decisiones. Esta percepción se sustenta en la alta frecuencia de menciones asociadas al tiempo (27 menciones) y a la respuesta operativa (17 menciones) identificadas en la tabla 9, lo que indica una reducción percibida en los tiempos de reacción ante incidentes.

El personal percibe que la integración de inteligencia artificial en los sistemas de monitoreo reduce de una manera significativa los falsos positivos, mejorando la precisión de las alertas. Esta conclusión respalda en la tabla 10, donde el termino falsos registra (17 menciones), alerta (13 menciones) y errores (6 menciones) brindando una mayor confianza en la información generada por los sistemas integrados.

Las entrevistas evidencian que los sistemas integrados de monitoreo físico y lógico son percibidos como herramientas que fortalecen la continuidad operativa y la seguridad aeroportuaria, fundamentándose en la tabla 14 donde seguridad alcanza (111 menciones) acompañada de continuidad (10 menciones) y riesgo (8 menciones) lo que confirma el impacto estratégico de la integración tecnológica en la estabilidad operativa.

5.3 RECOMENDACIONES

Avanzar en dirección a la implementación institucional de un panel integrado de alertas lógicas y físicas, debido a que el personal percibe que este tipo de plataforma mejora sustancialmente la rapidez y precisión en la toma de decisiones. Se sugiere iniciar con un piloto en áreas de mayor criticidad operativa.

Incorporar algoritmos de inteligencia artificial y modelos de visión computacional ajustados al contexto aeroportuario, con procesos de calibración continua para el aseguramiento de una reducción sostenida de falsos positivos y mejorar la relevación de alertas entregadas al personal.

Desarrollar una hoja de ruta institucional para el fortalecimiento de sistemas integrados de monitoreo físico lógico, orientada a mejorar la continuidad operativa y la mitigación de riesgos críticos. Esta hoja de ruta debe de incluir:

- Protocolos de interoperabilidad.

- Inversiones en infraestructura.

- Estandarización de procedimientos de respuesta.

CAPÍTULO VI. APLICABILIDAD

La presente propuesta tiene como finalidad fortalecer el sistema de monitoreo de seguridad cibernética y física del Servicio Aeroportuario Nacional por medio de la integración de inteligencia y visión artificial en una plataforma unificada de supervisión. Los hallazgos de la investigación evidenciaron brechas criticas derivadas de la fragmentación entre los sistemas actuales, la limitada correlación ente alertas físicas y lógicas, la dependencia de procesos manuales, y los desafíos operativos que afectan la precisión, continuidad y rapidez en la detección de amenazas en el aeropuerto Ramon Villeda Morales.

Este capítulo presenta una solución estructurada orientada en superar estas limitaciones defendiendo su alcance, justificación, descripción técnica, desarrollo propuesto y las medidas de control necesarias para asegurar s eficacia. Por lo tanto, se incorpora un cronograma de implementación, vinculación de la propuesta con los segmentos claves de la investigación y el presupuesto estimado. La adopción de este modelo permitirá al SAN la optimización de la gestión de incidentes, mejorar la capacidad de anticipación y respuesta y la reducción falsos positivos, robusteciendo la seguridad integral en una infraestructura aeroportuaria estratégica de alto valor.

6.1 NOMBRE DE LA PROPUESTA

El nombre de la propuesta es: “Sistema hibrido e inteligente de seguridad aeroportuaria por medio de visión artificial orientada en redes neuronales convencionales”

6.2 JUSTIFICACIÓN DE LA PROPUESTA

Los hallazgos obtenidos en esta investigación demostraron que el sistema de monitoreo del Servicio Aeroportuario Nacional presenta limitaciones estructurales que afectan de una manera directa la eficacia de la seguridad aeroportuaria. Entre las brechas identificadas destacan la fragmentación entre los sistemas de vigilancia cibernética y física, la ausencia de correlación automática ente la alta dependencia de procesos manuales, alertas de esa misma manera la presencia recurrente de falsos positivos que ralentizan la toma de decisiones y reducen la capacidad de detección temprana de amenazas. De la misma manera, el personal operativo expresa que la falta de integración tecnológica impacta de una forma negativa la continuidad de las operaciones en el aeropuerto Ramon Villeda Morales, particularmente frente a eventos críticos.

Estos resultados empíricos son consistentes con lo expuesto por Nystad et al. (2021),

quienes señalan que la integración progresiva de sistemas interconectados sin un enfoque de seguridad unificado aumenta las vulnerabilidades en infraestructuras sensibles. De esa misma forma, la investigación confirma lo planteado por Rakas et al. (2020) relacionado a que la falta de correlación entre componentes físicos y lógicos debilita la capacidad y disponibilidad de respuesta de los sistemas críticos.

Hay tres tipos de actores de amenazas cibernéticas que apuntan al sector de la aviación comercial: los estados-nación, los grupos APT (amenazas persistentes avanzadas), los grupos organizados de ciberdelincuentes y los hacktivistas. Los objetivos de estos grupos son obtener datos corporativos confidenciales (incluida la propiedad intelectual), rastrear a disidentes, robar o extorsionar dinero, obtener una ventaja geopolítica y/o apoyar una causa. (Ribeiro, 2024) En este contexto, el informe de Amin et al. (2024) reporta que los datos muestran que los ciberataques aumentaron un 131 % entre 2022 y 2023 en todo el sector de la aviación, donde la mayor parte de los ataques se centraron en los usuarios del espacio aéreo. Esto trae consecuencias financieras y ante la reputación del sector de la aviación que se derivan de los fallos que se dan en la ciberseguridad el cual son enormes.

Por lo cual el estudio señala que la incorporación de inteligencia y visión artificiales representa una oportunidad para la modernización de los procesos de seguridad, al conceder análisis más preciso, reducción de cargas operativas y respuestas más rápidas frente a eventos sensibles. La percepción del personal confirmo que un sistema unificado aumentaría la capacidad de anticipación, y mejoraría la precisión en la clasificación de incidentes por lo que permitiría la gestión de alertas hibridas con una mayor coherencia. Asimismo, la evidencia recopilada indica que la infraestructura aeroportuaria actual requiere la evolución hacia tecnologías capaces de fortalecer su resiliencia operativa y de alinearse con los estándares internacionales en materia de seguridad cibernética y física.

La propuesta de un Sistema hibrido e inteligente de seguridad aeroportuaria por medio de visión artificial orientada en redes neuronales convencionales se fundamenta teóricamente en la teoría de resiliencia organizacional, la cual sostiene que las organizaciones deben desarrollar capacidades de afrontamiento, anticipación y adaptación ante eventos disruptivos. En ese sentido, la automatización de la detección de amenazas y la correlación de alertas atribuyen directamente al fortalecimiento de la resiliencia operativa del SAN al mejorar la continuidad y reducir los

tiempos de reacción del servicio.

Igualmente, la teoría de la gestión del riesgo respalda la necesidad de integrar tecnologías capaces de identificar patrones inusuales y tener reducción de la incertidumbre operativa, permitiendo una mitigación proactiva de riesgos cibernéticos y físicos. La incorporación de modelos de visión computacional e inteligencia artificial responden a este enfoque al disminuir la dependencia exclusiva del factor humano y optimización de la precisión en la clasificación de incidentes, tal como lo señalan Z.-H. Chen & Juang, (2018) y Demir et al. (2020) en aplicaciones críticas de supervisión automatizada.

Por último, desde la teoría del control y supervisión, la propuesta se justifica al concebir la inteligencia artificial como un agente tecnológico que apoya la labor de supervisión continua, reduciendo errores humanos y fortaleciendo la gobernanza de los sistemas de seguridad. La integración de un panel unificado de alertas hibridas permite mejorar la toma de decisiones del personal del centro de operaciones, alineándose con los principios de control efectivo en entornos de alta complejidad.

Por lo tanto, la presente propuesta se justifica brindar un modelo integral que responde directamente a las deficiencias localizadas y las necesidades operativas del SAN. Su implementación permitirá la optimización de la gestión de incidentes, disminución de falsos positivos, reforzar la protección de una infraestructura estratégica de alto impacto para el país y la mejora de la continuidad operativa. Por esta razón, esta propuesta constituye un paso fundamental para el avance hacia un ecosistema de seguridad aeroportuario más eficiente, sostenible y robusto.

6.3 ALCANCE DE LA PROPUESTA

La presente propuesta abarca el diseño e implementación de un Sistema hibrido e inteligente de seguridad aeroportuaria por medio de visión artificial orientada en redes neuronales convencionales, orientado principalmente en las necesidades operativas del servicio aeroportuario nacional (SAN). Su alcance se comprende de la incorporación progresiva de tecnologías avanzadas para la detección, análisis y correlación automatizada de eventos de seguridad en el Aeropuerto Ramon Villeda Morales, teniendo en consideración tanto sus procesos actuales como las brechas identificadas en el estudio.

El proyecto incluye la integración de fuentes de datos provenientes de cámaras de

vigilancia, sensores, herramientas de ciberseguridad y registros operativos para la consolidación en una plataforma unificada capaz de generar alertas hibridas en tiempo real. De igual manera, el alcance contempla la automatización de procesos de detección, el fortalecimiento de la continuidad operativa, la reducción de falsos positivos y el fortalecimiento de la continuidad operativa en conjunto con la optimización de la toma de decisiones del personal del Centro de Operaciones.

De este mismo modo, la propuesta incorpora actividades relacionada con capacitación técnica a la persona, validación funcional por medio de pruebas controladas, estableciendo protocolos de operación y la identificación de métricas que brinden una evaluación de la efectividad del sistema. No se contempla dentro del alcance la sustitución completa de los sistemas existentes, caso contrario su integración y mejora por medio de componentes tecnológicos complementarios que aumenten el monitoreo cibernético y físico.

En términos operativos, el alcance se acota inicialmente al Aeropuerto Ramon Villeda Morales como caso piloto, con posibilidad de expansión futura a otras terminales administradas por el SAN, una vez evaluados la viabilidad técnica y resultados de la solución. El proyecto, por lo tanto, se concentra en el fortalecimiento de las capacidades actuales de supervisión por medio de un enfoque adaptable, escalable y alineado con el estudio realizado.

6.3.1 ENTREGABLES DE LA PROPUESTA.

Como resultado del proyecto, se establecen los siguientes entregables tangibles finales:

I. Arquitectura del sistema integrado de monitoreo, validada y documentada.

II. Plataforma unificada de monitoreo con integración de seguridad cibernética y física.

III. Modelos de visión artificial basados en redes neuronales convolucionales para detección de eventos físicos.

IV. Motor de correlación hibrida de alertas cibernéticas y físicas.

V. Protocolos operativos y de respuesta frente a incidentes híbridos.

VI. Dashboards operativos para el centro de operaciones.

VII. Plan de capacitación técnica y material formativo para el personal.

VIII. Informe de métricas de desempeño y validación funcional del sistema.

6.3.2 OBJETIVOS DE LA PROPUESTA.

6.3.2.1 OBJETIVO GENERAL.

Diseñar e implementar (S) un sistema hibrido e inteligente de seguridad aeroportuaria por medio de visión artificial orientada en redes neuronales convencionales en el aeropuerto Ramon Villeda Morales, integrando el monitoreo de seguridad cibernética y física (M) por medio de una plataforma unificada, utilizando la infraestructura tecnológica existente (A), con el fin de mejorar la detección, gestión y correlación de incidentes operativos (R) en un periodo máximo de seis meses (T).

6.3.2.2 OBJETIVOS ESPECIFICOS.

Integrar (S) las fuentes de seguridad cibernética y física existentes sensores, cámaras y sistemas de red en una plataforma unificada de monitoreo (M), sin sustituir los sistemas actuales del servicio aeroportuario nacional (A), con el propósito de centralizar la gestión de alertas y eventos de seguridad (R) durante la fase de implementación del proyecto (T).

Implementar (S) modelos de visión artificial basados en redes neuronales convencionales y un motor de correlación hibrida de alertas (M), aprovechando los recursos tecnológicos disponibles (A), para reducir la dependencia de procesos manuales y la disminución de falsos positivos en el monitoreo de seguridad (R) antes de la puesta en producción del sistema (T).

Capacitar (S) al personal del centro de operaciones y validar el funcionamiento del sistema por medio de pruebas controladas e indicadores técnicos de desempeño (M), utilizando metodologías de validación y entrenamiento operativo (A), con el fin de asegurar la correcta operación y adopción del sistema (R) previo a su despliegue formal como proyecto en el aeropuerto Ramon Villeda Morales (T).

6.3.3 LIMITACIONES DEL ALCANCE

A pesar de su diseño integral, es importante reconocer que existen limitaciones por el cual pueden influir en la efectividad y ejecución del proyecto:

Capacidad de almacenamiento y procesamiento: Por lo que la implementación de visión artificial y el análisis en tiempo real demanda recursos computacionales especializados, cuya disponibilidad podría ser limitada.

Infraestructura tecnológica múltiple: No todas las instalaciones aeroportuarias del SAN tienen un mismo nivel de modernización, lo que podría requerir ajustes técnicos para la integración

de los sistemas existentes.

Nivel de capacitación del personal: La adopción de tecnologías avanzadas puede verse afectada por las brechas de conocimiento técnico del personal operativo, lo que lo hará necesario una capacitación progresiva.

Dependencia de conectividad robusta: Donde el sistema requiere de una alta disponibilidad y redes estables para el aseguramiento de la transmisión continua de datos y la generación oportuna de alertas.

Costos de implementación y sostenibilidad: La inversión inicial en hardware, licencias, software, mantenimiento y licencias puede representar un desafío a nivel de presupuesto para el SAN.

No obstante, de estas limitaciones, la propuesta se ajustará de forma flexible para el aseguramiento de su efectividad y viabilidad, priorizando la integración gradual, el uso eficiente de los recursos disponibles y la capacitación continua. Con esto se busca el maximizar su impacto por medio de una implementación escalable que atienda las condiciones y necesidades reales del SAN, fortaleciendo así la seguridad cibernética y física de las instalaciones aeroportuarias.

6.4 DESCRIPCIÓN Y DESARROLLO

6.4.1 DESCRIPCIÓN

La propuesta se estructura en tres ejes fundamentales que se desarrollaran de una forma integral por el cual se supere las brechas identificadas en el sistema de monitoreo del Servicio Aeroportuario Nacional y fortalecimiento de la seguridad cibernética y física del Aeropuerto Ramon Villeda Morales. La definición de estos ejes responde a un enfoque metodológico de la industria, alineado con estándares internacionales de gestión de seguridad, mejora continua y continuidad operativa, garantizando así la coherencia, sostenibilidad y vialidad de la solución.

La estructura adoptada se fundamenta en principios establecidos en normas como ISO/IEC 27001, ISO/IEC 22301, ISO/IEC 20000, diversificada mente usado en proyectos tecnológicos de infraestructuras críticas.

6.4.1.1 AUTOMATIZACION DEL MONITOREO E INTEGRACION TECNOLOGICA.

Este eje presencia la implementación de una plataforma unificada que centralice la

información proveniente de cámaras de videovigilancia, herramientas de ciberseguridad, registros operativos y sensores perimetrales. Se integrarán modelos de visión artificial capaces de detectar comportamientos anómalos, eventos operacionales e intrusiones físicas por el cual son fuera de lo común, junto con sistemas de inteligencia artificial que identifiquen amenazas en redes, accesos no autorizados y anomalías en infraestructura citica. El motor de correlación hibrida permitirá relacionar alertas lógicas y físicas en tiempo real, disminuyendo falsos positivos y el fortalecimiento de la capacidad de reacción del centro de operaciones.

De acuerdo con ISO (2022) la automatización del monitoreo y la correlación de eventos se asientan en los principios de gestión de seguridad instruidos por la norma ISO/IEC 27001, por el cual promociona la integración de controles lógicos y físicos para la gestión de incidentes y la detección.

6.4.1.2 CAPACITACION TECNICA Y FORTALECIMIENTO OPERATIVO DEL PERSONAL.

Se desarrollará un programa de formación especializado dirigido al personal del Centro de operaciones, áreas técnicas involucradas y seguridad aeroportuaria. Este programa incluirá talleres prácticos acerca de la gestión de alertas basadas en inteligencia artificial, interpretación de datos del sistema, uso eficiente de la plataforma integrada y procedimientos de respuesta ante incidentes híbridos. Por consiguiente, se ofrecerán simulaciones de eventos reales utilizando escenario de visión artificial y ciber seguridad para el fortalecimiento de la capacidad de anticipación, reducción de la dependencia de procesos manuales y el aseguramiento de una adecuada adopción tecnológica por parte del personal esencial del SAN.

Como menciona ISO (2018) el eje de capacitación técnica se enfila con las buenas prácticas de gestión de servicios determinado por la ISO/IEC 20000-1:2018, en el que resaltan la importancia de las competencias del personal para la auténtica operación de los sistemas delicados.

6.4.1.3 MEJORA CONTINUA, OPTIMIZACION Y VALIDACION DEL SISTEMA

Para garantizar la sostenibilidad y efectividad de la solución, se realizarán pruebas técnicas periódicas, incluyendo validaciones funcionales, análisis de rendimiento en condiciones operativas reales y pruebas controladas de intrusión. Se instauran métricas de evaluación como tasa de falsos positivos, correlación efectiva de eventos, tiempo promedio de detección y continuidad operativa del sistema. Con base en los resultados, se efectuarán ajustes técnicos, mejoras en protocolos de

operación y actualización de algoritmos. Este proceso de mejora continua garantizará que el sistema se mantenga actualizado ante amenazas nuevas, ampliando su capacidad de adaptación y escalabilidad hacia otras terminales administradas por el SAN.

De tal manera ISO (2019) nos menciona que la validación y la mejora continua del sistema responden a los alineamientos de la norma ISO 22301:2019, lo que establece el uso del ciclo PDCA para el aseguramiento de la resiliencia organizacional y la continuidad operativa.

6.4.2 DESARROLLO

El desarrollo de la propuesta se organiza en tres fases estratégicas, por lo que cada una va acompañada de acciones específicas que permitirán garantizar la implementación efectiva del sistema integrado de monitoreo de seguridad cibernética y física basado en visión e inteligencia artificial. Por lo tanto, se incorpora una metodología de escalabilidad que permitirá replicar este modelo en otras terminales aeroportuarias administradas por el SAN, asegurando la expansión y sostenibilidad progresiva de la solución.

FASE 1: Diseño e integración tecnológica de la arquitectura del sistema

En esta fase se llevará a cabo el diseño e integración de la arquitectura tecnológica que permitirá unificar la vigilancia cibernética y física del Aeropuerto Ramon Villeda Morales. Se realizará un levantamiento técnico de los sistemas actuales (Sensores, firewalls. Cámaras, herramientas de ciberseguridad y registros operativos) y se desarrollara el modelo de interoperabilidad imprescindibles para la centralización de los datos en una única plataforma.

Se especifican e implementan modelos de visión artificial para la detección de conductas sospechosas, eventos relevantes en tiempo real e intrusiones, conjunto con los modelos de inteligencia artificial para la identificación de patrones de riesgo en la red y accesos no autorizados. Se desarrollará un motor de correlación hibrido que vincule eventos cibernéticos y físicos, priorizando aleras críticas y falsos positivos.

Entregables técnicos de la Fase 1:

- Documentos de arquitectura del sistema integrado de monitoreo.

- Diagramas de flujo de datos e interoperabilidad.

- Especificación técnica de modelos de visión artificial y algoritmos de inteligencia artificial.

- Manual técnico de integración para replicación en otros aeropuertos del SAN.

Estos entregables integran la base técnica del sistema y permiten su validación, escalabilidad y replicidad dentro del ecosistema aeroportuario del SAN.

FASE 2: Desarrollo de capacidades del personal e implementación operativa.

Esta fase se concentra en la puesta en marcha del sistema y en el fortalecimiento del personal responsable del monitoreo. Se instalará la plataforma integrada en el Centro de Operaciones, mapas de calor, análisis predictivo, dashboards y métricas en tiempo real.

Se diseñará un plan de capacitación especializado orientado al personal operativo, seguridad aeroportuaria y técnico, que anexará talleres prácticos acerca del uso de la plataforma, interpretación de alertas automatizadas y procedimientos de respuesta frente a incidentes híbridos. De igual forma, serán creados simulaciones operativas que permitirán la evaluación de la capacidad de reacción ante el equipo frente a distintos escenarios de riesgo.

Entregables técnicos de la Fase 2:

- Prototipo funcional del dashboard de monitoreo integrado.

- Plan de capacitación técnica con contenido y módulos definidos.

- Manual de usuario del sistema de monitoreo.

- Material de formación: manuales, presentaciones y guías operativas.

- Escenarios de simulación documentados para el entrenamiento operativo.

Para facilitar la escalabilidad se desarrollará un programa de capacitación replicable, con videos, guías operativas y manuales estandarizados que podrán ser adoptadas por otras terminales sin la necesidad de formar nuevos instructores desde cero.

FASE 3: Monitoreo continuo, validación y mejora continua.

En esta fase será evaluado el rendimiento del sistema por medio de pruebas funcionales, auditorias de seguridad cibernética y física, simulaciones y análisis de métricas operativas. Se emplearán herramientas de monitoreo avanzado para validación del desempeño de los modelos de inteligencia y visión artificial, correlación efectiva de eventos, tasas de detección, tiempos de reducción y respuesta a los falsos positivos.

Se establecerán rutinas de mantenimiento técnico y actualizaciones periódicas del sistema, de la misma manera protocolos para ajuste de los algoritmos de acuerdo con la evolución de amenazas emergentes. También se realizará un análisis de riesgo continuo que permitirá la identificación de vulnerabilidades y proponer mejoras constantes.

Entregables técnicos de la Fase 3:

- Matriz de indicadores de desempeño (KPIs).

- Informe de pruebas del sistema y validación funcional.

- Manual de mantenimiento y operación del sistema.

- Informe de análisis de riesgo y recomendaciones técnicas.

- Protocolo de actualización y mejora continua del algoritmo.

La metodología de escalabilidad partiendo de esta fase se elaborará un plan de mantenimiento y mejora continua estándar, que permitirá a otras terminales aeroportuarias, ajustar, implementar y mantener el sistema de manera autónoma.

6.4.3 VIABILIDAD ANALITICA Y PREPARACION DE DATOS

Los datos obtenidos en el presente estudio, provenientes de entrevistas semiestructuradas al personal operativo del Servicio Aeroportuario Nacional, constituyen un insumo valido para su explotación por medio de técnicas de inteligencia artificial. Estos datos corresponden primordialmente de la información no estructurada en formato textual, la cual fue procesada por medio de técnicas de limpieza, análisis de frecuencias léxicas y codificación, permitiendo su transformación en datos estructurados capaz de análisis automatizado.

6.4.3.1 CLASIFICACION DE DATOS.

Para efectos de aplicabilidad, los datos fueron clasificados en las siguientes categorías:

Datos operativos: Menciones asociadas a tiempo de respuesta (27 menciones), respuesta (17 menciones) y centralización (3 menciones).

Datos de precisión: referencia a falsos positivos (17 menciones), alertas (13 menciones) y errores (6 menciones).

Datos estratégicos: Seguridad (111 menciones), continuidad (10 menciones) y riesgo (8 menciones).

Daros organizacionales: Capacitación (5 menciones), usuario (5 menciones), y resistencia (1 mención).

Esta clasificación brinda la estructuración de los datos en variables de entrada para modelos analítico de aprendizaje automático.

6.4.3.2 EVALUACION DE CALIDAD DE DATOS.

La calidad de los datos fue evaluada considerando criterios de completitud, relevancia y consistencia. En términos de completitud, el 100% de las entrevistas realizadas fue transcrito y analizado, sin registros incompletos, Respecto a la relevancia, más del 85% de las menciones se concentró en categorías directamente vinculadas a los objetivos de la investigación. En cuanto a la consistencia, las categorías principales se repitieron en al menos el 90% de las entrevistas, evidenciando patrones confiables y estables, lo que confirma la aptitud del conjunto de datos para su uso como insumo en modelos analíticos y de aprendizaje automático.

El análisis exploratorio evidencio ausencia de valores faltantes y una distribución coherente de las respuestas, lo que señala un conjunto de datos confiable para su utilización en modelos de inteligencia artificial orientados al análisis de patrones y apoyo a la toma de decisiones.

6.4.3.3 ALIMENTACION DE DATOS A LA INTELIGENCIA ARTIFICIAL.

A partir de la estructuración realizada, los datos pueden alimentar modelos de procesamiento de lenguaje natural (NLP) para:

- Priorización de eventos operativos con base en contexto y frecuencia.
- Clasificación de patrones recurrentes asociados a falsos positivos.
- Identificación automática de alertas de acuerdo con criticidad.

De igual manera, los indicadores derivados pueden emplearse en modelos supervisados de clasificación o en sistemas de reglas inteligentes para apoyar la correlación de alertas cibernéticas y físicas en tiempo real.

6.4.4 ESTRATEGIA INTEGRAL DE ADOPCION DE LA INTELIGENCIA ARTIFICIAL

La adopción de la inteligencia artificial en la propuesta planteada se aborda de manera integral y estratégica, considerando la automatización de procesos, la experimentación controlada, la madurez de los datos, la ciberseguridad, el uso de la inteligencia artificial generativa, gobierno

institucional y la orquestación.

6.4.5.1 ESTRATEGIA DE AUTOMATIZACION DE PROCESOS.

La inteligencia artificial se orienta a la automatización de procesos clave del monitoreo de seguridad cibernética y física, individualmente en la correlación de alertas, priorización de eventos y reducción de la gestión manual, permitiendo una respuesta más oportuna y eficiente ante incidentes.

6.4.5.2 ESTRATEGIA DE MADUREZ DE DATOS.

Se establece una estrategia de madurez de datos basada en la estructuración, clasificación y evaluación de la calidad de la información generada por los sistemas de monitoreo. Esta estrategia permite evolucionar desde datos no estructurados hacia insumos analíticos confiables, aptos para análisis predictivo básico y modelos de aprendizaje automático.

6.4.5.3 EXPERIMENTACION PERSONAL O DEPARTAMENTAL DE INTELIGENCIA ARTIFICIAL.

La adopción de la inteligencia artificial se plantea inicialmente por medio de esquemas de experimentación a nivel departamental o personal, especialmente en áreas operativas como lo es el centro de operaciones de seguridad, facilitando pilotos controlados que permiten validar los modelos y su impacto frente a una implementación institucional.

6.4.5.4 ESTARTEGIA DE INTELIGENCIA ARTIFICIAL GENERATIVA ORIENTADA AL NEGOCIO.

La inteligencia artificial generativa se considera como un apoyo a las necesidades del negocio, enfocándose en la generación automática de reportes operativos, apoyo a la toma de decisiones y resúmenes de incidentes, evitando implementaciones que no aporten valor directo a la operación aeroportuaria.

6.5.4.5 ESTRATEGIA DE CIBERSEGURIDAD.

La implementación de inteligencia artificial se integra con una estrategia de ciber seguridad guiada a la protección de los datos, la detección temprana de amenazas, control de accesos, garantizando la integridad, confidencialidad y disponibilidad de la información utilizada por los modelos analíticos.

6.5.4.6 ORQUESTACION Y GOBIERNO

Por último, la adopción de la inteligencia artificial se articula bajo un esquema de

orquestación y gobierno institucional, sustentado en el marco COBIT 2019, que define responsabilidades, métricas de desempeño, mecanismos de control, asegurando un uso controlado, seguro y alineado con los objetivos del Servicio Aeroportuario Nacional.

6.4.5 MARCO DE GOBERNANZA PARA LA IMPLEMENTACION DE INTELIGENCIA ARTIFICIAL

La implementación de la propuesta se sustenta en un marco de gobernanza basado en COBIT 2019, el cual permite alinear el uso de inteligencia y visión artificial con los objetivos institucionales del Servicio Aeroportuario Nacional, garantizando el control de riesgo, la generación de valor, la optimización de recursos y la trazabilidad de las decisiones tecnológicas, asegurando que la adopción de soluciones inteligentes se realice de una manera sostenible, controlada y acorde a la criticidad del entorno aeroportuario.

En este contexto, la propuesta se articula principalmente con los siguientes procesos de COBIT 2019: EDM03- Asegurar la optimización del riesgo, APO12-Gestionar el riesgo, APO13-Gestionar la seguridad y DSS05-Gestionar los servicios de seguridad, los cuales proporcionan lineamientos para la supervisión, protección de la información, gestión del riesgo y operación segura de los sistemas inteligentes propuestos.

6.5 MEDIDAS DE CONTROL

Las medidas de control se sitúan a evaluar la eficiencia, sostenibilidad, eficiencia del sistema integrado de monitoreo de seguridad cibernética y física basado en inteligencia y visión artificial. Los indicadores definidos permitirán medir el desempeño del sistema en términos de detección de amenazas, tiempo de respuesta operativa y reducción de falsos operativos, correlación de alertas y satisfacción del personal técnico. Cada indicador cuenta con su frecuencia de herramientas de correlación, límites de desempeño aceptables y herramientas de recolección.

6.5.1 INDICADORES

6.5.1.1 AUDITORIAS TRIMESTRALES DE SEGURIDAD CIBERNETICA Y FISICA.

Cada tres meses se realizarán auditorias para evaluar el funcionamiento técnico del sistema integrado, verificando la calibración de cámaras el desempeño de los modelos de inteligencia artificial, el rendimiento de las herramientas de ciberseguridad y la correlación de alertas. Estas auditorias incluirán pruebas controladas de intrusión física, simulación de ciber ataques y la

revisión de logs del motor de correlación hibrida.

KPI

A. Porcentaje de sensores y cámaras operando con una precisión optima

Formula: $Disponibilidad\ (\%) = \frac{Tiempo\ operativo}{Tiempo\ total} x100$

Fuente de datos: Reportes de mantto y registro del sistema de monitoreo.

Frecuencia de medición: Trimestral.

Límites de control tolerables:

Mínimo aceptable: 96%

Objetivo esperado: ≥ 98.5%

Máximo esperado: 99.9%

B. Porcentaje de incidentes correctamente correlacionados entre la seguridad cibernética y física

Formula $Correlacion\ efectiva\ (\%) = \frac{Incidentes\ correctamente\ correlacionados}{Total\ de\ incidentes\ detectados} x100$

Fuente de datos: Reportes de auditoría y logs del motor de correlación hibrida.

Límites de control tolerables:

Mínimo aceptable: 75%

Objetivo esperado: ≥ 88%

Máximo esperado: 97%

C. Porcentaje de reducción de falsos positivos posterior a cada auditoria.

Formula: $Reduccion\ de\ falsos\ positivos\ (\%) = \frac{FP_{antes} - FP_{despues}}{FP_{antes}} x100$

Fuente de datos: Históricos de alertas del sistema integrado.

Frecuencia de medición: Trimestral.

Límites de control tolerables:

Mínimo aceptable: 12%

Objetivo esperado: ≥ 28%

Máximo esperado: 45%

6.5.1.2 EVALUACION PRE Y POST IMPLEMENTACION DEL SISTEMA DEL SISTEMA

Se realizarán mediciones antes y después de la puesta en marcha del sistema para la evaluación del impacto en la capacidad operativa del personal, la precisión de la detección de incidente y la eficiencia del monitoreo.

KPI

D. Nivel de conocimiento del personal operativo y técnico antes y después de la capacitación

Formula: Promedio de resultados de encuestas pre y post capacitación además de las evaluaciones técnicas.

$$Promedio\ (x) = \frac{\sum Resultado\ de\ ecuestas}{Numero\ de\ encuestas}$$

Fuente de datos: Resultados de encuestas estructuradas y evaluaciones.

Frecuencia de medición: Antes y después de la capacitación.

Límites de control tolerables:

Mínimo aceptable: 65%

Objetivo esperado: ≥ 88%

Máximo esperado: 99.9%

E. Porcentaje de adopción de los protocolos de respuesta basados en inteligencia artificial

Formula: $Adopcion\ de\ protocolos\ (\%) = \frac{Protocolos\ aplicados\ efectivamente}{Total\ de\ protocolos\ definidos} x100$

Fuente de datos: Registro de reportes operativos e incidentes.

Frecuencia de medición: Semestral.

Límites de control tolerables:

Mínimo aceptable: 78%

Objetivo esperado: ≥ 92%

Máximo esperado: 99.9%

F. Porcentaje de mejora en la clasificación de incidentes.

Formula: $Mejora\ en\ clasificacion\ (\%) = \frac{CI_{DESPUES} - CI_{ANTES}}{CI_{ANTES}} x100$

Donde CI= Clasificación de incidentes.

Fuente de datos: Reportes de incidentes del centro de operaciones.

Frecuencia: Semestral.

Mínimo aceptable: 25%

Objetivo esperado: ≥ 35%

Máximo esperado: 55%

6.5.1.3 MONITOREO ACTIVO CON LA PLATAFORMA INTEGRADA

Se utilizará la plataforma unificada para el seguimiento continuo a eventos cibernéticos y físicos en tiempo real. Se registrarán todas las alertas y medirán los tiempos de respuesta, la efectividad del motor de correlación y la cantidad de incidentes afectados.

KPI

G. Tiempo promedio de respuesta frente alertas criticas

Formula: $Tiempo\ promedio = \frac{\sum Tiempo\ de\ respuesta}{Numero\ de\ alertas\ criticas}$

Fuente de datos: Logs del centro de operaciones y sistema de tickets.

Frecuencia de medición: Mensual.

Máximo aceptable: 8 min

Objetivo esperado: ≤ 4 minutos

Optimo: ≤ 2 minutos

H. Porcentaje de amenazas detectadas e tiempo real y gestionadas antes de causar impacto en la operación.

$$Gestion\ (\%) = \frac{Amenazas\ atenuadas}{Amenazas\ localizadas} x100$$

Fuente de datos: Reportes de incidentes y plataforma integrada.

Frecuencia de medición: Mensual.

Mínimo aceptable: 75%

Objetivo esperado: ≥ 90%

Máximo esperado: 99.9%

I. Número de incidentes evitados o mitigados por la visión e inteligencia artificial.

Formula: $Incidentes\ resueltos = \sum Incidentes\ atenuados$

Fuentes de datos: Reportes del sistema integrado.

Frecuencia de medición: Trimestral.

Resultados esperados: Aumento progresivo ≥ 23% anual

6.5.1.4 DESEMPEÑO Y SATIFACCION DEL PERSONAL TECNICO

Se evaluará la percepción del personal responsable del sistema para la medición de facilidad de uso, utilidad práctica y efectividad en la toma de decisiones.

KPI

J. Porcentaje de incidencias operativas resueltas en el primer contacto.

Formula:

$$Resolucion\ (\%) = \frac{Incidencias\ solventadas\ en\ primer\ contacto}{Total\ de\ incidencias} x100$$

Fuente de datos: Registros de soporte técnico.

Frecuencia de medición: Mensual.

Mínimo aceptable: 75 %

Objetivo esperado: ≥ 88 %

Máximo esperado: 97 %

Nivel de satisfacción general con la plataforma integrada.

K. Formula: Promedio de encuestas tipo Likert (escala 1-5)

$$Promedio\ de\ encuestas\ (x) = \frac{\sum Evaluacion\ de\ satifaccion\ del\ personal.}{Numero\ encuestas}$$

Fuente de datos: Encuestas estructuradas.

Frecuencia de medición: Semestral.

Límites de control tolerables:

Mínimo aceptable: 3.8 / 5

Objetivo esperado: ≥ 4.1 / 5

Máximo esperado: 4.9 / 5

L. Porcentaje de personal capaz de operar el sistema sin asistencia técnica.

$$Autonomia\ (\%) = \frac{Personal\ independiente}{Total\ de\ personal} x100$$

Fuente de datos: Reportes de supervisión y evaluaciones operativas.

Frecuencia de medición: Semestral.

Límites de control tolerables:

Mínimo aceptable: 70 %

Objetivo esperado: ≥ 93 %

Máximo esperado: 99.9 %

6.5.2 PLAN DE SEGUIMIENTO

El plan de seguimiento garantizara la correcta sostenibilidad, operación y mejora continua del sistema integrado. Se compone de cuatro mecanismos principales:

6.5.2.1 PROTOCOLO DE AUDITORIAS TRIMESTRALES

Con revisión de sensores, servidores, cámaras, módulos de inteligencia artificial y firewall.

Simulación de ciberataques controlados para la validación en la correlación de alertas.

Pruebas de intrusión física simulada.

Generación de un informe con recomendaciones y hallazgos.

6.5.2.2 GESTION Y MONITOREO DE INCIDENTES.

Categorización y registro de incidentes por nivel de riesgo.

Configuración de alertas automáticas basadas en inteligencia artificial.

Respuesta inmediata del centro de operaciones de acuerdo a los protocolos de mitigación.

6..2.3 REPORTES PERIODICOS Y EVALUACION DE IMPACTO.

Identificación de áreas de mejoras y propuestas de optimización.

Análisis semestral del desempeño del sistema de acuerdo a KPI.

Informes comparativos entre periodos operativos.

6.5.2.4 CAPACITACION CONTINUA Y MECANISMO DE SOPORTE TECNICO.

Publicación de boletines, manuales y actualización de seguridad.

Soporte técnico al personal del SAN frente a incidencias operativas.

Capacitaciones periódicas ante tendencias de seguridad cibernética y física.

Entrenamiento para nuevas funcionalidades del sistema integrado.

6.6 CRONOGRAMA DE IMPLEMENTACIÓN Y PRESUPUESTO

La implementación del sistema basado en visión e inteligencia artificial será desarrollada de una manera progresiva por medio de fases estructuradas, permitiendo una ejecución controlada, mitigación de riesgos operativos, y evaluación continua.

Para la estimación de la duración de cada actividad se utilizó la metodología PERT, por la cual permite considerar la incertidumbre inherente a proyectos tecnológicos por medio de tres escenarios de tiempo:

Tiempo optimista (O): tiempo mínimo requerido si la actividad se ejecuta sin contratiempo.

Tiempo más probable (M): tiempo estimado bajo condiciones normales de operación.

Tiempo pesimista (P): tiempo máximo estimado en caso de dificultades o retrasos técnicos.

El tiempo esperado (TE) se calcula por medio de la formula:

$$TE = \frac{O + 4M + P}{6}$$

De la misma forma, para la evaluación de la incertidumbre del cronograma se calcula la

varianza de cada actividad por medio de la expresión:

$$V = \left(\frac{P - O}{6}\right)^2$$

Tabla 19. CRONOGRAMA DE IMPLEMENTACION.

FASE	ACTIVIDAD	O (DIAS)	M(DIAS)	P(DIAS)	TE(DIAS)	VARIANZA
Fase 1: planificación	Análisis de brechas y levantamiento de infraestructura	10	14	20	$\frac{10+4(14)+20}{6}$ =14.33	$\left(\frac{20-10}{6}\right)^2$ =*2.78*
	Diseño de la arquitectura del sistema integrado	12	16	22	$\frac{12+4(16)+22}{6}$ =16.33	$\left(\frac{22-12}{6}\right)^2$ =2.78
Fase 2: Capacitación	Capacitación técnica al personal de TI y operativo	10	14	20	$\frac{10+4(14)+20}{6}$ =14.33	$\left(\frac{20-10}{6}\right)^2$ =2.78
Fase 3: Implementación	Desarrollo de algoritmos de Visión e inteligencia artificial	15	20	30	$\frac{15+4(20)+30}{6}$ =20.83	$\left(\frac{30-15}{6}\right)^2$ =6.25
	Despliegue operativo e integración de sistemas.	18	24	36	$\frac{18+4(24)+36}{6}$ =25	$\left(\frac{36-18}{6}\right)^2$ =9
Fase 4: Evaluación y monitoreo.	Simulaciones, pruebas funcionales y monitoreo.	12	16	24	$\frac{12+4(16)+24}{6}$ =16.67	$\left(\frac{24-12}{6}\right)^2$ =4
	Optimización del sistema y ajustes finales.	10	14	20	$\frac{10+4(14)+20}{6}$ =14.33	$\left(\frac{20-10}{6}\right)^2$ =2.78

Fuente: Elaboración propia

Cálculo del tiempo total del proyecto

T_{Total}=14.33+16.33+14.33+20.83+25+16.67+14.33= 122 días

Cálculo de la varianza total

V_{Total}= 2.78+2.78+2.78+6.25+9+4+2.78+30.37 días

Desviación estándar total

σ_{total}= $\sqrt{30.37}$ =5.51 días

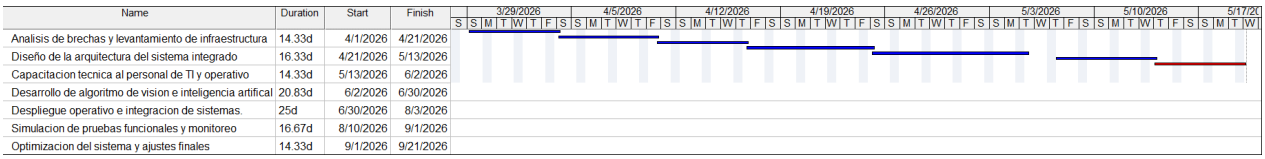


Figura 13. DIAGRAMA DE GANTT.

Fuente elaboración propia.

Tabla 20. PRESUPUESTO.

CONCEPTO	DESCRIPCION	COSTO UNITARIO (USD)	PERIOCIDAD	TOTAL (USD)	OBSERVACIONES
Infraestructura tecnológica	Almacenamiento, red y servidores.	28,000	1	28,000	Instalación inicial
Equipos de inteligencia artificial y cámaras	Sensores y cámaras IP inteligente	1,100	20	22,000	Equipos compatibles con visión artificial
Licencias y software	Plataformas de ciberseguridad	18,000	1	18,000	Licencias anuales
Desarrollo de algoritmos	Motor de correlación hibrida	15,000	1	15,000	Pruebas y desarrollo
Dashboards operativos	Tableros de control y visualización	7,000	1	7,000	Integración con SOC
Capacitacion técnica	Simulaciones y talleres	1,200	5 sesiones	6,000	Material didáctico
Pruebas y auditorias	Pruebas de seguridad y funcionalidades.	1,250	4 auditorias	5,000	Validación del sistema
Mantto y soporte	Soporte inicial.	4,000	1	4,000	Primer año
Total estimado				**105,000 usd**	

Fuente: Elaboración propia.

El presupuesto estimado para la implementación del sistema Híbrido de Seguridad aeroportuaria basado en visión e inteligencia artificial asciende a USD 105,000 se justifica en función del tratamiento de la explotación y estructuración de datos reales generados por los sistemas de monitoreo lógico y físico del aeropuerto. Cada componente presupuestado responde a la necesidad de transformar los datos del aeropuerto. Cada componente presupuestado responde a la necesidad de transformar datos no estructurados (eventos, alertas, registros y flujos visuales) en insumos aptos para modelos analíticos y de aprendizaje automático, permitiendo la reducción de falsos positivos, el fortalecimiento de la continuidad operativa, la priorización de alertas.

De igual manera, la inversión propuesta se orienta a una implementación escalable, priorizando soluciones y reutilizando datos existentes que maximizan el valor generado ante costos operativos relacionados a incidentes de seguridad e interrupciones del servicio.

6.6.1 JUSTIFICACION DEL RETORNO DE LA INVERSION (ROI)

El retorno de la inversión brinda la evaluación de la vialidad financiera del proyecto al comparar los beneficios económicos estimados ante la inversión realizada. En el contexto de la seguridad aeroportuaria, los beneficios no solo se reflejan en ahorros directos, sino también en la mitigación de pérdidas operativas, optimización del uso de recursos humanos, reducción de incidentes, disminución del impacto operativo y reputacional.

Para el cálculo del ROI se contemplan los siguientes beneficios anuales estimados, derivados de la implementación del sistema:

Tabla 21. CALCULO DEL ROI.

Concepto	Descripción	Beneficio estimado USD/ AÑO
Reducción de incidentes operativos.	Menor impacto por intrusiones, eventos y fallos no detectados.	36,000
Reducción de falsos positivos.	Maximización del tiempo del personal operativo.	17,000
Optimización de recursos humanos	Disminución de horas hombre por automatización.	23,000
Predisposición de eventos críticos	Atenuación de perdidas por interrupciones operativas.	19,000
Beneficio anual total estimado		95,000

Fuente: Elaboración propia.

CALCULO DEL ROI

Formula: $$ROI\ (\%) = \frac{Beneficio\ anual - Inversion\ inicial}{Inversion\ inicial} x100$$

$$ROI\ (\%) = \frac{95{,}000 - 105{,}000}{105{,}000} x100$$

$$ROI\ (\%) = -9.523\%$$

Durante el primer año, el proyecto presenta un ROI levemente negativo por la razón de la

inversión inicial. A pesar de eso, partir del segundo año, al no repetirse los costos de desarrollo e infraestructura, el sistema comienza a generar beneficios netos.

6.6.2 ROI PROYECTADO A 3 AÑO

Tabla 22.PROYECCION DE ROI A 3 AÑOS.

Año	Beneficio estimado (USD)	Costos recurrentes (USD)	Flujo neto
Año	95,000	105,000	-10,000
Año	95,000	23,000	72,000
Año	95,000	23,000	72,000
Total 3 años	285,000	151,000	134,000

Fuente: Elaboración propia.

$$ROI_{3\text{año}} = \frac{134{,}000}{105{,}000} x100 = 127.619\%$$

El proyecto se vuelve rentable partiendo del segundo año.

Presenta un ROI sostenido y positivo en el mediano plazo.

6.6.3 ANALISIS DE SENSIBILIDAD.

Dado que los beneficios estimados pueden tener variación de acuerdo con condiciones de madurez y operativas del sistema, por lo cual se realizó un análisis de sensibilidad teniendo en cuenta tres escenarios.

Tabla 23. SENSIBILIDAD.

Escenario	Beneficio anual (USD)	ROI a 3 años
Optimista (+20%)	114,000	182.8%
Moderado (Base)	95,000	129.5%
Pesimista (-20%)	76,000	76.5%

Fuente: Elaboración propia.

Incluso en un escenario pesimista, el proyecto mantiene un ROI positivo a tres años, por lo que da evidencia de su robustez financiera.

6.6.4 ANALISIS DE INCERTIDUMBRE.

La incertidumbre del proyecto se asocia especialmente en:

Curva de adopción del sistema por parte del personal.

Evolución de amenazas físicas y cibernéticas.

Variabilidad en la reducción real de incidentes.

Sin embargo, la capacitación progresiva, el uso de tecnologías escalables y la mejora continua del sistema reducen el riesgo financiero. Por lo tanto, al tratarse de un proyecto piloto, el SAN puede ajustar la inversión en fases posteriores con base en resultados medibles, reduciendo la exposición económica.

6.7 CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA

La propuesta planteada guarda una relación coherente y directa con los hallazgos recabados a lo largo de la investigación, respondiendo a las brechas identificadas en el sistema de monitoreo física y cibernética del Servicio Aeroportuario Nacional. El estudio evidencio limitaciones asociadas a la fragmentación de los sistemas de vigilancia, la dificultad para correlacionar alertas lógicas y físicas, la alta dependencia de procesos manuales, y sobre todo la dificultad para correlacionar alertas lógicas y físicas en tiempo real, lo que impacta negativamente sobre la capacidad de detección temprana y en la continuidad operativa del Aeropuerto Ramon Villeda Morales. En este contexto, la propuesta de integración de inteligencia y visión artificial surge como una respuesta directa a dichas problemáticas, transformando los resultados del análisis en acciones operativas y técnicas concisas.

Los incidentes recientes han puesto de manifiesto las vulnerabilidades de los sistemas críticos de aviación, lo que ha llevado a los organismos reguladores a exigir medidas de ciberseguridad reforzadas. Los nuevos requisitos de ciberseguridad de la FAA para la aviación comercial incluyen evaluaciones obligatorias de amenazas, protocolos de notificación de incidentes y auditorías de seguridad periódicas para las compañías aéreas y los proveedores de servicios de aviación. (Stevens, 2025)

Las acciones propuestas, como la implementación de una plataforma unificada de monitoreo, la correlación automatizada de eventos cibernéticos y físicos, el uso de algoritmos de inteligencia artificial para la detección de anomalías, se encuentran alineados con los objetivos de la investigación y con las percepciones recopiladas durante el estudio del caso. De esa misma manera, el modelo de evaluación, mejora progresiva y monitoreo continúo planteado en la

propuesta brindan la accesibilidad al seguimiento de los indicadores claves identificados en la investigación, como ser la reducción de falsos positivos, la mejora en los tiempos de respuesta y el fortalecimiento en la toma de decisiones del centro de operaciones.

La integración de tecnologías digitales, como los sistemas automatizados de control de vuelo, el almacenamiento de datos en la nube y las redes de comunicación en tiempo real, ha mejorado la eficiencia operativa. Sin embargo, esta transformación digital también ha convertido a la industria en un objetivo para los ciberdelincuentes. Abordar las amenazas a la ciberseguridad es imprescindible para garantizar la seguridad, la fiabilidad y la integridad de los sistemas de aviación. (Kapil, 2025)

En conjunto, esta propuesta no solo operacionaliza los hallazgos empíricos y teóricos de la investigación, sino que también contribuye al fortalecimiento de la resiliencia operativa y la seguridad integral del SAN. De esta manera, se asegura que la aplicabilidad del estudio sea escalable, sostenida y alineada con los estándares internacionales de seguridad aeroportuaria, consolidando un modelo de monitoreo robusto, eficiente y acorde a las necesidades estratégicas del sector aeroportuario hondureño.

REFERENCIAS BIBLIOGRÁFICAS

Acevedo, M. D., & Guisado, Á. C. (2024). Revisión del estado actual de la ciberseguridad en Colombia. *Estudios en Seguridad y Defensa*, *19*(38), 179–203. https://doi.org/10.25062/1900-8325.1999

Álvarez-Silva, O., Osorio, A., Ortega, S., & Agudelo-Restrepo, P. (2011). Estimation of the electric power potential using Pressure Retarded Osmosis in the Leon River's mouth: A first step for the harnessing of saline gradients in Colombia. *OCEANS 2011 IEEE - Spain*, 1–7. https://doi.org/10.1109/Oceans-Spain.2011.6003650

Amin, R., Wijngaart, T. van der, Dindol, A., & Rodgers, D. (2024, December 11). *Cyber threats in the aviation industry: Clyde & Co*. https://www.clydeco.com:443/insights/2024/11/cyber-threats-in-the-aviation-industry

ARSA. (2006). *Decreto Legislativo No. 170 – 2006 Ley de Transparencia y acceso a la información pública – ARSA*. https://arsateca.arsa.hn/decreto-legislativo-no-170-2006-ley-de-transparencia-y-acceso-a-la-informacion-publica/

Audretsch, D., & Belitski, M. (2021). Frank Knight, uncertainty and knowledge spillover entrepreneurship. *Journal of Institutional Economics*, *17*, 1–27. https://doi.org/10.1017/S1744137421000527

Chaki, A., Prashant, M., & Sen, P. (2010). A Comprehensive Market Analysis on Camera and Illumination Sensors for Image Processing and Machine Vision Applications. *2010 International Conference on Computational Intelligence and Communication Networks*, 382–385. https://doi.org/10.1109/CICN.2010.79

Cheffins, B. (2021, April 4). The Famous Article on the Theory of the Firm is Widely Misunderstood. *ProMarket*. https://www.promarket.org/2021/04/04/theory-firm-misunderstood-michael-jensen-william-meckling/

Chen, R., Liu, Y., & Zhou, F. (2021). Turning Danger into Safety: The Origin, Research Context and

Theoretical Framework of Organizational Resilience. *IEEE Access*, *9*, 48899–48913. https://doi.org/10.1109/ACCESS.2021.3069301

Chen, Y.-H., & Hu, P. (2020). Research on Cost-Effectiveness Evaluation Model Based on "Six Indexes" of Equipment. *2020 3rd International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE)*, 662–665. https://doi.org/10.1109/AEMCSE50948.2020.00145

Chen, Z.-H., & Juang, J.-C. (2018). Neural Network Learning to Identify Airport Runway Taxiway Numbers. *2018 International Symposium on Computer, Consumer and Control (IS3C)*, 153–157. https://doi.org/10.1109/IS3C.2018.00046

CONATEL. (2024). *Infome anual de los indicadores del sector de telecomunicaciones en honduras*. https://www.conatel.gob.hn/wp-content/uploads/2025/11/INFORME-ANUAL-DEL-SECTOR-DE-TELECOMUNICACIONES-2024-1-1.pdf

Conatel. (2025, February 9). *Institución – Conatel*. https://www.conatel.gob.hn/institucion/

Consejo de Europa. (2001, November 23). *Convenio de Budapest sobre la Ciberdelincuencia*. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Consejo de Europa. (2022, May 12). *Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas*. https://rm.coe.int/1680a83724

Creswell, J. W. (2013). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. SAGE.

CYBER DEFENSE, M. (2016, August 2). China 1937CN Team hackers attack airports in Vietnam. *Cyber Defense Magazine*. https://www.cyberdefensemagazine.com/china-1937cn-team-hackers-attack-airports-in-vietnam/

Deepthi, R. S., & Sankaraiah, S. (2011). Implementation of mobile platform using Qt and OpenCV for image processing applications. *2011 IEEE Conference on Open Systems*, 284–289. https://doi.org/10.1109/ICOS.2011.6079235

Demir, E., Yildiz, K., Demir, O., & Ulku, E. E. (2020). Computer Vision Based Intelligent 3D CNC Machines. *2020 Innovations in Intelligent Systems and Applications Conference (ASYU)*, 1–6. https://doi.org/10.1109/ASYU50717.2020.9259826

Diario oficial la gaceta. (2011, December 12). *DECRETO No. 243-2011*. https://www.conatel.gob.hn/doc/Regulacion/leyes/Ley_especial_comunicaciones_privadas.pdf

Diario oficial la gaceta. (2014, March 7). *DECRETO No. 325-2013*. EMPRESA NACIONAL DE ARTES GRÁFICAS. https://www.melarayasociados.com/legislacion/marzo2014/DECRETO-No.-325-2013-Reforma-a-Ley-Marco-del-Sector-de-Telecomunicaciones.pdf

Diario oficial la gaceta. (2015). *Decreto No. 149.2014*. https://investigacionjuridica.unah.edu.hn/assets/Investigacion-Juridica/paginas/boletin-informativo/Ley-Comercio-Electronico.pdf

Diario oficial la gaceta. (2019, May 10). *DECRETO No. 130-2017*. EMPRESA NACIONAL DE ARTES GRÁFICAS. https://www.tsc.gob.hn/web/leyes/Decreto_130-2017.pdf

Direccion de despacho. (2025, May 8). *Organigrama institucional del SAN*.

Erkek, I., & Irmak, E. (2025). Enhancing Cybersecurity of a Hydroelectric Power Plant Through Digital Twin Modeling and Explainable AI. *IEEE Access*, *13*, 41887–41908. https://doi.org/10.1109/ACCESS.2025.3547672

Gobeo, A., Fowler, C., & Buchanan, W. J. (2020). GDPR and Cyber Security for Business Information Systems. In *GDPR and Cyber Security for Business Information Systems* (pp. i–xix). River Publishers. https://ieeexplore.ieee.org/document/9228139

Hamui-Sutton, A. (2013). Un acercamiento a los métodos mixtos de investigación en educación médica. *Investigación en educación médica*, *2*(8), 211–216.

Hernandez Sampieri, R., Fernandez Collado, C., & Baptista Lucio, M. del P. (2014). *Metodología de la investigación* (Sexta edicion). McGRAW-HILL /INTERAMERICANA EDITORES, S.A. DE C.V.

Hernández-Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodologia de la investigacion: Las rutas cuantitativa, cualitativa y mixta* (septima edicion). McGRAW-HILL INTERAMERICANA EDITORES, S.A. de C. V.

ICAO. (2019, October). *Aviation Cybersecurity Strategy*. INTERNATIONAL CIVIL AVIATION ORGANIZATION. https://www.icao.int/sites/default/files/Meetings/a42/Documents/AVIATION-CYBERSECURITY-STRATEGY.EN_.pdf

International Trade Administration. (2024, January 23). *Filipinas—Tecnologías de la información y las comunicaciones*. https://www.trade.gov/country-commercial-guides/philippines-information-and-communications-technology

ISO. (2018). *ISO/IEC 20000-1:2018*. ISO. https://www.iso.org/standard/70636.html

ISO. (2019). *ISO 22301:2019(en), Security and resilience—Business continuity management systems—Requirements*. https://www.iso.org/obp/ui/en/#iso:std:iso:22301:ed-2:v1:en

ISO. (2022a). *ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-3:v1:en

ISO. (2022b). *ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-3:v1:en

Ju, Y., Wang, X., & Chen, X. (2019). Research on OMR Recognition Based on Convolutional Neural Network Tensorflow Platform. *2019 11th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, 688–691. https://doi.org/10.1109/ICMTMA.2019.00157

Kapil, G. (2025). *Cybersecurity Challenges in Aviation*. 17–21. https://doi.org/10.5281/zenodo.15058097

Li, J., Mei, X., Wang, J., Xie, B., & Xu, Y. (2020). Simulation Experiment Teaching for Airport Fire Escape

based on Virtual Reality and Artificial Intelligence Technology. *2020 IEEE 2nd International Conference on Civil Aviation Safety and Information Technology (ICCASIT*, 1014–1017. https://doi.org/10.1109/ICCASIT50869.2020.9368740

Liu, J., & Guan, X. (2010). Dynamic receding horizon control for airport capacity management. *2010 International Conference on Mechanic Automation and Control Engineering*, 2746–2749. https://doi.org/10.1109/MACE.2010.5535400

Molina Gomez, J., Murcia Yela, Y. C., Uron Rincon, L. E., Cordoba Gomez, L. C., Garzon Aristizabal, D. A., Garcia Filoth, G., Forero Varela, J. M., Sanchez Sanchez, J. A., Acuña Acuña, L. M., Mendoza Piedrahita, T. E., Diaz Molina, A., Barrios Perdomo, N., Maria Peraza, A., Andres Jimenez, C., Elberto Ortiz, E., & Cortes Hernandez, A. J. (2025). Lineamiento para la identificación de las infraestructuras críticas cibernéticas. *Ministerio de tecnologias de la informacion y las telecomunicaciones*, *5*, 49.

Moore, M. (2022, December 14). 45 Cybersecurity Statistics and Facts [2025]. *University of San Diego Online Degrees*. https://onlinedegrees.sandiego.edu/cyber-security-statistics/

Naciones unidas. (2020, June 23). *Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*. https://docs.un.org/es/A/75/123

Noor, U., & Ghazanfar, A. (2016). A survey revealing path towards service life cycle management in COBIT 5. *2016 Eleventh International Conference on Digital Information Management (ICDIM)*, 68–73. https://doi.org/10.1109/ICDIM.2016.7829754

Nystad, E., Simensen, J. E., & Raspotnig, C. (2021). Investigating operative cybersecurity awareness in air traffic control. *2021 14th International Conference on Security of Information and Networks (SIN)*, *1*, 1–8. https://doi.org/10.1109/SIN54109.2021.9699158

OACI. (2022). *Anexo 17_Seguridad de la aviacion* (Decimosegunda). https://www.dgac.gob.bo/wp-content/uploads/2022/10/Anexo17_12ed_Enm18_ES.pdf?utm

Odumesi, J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, *6*, 116–125. https://doi.org/10.5897/IJSA2013.0510

Otzen, T., & Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *International Journal of Morphology*, *35*(1), 227–232. https://doi.org/10.4067/S0717-95022017000100037

Pereira, R., & da Silva, M. M. (2010). ITIL maturity model. *5th Iberian Conference on Information Systems and Technologies*, 1–6. https://ieeexplore.ieee.org/document/5556698

Perona, A. M. (2010). *Ensayos sobre video, documental y cine*. Editorial Brujas. https://elibro.net/es/ereader/unitechn/78034

Raikov, A. N., & Pirani, M. (2022). Human-Machine Duality: What's Next in Cognitive Aspects of Artificial Intelligence? *IEEE Access*, *10*, 56296–56315. https://doi.org/10.1109/ACCESS.2022.3177657

Rakas, S. V. B., Stojanović, M. D., & Marković-Petrović, J. D. (2020). A Review of Research Work on Network-Based SCADA Intrusion Detection Systems. *IEEE Access*, *8*, 93083–93108. https://doi.org/10.1109/ACCESS.2020.2994961

Ramírez Pascual, B. (2023). *La ciberseguridad en la era de la Inteligencia Artificial: Dilemas y retos empresariales*. LA LEY Soluciones Legales S.A. https://elibro.net/es/ereader/unitechn/248924?page=57

Ribeiro, A. (2024, January 30). Aviation industry faces rising cybersecurity risks as new technologies drive adoption, says Aviation ISAC survey. *Industrial Cyber*. https://industrialcyber.co/reports/aviation-industry-faces-rising-cybersecurity-risks-as-new-technologies-drive-adoption-says-aviation-isac-survey/

Rodríguez, J. (2024, January 17). ✅ *Qué es el análisis de datos: Definición, etapas y ejemplos*. https://www.mundoposgrado.com/que-es-el-analisis-de-datos/

Salmons, J. (2024, February 14). *Methods Literature as Part of a Review*. Sage Research Methods

Community. https://researchmethodscommunity.sagepub.com/blog/methods-literature-as-part-of-a-review

Salomão, A. (2023, December 20). Entrevistas semiestructuradas en la investigación cualitativa. *Blog Mind the Graph*. https://mindthegraph.com/blog/es/nitel-arastirmalarda-yari-yapisal-gorusmeler/

Shaqwi, F. S., Audah, L., Hassan, M. H., Jubair, M. A., Abd Wahab, M. H., & Mostafa, S. A. (2021). A Concise Review of Deep Learning Deployment in 3D Computer Vision Systems. *2021 4th International Symposium on Agents, Multi-Agent Systems and Robotics (ISAMSR)*, 157–160. https://doi.org/10.1109/ISAMSR53229.2021.9567757

Simons, H. (2013). *El estudio de caso: Teoría y práctica*. Ediciones Morata, S. L. https://elibro.net/es/ereader/unitechn/51828

Smith, R. (2016). Performance of MPI Codes Written in Python with NumPy and mpi4py. *2016 6th Workshop on Python for High-Performance and Scientific Computing (PyHPC)*, 45–51. https://doi.org/10.1109/PyHPC.2016.010

Song, F. (2025). Integration of Sustainability and Civic Moraity in New-Era Educational Technology: Methods for Developing Digital Tools for Lifelong Learning and Social Responsibility. *2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA)*, 1–5. https://doi.org/10.1109/ICHORA65333.2025.11017194

Spatari, N. (2025). Building Safe Digital Environments for Children: AI Regulatory Sandbox and Pilot Project Insights. *2025 12th International Conference on Future Internet of Things and Cloud (FiCloud)*, 459–466. https://doi.org/10.1109/FiCloud66139.2025.00070

Stevens, M. (2025, September 17). *Cybersecurity Challenges and Solutions for Modern Aviation Infrastructure*. Aviation Conference. https://aviationconference.com

Traynor, O. (2025, August 26). The Rising Risk of Aviation Cyberattacks. *CybelAngel*.

https://cybelangel.com/blog/the-global-impact-of-aviation-cyberattacks/

Wang, S., Xu, D., & Yan, S. (2010). Analysis and application of Wireshark in TCP/IP protocol teaching. *2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT)*, *2*, 269–272. https://doi.org/10.1109/EDT.2010.5496372

Yin, R. K. (2009). *Case Study Research: Design and Methods*. SAGE.

Yin, R. K. (2017). *Case Study Research and Applications: Design and Methods*. SAGE Publications.

Zafire. (2024, August 23). Aviation Cyber Security: The Potential Threats, Impact and Solutions. *Zafire*. https://www.zafire.com/blog/2024/08/23/cybersecurity-in-aviation/

Zhang, Z. (2019). Technologies Raise the Effectiveness of Airport Security Control. *2019 IEEE 1st International Conference on Civil Aviation Safety and Information Technology (ICCASIT)*, 431–434. https://doi.org/10.1109/ICCASIT48058.2019.8973152

Anexo 2. ESTRUCTURA DE GUIA DE ENTREVISTA

Guía de Entrevista a expertos en ciber seguridad del Servicio Aeroportuario Nacional acerca de seguridad física y cibernética.

Introducción: Estimado (a) usuario (a), agradecemos su facilidad para la colaboración en esta investigación para la evaluación de la eficacia en la integración de visión e inteligencia artificial en el monitoreo de seguridad física y cibernética. El propósito de esta entrevista es conocer su experiencia y percepción en relación con los sistemas de monitoreo empleado en el aeropuerto, con especial interés en la integración de inteligencia y visión artificial dentro de las plataformas de seguridad cibernética y física. La información que usted brinde será de gran valor para la comprensión de manera contextualizada y practica sobre la eficacia de estas tecnologías, brindando insumos para la formulación de propuestas que fortifiquen la seguridad del aeropuerto.

Tiempo estimado: La duración aproximada de la entrevista será 20 a 30 min, con la posibilidad de haber extensión breve de acuerdo con la profundidad de las respuestas.

Confidencialidad: Toda la información recabada será tratada de una manera anónima y confidencial. Los datos recabados serán utilizados de una exclusiva manera con fines académicos evitando cualquier vinculación de las respuestas con la identidad profesional o personal del participante exceptuando consentimiento expreso.

Consentimiento: La participación de la entrevista será voluntaria, y podría interrumpirse en cualquier momento por solicitud del entrevistado. La sesión será grabada precisamente con autorización previa, con el fin de tener aseguramiento de la precisión del análisis de la información y el resguardo de veracidad en los hallazgos

Instrucciones: La entrevista abarca preguntas abiertas para entender sus experiencias y percepciones acerca del uso de inteligencia artificial en seguridad y ciberseguridad. No hay respuestas incorrectas o correctas, lo sustancial es su perspectiva profesional, que ayudara a enriquecer la investigación

¿Como describiría su experiencia en la gestión de alertas de seguridad con los sistemas tradicionales manuales o independientes en el aeropuerto? *

¿Cuál es su percepción acerca de la integración de sistemas de visión artificial con plataformas de seguridad cibernética en relación con los sistemas convencionales? *

Desde su experiencia, ¿Cree que la implementación de estos sistemas integrados ha aportado a la reducción de las respuestas y tiempos de detección frente a incidentes de seguridad? ¿Por qué? *

¿Considera que la visualización centralizada de alertas lógicas físicas enriquece la rapidez y precisión a la toma de decisiones frente a un incidente de seguridad? Explique *

¿Ha notado una disminución en los falsos positivos al emplear sistemas integrados de monitoreó? ¿Cómo impacta esto en la eficacia de su trabajo? *

¿De qué manera cree que la integración de estos sistemas impacta la continuidad en la mitigación y operación de riesgos del aeropuerto, tomando en cuenta aspectos sociales, ambientales y económicos? *

¿Cuáles son los principales limitaciones y desafíos que ha experimentado al usar sistemas de inteligencia y visión artificial en el monitoreo de seguridad? *

¿Qué ajustes o mejoras propondría par la optimización de la integración de sistemas de inteligencia y visión artificial en el monitoreo de seguridad del aeropuerto? *