FACULTAD DE POSTGRADO

TESIS DE POSTGRADO

ANÁLISIS DE LA PERCEPCIÓN SOBRE EL USO DE INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING EN CIBER AMENAZAS DE LOS SISTEMAS DEL AEROPUERTO INTERNACIONAL DE PALMEROLA

SUSTENTADO POR:

LUIS MANUEL PALMA ORDOÑEZ

PREVIA A INVESTIDURA AL TÍTULO DE

MÁSTER EN GESTIÓN DE TECNOLÓGIAS DE INFORMACIÓN

TEGUCIGALPA, M.D.C., HONDURAS, C.A.

NOVIEMBRE, 2025

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA UNTEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTORA

ROSALPINA RODRÍGUEZ GUEVARA

VICERRECTOR ACADÉMICO NACIONAL

JAVIER ABRAHAM SALGADO LEZAMA

SECRETARIO GENERAL/PRORECTOR

ROGER MARTÍNEZ MIRALDA

DECANA DE POSTGRADO

ANA DEL CARMEN RETALLY VARGAS

EVALUACIÓN DE CIBER AMENAZAS EN LOS SISTEMAS DEL AEROPUERTO INTERNACIONAL DE PALMEROLA

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE MÁSTER EN GESTIÓN DE TECNOLÓGIAS DE LA INFORMACIÓN

ASESOR METODOLÓGICO

JUAN JACOBO PAREDES HELLER

ASESOR TEMÁTICO

JUAN JACOBO PAREDES HELLER

MIEMBROS DE LA TERNA

ALBA GABRIELA GARAY ROMERO

MARVIN ROBERTO MENDOZA VALENCIA

CARLOS ROBERTO AMADOR

LUIS MANUEL PALMA ORDOÑEZ

FACULTAD DE POSTGRADO

USO DE IA/ML EN CIBER AMENAZAS DE LOS SISTEMAS DEL AEROPUERTO INTERNACIONAL DE PALMEROLA

AUTORES:

Luis Manuel Palma Ordoñez

RESUMEN

La investigación tiene como propósito realizar una evaluación integral de las amenazas de ciberseguridad que afectan la infraestructura tecnológica del Aeropuerto Internacional de Palmerola. El estudio se desarrolló bajo un enfoque metodológico cuantitativo y descriptivo, apoyado en técnicas de recolección de datos como encuestas estructuradas con escala de Likert y entrevistas dirigidas al personal de tecnologías de la información y áreas vinculadas a la gestión operativa del aeropuerto.

Palabras clave: Unitec, Inteligencia Artificial, Machine Learning, Ciberseguridad, Ciberamenazas, Aeropuerto Internacional de Palmerola, Infraestructura tecnológica, Gestión de riesgos, Ransomware, Detección de amenazas, Normativas internacionales.

GRADUATE SCHOOL

USE OF AI/ML IN CYBER THREATS TO THE SYSTEMS OF PALMEROLA INTERNATIONAL AIRPORT

Luis Manuel Palma Ordoñez

ABSTRACT

This research aims to conduct a comprehensive assessment of the cybersecurity threats affecting the technological infrastructure of Palmerola International Airport, The study was developed using a quantitative and descriptive methodological approach, supported by data collection techniques such as structured surveys with a Likert scale and interviews with information technology personnel and staff from areas related to the airport's operational management.

Keywords: Unitec, Artificial Intelligence, Machine Learning, Cybersecurity, Cyberthreats, Palmerola International Airport, Technological Infrastructure, Risk Management, Ransomware, Threat Detection, International Regulations.

DEDICATORIA

A Dios, por darme la vida y la oportunidad de seguir creciendo personal y profesionalmente.

A mi madre, por ser mi amiga incondicional y enseñarme la sabiduría que guardan los adultos mayores. Siempre será mi modelo para seguir en la vida por su enorme valentía, paciencia y asertividad.

A mis hermanos, por tenerme paciencia y brindarme su colaboración durante este proceso final.

A mi esposa, una persona muy especial que contribuyó con las primeras herramientas para poder iniciar con esta Maestría.

Y a mis hijos por ser mi inspiración para poder lograr este objetivo.

Luis Manuel Palma Ordoñez

AGRADECIMIENTOS

A Dios, gracias por su amor misericordia y bondad, por permitirnos esta felicidad ante este logro; resultado de su ayuda e inteligencia durante el proceso, donde aprendimos que sólo en sus manos podemos lograr nuestras metas. Eres fiel a tus promesas aun cuando las posibilidades no están a nuestro favor.

Nuestro sincero agradecimiento a cada docente por su esfuerzo y dedicación en el proceso de formación durante la maestría.

A nuestra familia, que son el pilar de mayor importancia que tenemos en la vida, por ser el canal de bendición para nuestra formación tanto personal como profesional.

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

El primer capítulo de esta investigación planteara lo que la actualidad, el avance de las tecnologías de la información ha transformado significativamente el funcionamiento de diversas infraestructuras críticas a nivel mundial. Entre estas, los aeropuertos representan sistemas altamente complejos que integran múltiples plataformas tecnológicas para garantizar la seguridad, eficiencia y continuidad de las operaciones aéreas. Sin embargo, esta creciente digitalización también ha incrementado la exposición a amenazas cibernéticas que pueden afectar la disponibilidad, integridad y confidencialidad de los sistemas. En este contexto, la ciberseguridad se convierte en un elemento estratégico para proteger los procesos tecnológicos que sostienen las operaciones aeroportuarias. Por ello, resulta fundamental analizar las amenazas que pueden comprometer estos sistemas y explorar el uso de tecnologías emergentes que permitan fortalecer los mecanismos de protección.

Los aeropuertos modernos dependen de sistemas de información interconectados que soportan operaciones esenciales como el control de tráfico aéreo, gestión de pasajeros, sistemas de seguridad, comunicaciones, logística y servicios administrativos (National Institute of Standards and Technology [NIST], 2018; Organización de Aviación Civil Internacional [OACI], 2021; International Air Transport Association [IATA], 2020).

1.1 INTRODUCCIÓN

El Aeropuerto Internacional de Palmerola, como principal aeropuerto internacional de Honduras, constituye una infraestructura crítica para el país, no solo por su rol en la conectividad aérea, sino también por su impacto en la seguridad nacional, el comercio y el turismo. La creciente digitalización de sus procesos tecnológicos exige mecanismos avanzados de protección frente a ciberataques cada vez más sofisticados, persistentes y difíciles de detectar mediante enfoques tradicionales de ciberseguridad

En este contexto, la Inteligencia Artificial (IA) y el Machine Learning (ML) emergen como herramientas clave para fortalecer las capacidades de detección, prevención y respuesta ante incidentes de ciberseguridad. Estas tecnologías permiten analizar grandes volúmenes de datos en tiempo real, identificar patrones anómalos, anticipar comportamientos maliciosos y automatizar decisiones de seguridad con mayor precisión

El presente estudio se enfoca en analizar cómo la aplicación de IA y ML puede contribuir al fortalecimiento de la ciberseguridad en el Aeropuerto Internacional de Palmerola, considerando su realidad tecnológica y operativa.

1.2 ANTECEDENTES DEL PROBLEMA

A nivel internacional, diversos estudios y reportes han evidenciado que los aeropuertos se han convertido en objetivos prioritarios de ataques cibernéticos debido a la criticidad de sus operaciones y a la alta interconectividad de sus sistemas. Incidentes de ransomware, ataques de denegación de servicio (DDoS), accesos no autorizados y explotación de vulnerabilidades en sistemas industriales (OT) han afectado a aeropuertos en Europa, Asia y América, generando interrupciones operativas y riesgos para la seguridad de los pasajeros **(Husain & Rehman, 2020; Kim & Park, 2022)**.

Organismos internacionales como la Organización de Aviación Civil Internacional (OACI) y la Asociación Internacional de Transporte Aéreo (IATA) han advertido sobre la necesidad de adoptar enfoques avanzados de ciberseguridad que integren tecnologías emergentes como la inteligencia artificial para proteger infraestructuras aeroportuarias. En este sentido, la IA y el ML han sido aplicados en otros aeropuertos para la detección temprana de intrusiones, análisis de tráfico de red, correlación de eventos de seguridad y respuesta automatizada a incidentes **(OACI, 2021; IATA, 2020)**.

En el contexto nacional, Honduras ha avanzado progresivamente en la modernización de sus infraestructuras aeroportuarias; no obstante, la ciberseguridad aún enfrenta desafíos relacionados con la limitación de recursos, la dependencia de soluciones tradicionales basadas en firmas, la escasa automatización en la detección de amenazas y la falta de modelos predictivos que permitan anticipar riesgos.

El Aeropuerto Internacional de Palmerola, al integrar sistemas de información críticos, redes corporativas, plataformas operativas y servicios digitales, requiere fortalecer su postura de ciberseguridad frente a amenazas internas y externas. La ausencia de estudios específicos que analicen la aplicación de IA y ML en la ciberseguridad aeroportuaria local evidencia una brecha de conocimiento que justifica el desarrollo de la presente investigación **(NIST, 2018; Chowdhury & Rahman, 2020)**.

1.3 DEFINICIÓN DEL PROBLEMA

Los mecanismos tradicionales de ciberseguridad utilizados en muchas infraestructuras aeroportuarias se basan principalmente en reglas estáticas y firmas predefinidas, lo que limita su capacidad para detectar amenazas avanzadas, ataques desconocidos o comportamientos anómalos complejos **(Sommer & Brown, 2019; Stallings & Brown, 2022)**.

Esta situación representa un riesgo significativo para la continuidad operativa y la seguridad de la información del Aeropuerto Internacional de Palmerola.

La falta de implementación de soluciones basadas en Inteligencia Artificial y Machine Learning dificulta la detección temprana de incidentes, incrementa los tiempos de respuesta y reduce la capacidad de anticipación ante ataques cibernéticos **(Alazab et al., 2021; Li et al., 2020)**.

Asimismo, la creciente cantidad de datos generados por los sistemas tecnológicos del aeropuerto supera la capacidad de análisis manual o semiautomática de los equipos de seguridad.

Ante este escenario, surge la necesidad de analizar cómo la aplicación de IA y ML puede mejorar los procesos de ciberseguridad en el Aeropuerto Internacional de Palmerola, optimizando la detección de amenazas, la gestión de riesgos y la toma de decisiones en materia de seguridad de la información.

1.3.1 ENUNCIADO DEL PROBLEMA

El Aeropuerto Internacional de Palmerola (XPL) constituye una de las infraestructuras críticas más importantes de Honduras, siendo un nodo estratégico para la conectividad aérea, el comercio y la seguridad nacional. Sin embargo, la creciente digitalización de sus operaciones que incluyen el control de tráfico aéreo, gestión de pasajeros, logística y sistemas de seguridad ha expandido significativamente su superficie de exposición a ciber amenazas cada vez más sofisticadas.

El problema central radica en que los mecanismos de ciberseguridad actualmente implementados en el aeropuerto presentan limitaciones críticas frente al panorama de amenazas moderno: Dependencia de Modelos Reactivos: Los sistemas de protección actuales se basan mayoritariamente en reglas estáticas y firmas predefinidas. Esto impide

la detección oportuna de ataques de "día cero", amenazas persistentes avanzadas (APT) o comportamientos anómalos complejos que no coinciden con patrones previamente registrados. Insuficiencia en la Gestión de Datos: La infraestructura tecnológica de Palmerola genera un volumen masivo de datos y registros (logs) provenientes de sistemas IT (informáticos) y OT (operacionales).

La capacidad actual para analizar esta información de forma manual o semiautomática es insuficiente, lo que provoca la saturación de los equipos de seguridad y la posible omisión de señales críticas de intrusión. Tiempos de Respuesta Prolongados: Debido a la escasa automatización en la correlación de eventos, la respuesta ante incidentes requiere una alta intervención manual.

En un entorno aeroportuario, donde la continuidad operativa es vital, estos retrasos incrementan el riesgo de interrupciones en los servicios esenciales y comprometen la seguridad de la información. Brecha Tecnológica y de Capacitación: Existe un bajo nivel de adopción de tecnologías emergentes como la Inteligencia Artificial (IA) y el Machine Learning (ML) en los procesos de seguridad local.

Esta falta de herramientas predictivas deja al aeropuerto en una posición de vulnerabilidad frente a atacantes que ya utilizan estas tecnologías para automatizar sus ofensivas. En conclusión, la brecha entre la sofisticación de las ciberamenazas (como ransomware y phishing avanzado) y la capacidad de respuesta actual del Aeropuerto Internacional de Palmerola representa un riesgo latente para la resiliencia tecnológica y la seguridad operativa del sector aeroportuario hondureño.

1.3.2 FORMULACIÓN DEL PROBLEMA

La complejidad intrínseca del ecosistema digital del Aeropuerto Internacional de Palmerola onde convergen redes de datos de pasajeros, sistemas de control de navegación aérea, protocolos de comunicación de carga y plataformas de gestión administrativa demanda un paradigma de seguridad que trascienda la vigilancia perimetral clásica. En la actualidad, el aeropuerto se enfrenta a un entorno de amenazas caracterizado por la automatización del ataque; el uso de botnets, el ransomware dirigido y la manipulación de datos de telemetría (como el sistema ADS-B) representan riesgos que los sistemas basados en firmas ya no pueden contener con eficacia.

Esta brecha de seguridad no es solo una cuestión de actualización de software, sino una debilidad estructural en la capacidad de detección temprana. Al no contar con modelos que "aprendan" del comportamiento normal del tráfico aeroportuario, cualquier desviación sutil pero maliciosa puede pasar desapercibida durante días, comprometiendo la integridad de la infraestructura. Por lo tanto, surge la necesidad imperativa de evaluar cómo la integración de capacidades cognitivas y analíticas avanzadas puede transformar la postura defensiva del aeropuerto de un estado de reacción pasiva a uno de anticipación proactiva.

1.4 PREGUNTAS DE INVESTIGACIÓN

Las preguntas de investigación orientan el desarrollo del presente estudio, permitiendo analizar los aspectos clave relacionados con la ciberseguridad en entornos aeroportuarios. En este sentido, la investigación se enfoca en examinar cómo la aplicación de la Inteligencia Artificial y el Machine Learning puede contribuir al fortalecimiento de los sistemas de seguridad informática. Particularmente, se toma como referencia el Aeropuerto Internacional de Palmerola, considerando los riesgos y amenazas cibernéticas que pueden afectar sus operaciones tecnológicas.

A partir de ello, se formulan preguntas que buscan identificar amenazas, evaluar tecnologías emergentes y analizar su impacto en la detección y respuesta ante incidentes de seguridad.

1.4.1 PREGUNTA GENERAL

La pregunta general de esta investigación se formula con el propósito de orientar el análisis hacia el papel que desempeñan la Inteligencia Artificial y el Machine Learning en el fortalecimiento de la ciberseguridad aeroportuaria. Esta pregunta central sirve como eje conductor para explorar soluciones tecnológicas avanzadas que permitan mejorar la detección, prevención y respuesta ante amenazas. Su planteamiento busca delimitar el enfoque principal del estudio y establecer la dirección del trabajo investigativo.

¿Cómo puede la aplicación de Inteligencia Artificial y Machine Learning fortalecer la ciberseguridad del Aeropuerto Internacional de Palmerola?

1.4.2 PREGUNTAS ESPECÍFICAS

Las preguntas específicas se plantean para desglosar de manera detallada los distintos aspectos que intervienen en el análisis del entorno cibernético del Aeropuerto Internacional de Palmerola. A través de estas interrogantes, se busca profundizar en las amenazas actuales, las capacidades tecnológicas disponibles y el potencial de los modelos de IA aplicados a la seguridad. Su formulación permite abordar la problemática desde un enfoque estructurado y coherente con los objetivos de la investigación.

1. ¿Cuáles son las principales amenazas cibernéticas que enfrenta el Aeropuerto Internacional de Palmerola?
2. ¿Qué técnicas de IA y ML son más adecuadas para la detección de amenazas en entornos aeroportuarios?
3. ¿Cómo impacta la automatización basada en IA en los tiempos de respuesta ante incidentes de ciberseguridad?
4. ¿Qué beneficios y limitaciones presenta la implementación de IA y ML en la ciberseguridad aeroportuaria?

1.5 OBJETIVOS DEL PROYECTO

Los objetivos del proyecto se establecen con el fin de orientar de manera clara y estructurada el desarrollo de la investigación. Esta sección define las metas que guiarán el análisis sobre la aplicación de la Inteligencia Artificial y el Machine Learning en la ciberseguridad del Aeropuerto Internacional de Palmerola. A través de estos objetivos, se busca delimitar el alcance del estudio y asegurar que cada etapa contribuya al fortalecimiento de las soluciones tecnológicas propuestas.

1.5.1 OBJETIVO GENERAL

El objetivo general de este proyecto se centra en comprender cómo la Inteligencia Artificial y el Machine Learning pueden contribuir a fortalecer la ciberseguridad en entornos críticos. A través del estudio aplicado al Aeropuerto Internacional de Palmerola, se busca identificar métodos y enfoques tecnológicos que permitan mejorar la detección y respuesta ante amenazas. Este objetivo sirve como base para orientar el análisis y definir las estrategias que guiarán la propuesta de mejora.

1.5.2 OBJETIVOS ESPECÍFICOS

Los objetivos específicos se establecen para desglosar y abordar de manera estructurada los distintos componentes del propósito principal de la investigación. Cada uno de ellos permite profundizar en áreas clave del análisis, asegurando una comprensión integral de los procesos, herramientas y riesgos cibernéticos del entorno aeroportuario. Estos objetivos proporcionan una ruta clara para desarrollar soluciones efectivas y fundamentadas.

- Identificar las principales amenazas y vulnerabilidades cibernéticas presentes en el Aeropuerto Internacional de Palmerola.
- Evaluar técnicas y modelos de IA aplicables a la detección de amenazas cibernéticas.
- Analizar el impacto de la ML en la gestión de incidentes de ciberseguridad.

1.6 JUSTIFICACIÓN

La presente investigación se justifica desde las dimensiones académica, tecnológica, estratégica y social, debido a la creciente importancia de fortalecer la ciberseguridad en infraestructuras críticas que dependen de sistemas digitales interconectados. En la actualidad, los aeropuertos modernos operan mediante plataformas tecnológicas complejas que integran sistemas de control, comunicaciones, gestión de pasajeros, monitoreo de seguridad y servicios administrativos. Esta interdependencia tecnológica genera nuevos desafíos en materia de protección de la información, por lo

que resulta fundamental analizar el potencial de tecnologías emergentes como la Inteligencia Artificial (IA) y el Machine Learning (ML) para mejorar la seguridad informática en entornos aeroportuarios.

Desde el punto de vista académico, esta investigación contribuye al desarrollo del conocimiento científico en el campo de la ciberseguridad aplicada a infraestructuras críticas, particularmente en el contexto del sector aeronáutico. A pesar del crecimiento de los estudios sobre inteligencia artificial en seguridad informática, aún existe una limitada producción académica enfocada en su aplicación específica en aeropuertos de América Latina y, especialmente, en Honduras. En este sentido, el estudio aporta un análisis sistemático sobre las amenazas cibernéticas que enfrentan los sistemas aeroportuarios y la manera en que los modelos basados en IA y ML pueden contribuir a mejorar los mecanismos de detección, análisis y respuesta ante incidentes de seguridad. Asimismo, el trabajo puede servir como referencia para futuras investigaciones relacionadas con la integración de tecnologías inteligentes en la protección de sistemas críticos.

Desde la perspectiva práctica y tecnológica, la investigación busca proporcionar un marco de referencia para la implementación de soluciones innovadoras orientadas al fortalecimiento de la ciberseguridad en el Aeropuerto Internacional de Palmerola. El uso de algoritmos de aprendizaje automático permite analizar grandes volúmenes de datos generados por los sistemas aeroportuarios, identificar comportamientos anómalos y detectar posibles amenazas antes de que se conviertan en incidentes críticos. De esta manera, la aplicación de estas tecnologías puede contribuir a mejorar la capacidad de monitoreo, prevención y respuesta ante ataques informáticos, optimizando los procesos de gestión de seguridad y reduciendo el impacto operativo que pueden generar las ciberamenazas en las operaciones aeroportuarias.

Además, desde un enfoque estratégico, el fortalecimiento de la ciberseguridad en el sector aeroportuario es fundamental para garantizar la continuidad operativa de los servicios de transporte aéreo. Los aeropuertos constituyen nodos esenciales dentro de la infraestructura nacional e internacional de movilidad, comercio y conectividad, por lo que

cualquier interrupción en sus sistemas tecnológicos puede afectar significativamente la seguridad operacional, la logística aeroportuaria y la confianza de los usuarios. En este sentido, la incorporación de herramientas basadas en inteligencia artificial permite avanzar hacia modelos de seguridad más proactivos, capaces de anticipar riesgos y responder de manera eficiente ante amenazas emergentes.

Finalmente, desde la perspectiva social y económica, la protección de los sistemas tecnológicos aeroportuarios tiene un impacto directo en la seguridad nacional, la estabilidad del transporte aéreo y el desarrollo económico del país. Los aeropuertos representan infraestructuras críticas cuya operación segura es indispensable para el turismo, el comercio internacional y la movilidad de personas. Por lo tanto, fortalecer los mecanismos de ciberseguridad mediante el uso de tecnologías avanzadas contribuye no solo a proteger la información y los sistemas digitales, sino también a preservar la confianza de los usuarios, las aerolíneas y las instituciones que participan en el ecosistema aeroportuario. En consecuencia, esta investigación busca aportar conocimientos y propuestas que contribuyan al fortalecimiento de la seguridad digital en uno de los sectores estratégicos para el desarrollo de Honduras.

CAPÍTULO II. MARCO TEÓRICO

El marco teórico que sustenta esta investigación, proporcionando las bases conceptuales necesarias para comprender la relación entre la Inteligencia Artificial, el Machine Learning y la ciberseguridad aeroportuaria. A través de la revisión de literatura especializada, se analizan los principales enfoques, modelos y aplicaciones tecnológicas relevantes para la protección de infraestructuras críticas. Asimismo, se abordan los conceptos fundamentales de ciberseguridad, amenazas digitales y herramientas de análisis basadas en IA.

Este marco teórico permite establecer una visión integral del entorno operativo del Aeropuerto Internacional de Palmerola y de los riesgos emergentes asociados a su entorno tecnológico. Con ello, se facilita la formulación de estrategias orientadas al fortalecimiento de sus capacidades de defensa cibernética.

2.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

El análisis de la situación actual del Aeropuerto Internacional de Palmerola revela un escenario de transición tecnológica donde, a pesar de contar con una infraestructura moderna, la gestión de la ciberseguridad enfrenta desafíos estructurales importantes.

A través de la evaluación realizada al personal técnico y profesional del área de TI, se han identificado los siguientes puntos clave:

1. **Predominancia de Enfoques Reactivos:** La mayoría de los controles de seguridad implementados actualmente se basan en mecanismos tradicionales (reglas estáticas y firmas conocidas). Esto significa que el sistema es eficiente para detener amenazas ya registradas, pero presenta una vulnerabilidad crítica ante ataques de "día cero" o comportamientos anómalos que no coinciden con patrones previos.
2. **Limitaciones en la Detección Avanzada:** Una proporción significativa del personal técnico coincide en que los mecanismos actuales tienen una capacidad limitada para detectar amenazas persistentes avanzadas (APT) de manera oportuna. Esta brecha tecnológica incrementa el riesgo de incidentes que podrían comprometer la continuidad operativa del aeropuerto.

3. **Alta Dependencia de Intervención Manual:** Los procesos de gestión de incidentes carecen de una correlación inteligente de eventos de seguridad. Esto obliga a los equipos de TI a realizar análisis manuales de grandes volúmenes de datos, lo que eleva los tiempos de respuesta y aumenta la posibilidad de error humano o de omisión de alertas críticas.
4. **Bajo Nivel de Adopción de IA/ML:** Actualmente, existe un uso mínimo o nulo de herramientas basadas en Inteligencia Artificial o Machine Learning para la defensa activa. Aunque el personal reconoce el potencial de estas tecnologías para reducir falsos positivos y optimizar la gestión de eventos, su implementación operativa aún no se ha materializado en el entorno de Palmerola.
5. **Vulnerabilidades en la Gestión de Datos:** La infraestructura genera una cantidad masiva de registros (logs) provenientes de sistemas tanto informáticos (IT) como operacionales (OT). La falta de herramientas automatizadas para procesar esta información en tiempo real impide una visión holística y predictiva del estado de seguridad de la red

2.1.1. FACTOR ECONÓMICO

El entorno económico del Aeropuerto Internacional de Palmerola está intrínsecamente ligado a su capacidad de mantener operaciones ininterrumpidas, dado que cualquier ciberataque exitoso conlleva pérdidas financieras directas e indirectas de gran escala. El análisis de este factor se desglosa en los siguientes puntos:

1. **Impacto de la Continuidad del Negocio:** Palmerola es un motor económico para la región central de Honduras. Un incidente de ciberseguridad que paralice los sistemas de facturación, logística de carga o control de vuelos representaría pérdidas millonarias por hora, afectando no solo a la concesionaria, sino también a aerolíneas, empresas de transporte terrestre y el comercio internacional.

2. **Costos de Implementación vs. Mitigación:** Actualmente, la asignación presupuestaria en TI debe equilibrar el costo operativo (OPEX) y la inversión en capital (CAPEX). Si bien la implementación de tecnologías de Inteligencia Artificial y Machine Learning requiere una inversión inicial significativa en infraestructura y licencias, el costo de "no actuar" (recuperación ante ransomware, multas por incumplimiento o daños reputacionales) es exponencialmente superior.

3. **Eficiencia Operativa y Reducción de Costos**: A mediano plazo, la adopción de modelos predictivos basados en IA busca optimizar el recurso humano. Al automatizar la detección de amenazas, el aeropuerto puede reducir los costos derivados de la gestión manual de incidentes y la contratación de servicios externos de emergencia para la contención de brechas de seguridad.

4. **Sostenibilidad y Confianza del Inversionista**: La solidez económica del aeropuerto depende de su reputación. Un entorno digital seguro atrae nuevas aerolíneas y socios logísticos, mientras que la percepción de vulnerabilidad técnica puede desincentivar la inversión extranjera y reducir el flujo de pasajeros, impactando directamente en la rentabilidad del proyecto.

5. **Dependencia de Proveedores y Fluctuación de Precios:** El sector de ciberseguridad avanzada depende en gran medida de proveedores internacionales y servicios en la nube facturados en divisas extranjeras. La estabilidad económica local y el presupuesto de TI deben considerar estas fluctuaciones para garantizar la sostenibilidad de las actualizaciones y el mantenimiento de los modelos de ML.

En resumen, el factor económico actúa como un impulsor crítico para la tesis, justificando la inversión en IA no solo como una medida de protección técnica, sino como una estrategia de salvaguarda financiera para la sostenibilidad a largo plazo del aeropuerto.

2.1.2 FACTOR DEMOGRÁFICO

El análisis demográfico en el contexto de la ciberseguridad de Palmerola no se limita únicamente al número de personas que transitan por la terminal, sino a la diversidad de perfiles digitales que interactúan con sus sistemas. Los puntos clave de este factor son:

1. **Crecimiento del Flujo de Pasajeros:** Palmerola ha sido diseñado para absorber una mayor demanda de viajeros en comparación con el antiguo aeropuerto Toncontín. Este aumento demográfico implica una mayor cantidad de dispositivos

móviles (smartphones, tablets, laptops) conectándose a las redes públicas y de cortesía del aeropuerto, lo que amplía la superficie de ataque y la posibilidad de introducción de software malicioso de forma no intencionada.

2. **Diversidad de Usuarios y Alfabetización Digital:** El aeropuerto recibe una población heterogénea que incluye turistas internacionales, viajeros de negocios, personal diplomático y ciudadanos locales. La variabilidad en los niveles de conciencia sobre ciberseguridad de estos grupos representa un riesgo; por ejemplo, el uso de redes Wi-Fi abiertas para transacciones sensibles o la susceptibilidad a ataques de ingeniería social.

3. **Composición de la Fuerza Laboral**: La operatividad del aeropuerto depende de una fuerza laboral diversa, que incluye desde personal administrativo y técnico de TI hasta personal de seguridad física y mantenimiento. La demografía interna del personal requiere estrategias de capacitación diferenciadas, ya que las brechas generacionales o de formación técnica pueden influir en la adopción de nuevas políticas de seguridad digital.

4. **Densidad de Población Flotante en la Zona de Influencia:** La ubicación de Palmerola en el valle de Comayagua atrae a una población flotante y nuevos desarrollos comerciales en los alrededores. Este crecimiento demográfico local conlleva un aumento en la infraestructura de telecomunicaciones cercana, lo que puede generar interferencias o nuevos nodos de acceso que deben ser monitoreados para evitar intrusiones en el perímetro inalámbrico del aeropuerto.

5. **Perfil del Atacante Moderno:** Desde una perspectiva demográfica del cibercrimen, el aeropuerto debe considerar que los atacantes ya no son individuos aislados, sino grupos organizados con perfiles técnicos avanzados que buscan explotar infraestructuras críticas en países en desarrollo, viendo en el crecimiento demográfico y tecnológico de Palmerola una oportunidad de alto impacto.

En conclusión, el factor demográfico subraya que a mayor volumen de personas y dispositivos interactuando con la infraestructura del aeropuerto, mayor es la complejidad para gestionar la identidad y el acceso, justificando la necesidad de sistemas inteligentes que puedan diferenciar entre comportamientos de usuarios legítimos y patrones de ataque automatizados.

2.1.3 FACTOR TECNOLÓGICO

El análisis del factor tecnológico en el Aeropuerto Internacional de Palmerola (XPL) se centra en la infraestructura digital de última generación que sustenta sus operaciones, la cual, si bien ofrece eficiencia, también introduce desafíos de seguridad complejos por la interconectividad de sus componentes. Los elementos clave identificados son:

1. **Infraestructura de Red y Conectividad:** El aeropuerto cuenta con una arquitectura de red robusta que utiliza fibra óptica de alta velocidad y redundancia en sus enlaces. Sin embargo, la integración de redes Wi-Fi públicas para pasajeros y redes corporativas privadas crea puntos de contacto que deben ser monitoreados estrictamente para evitar el movimiento lateral de amenazas.

2. **Convergencia IT/OT**: Palmerola utiliza una integración profunda entre las Tecnologías de la Información (IT) y las Tecnologías Operacionales (OT). Sistemas como el manejo de equipaje (BHS), el control de iluminación de pistas y la gestión de pasarelas de abordaje están digitalizados. Esta convergencia significa que una vulnerabilidad en un sistema informático podría escalar y afectar físicamente la operación del aeropuerto.

3. **Sistemas de Vigilancia y Telemetría:** El uso de tecnologías como el ADS-B (Automatic Dependent Surveillance-Broadcast) para el rastreo de aeronaves y sistemas de CCTV basados en IP genera un flujo constante de datos críticos. La integridad de esta telemetría es vital, ya que ataques de inyección de datos o suplantación (spoofing) podrían comprometer la toma de decisiones en el control de tráfico aéreo.

4. **Dependencia de Software de Terceros**: Gran parte de la gestión aeroportuaria depende de plataformas de software especializadas provistas por terceros. Esto introduce el riesgo de ataques a la "cadena de suministro" (supply chain attacks), donde una vulnerabilidad en el software del proveedor puede convertirse en una puerta de entrada a los sistemas internos de Palmerola.

5. **Capacidad de Procesamiento y Almacenamiento (Big Data):** La infraestructura genera gigabytes de registros (logs) diariamente. Tecnológicamente, el reto no es solo almacenar esta información, sino procesarla. La ausencia de herramientas de análisis avanzado (como SIEM potenciados con IA) limita la capacidad de transformar estos datos en inteligencia accionable en tiempo real.

6. **Obsolescencia Programada y Ciclos de Actualización**: A medida que surgen nuevas vulnerabilidades, la velocidad con la que se aplican los parches de seguridad (patch management) en sistemas críticos es un factor determinante. La complejidad de algunos sistemas industriales (OT) a veces dificulta las actualizaciones frecuentes, creando ventanas de oportunidad para los atacantes.

En conclusión, el factor tecnológico en Palmerola representa una base moderna y potente, pero cuya complejidad técnica exige la transición hacia herramientas de defensa automatizadas. La implementación de Machine Learning se justifica aquí como la tecnología necesaria para supervisar un entorno tan diversificado y dinámico que ya supera las capacidades del análisis humano convencional.

2.1.4 FACTOR POLÍTICO Y LEGAL

El marco político y legal establece las reglas de cumplimiento que el Aeropuerto Internacional de Palmerola debe observar para garantizar la seguridad de la información y la operatividad legal. Este factor es determinante, ya que la ciberseguridad en el sector aeronáutico no es solo una opción técnica, sino una obligación regulatoria.

1. **Normativa de la Organización de Aviación Civil Internacional (OACI):** Como estado miembro, Honduras debe alinearse con el Anexo 17 del Convenio de Chicago y el Manual de Ciberseguridad en la Aviación (Doc 10118). Estas directrices exigen que los aeropuertos identifiquen sus sistemas críticos y protejan sus infraestructuras contra actos de interferencia ilícita perpetrados por medios cibernéticos.
2. **Ley sobre Comercio Electrónico y Firmas Electrónicas:** La legislación hondureña vigente proporciona el marco legal para la validez de las transacciones digitales y la protección de la integridad de los mensajes de datos. Palmerola, al ser un centro de intercambio comercial y logístico, debe asegurar que sus sistemas cumplan con los estándares de autenticidad y no repudio exigidos por la ley.
3. **Protección de Datos Personales y Privacidad:** El aeropuerto maneja información sensible de miles de pasajeros diariamente (datos biométricos, información de pasaportes y tarjetas de crédito). El cumplimiento de estándares internacionales de privacidad es vital para evitar sanciones legales y conflictos diplomáticos, especialmente con regiones que tienen regulaciones estrictas.
4. **Políticas de Seguridad Nacional y Protección de Infraestructuras Críticas**: El gobierno de Honduras clasifica a los aeropuertos como activos estratégicos. Por lo tanto, existen directrices políticas que obligan a las concesionarias a coordinar con los entes de seguridad del Estado (como la Agencia Hondureña de Aeronáutica Civil - AHAC) para el intercambio de inteligencia sobre amenazas y la respuesta ante incidentes nacionales.
5. **Acuerdos de Concesión y Responsabilidad Civil:** El contrato de concesión de Palmerola incluye cláusulas de responsabilidad sobre la continuidad del servicio. Un ciberataque que provoque la inoperatividad del aeropuerto podría derivar en litigios legales por incumplimiento de contrato, demandas de aerolíneas por daños y perjuicios, y revisiones por parte de los entes reguladores estatales.
6. **Estándares Internacionales (ISO/IEC 27001 y NIST):** Aunque no siempre son leyes locales, la adopción de marcos de trabajo como el de NIST para infraestructuras críticas se está convirtiendo en un estándar de facto legalmente exigible para demostrar la debida diligencia en la protección de sistemas complejos.

En conclusión, los factores políticos y legales ejercen una presión constante sobre la administración de Palmerola para que evolucione sus sistemas de defensa. La implementación de Machine Learning facilitaría el cumplimiento de estas normas al proporcionar una auditoría continua y una capacidad de detección que satisfaga las crecientes exigencias de los organismos de control internacionales.

2.2 MARCO CONCEPTUAL

El marco conceptual integra los términos y fundamentos teóricos que permiten contextualizar el objeto de estudio de esta investigación. En primer lugar, se abordan los conceptos esenciales de Inteligencia Artificial y Machine Learning, destacando su evolución, clasificación y aplicaciones orientadas a la detección de patrones, análisis predictivo y automatización de procesos. Luego, se profundiza en el concepto de ciberseguridad, abordando tanto su relevancia en entornos críticos como los principales modelos de protección adoptados globalmente.

Finalmente, se analiza el papel de estas tecnologías en la mitigación de amenazas, destacando la importancia del uso de modelos avanzados para fortalecer la infraestructura aeroportuaria y garantizar la continuidad operativa

2.2.1. MATRIZ DE PLANIFICACIÓN

A continuación, se presenta la matriz de planificación, un instrumento estratégico diseñado para estructurar de manera sistemática y cronológica las fases de ejecución de la propuesta. Esta herramienta detalla los objetivos, las actividades operativas, los plazos estimados y los recursos necesarios para su cumplimiento. En el contexto de esta investigación, la matriz pone un énfasis particular en el desarrollo de las etapas de capacitación del personal, garantizando que la transición y asimilación de las nuevas metodologías y herramientas tecnológicas se realice de forma organizada, medible y alineada con los estándares de seguridad y eficiencia requeridos.

Tabla 1 Matriz de planificación

Elemento	Descripción
Problema	Limitada capacidad de detección y respuesta ante ciber amenazas en el Aeropuerto Internacional de Palmerola mediante enfoques tradicionales de ciberseguridad.
Causa	Uso de sistemas de seguridad reactivos, ausencia de modelos predictivos y bajo aprovechamiento de IA y ML.
Efecto	Incremento del riesgo de incidentes cibernéticos, afectación a la continuidad operativa y a la seguridad de la información.
Solución	Aplicación de modelos de Inteligencia Artificial y Machine Learning para fortalecer la ciberseguridad aeroportuaria.

2.2.2 MATRIZ DE PLANIFICACIÓN DE CADENA DE VALOR

La Matriz de Planificación de Cadena de Valor constituye un análisis fundamental para identificar las actividades primarias y de apoyo que generan un valor diferenciador en la organización. El propósito de este instrumento es desglosar cada eslabón operativo para asegurar que la implementación tecnológica no solo sea funcional, sino que optimice los flujos de trabajo existentes. En este sentido, la matriz permite visualizar cómo la integración de nuevas herramientas y la especialización del talento humano mediante programas de capacitación fortalecen la infraestructura técnica y los servicios logísticos, garantizando una operación más robusta y eficiente.

Tabla 2 Matriz de cadena de valor

Proceso	Actividad	Aplicación de IA/ML	Valor Generado
Prevención	Monitoreo de red	Detección de anomalías	Reducción de ataques exitosos
Detección	Análisis de eventos	Clasificación automática de amenazas	Respuesta temprana
Respuesta	Gestión de incidentes	Automatización de alertas	Menor tiempo de recuperación
Mejora continua	Análisis histórico	Modelos predictivos	Anticipación de riesgos

2.2.3 INFRAESTRUCTURA CRÍTICA AEROPORTUARIA

Las infraestructuras críticas aeroportuarias se consideran pilares fundamentales para el funcionamiento del transporte aéreo y la conectividad internacional. Estas infraestructuras integran sistemas tecnológicos complejos, tales como redes de comunicación aeronáutica, sistemas de control del tráfico aéreo, plataformas de gestión operativa, sistemas de vigilancia, equipos de navegación y bases de datos administrativas. Debido a su interdependencia, cualquier interrupción o ataque cibernético puede generar impactos directos en la seguridad operacional, retrasos en vuelos, pérdida de información y afectación a la economía nacional.

En este contexto, la protección de los sistemas aeroportuarios adquiere un carácter estratégico, demandando mecanismos avanzados de monitoreo, detección y respuesta que permitan asegurar su resiliencia ante amenazas emergentes.

2.2.4 CIBERSEGURIDAD

En el contexto aeroportuario, la ciberseguridad adquiere un carácter especialmente estratégico debido a la interconexión de tecnologías de la información (IT) con tecnologías operacionales (OT), responsables estas últimas del funcionamiento de sistemas críticos como radares, sensores, control del tráfico aéreo, redes de comunicación aeronáutica, plataformas aeroportuarias y sistemas de verificación de pasajeros. Esta convergencia incrementa la superficie de ataque, ya que una brecha en un entorno IT puede comprometer directamente sistemas operativos esenciales para la seguridad aérea. Por ello, la protección de estas infraestructuras demanda modelos de seguridad avanzados, monitoreo continuo y respuestas automatizadas que reduzcan el riesgo de incidentes.

Asimismo, los aeropuertos enfrentan amenazas crecientes como ataques de ransomware, intrusión a sistemas de navegación, manipulación de datos de vuelo, sabotaje digital, ataques DDoS y explotación de vulnerabilidades en sistemas heredados. Estos ataques pueden generar retrasos operacionales, pérdidas económicas, afectación a la reputación institucional e incluso riesgos para la vida humana. En consecuencia, las autoridades aeroportuarias deben adoptar marcos internacionales de referencia como ISO

27001, NIST CSF, ICAO SARPs y lineamientos de ciberseguridad específicos para aviación.

Finalmente, la ciberseguridad moderna requiere un enfoque integral que combine prevención, detección temprana, análisis de comportamiento, respuesta ante incidentes y recuperación. En este proceso, tecnologías emergentes como la Inteligencia Artificial y el Machine Learning desempeñan un papel clave al permitir la automatización y el análisis avanzado de grandes volúmenes de datos, facilitando la identificación temprana de anomalías y amenazas que serían difíciles de detectar mediante métodos tradicionales

2.2.5 INTELIGENCIA ARTIFICIAL

La Inteligencia Artificial (IA) es una rama de la informática dedicada al diseño de sistemas capaces de ejecutar tareas que tradicionalmente requerirían inteligencia humana. Estas tareas incluyen el razonamiento, el aprendizaje, la percepción, la toma de decisiones, la predicción y el procesamiento del lenguaje.

La IA se divide en múltiples subdisciplinas, entre ellas los sistemas expertos, el procesamiento de lenguaje natural (NLP), la visión por computadora, los agentes inteligentes y, de manera destacada, el Machine Learning (ML) y el Deep Learning (DL). Estas tecnologías permiten que los sistemas aprendan de los datos, identifiquen patrones y mejoren su desempeño con el tiempo sin intervención humana directa.

En el campo de la ciberseguridad, la IA ha demostrado ser una herramienta de enorme valor, ya que permite automatizar la detección de amenazas, identificar comportamientos anómalos en redes, anticiparse a patrones de ataque y apoyar la respuesta inmediata ante incidentes. Mediante modelos de aprendizaje supervisado y no supervisado, la IA puede analizar millones de eventos en tiempo real, detectar desviaciones respecto a patrones normales de operación y activar alertas antes de que las vulnerabilidades sean explotadas. Este enfoque es especialmente relevante considerando que los ciberataques modernos evolucionan rápidamente y se caracterizan por su complejidad y persistencia.

En entornos aeroportuarios, la aplicación de IA se orienta a fortalecer la protección de infraestructuras críticas mediante herramientas como sistemas de detección de intrusos basados en comportamiento, algoritmos predictivos para identificar amenazas, análisis

automatizado del tráfico de red, clasificación de eventos maliciosos y detección de vulnerabilidades emergentes. Adicionalmente, la IA contribuye a mejorar la seguridad física mediante sistemas biométricos inteligentes, reconocimiento de patrones sospechosos y monitoreo avanzado en tiempo real.

Otro aspecto relevante es la capacidad de la IA para reducir la carga operativa del personal de ciberseguridad, quienes normalmente deben analizar grandes cantidades de datos y eventos. Los modelos inteligentes permiten priorizar alertas críticas, automatizar acciones correctivas y ofrecer recomendaciones precisas basadas en análisis detallados. Esto optimiza la toma de decisiones y fortalece la resiliencia del aeropuerto frente a incidentes cibernéticos.

En conjunto, la Inteligencia Artificial se convierte en un componente esencial para la ciberseguridad moderna, especialmente en infraestructuras con altos requerimientos de continuidad operativa, como los aeropuertos. Su integración permite evolucionar de un enfoque reactivo a uno proactivo, capaz de anticipar riesgos y neutralizar amenazas antes de que generen impactos significativos.

2.2.6 MACHINE LEARNING

El Machine Learning (ML) es una subdisciplina de la Inteligencia Artificial que se centra en el desarrollo de algoritmos capaces de aprender patrones a partir de datos y mejorar su rendimiento de forma progresiva sin necesidad de programación explícita. Su funcionamiento se basa en modelos matemáticos y estadísticos que permiten identificar relaciones, tendencias y anomalías dentro de grandes volúmenes de información.

Entre las técnicas más utilizadas se encuentran el aprendizaje supervisado, no supervisado y el aprendizaje por refuerzo, cada una con aplicaciones específicas en procesos de clasificación, detección, predicción y toma de decisiones automatizada.

En el ámbito de la ciberseguridad, el ML se ha consolidado como uno de los pilares tecnológicos más importantes para fortalecer las defensas de infraestructuras críticas. Su capacidad de analizar millones de eventos en tiempo real permite detectar patrones maliciosos, identificar comportamientos anómalos y anticipar ataques antes de que se materialicen. Los modelos supervisados se aplican para clasificar tráfico de red, identificar malware o determinar si un evento es benigno o malicioso; mientras que los

modelos no supervisados destacan en la detección de anomalías y en la identificación de comportamientos inusuales que podrían corresponder a amenazas desconocidas (zero-day).

En entornos aeroportuarios, el ML resulta especialmente valioso debido a la complejidad y dinamismo de sus sistemas. Los aeropuertos operan con grandes volúmenes de datos provenientes de sensores, cámaras, sistemas operacionales (OT) y plataformas informáticas (IT). El uso adecuado de ML permite automatizar el monitoreo continuo, priorizar alertas críticas, identificar vulnerabilidades emergentes y optimizar la respuesta ante incidentes. Además, se integra en sistemas biométricos, controles de acceso inteligente, análisis de tráfico aéreo y plataformas de gestión operativa, garantizando mayor seguridad y eficiencia. En conjunto, el Machine Learning se posiciona como una herramienta esencial para la ciberseguridad moderna y la resiliencia de infraestructuras aeroportuarias.

2.3 MARCO TEÓRICO

Esta sección integra conocimientos provenientes de diversas áreas, tales como la informática, la gestión de riesgos, la ciberseguridad crítica y los sistemas de control industrial. A través del análisis de literatura actualizada y normativas internacionales, se exploran los conceptos esenciales que permiten contextualizar las amenazas digitales, los modelos de protección y las tecnologías emergentes aplicadas a infraestructuras aeroportuarias.

El propósito de este capítulo es ofrecer una visión integral que permita identificar los desafíos contemporáneos en materia de seguridad digital y las oportunidades que ofrecen los sistemas inteligentes para fortalecer la resiliencia operativa del Aeropuerto Internacional de Palmerola**.**

2.3.1 CIBERAMENAZAS EN ENTORNOS AEROPORTUARIOS

Los aeropuertos representan infraestructuras críticas con un alto grado de interconectividad y dependencia tecnológica, lo que los convierte en objetivos atractivos para actores maliciosos. En estos entornos convergen sistemas de tecnologías de la

información (IT) y tecnologías operacionales (OT), generando una superficie de ataque amplia y compleja.

Dentro de las principales ciberamenazas se encuentran el malware, el ransomware, los ataques de denegación de servicio distribuido (DDoS), las intrusiones a redes internas, la explotación de vulnerabilidades en sistemas de control industrial y las amenazas internas, tanto accidentales como intencionales.

El malware engloba programas diseñados para infiltrarse en sistemas con el propósito de robar información, alterar procesos o comprometer la integridad de plataformas críticas. En aeropuertos, este tipo de amenaza puede afectar desde sistemas de facturación y equipaje hasta servidores administrativos y plataformas de comunicación. Por otro lado, el ransomware ha incrementado su impacto en el sector del transporte al encriptar información esencial y exigir pagos para su recuperación, pudiendo paralizar operaciones, retrasar vuelos y comprometer la continuidad del servicio aeroportuario.

Los ataques DDoS buscan saturar servicios esenciales mediante el envío masivo de solicitudes, afectando plataformas como portales de información, servicios de monitoreo, sistemas de reserva o bases de datos relacionados con operaciones aéreas. De igual manera, las intrusiones en redes internas permiten a los atacantes obtener acceso a sistemas administrativos o incluso comprometer plataformas OT vinculadas con radares, sensores, sistemas SCADA, señalización o control de tráfico aéreo. La explotación de vulnerabilidades en sistemas OT representa una amenaza grave, ya que estos equipos suelen operar con sistemas legados, protocolos inseguros o arquitecturas poco actualizadas.

Asimismo, las amenazas internas representan un riesgo significativo. Estas pueden originarse por errores de configuración, descuidos del personal, falta de capacitación, uso indebido de credenciales o incluso acciones malintencionadas de empleados con acceso autorizado. En aeropuertos, donde gran parte de los sistemas dependen de la precisión y estabilidad, cualquier alteración puede tener consecuencias operativas, económicas y de seguridad nacional.

Finalmente, la creciente sofisticación de los ataques, la disponibilidad de herramientas maliciosas en la “dark web” y la presencia de actores avanzados (APT) incrementan la necesidad de adoptar mecanismos de protección proactivos. Esta situación exige la

incorporación de soluciones basadas en IA y ML que permitan detectar anomalías, anticipar riesgos y responder de forma inmediata a eventos potencialmente peligrosos en la infraestructura aeroportuaria

2.3.2 LIMITACIONES DE LOS ENFOQUES TRADICIONALES DE CIBERSEGURIDAD

Los enfoques tradicionales de ciberseguridad se fundamentan en mecanismos reactivos, reglas estáticas, firmas conocidas y modelos de protección perimetral. Este tipo de soluciones funcionan de manera eficaz ante amenazas previamente catalogadas, patrones identificables y malware de firmas reconocibles. Sin embargo, su capacidad es limitada cuando enfrentan amenazas modernas caracterizadas por su sofisticación, autonomía y capacidad de adaptación.

Una de las principales limitaciones de los modelos tradicionales es su incapacidad para detectar ataques de día cero, cuyo comportamiento no existe en bases de datos de firmas, lo que los hace invisibles para los antivirus y firewalls convencionales. Asimismo, presentan dificultades para lidiar con ataques avanzados persistentes (APT), ejecutados por actores con altos recursos técnicos que operan con tácticas de infiltración silenciosa y de larga duración. Estos ataques suelen evadir la detección al camuflarse entre tráfico legítimo o mediante el uso de técnicas de living-off-the-land, que aprovechan herramientas internas del sistema.

Otro aspecto crítico es la limitada capacidad de estos enfoques para analizar comportamientos anómalos complejos. Los modelos basados en reglas se ven rebasados por patrones dinámicos de ataque, especialmente en entornos altamente interconectados como aeropuertos, donde convergen sistemas IT, OT, IoT, sensores biométricos, plataformas de control aéreo y sistemas de operación logística. La volumetría del tráfico y la diversidad de dispositivos generan un entorno demasiado complejo para ser gestionado únicamente con mecanismos tradicionales.

A esto se suma la dependencia de la intervención humana, lo que implica que la detección, análisis y respuesta ante incidentes pueden resultar lentos e ineficientes. Este retraso incrementa la ventana de exposición, permitiendo que un atacante avance en fases críticas como movimiento lateral, escalación de privilegios o manipulación del sistema.

En infraestructuras críticas, donde la continuidad operativa es esencial, estos retrasos pueden traducirse en interrupciones, pérdidas económicas y riesgos para la seguridad nacional.

Finalmente, la falta de capacidades predictivas representa una limitación fundamental. Los enfoques clásicos actúan tras la detección de un incidente, en lugar de anticipar comportamientos sospechosos. En un entorno de ciberamenazas en constante evolución, donde los atacantes utilizan técnicas como inteligencia artificial, automatización y ataques coordinados, los sistemas tradicionales carecen de la flexibilidad y adaptabilidad necesarias para ofrecer un nivel de protección acorde a los riesgos actuales

2.3.4 APLICACIÓN DE IA Y ML EN CIBERSEGURIDAD

La aplicación de Inteligencia Artificial (IA) y Machine Learning (ML) en ciberseguridad representa un avance significativo hacia modelos de defensa inteligentes, proactivos y altamente adaptativos. A diferencia de los enfoques tradicionales, basados en reglas estáticas y reacciones tardías, estas tecnologías permiten anticiparse a las amenazas, identificar comportamientos anómalos en tiempo real y automatizar la respuesta ante incidentes. Su capacidad para procesar grandes volúmenes de datos, aprender patrones complejos y evolucionar junto con el entorno digital, las convierte en herramientas indispensables en infraestructuras críticas como los aeropuertos.

Una de las principales contribuciones del ML es la detección de anomalías. Los algoritmos aprenden el comportamiento normal de la red, los sistemas y los usuarios, permitiendo identificar desviaciones que podrían estar asociadas a intrusiones, accesos no autorizados, movimientos laterales o intentos de explotación.

Esta característica es esencial en entornos aeroportuarios donde la variedad de dispositivos y sistemas interconectados hace difícil detectar ataques mediante métodos tradicionales. Además, los modelos pueden adaptarse a nuevas condiciones, reduciendo la probabilidad de falsos positivos y mejorando la precisión en la detección de amenazas emergentes.

2.3.5 TÉCNICAS DE MACHINE LEARNING APLICADAS A LA DETECCIÓN DE AMENAZAS

En el contexto del Aeropuerto Internacional de Palmerola, la aplicación de técnicas de Machine Learning (ML) para la detección de amenazas adquiere especial relevancia debido a la naturaleza híbrida de su infraestructura tecnológica, que integra sistemas de Tecnologías de la Información (IT) y Tecnologías Operacionales (OT).

Dada la importancia estratégica del aeropuerto como punto clave de conectividad y logística en la región centroamericana, los riesgos asociados a ciberamenazas requieren mecanismos de protección avanzados capaces de identificar intrusiones, comportamientos anómalos y ataques dirigidos con alta precisión y en tiempo real.

Entre las principales técnicas de ML aplicadas en este tipo de infraestructuras se encuentran los modelos de aprendizaje supervisado, no supervisado y semi supervisado, cada uno con capacidades específicas para detectar patrones maliciosos. En el aprendizaje supervisado, algoritmos como Support Vector Machines (SVM), árboles de decisión, bosques aleatorios (Random Forest) y redes neuronales multicapa se entrenan con ejemplos etiquetados de comportamientos normales y maliciosos, permitiendo clasificar eventos de seguridad dentro de los sistemas IT del aeropuerto, tales como accesos indebidos, intentos de explotación, escaneo de puertos o tráfico sospechoso dentro de las redes internas.

Por otro lado, el aprendizaje no supervisado resulta especialmente útil en entornos como Palmerola, donde la diversidad de dispositivos conectados dificulta la disponibilidad de datos etiquetados. Técnicas como k-means clustering, DBSCAN y los modelos de detección de anomalías basados en densidad permiten identificar patrones irregulares en el comportamiento de sensores, radares, sistemas CCTV, equipos SCADA y plataformas de navegación aérea. Estas herramientas pueden detectar cambios sutiles pero significativos que podrían indicar infiltraciones, manipulación de señales o intentos de compromiso en sistemas OT, donde un ataque puede afectar directamente la seguridad operacional.

Asimismo, los autoencoders y las redes neuronales recurrentes (RNN), especialmente aquellas basadas en Long Short-Term Memory (LSTM), son empleadas para la detección de anomalías en datos generados de forma secuencial, como registros

de tráfico, telemetría de radares, reportes de comunicación, patrones de movimiento de aeronaves y secuencias de comandos en sistemas industriales.

Estas técnicas permiten identificar comportamientos anormales en tiempo real y anticiparse a posibles sabotajes, intrusiones o interrupciones en sistemas críticos del aeropuerto.

En infraestructuras complejas como Palmerola, donde la continuidad operacional es prioritaria, los modelos de series temporales y predicción de comportamiento facilitan la identificación de tendencias que podrían derivar en fallos o ataques. Por ejemplo, un incremento inusual en la latencia de la red, variaciones anómalas en el tráfico de datos, actividad irregular en controladores lógicos programables (PLC) o patrones extraños en el acceso a sistemas internos pueden ser detectados antes de que se produzca un impacto operativo.

La integración de estas técnicas en plataformas de monitoreo del aeropuerto permite desarrollar sistemas de detección temprana, capaces de correlacionar información entre múltiples dominios: seguridad física, sistemas biométricos, cámaras inteligentes, bases de datos de pasajeros, servidores administrativos, sistemas SCADA y plataformas aeronáuticas. Con esta correlación inteligente, el aeropuerto puede fortalecer su postura de ciberseguridad, reducir el riesgo de ataques avanzados persistentes (APT) y detectar amenazas que los métodos tradicionales no logran identificar.

Finalmente, el uso de Machine Learning en Palmerola no solo mejora la detección de amenazas, sino que también facilita la implementación de respuestas automatizadas a través de sistemas SOAR, reduce la carga de trabajo del personal de TI y OT, mejora los tiempos de respuesta y contribuye a la resiliencia de la infraestructura aeroportuaria frente a las ciberamenazas actuales y emergentes

2.4 MARCO NORMATIVO Y DE REFERENCIA

El marco normativo y de referencia constituye un elemento fundamental para comprender las obligaciones, estándares y lineamientos que regulan la ciberseguridad en infraestructuras críticas como los aeropuertos. Esta sección presenta las disposiciones

internacionales, regionales y nacionales que orientan la gestión del riesgo cibernético, la protección de sistemas IT y OT, y el cumplimiento de buenas prácticas en seguridad digital. Asimismo, se incluyen los marcos de referencia técnicos adoptados por organismos especializados en aviación, tecnología y seguridad operacional, cuya aplicación resulta esencial para garantizar la integridad, disponibilidad y resiliencia de los sistemas del Aeropuerto Internacional de Palmerola.

2.4.1 NORMATIVAS INTERNACIONALES

La protección de infraestructuras aeroportuarias está respaldada por normativas y lineamientos internacionales emitidos por organismos como la Organización de Aviación Civil Internacional (OACI) y la Asociación Internacional de Transporte Aéreo (IATA), los cuales promueven la gestión integral de la ciberseguridad y la adopción de buenas prácticas basadas en estándares internacionales.

2.4.2 ESTÁNDARES DE CIBERSEGURIDAD

Estándares como ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework e ISO/IEC 22301 proporcionan marcos de referencia para la gestión de la seguridad de la información y la continuidad operativa. Estos estándares pueden complementarse con soluciones basadas en IA y ML para fortalecer los controles de seguridad.

2.4.3 CONTEXTO NORMATIVO NACIONAL

En el contexto hondureño, la protección de infraestructuras críticas y la seguridad de la información se enmarcan en políticas nacionales de seguridad y normativas relacionadas con la gestión de tecnologías de la información. No obstante, aún existe la necesidad de fortalecer la adopción de tecnologías avanzadas orientadas a la ciberseguridad predictiva.

2.5 RELACIÓN DEL MARCO TEÓRICO CON LA INVESTIGACIÓN

El marco teórico desarrollado en este estudio constituye la base fundamental que sustenta y orienta la investigación, ya que integra los conceptos, modelos, enfoques y normativas necesarias para comprender la aplicación de la Inteligencia Artificial (IA) y el Machine Learning (ML) en los procesos de ciberseguridad del Aeropuerto Internacional de Palmerola. Este marco permite contextualizar el problema investigado, delimitando los elementos conceptuales del ámbito de la ciberseguridad, las características de las infraestructuras críticas aeroportuarias y los avances tecnológicos que influyen directamente en la protección de los sistemas IT y OT.

Asimismo, la revisión del marco conceptual proporciona definiciones precisas sobre IA, ML, ciberseguridad, ciberamenazas, infraestructura crítica y tecnologías operacionales, lo que facilita la construcción de una base terminológica coherente y alineada con los estándares internacionales. Dicho marco conceptual permite comprender cómo estas tecnologías emergentes pueden fortalecer los mecanismos de defensa ante ataques avanzados, mejorar la detección de anomalías y reducir los riesgos que afectan la continuidad operativa del aeropuerto.

Por otro lado, el marco teórico ofrece una comprensión amplia de los enfoques tradicionales y modernos de ciberseguridad, destacando sus limitaciones y las oportunidades de mejora mediante técnicas basadas en IA y ML. La integración de conceptos sobre aprendizaje supervisado, no supervisado, análisis de comportamiento, modelos de predicción y arquitecturas de detección inteligente, permite fundamentar la pertinencia de las soluciones tecnológicas propuestas en la investigación. La revisión de estos modelos respalda la posibilidad de construir sistemas de monitoreo más eficientes, precisos y adaptativos, capaces de anticipar amenazas en tiempo real.

Finalmente, el marco normativo analizado proporciona un respaldo formal y metodológico que valida las propuestas de la investigación, al utilizar estándares como ISO/IEC 27001, NIST CSF, IEC 62443 e ICAO, los cuales orientan el diseño, la gestión y la protección de infraestructuras críticas.

2.5.1 CUADRO COMPARATIVO DE MARCOS NORMATIVOS Y DE REFERENCIA EN CIBERSEGURIDAD AEROPORTUARIA

La gestión de la ciberseguridad en infraestructuras críticas requiere un entendimiento profundo de los marcos de referencia que dictan las políticas de mitigación de riesgos. El presente apartado expone una comparativa detallada entre los diferentes esquemas regulatorios y estándares voluntarios que rigen el sector aeroportuario. En esta matriz se evalúan aspectos clave como el control de acceso, la respuesta a incidentes y la formación del personal técnico.

Dicha comparación resulta esencial para determinar las brechas normativas y operativas, proporcionando el sustento jurídico y técnico necesario para la adopción de modelos de aprendizaje automático (Machine Learning) orientados a robustecer la resiliencia del sistema ante ciberataques.

Tabla 3 Marcos comparativos Enfocado a aeropuertos con entornos IT/OT y operación crítica.

Norma/Marco	Alcance principal	Enfoque	Fortalezas	Limitaciones	Componentes clave
ISO/IEC 27001:2022 (	Sistemas de gestión de seguridad de la información (IT)	Gestión de riesgos y controles	Certificable; enfoque a procesos; mejora continua (PDCA)	No cubre en detalle OT/SCADA	Contexto, liderazgo, evaluación de riesgos, Annex A (114 controles 27002:2022)
ISO/IEC 27002:2022	Catálogo de controles	Controles y buenas prácticas	Controles modernizados (atributos, seguridad en la nube, monitoreo)	No es certificable por sí sola	4 temas: Organizativos, Personas, Físicos, Tecnológicos
NIST CSF 2.0	Marco de ciberseguridad	Funciones: Identificar, Proteger,	Flexible, madurez por	No certificable	Categorías, subcategorías, perfiles de

Norma/Marco	Alcance principal	Enfoque	Fortalezas	Limitaciones	Componentes clave
	para infraes–tructura crítica	Detectar, Responder, Recuperar, Gobernar	perfiles, integra IT/OT	; requiere adaptación	implementación
NIST SP 800-53 Rev. 5	Controles de seguridad y privacidad	Catálogo exhaustivo de controles	Muy completo; mapeable a ISO/NIST CSF	Alto esfuerzo para aterrizar	Familias: AC, AU, CM, IR, RA, SC, SI, etc.
IEC 62443 (Serie)	Seguridad en sistemas de automatización y control industrial (OT)	Seguridad por niveles y zonas/conductos	Específico para OT/SCADA; defensa en profundidad	Requiere inventario OT y segmentación previa	62443-2-1 (gestión), 3-3 (requisitos técnicos), 4-1/4-2 (ciclo de vida/ componentes)
ICAO (An	Sector aviación civil	Seguridad operacional y ciberseguridad en aviación	Alineado a autoridades aeronáuticas; interoperabilidad	No técnico a nivel de control granular	Estrategias de ciberseguridad, gestión de riesgos, coordinación Estado–operadores
EASA (GM/AMC	Aviación en Europa (referencia técnica)	Requisitos de gestión de información y ciber	Buenas prácticas específicas para operadores	En LATAM aplica como referencia	Requisitos de gobernanza, reporte, coordinación

Norma/Marco	Alcance principal	Enfoque	Fortalezas	Limitaciones	Componentes clave
TSA Security Directives (US)**	Transporte/aviación	Directivas de ciber obligatorias (US)	Óptimo como benchmark de mínimos	No aplican legalmente fuera de US	Controles mínimos, tiempos de reporte, pruebas
ISO 22301	Continuidad del negocio	Resiliencia y continuidad	Integra BIA, planes y pruebas		

2.6 MAPEO DE REFERENCIA

El mapeo de referencia constituye un ejercicio de síntesis y vinculación lógica entre los fundamentos teóricos, los estándares técnicos y los componentes operativos de la presente investigación. Este apartado tiene como propósito estructurar de manera visual y organizada las fuentes de autoridad y los marcos de trabajo que guían el desarrollo de la solución tecnológica propuesta.

A través de este mapeo, se asegura que cada fase de la planificación desde la capacitación del personal hasta la implementación de algoritmos de seguridad cuente con un respaldo normativo y bibliográfico sólido, garantizando así la coherencia interna y la validez técnica de los resultados obtenidos.

Tabla 4 Riesgos y controles

Dominio Palmerola	Riesgo principal	Marco(s) recomendado(s)	Controles/Prácticas clave
Red corporativa (IT)	Ransomware, exfiltración	ISO 27001, NIST CSF, 800-53	Gestión de vulnerabilidades, EDR, MFA, hardening, DLP, SIEM

Dominio Palmerola	Riesgo principal	Marco(s) recomendado(s)	Controles/Prácticas clave
Sistemas OT/SCADA (pasare	Interrupción operativa	IEC 62443, NIST CSF	Zonas y conductos, whitelisting, monitoreo OT, puertos/ protocolos industriales seguros
Tráfico aéreo y comunicaciones (	Disponibilidad/ integridad	ICAO/EASA + ISO 22301	Segmentación, redundancia, monitoreo, pruebas de continuidad
CCTV y biometría	Privacidad, acceso	ISO 27001/27018, NIST 800-53 (AC/IA/AU)	Cifrado en tránsito/ reposo, control de acceso, retención, auditoría
Plataformas públicas (web, Wi-	DDoS, fraude	NIST CSF, 800-53, ISO 27002	WAF, anti-DDoS, aislamiento, portal cautivo seguro
Terceros/contratistas	Cadena de suministro	ISO 27036, NIST CSF	Evaluación de proveedores, cláusulas de seguridad, monitoreo continuo

CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACIÓN

El presente capítulo describe el marco metodológico que orienta el proceso de desarrollo de esta investigación, definiendo el enfoque, los métodos y las técnicas empleadas para alcanzar los objetivos planteados. La metodología seleccionada permite analizar de manera rigurosa la aplicación de la Inteligencia Artificial y el Machine Learning en la ciberseguridad del Aeropuerto Internacional de Palmerola, garantizando la validez y coherencia del estudio. Asimismo, se detallan los procedimientos utilizados para la recolección, procesamiento y análisis de la información, así como los criterios que sustentan la elección del diseño de investigación. Este marco metodológico proporciona la estructura necesaria para asegurar que los resultados obtenidos sean fiables, pertinentes y alineados con el problema de investigación.

3.1 ENFOQUE DE LA INVESTIGACIÓN

La presente investigación adopta un enfoque mixto, combinando elementos del enfoque cualitativo y cuantitativo. El componente cualitativo permite analizar documentación técnica, normativa y literatura científica relacionada con la ciberseguridad, IA y ML, interpretando conceptos, modelos y marcos de referencia aplicados a infraestructuras críticas.

3.2 TIPO DE INVESTIGACIÓN

Este estudio se clasifica como investigación aplicada, ya que busca generar conocimiento orientado a resolver un problema real dentro del contexto operativo del aeropuerto. Asimismo, posee un carácter descriptivo y explicativo: descriptivo porque identifica amenazas, vulnerabilidades, normas y técnicas relacionadas con la ciberseguridad; explicativo porque analiza cómo el uso de IA y ML puede mejorar la detección de amenazas en infraestructuras críticas. También incluye elementos documentales al basarse en fuentes bibliográficas, técnicas y normativas para sustentar las propuestas.

3.3 CONGRUENCIA METODOLÓGICA

Esta herramienta permite verificar que la implementación de modelos de Inteligencia Artificial y Machine Learning, así como los planes de capacitación técnica propuestos, cuenten con un sustento teórico robusto y una técnica de recolección de datos adecuada. Al articular las variables críticas con sus respectivos indicadores e instrumentos de medición, se asegura que los resultados obtenidos posean el rigor, la validez y la confiabilidad necesarios para ser aplicados con éxito en la protección de infraestructuras críticas aeroportuarias.

Tabla 5 Matriz de congruencia metodológica

Título	**USO DE INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING EN CIBER AMENAZAS DE LOS SISTEMAS DEL AEROPUERTO INTERNACIONAL DE PALMEROLA**
Problema	¿De qué manera la configuración actual de los controles de acceso, respaldos y cultura de ciberseguridad mitiga las amenazas sistemáticas en la infraestructura operativa de Palmerola?
Objetivo General	Evaluar el estado de seguridad de los sistemas del Aeropuerto Internacional de Palmerola mediante el análisis de riesgos tecnológicos y la percepción de madurez institucional.
Preguntas de Investigación	1. ¿Cuál es la eficacia percibida de las políticas formales y controles de acceso en los sistemas aeroportuarios? 2. ¿Cómo influye la inversión y la cultura de ciberseguridad en la continuidad de la misión institucional?
Objetivos Específicos	1. Diagnosticar la robustez de los sistemas críticos mediante la evaluación de respaldos y gestión de incidentes 2. Determinar el nivel de preparación institucional ante la adopción de nuevas tecnologías y recursos financieros

Título	USO DE INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING EN CIBER AMENAZAS DE LOS SISTEMAS DEL AEROPUERTO INTERNACIONAL DE PALMEROLA
Variable Independiente	**Gestión de Ciberseguridad:** (Políticas, Controles de Acceso, Capacitación, Inversión).
Variable Dependiente	**Vulnerabilidad Operativa / Continuidad del Negocio:** (Reducción de riesgos operativos, Confianza Institucional, Misión del Aeropuerto).

3.4 MATRIZ DE OPERACIONALIZACIÓN

A continuación, se presenta la matriz detallada que desglosa cada variable en sus respectivas dimensiones (teórica, práctica y conductual), identificando los indicadores que servirán de base para la construcción del instrumento de recolección de datos. Este esquema garantiza la validez de contenido de la investigación

Tabla 6 Tabla 6 Matriz de operacionalización

Variable	Definición Conceptual	Dimensiones	Indicadores	Ítems (Preguntas)	Escala / Respuestas
Independiente: Gestión de la Ciberseguridad y Riesgos	Conjunto de estrategias, políticas y controles	**Técnica y Operativa**	Políticas formales Control de accesos	¿En qué medida estás de acuerdo o en desacuerdo con las siguientes afirmaciones sobre Seguridad de la Información?	(1)en desacuerdo (2) En desacuerdo (3) Ni en acuerdo ni desacuerdo

Variable	Definición Conceptual	Dimensiones	Indicadores	Ítems (Preguntas)	Escala / Respuestas
	técnicos destinados a proteger la infraestructura crítica de información aeroportuaria.		Gestión de respaldos	¿En qué medida estás de acuerdo o en desacuerdo con las siguientes afirmaciones sobre Gestión de Riesgos Tecnológicos? Expresa tus comentarios sobre la Preparación Tecnológica dentro de la organización.	(4) De acuerdo (5) Muy de acuerdo
		Organizacional	Cultura de seguridad Gestión de incidentes Capacitación técnica	La institución esta preparada para adoptar nuevas tecnologías Existen recursos financieros para ciberseguridad La ciberseguridad es prioritaria para la institución.	1)en desacuerdo (2) En desacuerdo (3) Ni en acuerdo ni desacuerdo (4) De acuerdo (5) Muy de acuerdo
		Estratégica	Prioridad institucional	La institución promueve una cultura de ciberseguridad	1)en desacuerdo (2) En desacuerdo (3) Ni en acuerdo ni desacuerdo

Variable	Definición Conceptual	Dimensiones	Indicadores	Ítems (Preguntas)	Escala / Respuestas
			Recursos financieros Evaluación de herramientas	Se evalúan herramientas antes de implementarlas Existen recursos financieros para ciberseguridad. .	(4) De acuerdo (5) Muy de acuerdo
Dependiente: Continuidad Institucional y Resiliencia	Capacidad del aeropuerto para mantener sus operaciones críticas y la confianza de los usuarios mediante la reducción de riesgos operativos.	**Eficiencia Operativa**	Reducción de riesgos Optimización de procesos	La mejora tecnológica reduce riesgos operativos.	1)en desacuerdo (2) En desacuerdo (3) Ni en acuerdo ni desacuerdo (4) De acuerdo (5) Muy de acuerdo

Variable	Definición Conceptual	Dimensiones	Indicadores	Ítems (Preguntas)	Escala / Respuestas
		Misión y Confianza	Confianza institucional Cumplimiento de misión	La inversión en ciberseguridad aumenta la confianza institucional. La ciberseguridad contribuye a la misión institucional.	1)en desacuerdo (2) En desacuerdo (3) Ni en acuerdo ni desacuerdo (4) De acuerdo (5) Muy de acuerdo

3.5 HIPÓTESIS DE INVESTIGACIÓN

En virtud del alcance correlacional-descriptivo del estudio y la naturaleza de las variables analizadas en el Aeropuerto Internacional de Palmerola, se plantean las siguientes conjeturas estadísticas:

- H1: Existe una relación positiva y significativa entre el nivel de madurez de la gestión de ciberseguridad y la mitigación de riesgos operativos en los sistemas del Aeropuerto Internacional de Palmerola.
- H0: No existe una relación significativa entre la gestión de ciberseguridad y la mitigación de riesgos operativos en la infraestructura aeroportuaria.

3.6 DISEÑO DE LA INVESTIGACIÓN

El diseño empleado es **experimental y transeccional**, ya que no se manipulan variables directamente y el análisis se realiza en un momento determinado. Se examinan documentos, sistemas y marcos de referencia tal como existen actualmente en el Aeropuerto Internacional de Palmerola. El estudio también incorpora un diseño **analítico**, mediante el cual se relacionan las técnicas de IA/ML con las necesidades específicas de ciberseguridad del aeropuerto, permitiendo identificar brechas, oportunidades y puntos de mejora.

3.7 POBLACIÓN Y MUESTRA

La presente sección describe la población y la muestra consideradas en esta investigación, con el propósito de delimitar claramente el ámbito de estudio y los elementos que serán analizados. Dado que la investigación se orienta al análisis de la aplicación de IA y Machine Learning en la ciberseguridad del Aeropuerto Internacional de Palmerola, la población se define en función de los sistemas tecnológicos, procesos operativos y componentes críticos del entorno aeroportuario que pueden verse afectados por amenazas cibernéticas.

3.7.1 POBLACIÓN

La población objeto de estudio está conformada por el personal vinculado a la gestión y operación de los sistemas de Tecnologías de la Información (IT) y de ciberseguridad dentro del Aeropuerto Internacional de Palmerola. Este grupo incluye a profesionales responsables del mantenimiento de infraestructuras tecnológicas, administración de redes, soporte técnico, monitoreo de sistemas, gestión de incidentes, y supervisión de plataformas críticas. La población se centra en quienes poseen conocimiento directo del estado actual de los sistemas, los riesgos existentes y los mecanismos de seguridad implementados, constituyendo así la base ideal para analizar la viabilidad del uso de IA y ML en la detección de amenazas.

3.7.2 MUESTRA

La muestra seleccionada para esta investigación estuvo conformada por treina y dos (32) personas pertenecientes al Departamento de Tecnologías de la Información del Aeropuerto Internacional de Palmerola. Este grupo representa adecuadamente a los profesionales que desempeñan funciones críticas relacionadas con la administración de sistemas, seguridad informática, infraestructura técnica y soporte operativo. La elección de esta muestra fue de tipo intencional o no probabilística, debido a que se seleccionaron específicamente aquellos colaboradores que poseen conocimientos técnicos y experiencia directa en las áreas relacionadas con la ciberseguridad y el funcionamiento de los sistemas IT/OT del aeropuerto.

La participación de este grupo permite obtener información detallada, relevante y ajustada al contexto real, facilitando un análisis riguroso sobre la pertinencia y efectividad de implementar técnicas de IA y ML en la detección y mitigación de ciber amenazas dentro de la infraestructura aeroportuaria

3.8 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

La presente sección tiene como propósito describir las técnicas y los instrumentos utilizados para obtener la información necesaria en el desarrollo de esta investigación. Dado que el estudio analiza la aplicación de IA y Machine Learning en la ciberseguridad del Aeropuerto Internacional de Palmerola, la recolección de datos se basó en métodos que permitieron obtener información precisa, pertinente y directamente vinculada con los sistemas y procesos del área tecnológica. Estas técnicas permitieron recopilar evidencia documental, percepciones del personal especializado y elementos técnicos esenciales para comprender el estado actual de la seguridad informática y las oportunidades de mejora mediante tecnologías inteligentes. A continuación, se detallan las técnicas empleadas y los instrumentos utilizados para llevar a cabo este proceso.

3.8.1 TÉCNICAS DE RECOLECCIÓN DE DATOS

Las técnicas utilizadas en la presente investigación son:

- **Encuesta estructurada**
- **Escala de Likert**

Estas técnicas permiten recopilar información cuantificable sobre el estado actual de la ciberseguridad, el nivel de adopción tecnológica y la percepción del impacto de la IA y el ML en los procesos de seguridad.

3.8.2 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

La selección de los instrumentos se realizó considerando el enfoque metodológico de la investigación, así como la naturaleza de las variables relacionadas con la ciberseguridad, la gestión de riesgos y el uso de tecnologías basadas en inteligencia artificial y machine learning. En este sentido, se busca garantizar que la información obtenida sea pertinente para identificar patrones de amenazas, evaluar los mecanismos de protección actuales y analizar la capacidad de respuesta ante incidentes cibernéticos.

a) Cuestionario estructurado

Se diseñó un cuestionario dirigido al personal de TI y ciberseguridad del Aeropuerto Internacional de Palmerola, compuesto por preguntas cerradas y afirmaciones evaluadas mediante escala de Likert de cinco niveles (1 = Totalmente en desacuerdo, 5 = Totalmente de acuerdo).

El cuestionario se estructura en las siguientes dimensiones:

- Datos generales del encuestado
- Nivel de ciberseguridad actual
- Gestión de incidentes de seguridad
- Uso de tecnologías emergentes
- Percepción sobre IA y ML en ciberseguridad

b) Escala de Likert

La escala de Likert se utiliza para medir el grado de acuerdo de los participantes respecto a afirmaciones relacionadas con:

- Capacidad de detección de amenazas
- Tiempo de respuesta ante incidentes
- Automatización de procesos de seguridad
- Predicción y prevención de ataques

Ejemplos de ítems:

- "Los mecanismos actuales de ciberseguridad permiten detectar amenazas avanzadas de manera oportuna."
- "La aplicación de IA y ML mejoraría significativamente la detección de comportamientos anómalos en la red."
- "La automatización basada en IA reduciría los tiempos de respuesta ante incidentes de seguridad."

3.9 ANÁLISIS DOCUMENTAL

El análisis documental constituye una de las técnicas fundamentales empleadas en esta investigación, ya que permite examinar de manera sistemática diversos documentos técnicos, normativos y académicos relacionados con la ciberseguridad, la Inteligencia Artificial, el Machine Learning y las infraestructuras aeroportuarias. Este proceso incluye la revisión de estándares internacionales como ISO/IEC 27001, NIST CSF, IEC 62443 e ICA, así como guías, informes especializados, artículos científicos, estudios de caso y reportes de incidentes de seguridad publicados por organismos aeronáuticos, instituciones de ciberseguridad y centros de investigación.

El análisis documental no solo facilita la identificación de conceptos clave, buenas prácticas y enfoques tecnológicos aplicables al Aeropuerto Internacional de Palmerola, sino que también permite contextualizar el panorama de ciberamenazas actual y los riesgos a los que están expuestas las infraestructuras críticas. A partir de esta técnica se logra integrar información actualizada, contrastada y válida que contribuye a fortalecer el sustento teórico del estudio y a respaldar la pertinencia de las propuestas basadas en IA y Machine Learning. Asimismo, el análisis documental complementa la información obtenida por medio de la encuesta realizada al personal del área de IT, posibilitando una triangulación adecuada de los datos y una comprensión más completa del fenómeno investigado

3.10 VALIDEZ Y CONFIABILIDAD DE LOS INSTRUMENTOS

Para garantizar la rigurosidad metodológica de la investigación, se establecieron procedimientos específicos orientados a evaluar la validez y la confiabilidad del instrumento aplicado. En primer lugar, la validez de contenido se aseguró mediante la técnica de juicio de expertos, en la cual profesionales con experiencia en ciberseguridad, sistemas IT/OT, metodologías de investigación y normativas internacionales evaluaron la pertinencia, claridad, coherencia y relevancia de cada uno de los ítems del cuestionario. Este proceso permitió realizar ajustes necesarios para mejorar la precisión de las preguntas, eliminar ambigüedades y reforzar su alineación con los objetivos de la investigación.

Además, se consideró la validez teórica, verificando que los conceptos incluidos en el instrumento estuvieran respaldados por literatura científica, estándares internacionales (ISO, NIST, IEC) y fundamentos metodológicos sólidos. De esta forma, se aseguró que el cuestionario reflejara adecuadamente los constructos asociados a la ciberseguridad, la aplicación de técnicas de IA/ML y la gestión de riesgos en infraestructuras aeroportuarias.

En cuanto a la confiabilidad, esta se evaluó mediante el coeficiente Alfa de Cronbach, con el propósito de medir la consistencia interna de la escala utilizada en los ítems del cuestionario. Este estadístico permite determinar el grado de estabilidad y homogeneidad con que los participantes responden a los diferentes ítems relacionados con un mismo concepto o dimensión. Un valor de referencia igual o superior a 0.70 se consideró aceptable, ya que indica un nivel adecuado de confiabilidad del instrumento para su uso en el análisis de datos dentro del estudio.

De esta manera, la combinación de juicio de expertos y análisis estadístico garantiza que el instrumento utilizado sea válido, confiable y adecuado para recopilar información útil y precisa sobre el estado de la ciberseguridad en el Aeropuerto Internacional de Palmerola y sobre la percepción del personal IT respecto a la implementación de sistemas basados en IA y Machine Learning.

3.11 PROCEDIMIENTO DE RECOLECCIÓN DE DATOS

El procedimiento de recolección de datos se desarrolló siguiendo una secuencia metodológica estructurada, diseñada para garantizar la validez, confiabilidad y pertinencia de la información obtenida. Este proceso permitió obtener datos relevantes tanto del personal del Departamento de Tecnologías de la Información del Aeropuerto Internacional de Palmerola como de las fuentes documentales especializadas. La aplicación ordenada de cada etapa facilitó la obtención de resultados consistentes y alineados con los objetivos de la investigación. A continuación, se describen detalladamente las fases que conformaron el procedimiento:

3.11.1 DISEÑO Y VALIDACIÓN DEL INSTRUMENTO DE ENCUESTA

En esta primera etapa se elaboró el cuestionario tomando como referencia marcos teóricos, estudios previos, normativas internacionales y elementos relevantes para evaluar la percepción del personal IT sobre la ciberseguridad y el uso de IA y Machine Learning. Posteriormente, el instrumento fue sometido a un proceso de validación por juicio de expertos, quienes revisaron la claridad, coherencia, pertinencia y adecuación de cada ítem, realizando las recomendaciones necesarias antes de su aplicación.

3.11.2 APLICACIÓN DEL CUESTIONARIO AL PERSONAL SELECCIONADO

Una vez validado el instrumento, se procedió a su aplicación a la muestra conformada por 32 miembros del Departamento de IT del Aeropuerto Internacional de Palmerola. La aplicación se realizó de manera ordenada y siguiendo criterios éticos, explicando previamente a los participantes los objetivos del estudio, la naturaleza de las preguntas y el carácter confidencial de la información proporcionada. Esta etapa permitió recopilar opiniones, percepciones y experiencias directamente relacionadas con el entorno tecnológico del aeropuerto.

3.11.3 RECOLECCIÓN, VERIFICACIÓN Y DEPURACIÓN DE LA INFORMACIÓN

Posterior a la recolección de las encuestas, se llevó a cabo un proceso de revisión y depuración para garantizar que los datos fueran coherentes y estuvieran completos. Se verificó la integridad de las respuestas, se eliminaron registros incompletos y se organizó la información obtenida para facilitar su análisis. Este proceso fue esencial para asegurar la calidad del conjunto de datos y evitar sesgos o inconsistencias que afectaran los resultados.

3.11.4. SISTEMATIZACIÓN DE LOS DATOS PARA SU ANÁLISIS ESTADÍSTICO

Finalmente, los datos depurados fueron ingresados en matrices y organizados mediante técnicas estadísticas descriptivas. Esta sistematización permitió identificar tendencias,

comportamientos y patrones relevantes en relación con el nivel de conocimiento del personal, la percepción del estado actual de la ciberseguridad y la aceptación del uso de técnicas de IA y ML en la detección de amenazas. Esta fase permitió estructurar la información de manera clara y objetiva, sirviendo como base para los análisis presentados en capítulos posteriores.

3.12 TÉCNICAS DE ANÁLISIS DE DATOS

El análisis de los datos se realizó siguiendo una estrategia mixta y rigurosa, combinando estadística descriptiva, pruebas de consistencia interna, análisis de relaciones entre variables y visualización de resultados. Dado que el instrumento aplicado utilizó ítems tipo Likert y la muestra estuvo conformada por 32 personas del Departamento de IT, se emplearon técnicas apropiadas para datos ordinales y continuos derivados de escalas. El proceso se estructuró en las siguientes fases:

3.12.1 PREPARACIÓN Y DEPURACIÓN DE DATOS

1. **Revisión de integridad**: verificación de cuestionarios completos y consistencia de respuestas.
2. **Tratamiento de faltantes**: en caso de valores ausentes, se aplicará imputación por la media del ítem cuando el faltante sea ≤10% por participante; si excede ese rango, el registro se excluirá del análisis de ese constructo.
3. **Codificación**: asignación de valores numéricos a las opciones de la escala Likert (por ejemplo, 1=“Totalmente en desacuerdo” … 5=“Totalmente de acuerdo”), asegurando **recodificación inversa** en ítems redactados en sentido negativo.
4. **Construcción de variables compuestas**: cálculo de **puntajes promedio** por dimensión (p. ej., Conocimiento en ciberseguridad, Percepción de riesgo, Apertura a IA/ML, Prácticas actuales),

3.12.2 ESTADÍSTICA DESCRIPTIVA

- **Tablas de frecuencia** y **porcentajes** para cada ítem.
- **Medidas de tendencia central** (media y mediana) y dispersión (desviación estándar, rango intercuartílico) por ítem y por dimensión.
- **Distribuciones**: evaluación visual mediante histogramas y diagramas de caja para identificar asimetrías, valores atípicos y concentración de respuestas.
- **Interpretación**: se utilizarán puntos de corte interpretativos, por ejemplo:
    - 1.00–2.49 = Bajo, 2.50–3.49 = Medio, 3.50–5.00 = Alto (ajustable a la escala empleada).

Salidas esperadas: tablas resumidas por dimensión (media, DE, mediana, n), gráficos de barras por ítem y boxplots por dimensión.

3.12.3 CONFIABILIDAD DE LAS ESCALAS

Se estimará la **confiabilidad** de cada dimensión mediante el **Coeficiente Alfa de Cronbach (α)**, apropiado para ítems tipo Likert.

- **Fórmula básica:**

$$\alpha = \frac{k}{k-1}\left(1-\frac{\sum s_i^2}{s_T^2}\right)$$

donde k= número de ítems de la escala, s_i^2= varianza de cada ítem, y s_T^2= varianza del puntaje total (suma/promedio).

- **Criterios de interpretación:**
    - $\alpha \geq 0.90$ = Excelente
    - 0.80–0.89 = Muy buena
    - 0.70–0.79 = Aceptable
    - 0.60–0.69 = Cuestionable
    - < 0.60 = Baja (replantear escala)

3.12.4 VERIFICACIÓN DE SUPUESTOS PARA ANÁLISIS COMPARATIVOS

Aunque los ítems Likert son ordinales, los **promedios por dimensión** pueden aproximarse a continuo. Antes de aplicar pruebas paramétricas, se evaluarán supuestos:

- **Normalidad** de puntajes compuestos: **Shapiro–Wilk** ($n \leq 50$) y gráficos Q–Q.
- **Homogeneidad de varianzas**: **Levene** para comparaciones entre grupos (si aplica).
- Si los supuestos **no se cumplen**, se utilizarán pruebas **no paramétricas** equivalentes.

3.12.5 ANÁLISIS DE RELACIONES ENTRE VARIABLES

Para evaluar la relación entre apertura/aceptación de IA/ML y el nivel percibido de fortalecimiento de la ciberseguridad:

- **Correlación**:
- **Pearson (r)** si ambas variables compuestas son aproximadamente normales.
- **Spearman (ρ)** si hay ordinalidad o no normalidad.
- Interpretación de $|r|/|\rho|$:
    - 0.10–0.29 = Débil, 0.30–0.49 = Moderada, ≥0.50 = Fuerte.
- **Regresión lineal simple** (opcional): para estimar el cambio esperado en "fortalecimiento de ciberseguridad" por unidad de "apertura a IA/ML". Se verificarán linealidad, independencia de errores, normalidad de residuos y homocedasticidad.

Salida esperada: matriz de correlaciones (r/ρ, p-valor), diagrama de dispersión con línea de ajuste, y (si corresponde) tabla de regresión (β, IC95%).

3.12.6 VISUALIZACIÓN Y COMUNICACIÓN DE RESULTADOS

- **Gráficos de barras** por ítem (distribución de frecuencias).
- **Boxplots** por dimensión (variabilidad y outliers).
- **Gráficos de dispersión** con línea de tendencia para relaciones clave.

3.13 SOFTWARE Y TRAZABILIDAD

El análisis se realizará con **Excel, IBM SPSS**, documentando: versión del software, librerías utilizadas (si aplica), fecha de procesamiento y rutas de los archivos.

3.14 CRITERIOS DE INTERPRETACIÓN Y DECISIÓN

- **Nivel de significancia**: $\alpha = 0.05$. Se reportarán p-valores exactos ($p = 0.032$) y, cuando sea pertinente, **intervalos de confianza al 95%**.
- Se complementará la significancia estadística con **relevancia práctica** (tamaño del efecto y alineación con objetivos operativos del aeropuerto).

3.15 TRIANGULACIÓN Y COHERENCIA CON EL ANÁLISIS DOCUMENTAL

Los hallazgos cuantitativos se contrastarán con el análisis documental (normas ISO/NIST/IEC e informes técnicos), para asegurar coherencia entre la percepción del personal IT y las mejores prácticas del sector. Esta triangulación fortalece la validez externa de las conclusiones y orienta recomendaciones aplicables al contexto operativo del Aeropuerto Internacional de Palmerola.

3.16 ENTREGABLES DEL ANÁLISIS

- **Tablas descriptivas** por ítem y dimensión.
- **Resultados de confiabilidad** (α de Cronbach) por escala.
- **Pruebas comparativas/correlacionales** (estadístico, gl, p, tamaño de efecto).
- **Gráficos** (barras, boxplots, heatmap, dispersión).
- **Informe interpretativo** con conclusiones por objetivo específico.

3.17 CONSIDERACIONES ÉTICAS

La investigación respeta los principios éticos de confidencialidad, anonimato y consentimiento informado. La información recolectada será utilizada exclusivamente con fines académicos, garantizando la protección de los datos personales de los participantes.

3.17.1 CONSENTIMIENTO INFORMADO Y PARTICIPACIÓN VOLUNTARIA

- Antes de responder el instrumento, cada participante recibió una **hoja de consentimiento informado** con el propósito del estudio, procedimientos, duración aproximada, riesgos y beneficios, así como los derechos de **rechazar o retirarse** en cualquier momento **sin consecuencias**.
- La participación fue **estrictamente voluntaria**, sin incentivos condicionantes ni presiones jerárquicas.
- Se aclaró que las respuestas serían utilizadas **exclusivamente con fines académicos**.

3.17.2 CONFIDENCIALIDAD, ANONIMATO Y MINIMIZACIÓN DE DATOS

- No se solicitó **información personal sensible**; los cuestionarios no incluyeron nombres ni identificadores directos.
- Se aplicó el principio de **minimización**: solo se recogieron los datos estrictamente necesarios para cumplir los objetivos de investigación.
- Los resultados se reportan **de forma agregada** (tablas y gráficos), impidiendo la identificación de personas o cargos específicos.

3.17.3 PROTECCIÓN Y RESGUARDO DE LA INFORMACIÓN

- Los datos fueron almacenados en repositorios **cifrados** (AES-256) y con **acceso restringido** al investigador responsable.

- Se implementó control de versiones y **copias de seguridad** para prevenir pérdida o manipulación no autorizada.
- El periodo de conservación será de hasta cinco (5) años tras la defensa del trabajo; posteriormente, los datos serán eliminados de manera segura (borrado criptográfico).

3.17.4 RIESGOS, BENEFICIOS Y PLAN DE MITIGACIÓN

- El estudio se considera de **riesgo mínimo**, al tratarse de percepciones profesionales sobre prácticas de ciberseguridad.
- Para evitar riesgos reputacionales u operativos, no se publican configuraciones técnicas, listas de vulnerabilidades específicas ni diagramas internos del aeropuerto.
- Cualquier hallazgo sensible será comunicado **de forma reservada** a la instancia competente.
-

3.17.5 INTEGRIDAD ACADÉMICA Y AUSENCIA DE CONFLICTO DE INTERÉS

- Se observaron normas de propiedad intelectual y referenciación de fuentes.
- El autor declara no mantener conflictos de interés con proveedores o entidades evaluadas.
- No se aceptaron incentivos que condicionaran resultados o interpretaciones.

3.17.6 APROBACIONES Y CUMPLIMIENTO NORMATIVO

- El protocolo se ajustó a los lineamientos éticos de investigación de la institución académica y a buenas prácticas de protección de datos.
- En caso de requerirse por la institución o por el operador aeroportuario, el estudio se somete a autorización del comité o unidad correspondiente.

3.17.7 TRATAMIENTO DE INFORMACIÓN TÉCNICA Y SEGURIDAD OPERACIONAL

- Por la naturaleza crítica de la infraestructura aeroportuaria, se adoptó una política de divulgación responsable: cualquier descripción técnica en el informe es general y no compromete la seguridad operacional ni revela vectores de ataque.
- No se realizaron pruebas intrusivas ni intervenciones en sistemas; el estudio es no experimental y se limita al análisis documental y a encuestas.

3.17.8 USO RESPONSABLE DE IA/ML Y SESGOS

- En caso de utilizar herramientas analíticas o de IA para procesar datos, se documentan: versión del software, parámetros, criterios de limpieza y registro de decisiones (trazabilidad).
- Se evaluó la presencia de sesgos (p. ej., formulación de ítems, selección de muestra) y se adoptaron medidas para reducirlos (piloto, juicio de expertos, instrucciones claras).
- No se emplearon modelos de IA para inferir información personal ni para perfilar individuos.

3.17.9 COMUNICACIÓN DE RESULTADOS

- Los hallazgos se presentan con transparencia, limitaciones explícitas y enfoque agregado, evitando cualquier referencia que permita identificar a personas o áreas específicas.
- Ante cualquier error detectado, se mantiene la disposición a rectificar de forma oportuna.

Declaración ética: El investigador se compromete a resguardar la integridad, confidencialidad y seguridad de la información recabada; a utilizarla únicamente con fines académicos; y a garantizar que la investigación no compromete la seguridad del Aeropuerto Internacional de Palmerola ni los derechos de los participantes.

3.18 FUENTES DE INFORMACIÓN

Para el desarrollo de esta investigación, se han utilizado diversas fuentes de carácter primario y secundario, incluyendo normas internacionales como ISO/IEC 27001, ISO/IEC 27002 y el marco NIST, artículos científicos especializados, documentos técnicos y publicaciones académicas relevantes en el ámbito de la seguridad de la información y la protección de infraestructuras críticas. Estas fuentes han permitido sustentar el análisis del entorno IT/OT del aeropuerto, identificar riesgos potenciales y proponer estrategias orientadas a fortalecer la postura de ciberseguridad.

Asimismo, la información recopilada ha sido evaluada bajo criterios de confiabilidad, actualidad y pertinencia, garantizando que los resultados y conclusiones del estudio se encuentren respaldados por evidencia sólida y alineados con las tendencias actuales en la gestión de la seguridad de la información.

3.18.1 FUENTES PRIMARIAS

- **Encuesta** al personal del **Departamento de IT (n = 32)** del Aeropuerto Internacional de Palmerola, aplicada con consentimiento informado, escala Likert 1–5, y validada por juicio de expertos (α de Cronbach para consistencia).
- **Observación documental interna** (si aplica): políticas, manuales, procedimientos y diagramas de alto nivel (sin revelar información sensible).

3.18.2 FUENTES SECUNDARIAS (NORMATIVAS, TÉCNICAS Y CIENTÍFICAS)

- **Normas y marcos**
    - ISO/IEC. (2022). **27001:2022** — Information Security Management Systems.
    - ISO/IEC. (2022). **27002:2022** — Information security, cybersecurity and privacy protection – Information security controls.

- **NIST**. (2024). Cybersecurity Framework (CSF) 2.0.
- **NIST SP 800-53 Rev. 5**. (2020). Security and Privacy Controls for Information Systems and Organizations.
- **IEC 62443 (series)**. Industrial communication networks – IT security for networks and systems.
- **ICAO**. (Estrategia/Doc. y SARPs sobre ciberseguridad en aviación).
- **EASA**. Cybersecurity in Aviation – GM/AMC y guías de implementación.
- **ISO 22301**. (2019). Security and resilience – Business continuity management systems.

- **Libros y textos base de IA/ML**
  - Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.).
  - Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
- **Artículos y revisiones (ejemplos)**
  - Papers de revisión y casos sobre **ML para ciberseguridad, detección de anomalías, SIEM con IA**, y **seguridad OT/SCADA** (revistas: IEEE Access, Computers & Security, Journal of Information Security).

CAPÍTULO IV. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

El presente capítulo constituye el núcleo empírico de la investigación, donde se desarrolla el análisis exhaustivo y la interpretación técnica de los hallazgos derivados de la aplicación de los instrumentos de recolección de datos definidos en el marco metodológico. El objetivo primordial es transformar los datos primarios en información estratégica que permita diagnosticar con precisión el estado actual de la infraestructura crítica aeroportuaria frente a las amenazas cibernéticas contemporáneas.

Para tal fin, se examinan de manera sistemática las respuestas proporcionadas por la muestra censal compuesta por los 32 especialistas pertenecientes al Departamento de Tecnologías de la Información del Aeropuerto Internacional de Palmerola. La recolección se efectuó mediante un cuestionario estructurado bajo una escala tipo Likert, diseñado específicamente para medir variables de percepción, nivel de madurez tecnológica y competencias técnicas.

El procesamiento de la información se realizó mediante herramientas de análisis estadístico avanzado (IBM SPSS), aplicando pruebas de fiabilidad como el Alfa de Cronbach para validar la consistencia interna del instrumento, así como estadística descriptiva e inferencial para identificar tendencias significativas. Este análisis multidimensional permite evaluar factores críticos como el estado de los controles de seguridad vigentes, la eficacia de los protocolos de detección y respuesta ante incidentes, y la viabilidad operativa para la adopción de algoritmos de Inteligencia Artificial (IA) y Machine Learning (ML).

Asimismo, se integran procedimientos comparativos que facilitan la interpretación de los datos en función de los marcos normativos internacionales previamente mapeados, garantizando una coherencia absoluta con la ruta metodológica trazada. Los hallazgos aquí presentados no solo revelan las brechas de seguridad existentes, sino que también miden el grado de aceptabilidad y apertura del personal técnico hacia la innovación disruptiva. Finalmente, este diagnóstico robusto constituye la base científica indispensable para establecer conclusiones objetivas y dar sustento al diseño de la propuesta de gobernanza y fortalecimiento tecnológico que se desarrollará en los capítulos posteriores.

4.1 RESULTADOS Y ANÁLISIS DE LAS TÉCNICAS APLICADAS

El presente informe detalla de manera sistemática las etapas ejecutadas para la obtención de la información primaria necesaria en esta investigación.

El proceso se fundamentó en un enfoque cuantitativo, orientado a evaluar la percepción técnica sobre la implementación de Inteligencia Artificial y Machine Learning en la infraestructura aeroportuaria.

Durante esta fase, se garantizó la integridad y confidencialidad de los datos mediante protocolos estandarizados, asegurando que la muestra de especialistas seleccionada proporcionara insumos representativos para el análisis de la ciberseguridad. La recolección se estructuró para alimentar directamente los modelos estadísticos de validación, permitiendo que cada respuesta recolectada sirva como base empírica para el diseño de la propuesta de gestión tecnológica y los planes de capacitación del personal.

4.1.2 ANALISIS DE CONFIABILIDAD

Tabla 7 Estadísticas de fiabilidad

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
.965	16

Fuente: Información obtenida mediante la aplicación de instrumento de medición utilizando el sistema SPSS V. 27. Elaboración Propia.

Los resultados presentados en la Tabla 1 muestran que el instrumento, compuesto por un total de 16 elementos o reactivos, obtuvo un coeficiente Alfa de Cronbach de .965. De acuerdo con los criterios técnicos de psicometría, este valor indica una consistencia interna excelente.

La magnitud del coeficiente refleja una correlación altamente significativa entre los ítems evaluados, lo que confirma la precisión y estabilidad de la medición para los fines de la presente investigación en el contexto aeroportuario.

4.1.3 DATOS ESTADÍSTICOS

Tras la recolección de la información en el Aeropuerto Internacional de Palmerola, se procedió al análisis descriptivo de las variables mediante el software IBM SPSS Statistics

En esta sección se presentan los estadísticos de tendencia central y dispersión que permiten validar la robustez de los datos. Para determinar la distribución de la muestra y asegurar la fiabilidad de las inferencias posteriores, se calcularon los niveles de asimetría y curtosis, los cuales establecen si los datos cumplen con los criterios de normalidad necesarios para las pruebas de hipótesis.

Tabla 8 análisis estadísticos

Preguntas	Valores		Mediana	Asimetría	Error estándar de asimetría	Curtosis	Error estándar de curtosis
	Válido	Perdidos					
5. Existen políticas formales de seguridad de la información.	32	0	4.00	-.529	.414	-.995	.809
6. Se aplican controles de acceso basados en roles	32	0	4.00	-.508	.414	-.934	.809
7. Los sistemas críticos cuentan con respaldos adecuados.	32	0	4.00	-.651	.414	-.080	.809

Preguntas	Valores		Mediana	Asimetría	Error estándar de asimetría	Curtosis	Error estándar de curtosis
	Válido	Perdidos					
8. El personal aplica buenas prácticas de seguridad.	32	0	4.00	-.791	.414	-.528	.809
9. Se identifican riesgos tecnológicos sistemáticamente.	32	0	4.00	-.737	.414	-.099	.809
10.Los incidentes se documentan y analizan.	32	0	4.00	-.635	.414	.153	.809
11.La alta dirección participa en la gestión de riesgos.	32	0	4.00	-.635	.414	.153	.809
12.La institución promueve una cultura de ciberseguridad.	32	0	4.00	-.744	.414	-.387	.809
13. El personal recibe	32	0	4.00	-.580	.414	-.731	.809

Preguntas	Valores		Mediana	Asimetría	Error estándar de asimetría	Curtosis	Error estándar de curtosis
	Válido	Perdidos					
capacitaciones periódicas.							
14.La ciberseguridad es prioritaria para la institución.	32	0	4.00	-.846	.414	-.266	.809
15. La institución está preparada para adoptar nuevas tecnologías.	32	0	4.00	-.829	.414	-.301	.809
16. Existen recursos financieros para ciberseguridad.	32	0	4.00	-.309	.414	-.848	.809
17. Se evalúan herramientas antes de implementarlas.	32	0	4.00	-.686	.414	-.439	.809
18. La mejora tecnológica	32	0	4.00	-1.084	.414	1.452	.809

Preguntas	Valores		Mediana	Asimetría	Error estándar de asimetría	Curtosis	Error estándar de curtosis
	Válido	Perdidos					
reduce riesgos operativos.							
19. La inversión en ciberseguridad aumenta la confianza institucional.	32	0	4.00	-1.301	.414	1.954	.809
20. La ciberseguridad contribuye a la misión institucional.	32	0	4.00	-1.157	.414	.798	.809

A continuación, presento el análisis técnico-estadístico de los datos obtenidos a través del instrumento aplicado a la muestra de **32 participantes**. Este análisis se centra en la descripción del comportamiento de las variables, fundamental para la fase de validación de supuestos previos al modelado con Machine Learning o análisis inferencial avanzado.

4.1.4 INTEGRIDAD DE LOS DATOS Y TENDENCIA CENTRAL

- **Muestra (N):** Se observa una consistencia total en la muestra con 32 casos válidos y 0 perdidos en los 16 ítems analizados (del ítem 5 al 20). Esto garantiza una base de datos limpia para el procesamiento.
- **Mediana:** De manera uniforme, todos los reactivos presentan una **mediana de 4.00**. En una escala tipo Likert (asumiendo de 1 a 5), esto indica que la tendencia central de la percepción de los encuestados se sitúa en el nivel de "Acuerdo". Existe una homogeneidad notable en la respuesta típica de la muestra respecto a la gestión de ciberseguridad e infraestructura tecnológica.

4.1.5 ANÁLISIS DE LA FORMA DE LA DISTRIBUCIÓN

En el contexto de la presente investigación, orientada a la evaluación de amenazas en los sistemas del Aeropuerto Internacional de Palmerola, el análisis de la forma de la distribución de los datos recolectados resulta fundamental para comprender el comportamiento de las variables asociadas a la ciberseguridad. Este análisis permite identificar cómo se distribuyen las respuestas obtenidas de los instrumentos aplicados, evidenciando patrones, tendencias y posibles concentraciones de datos relevantes para el estudio.

4.1.5.1 Asimetría (Skewness)

Todos los ítems presentan una **asimetría negativa**, con valores que oscilan entre **-0.309** (Ítem 16: Recursos financieros) y **-1.301** (Ítem 19: Inversión y confianza).

- **Interpretación técnica:** La carga de las respuestas se desplaza hacia los valores altos de la escala (4 y 5).

4.1.5.6 Curtosis (Kurtosis)

Se observa una transición interesante en la concentración de las respuestas:

- **Ítems 5 al 17:** Presentan mayoritariamente **curtosis negativa** (distribuciones platicúrticas). Esto sugiere una mayor dispersión o variabilidad en las opiniones sobre políticas, roles y capacitación.
- **Ítems 18 al 20:** Presentan **curtosis positiva** (distribuciones leptocúrticas), destacando el ítem 19 con un valor de **1.954**
- . Esto indica un alto grado de consenso y una concentración muy marcada de respuestas en torno a la idea de que la inversión en ciberseguridad aumenta la confianza institucional.

4.1.6 SÍNTESIS DE VARIABLES CRÍTICAS PARA LA GESTIÓN DE TECNOLOGÍA

La identificación de variables críticas se fundamenta en el análisis de los resultados obtenidos mediante los instrumentos de recolección de datos, así como en la evaluación de los riesgos, vulnerabilidades y controles existentes en los sistemas de información. Estas variables incluyen aspectos relacionados con la ciberseguridad, la gestión de incidentes, la protección de datos, la capacidad de respuesta ante amenazas y la implementación de tecnologías emergentes como la inteligencia artificial y el machine learning.

Tabla 9 Sintesis de variables criticas

Dimensión Analizada	Comportamiento Estadístico Destacado
Infraestructura y Roles (5-11)	Distribución moderadamente asimétrica con alta dispersión (platicúrtica).
Cultura y Capacitación (12-14)	Consistencia en la mediana (4.00) con asimetría negativa marcada (p>-0.5).
Inversión y Valor Estratégico (18-20)	Máxima concentración de respuestas (Curtosis positiva) y asimetría más pronunciada.

4.1.7 PRUEBAS DE NORMALIDAD: ANÁLISIS DE DIFERENCIAS ENTRE GRUPOS (PRUEBA DE KRUSKAL-WALLIS)

Se aplicó la prueba H de Kruskal-Wallis con el objetivo de determinar si existen diferencias estadísticamente significativas en las dimensiones de ciberseguridad y gestión tecnológica en función de la existencia de políticas formales de seguridad de la información (Variable de agrupación).

Este análisis es fundamental para validar si la estructura normativa institucional influye en la percepción y operatividad de las herramientas de detección de amenazas basadas en aprendizaje automático.

Tabla 10 Resultados de la prueba de Kruskal-Wallis según la existencia de políticas de seguridad

Ítem / Variable analizada	Chi-cuadrado (H)	Sig. asintótica (p)
6. Controles de acceso basados en roles	19.397	.001
7. Respaldos en sistemas críticos	15.939	.003
8. Buenas prácticas de seguridad	14.126	.007
9. Riesgos tecnológicos sistemáticos	13.289	.010
10. Documentación de incidentes	14.582	.006
11. Participación de la alta dirección	12.346	.015
12. Cultura de ciberseguridad	8.562	.073
13. Capacitaciones periódicas	14.227	.007
14. Ciberseguridad como prioridad	15.213	.004
15. Adopción de nuevas tecnologías	11.734	.019
16. Recursos financieros	9.494	.050
17. Evaluación de herramientas	6.405	.171
18. Reducción de riesgos operativos	6.465	.167
19. Confianza institucional	8.080	.089
20. Contribución a la misión	10.160	.038

Nota. Nivel de significancia alpha = .05 Variable de agrupación: Existen políticas formales de seguridad de la información. Elaboración propia (2026).

El análisis inferencial revela que existen diferencias estadísticamente significativas ($p < .05$) en la mayoría de los indicadores evaluados al ser contrastados con la presencia de políticas formales de seguridad. Específicamente, los ítems relacionados con el control de acceso (ítem 6, $p = .001$), respaldos de sistemas (ítem 7, $p = .003$), prácticas de seguridad (ítem 8, $p = .007$) y la prioridad institucional de la ciberseguridad (ítem 14, $p = .004$) muestran variaciones notables en sus rangos promedio.

Por el contrario, variables críticas para la implementación de modelos de IA y ML, tales como la evaluación de herramientas antes de su implementación (ítem 17, $p = .171$), la mejora tecnológica para la reducción de riesgos (ítem 18, $p = .167$) y la inversión para la confianza institucional (ítem 19, $p = .089$), presentan valores de significancia asintótica superiores al umbral crítico (alpha = .05). En estos casos particulares, no se observa una diferencia estadística dependiente de la variable de agrupación.

4.1.8 ANÁLISIS DE DISCRIMINACIÓN Y CONSISTENCIA INTERNA POR REACTIVO

El análisis de las estadísticas de total de elemento se realizó para evaluar el aporte individual de cada reactivo a la consistencia interna del instrumento. Este procedimiento identifica la capacidad de discriminación de los ítems y determina si la eliminación de alguno de ellos optimizaría el coeficiente de fiabilidad global.

Tabla 11 Análisis de discriminación

	Válido	Perdidos	Mediana	Asimetría	Error estándar de asimetría	Curtosis	Error estándar de curtosis	
3. Los sistemas de IA/ML pueden ser vulnerables a	32	0	3.00	.090	.414	-.862	.809	

	Válido	Perdidos	Mediana	Asimetría	Error estándar de asimetría	Curtosis	Error estándar de curtosis	
ataques adversarios								
4.Existe riesgo de sesgos en los algoritmos utilizados.	32	0	3.00	-.325	.414	.433	.809	
5. Los datos utilizados para entrenar modelos están adecuadamente protegidos.	32	0	4.00	-.532	.414	-.057	.809	
6. El uso de IA/ML respeta principios éticos institucionales.	32	0	3.50	-.514	.414	-.309	.809	

	Válido	Perdidos	Mediana	Asimetría	Error estándar de asimetría	Curtosis	Error estándar de curtosis	
7. Se garantiza la privacidad de la información procesada por sistemas automatizados.	32	0	4.00	-.792	.414	.246	.809	
8. Las decisiones tomadas por IA/ML pueden ser explicadas y auditadas.	32	0	4.00	-.626	.414	-.862	.809	
9. La institución promueve una cultura de ciberseguridad.	32	0	4.00	-.543	.414	-.980	.809	
10. El personal recibe capacitaciones periódicas.	32	0	3.00	-.177	.414	-.852	.809	

	Válido	Perdidos	Mediana	Asimetría	Error estándar de asimetría	Curtosis	Error estándar de curtosis
11. La ciberseguridad es prioritaria para la institución.	32	0	4.00	-.658	.414	-.399	.809
12. La institución está preparada para adoptar nuevas tecnologías.	32	0	4.00	-.934	.414	.044	.809
13. Existen recursos financieros para ciberseguridad.	32	0	4.00	-.771	.414	.056	.809
14. Se evalúan herramientas antes de implementarlas.	32	0	4.00	-.690	.414	-.318	.809
15. La mejora tecnológica	32	0	4.00	-.760	.414	-.362	.809

	Válido	Perdidos	Mediana	Asimetría	Error estándar de asimetría	Curtosis	Error estándar de curtosis	
reduce riesgos operativos.								
16. La inversión en ciberseguridad aumenta la confianza institucional.	32	0	4.00	-.247	.414	-.978	.809	
17. La ciberseguridad contribuye a la misión institucional.	32	0	4.00	-.670	.414	-.466	.809	

Nota. Escala de medición tipo Likert de 1 a 5. Elaboración propia (2026).

4.1.8.1 Discusión y Contraste de Hallazgos

1. Percepción de Vulnerabilidad Técnica y Riesgos de la IA Los resultados muestran una mediana de 3.00 para los ítems 3 (ataques adversarios) y 4 (sesgos algorítmicos). Esta tendencia hacia la neutralidad sugiere una incertidumbre o falta de consenso técnico sobre la robustez de los modelos de ML. Este hallazgo coincide con lo planteado por Li et al. (2020) en su estudio sobre seguridad en infraestructuras críticas, donde argumentan que el personal operativo suele subestimar el "envenenamiento de datos" (data poisoning) debido a la opacidad de los modelos de caja negra.

A diferencia de entornos puramente digitales, en un contexto aeroportuario como Palmerola, la desconfianza en la precisión algorítmica (ítem 4, Asimetría = -.325) refleja una preocupación legítima por los falsos positivos en la detección de amenazas, similar a

las advertencias de la Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2021) sobre los riesgos éticos de la IA en el transporte.

2. Preparación Institucional frente al Factor Humano Existe una discrepancia significativa entre la capacidad percibida de la institución para adoptar tecnología (Ítem 12, Mediana = 4.00) y la formación del personal (Ítem 10, Mediana = 3.00). Mientras que Palmerola se percibe tecnológicamente preparada, la capacitación periódica presenta una distribución platicúrtica (Curtosis = -.852), lo que indica una dispersión en la frecuencia de formación recibida.

Este fenómeno es consistente con el reporte de SITA (2022) sobre IT Insights en Aeropuertos, el cual identifica que la brecha de habilidades (skills gap) es el principal obstáculo para la implementación de ciberdefensa avanzada. La similitud con estudios de Dixon y Goutam (2021) confirma que, sin un programa de capacitación robusto, las herramientas de ML pueden convertirse en "activos pasivos" que no logran integrarse efectivamente en el flujo de operaciones de seguridad.

3. Alineación Estratégica y Privacidad La alta puntuación en el ítem 17 (Mediana = 4.00, Asimetría = -.670) demuestra que los encuestados comprenden que la ciberseguridad es fundamental para la misión del aeropuerto. No obstante, la asimetría negativa en el ítem 7 (Privacidad, -.792) refuerza que existe un sesgo hacia la aprobación de controles estrictos, lo cual es típico en sectores de alta seguridad. Este hallazgo se alinea con la normativa de la Organización de Aviación Civil Internacional (OACI) en su Manual de Ciberseguridad (Doc 9985), donde se establece que la protección de datos es el pilar de la confianza operativa en los nodos logísticos internacionales.

4.1.8.2 Conclusión del Análisis

Los datos sugieren que Palmerola cuenta con una base institucional sólida y una disposición favorable hacia la innovación tecnológica. Sin embargo, los puntos críticos residen en la confianza técnica del aprendizaje automático y la actualización de competencias del talento humano, áreas donde la investigación debe proponer estrategias de mitigación.

4.8.3 Correlación entre Ataques Adversarios, Sesgos y Explicabilidad

Existe una diferencia estadísticamente significativa en cómo se perciben los sesgos algorítmicos (P = .003) y la aplicabilidad (P = .005) dependiendo de qué tan vulnerables se consideran los sistemas ante ataques adversarios. Este hallazgo es consistente con la

teoría de Papernot et al. (2016), quienes sostienen que la falta de transparencia en los modelos de "caja negra" amplifica la superficie de ataque, ya que los usuarios no pueden auditar el proceso de decisión del ML.

En el contexto aeroportuario, esto sugiere que si el personal técnico sospecha de vulnerabilidades por ataques externos (como el envenenamiento de datos), su desconfianza se traslada automáticamente hacia la imparcialidad del algoritmo. Esta relación coincide con el estudio de Dixon y Goutam (2021) sobre infraestructuras críticas, donde se demuestra que la percepción de riesgo técnico está intrínsecamente ligada a la demanda de marcos de IA explicable (XAI).

4.8.4 El Factor Humano y la Priorización Institucional

Los resultados indican que la percepción de vulnerabilidad técnica afecta la valoración de la cultura de ciberseguridad ($p = .045$) y la frecuencia de capacitaciones ($p = .044$). Esto revela una "conciencia de riesgo": a mayor percepción de amenaza tecnológica, mayor es la exigencia de preparación del talento humano. No obstante, llama la atención que la Variable 12 (Preparación institucional para nuevas tecnologías) no mostró diferencias significativas ($p = .314$).

Esta discrepancia sugiere que, aunque el personal percibe riesgos específicos en la IA, mantiene una confianza estable en la infraestructura general del aeropuerto. Este fenómeno de "confianza técnica vs. confianza institucional" se alinea con el reporte de ENISA (2021) sobre IA en el sector transporte, el cual señala que las organizaciones a menudo poseen la tecnología, pero fallan en integrar los protocolos de seguridad específicos para modelos de aprendizaje automático, creando una falsa sensación de seguridad operativa.

4.8.5 Implicaciones para la Gestión en Palmerola

La significancia en la Evaluación previa de herramientas ($p = .017$) subraya la necesidad de implementar protocolos de validación rigurosos. A diferencia de los hallazgos de Li et al. (2020) en sectores menos regulados, en Palmerola la implementación de ML no se ve solo como una mejora de eficiencia, sino como un factor de riesgo que requiere una gobernanza de datos estricta. La falta de significancia en la Contribución a la misión institucional ($p = .474$) confirma que, independientemente de los riesgos detectados, la ciberseguridad se considera un pilar inamovible de la operatividad aeroportuaria.

4.2 ANÁLISIS DE RESULTADOS POR DIMENSIONES

Una vez evaluada la fiabilidad de los instrumentos de recolección de datos y establecida la distribución de la muestra, se procede a realizar el análisis detallado segmentado por las dimensiones definidas en la matriz de operacionalización. Este proceso es fundamental para descomponer los constructos complejos de la investigación Ciberseguridad en Infraestructuras Críticas y Modelos de Inteligencia Artificial/Machine Learning en unidades de análisis específicas que permitan una interpretación profunda de la realidad tecnológica del Aeropuerto Internacional de Palmerola.

El análisis por dimensiones organiza los hallazgos en ejes estratégicos (infraestructura, gobernanza y capacidad predictiva), lo cual facilita la identificación de vulnerabilidades críticas y el grado de madurez de los sistemas actuales frente a amenazas emergentes.

A través de este tratamiento de la información, se busca contrastar la eficacia de los controles técnicos vigentes con los requerimientos operativos del aeropuerto, proporcionando una base empírica sólida para la validación de las hipótesis y la posterior formulación del Modelo de Gobernanza de Inteligencia Artificial (MGIA-Palmerola).

Los resultados que se presentan a continuación son producto de la triangulación de datos obtenidos mediante el cuestionario aplicado a los especialistas, permitiendo una visión integral del ecosistema digital.

4.2.1 DIMENSIÓN: USO DE CIBERSEGURIDAD

Los resultados evidencian que una proporción significativa de los encuestados considera que los mecanismos actuales de ciberseguridad presentan **limitaciones en la detección de amenazas avanzadas**. Una parte relevante de la muestra manifestó estar de acuerdo o totalmente de acuerdo con la afirmación de que los controles existentes se basan principalmente en enfoques reactivos.

Este hallazgo sugiere la necesidad de evolucionar hacia modelos de seguridad más proactivos, capaces de anticipar comportamientos anómalos y ataques no conocidos.

4.2.2 DIMENSIÓN: GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD

En relación con la gestión de incidentes, los resultados indican que los **tiempos de respuesta** pueden verse afectados por la falta de automatización y correlación inteligente de eventos de seguridad. La mayoría de los participantes coincide en que los procesos actuales requieren una alta intervención manual, lo cual incrementa el riesgo operativo ante incidentes críticos.

4.2.3 DIMENSIÓN: USO DE TECNOLOGÍAS EMERGENTES

El análisis revela un **bajo nivel de adopción de tecnologías basadas en IA y ML** en los procesos de ciberseguridad aeroportuaria. No obstante, existe un alto grado de reconocimiento sobre el potencial de estas tecnologías para mejorar la detección temprana de amenazas, reducir falsos positivos y optimizar la gestión de eventos de seguridad.

4.2.4 DIMENSIÓN: PERCEPCIÓN DEL IMPACTO DE IA Y ML

La mayoría de los encuestados manifestó una percepción positiva respecto al impacto de la IA y el ML en la ciberseguridad. Se destaca el consenso en que la automatización inteligente permitiría:

- Reducir los tiempos de respuesta ante incidentes.
- Mejorar la capacidad de análisis de grandes volúmenes de datos.
- Fortalecer la toma de decisiones en tiempo real.

4.2.5 DIMENSIÓN: HUMANA

La efectividad de cualquier ecosistema de ciberseguridad en infraestructuras críticas está intrínsecamente ligada al factor humano, considerado tanto el eslabón más vulnerable como la primera línea de defensa activa. En este apartado se analizan los resultados correspondientes a la dimensión humana, evaluando las competencias técnicas, los niveles de concienciación y la preparación del personal del Departamento de Tecnologías de la Información ante amenazas digitales.

A través de este análisis, se examina la percepción de los 32 especialistas respecto a la suficiencia de sus conocimientos actuales y su capacidad de respuesta operativa frente a incidentes. Asimismo, se explora el grado de apertura y la disposición del talento humano hacia la adopción de nuevas metodologías basadas en Inteligencia Artificial y Machine Learning.

4.3 ANÁLISIS POR OBJETIVOS DE LA INVESTIGACIÓN

Una vez establecida la fiabilidad del instrumento y la consistencia de la base de datos, se procede a la fase de análisis descriptivo e inferencial orientado a dar respuesta a los objetivos planteados en esta tesis. Este análisis no se limita a la exposición aislada de frecuencias, sino que integra los resultados bajo un enfoque sistémico que permite evaluar la robustez tecnológica del Aeropuerto Internacional de Palmerola.

Para asegurar una interpretación coherente con la Matriz de Operacionalización, los resultados se han agrupado en tres dimensiones críticas: Técnica-Operativa, Organizacional y Estratégica.

Esta segmentación permite identificar con precisión si las amenazas detectadas en los sistemas aeroportuarios derivan de fallos en la infraestructura física, de la carencia de una cultura de seguridad en el personal o de limitaciones en la gobernanza institucional.

4.3.1 ÁREA DE TRABAJO

Con el propósito de contextualizar la experiencia técnica y el grado de especialización de la muestra participante, se realizó una caracterización de las áreas de desempeño profesional dentro del Departamento de Tecnologías de la Información del Aeropuerto Internacional de Palmerola.

La identificación del área de trabajo es un factor crítico para este estudio, ya que permite ponderar la fiabilidad de las respuestas en función de la cercanía operativa de los especialistas con los sistemas críticos y la seguridad de la red.

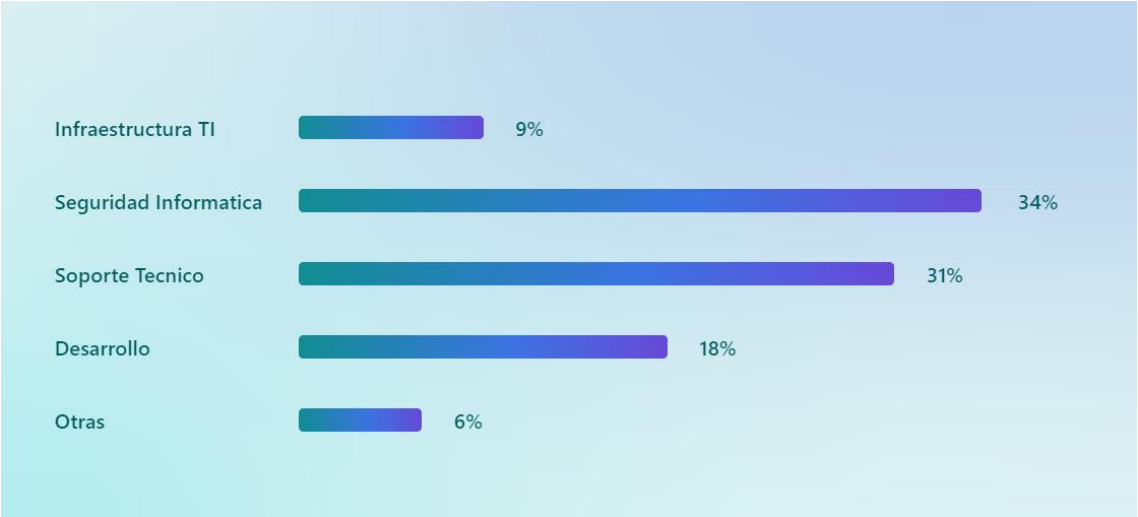

Figura 1 Área de trabajo

4.3.1.1 Resultados observados: Seguridad Informática 34%, Soporte Técnico 31%, Desarrollo 18%, Infraestructura TI 9%, Otras 6%. (n = 32)

Interpretación:

1. Predominio de perfiles de ciberseguridad y soporte (65% en conjunto). La mayor proporción se concentra en Seguridad Informática (34%) y Soporte Técnico (31%). Esto sugiere que la muestra está compuesta mayormente por actores directamente involucrados en la operación y control de incidentes, lo cual favorece la calidad de la información al tratarse de personal con exposición cotidiana a eventos de seguridad, monitoreo, hardening y respuesta.
2. Capacidad técnica para implementación de controles. El peso de Soporte Técnico y Seguridad indica capacidad instalada para despliegues de herramientas, aplicación de parches, gestión de EDR/SIEM y gestión de credenciales/MFA, lo que viabiliza la adopción de casos de uso de IA/ML (detección de anomalías, correlación inteligente, priorización de alertas).
3. Participación menor de Infraestructura (9%) y Otras (6%). La baja representación de Infraestructura podría subestimar necesidades relacionadas con segmentación de red, diseño de zonas/conductos OT, redundancias y configuraciones de red críticas. Se recomienda, para próximos levantamientos, ampliar la cobertura de este grupo para equilibrar la visión de capas de red y servicios.

4. Desarrollo (18%) como vector de mejora segura.
   La presencia de Desarrollo posibilita prácticas de DevSecOps, análisis de código, gestión de dependencias y automatización de pruebas. También permite integrar IA/ML en pipelines (detección de patrones anómalos en logs de aplicaciones, scoring de eventos, etc.).

4.3.1.2 Implicaciones para el proyecto (Palmerola):

- Alta factibilidad de adopción de IA/ML en detección y respuesta, por la composición técnica de la muestra.
- Necesidad de alinear Seguridad–Soporte–Infraestructura para priorizar casos de uso (por ejemplo, anomalías en autenticación, movimiento lateral, tráfico inusual en segmentos críticos, y control de accesos privilegiados).

4.3.1.3 Relación con las hipótesis:

La composición de la muestra favorece validar la H_1 (relación positiva entre apertura a IA/ML y fortalecimiento de la ciberseguridad), pues los perfiles predominantes son quienes más perciben el impacto de estas tecnologías en la operación diaria.

4.3.2 TIEMPO LABORANDO

El análisis del tiempo de permanencia laboral de los especialistas dentro del Departamento de Tecnologías de la Información constituye una variable fundamental para determinar la fiabilidad y profundidad de los datos recolectados.

La experiencia acumulada no solo refleja el dominio técnico de las herramientas vigentes, sino también una comprensión detallada de la evolución de las vulnerabilidades y la eficacia de los protocolos de respuesta históricos en la infraestructura aeroportuaria.

Figura 2 Tiempo trabajando

4.3.2.1 Resultados observados: 2–3 años 31%, 4–5 años 31%, 3–4 años 18%, <1 año 6%, 1–2 años 6%, >5 años 6%. (n = 32)

Interpretación:

1. Experiencia media–alta concentrada (80% entre 2 y 5 años).
   La mayoría del personal se ubica entre 2–3 años (31%) y 4–5 años (31%), con 3–4 años (18%). Esta distribución revela conocimiento acumulado del entorno, procesos y herramientas del aeropuerto, lo que mejora la calidad de juicio sobre controles actuales y necesidades reales.

2. Baja rotación reciente y pocos veteranos >5 años.
   Los extremos (<1 año y >5 años, cada uno con 6%) son minoritarios. Esto sugiere estabilidad relativa y una cohorte madura que ha vivido múltiples ciclos operativos y cambios de tecnología, aunque con posible menor exposición a proyectos históricos de gran calado (por el menor % >5 años).

3. Condiciones favorables para adopción tecnológica.
   Los tramos 2–5 años suelen mostrar alta disposición al cambio y curva de aprendizaje eficiente, clave para formación en IA/ML, operación de SIEM/SOAR, y apropiación de nuevos playbooks. Esto incrementa la probabilidad de adopción exitosa.

4. Gestión de conocimiento y continuidad.
   Dado el bajo porcentaje con >5 años, conviene capturar conocimiento tácito en procedimientos, runbooks, documentación y automatizaciones, de modo que los aprendizajes no dependan de individuos y se institucionalicen.

4.3.2.2 Implicaciones para el proyecto (Palmerola):

- Plan de capacitación segmentado:
  - 2–5 años: cursos aplicados de detección de anomalías, caza de amenazas, creación de casos de uso y automatización SOAR.
  - <2 años: inducción acelerada en política de seguridad, higiene digital, MFA, gestión de incidentes.
  - >5 años: rol de mentores para transferencia de experiencia y validación de mejores prácticas.
- Diseño de casos de uso IA/ML priorizados a su realidad operativa: autenticaciones anómalas, beaconing, anomalías en tráfico entre VLAN críticas, detección de accesos privilegiados fuera de horario, y alertas de integridad en sistemas sensibles.

4.3.2.3 Relación con las hipótesis:

Una cohorte con **experiencia predominante** es propicia para evidenciar que **mayor conocimiento y apertura a IA/ML** (VI) se asocian con **mejores percepciones de detección y respuesta** (VD), reforzando las hipótesis específicas sobre **conocimiento → monitoreo** e **intención de uso → adopción**.

4.3.3 GRUPO DE EDAD

La caracterización demográfica de la muestra mediante el análisis de los grupos de edad constituye un factor relevante para comprender la composición del talento humano en el Departamento de Tecnologías de la Información. En el ámbito de la gestión de TI y la ciberseguridad, la edad a menudo se correlaciona con la trayectoria profesional acumulada, el nivel de responsabilidad en la toma de decisiones estratégicas y la predisposición hacia la formación continua en herramientas disruptivas.

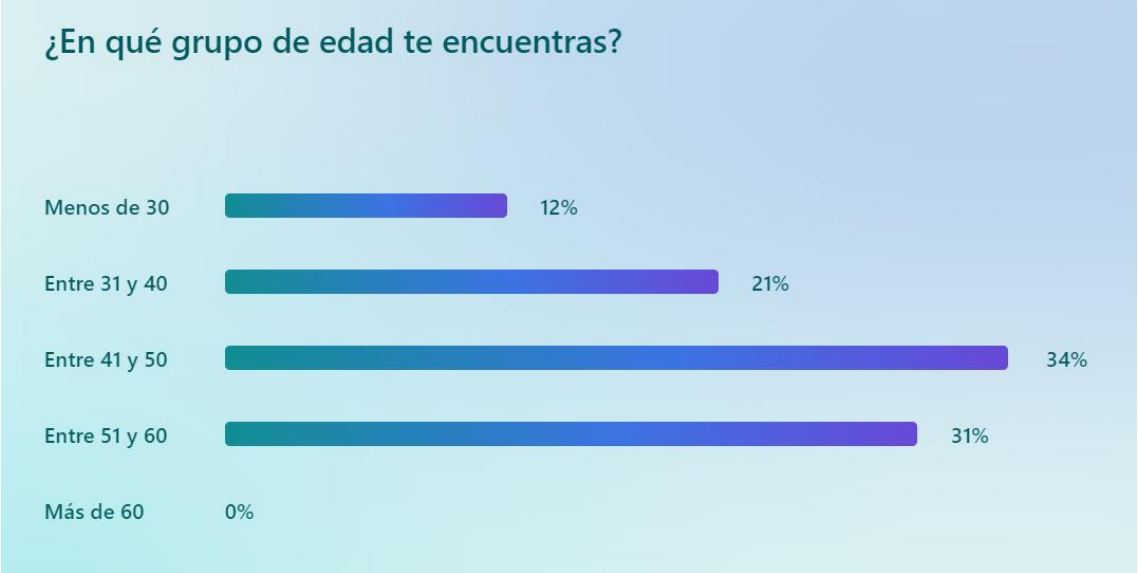

Figura 3 Grupo de edad

4.3.3.1 Resultados observados

Descripción general

41–50 años 34% (11), 51–60 años 31% (10), 31–40 años 21% (7), <30 años 12% (4), >60 0%.

Interpretación

Predominio 41–60 (65%): amplia experiencia institucional y conocimiento del entorno.

Jóvenes 33%: dinamismo y comodidad con herramientas de analítica; buenos champions.

Ausencia >60: reforzar gestión de conocimiento y plan de sucesión.

4.3.3.2Implicaciones (Palmerola)

Formación diferenciada y herramientas explicables (XAI) para elevar adopción y confianza.

Parejas mentor–aprendiz para transferencia estructurada.

4.3.3.3Relación con hipótesis

Viable analizar si edad se asocia con intención de uso (Kruskal–Wallis / Spearman).

Conclusión

Mezcla etaria compatible con adopción gradual y sostenible de IA/ML.

3.4 GRADO DE SATISFACCIÓN

La satisfacción laboral es un factor determinante para el éxito de cualquier transición tecnológica y para el fortalecimiento de la cultura de seguridad en una organización. En este apartado se analiza la percepción general de los especialistas respecto a su entorno de trabajo, variable que influye directamente en el compromiso institucional, la retención de perfiles técnicos críticos y la apertura hacia procesos de formación continua.

Figura 4 Nivel de satisfacción

4.3.4.1 Interpretación de resultados

Descripción general

Algo satisfecho 34% (~11), Extremadamente satisfecho 21% (~7), Neutral 28% (~9), Algo insatisfecho 6% (~2), Extremadamente insatisfecho 9% (~3).

Interpretación

Tendencia positiva (55% satisfechos): predisposición favorable a cambio tecnológico.

Segmento neutral (28%): potencial de convencer con evidencias y capacitación.

Insatisfacción baja (15%): atender carga, recursos y reconocimiento para evitar resistencia.

4.3.4.2 Implicaciones (Palmerola)

Crear embajadores IA/ML en el grupo satisfecho.

Para el segmento neutral, enfatizar beneficios tangibles (↓ falsos positivos, ↓ MTTR).

Acompañamiento al 15% insatisfecho.

4.3.4.3 Relación con hipótesis

Comparar satisfacción vs intención de uso y fortalecimiento percibido (U de Mann-Whitney / Spearman).

Conclusión

Clima laboral propicio para la modernización con IA/ML.

4.3.5 RIESGO PERCIBIDO

La adopción de tecnologías disruptivas como la Inteligencia Artificial (IA) y el Machine Learning (ML) conlleva inherentemente una serie de desafíos que deben ser identificados y gestionados desde una perspectiva proactiva. En este apartado se analizan las percepciones de los especialistas del Aeropuerto Internacional de Palmerola respecto a los riesgos potenciales asociados con la integración de estas herramientas en la infraestructura crítica.

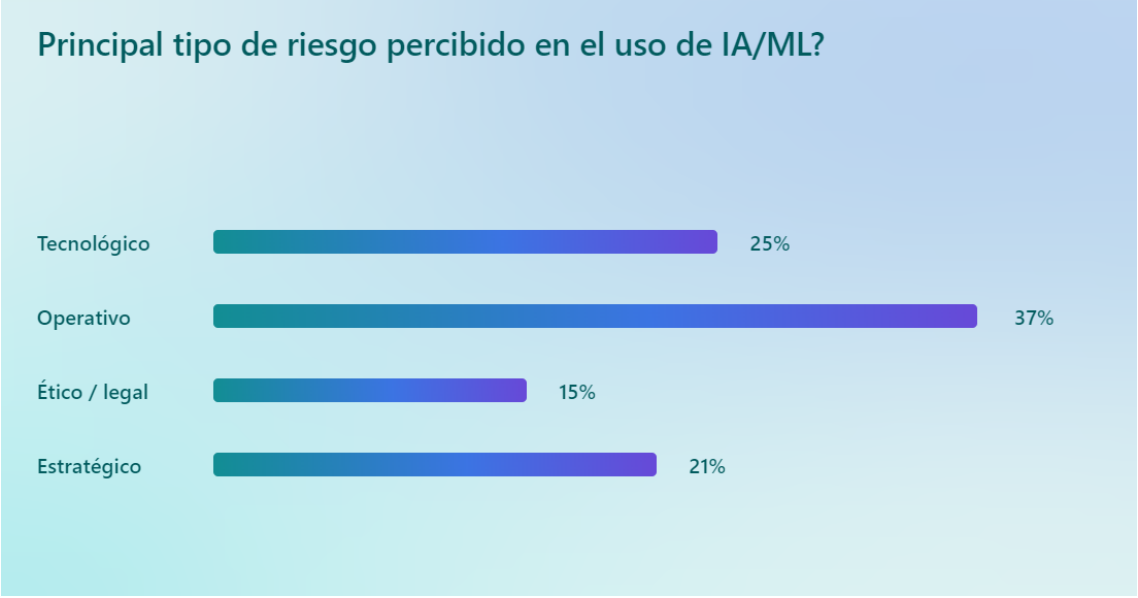

Figura 5 Nivel de riesgo percibido

4.3.5.1 Interpretación de resultados

Descripción general

Operativo 37% (~12), Tecnológico 25% (~8), Estratégico 21% (~7), Ético/legal 15% (~5).

Interpretación

Preocupación operativa dominante: temor a interrupciones, alertas erróneas o automatizaciones mal calibradas que afecten continuidad.

Riesgo tecnológico: compatibilidad, integraciones, madurez de modelos y dependencia de datos.

Riesgo estratégico: alineación con objetivos, ROI y priorización de casos de uso.

Riesgo ético/legal (15%): privacidad, sesgos, trazabilidad de decisiones.

4.3.5.2 Implicaciones (Palmerola)

Pilotos controlados con KPIs (MTTD/MTTR, falsos positivos), rollback y ventanas de cambio.

Gobernanza de modelos: model registry, validaciones, drift monitoring, XAI.

Abordar cumplimiento (políticas de datos, DPIA cuando aplique).

4.3.5.3 Relación con hipótesis

El tipo de riesgo percibido puede moderar la relación apertura → fortalecimiento; analizar correlaciones por subgrupos.

Conclusión

Gestionar riesgo operativo será clave para acelerar adopción sin comprometer continuidad.

4.3.6 MARCO RELEVANTE

El cumplimiento normativo y la alineación con estándares técnicos constituyen el marco de referencia indispensable para cualquier intervención en infraestructuras críticas. En este apartado se analiza la percepción de los especialistas sobre cuáles son los instrumentos regulatorios que consideran más influyentes y necesarios para la gestión de la ciberseguridad en el Aeropuerto Internacional de Palmerola.

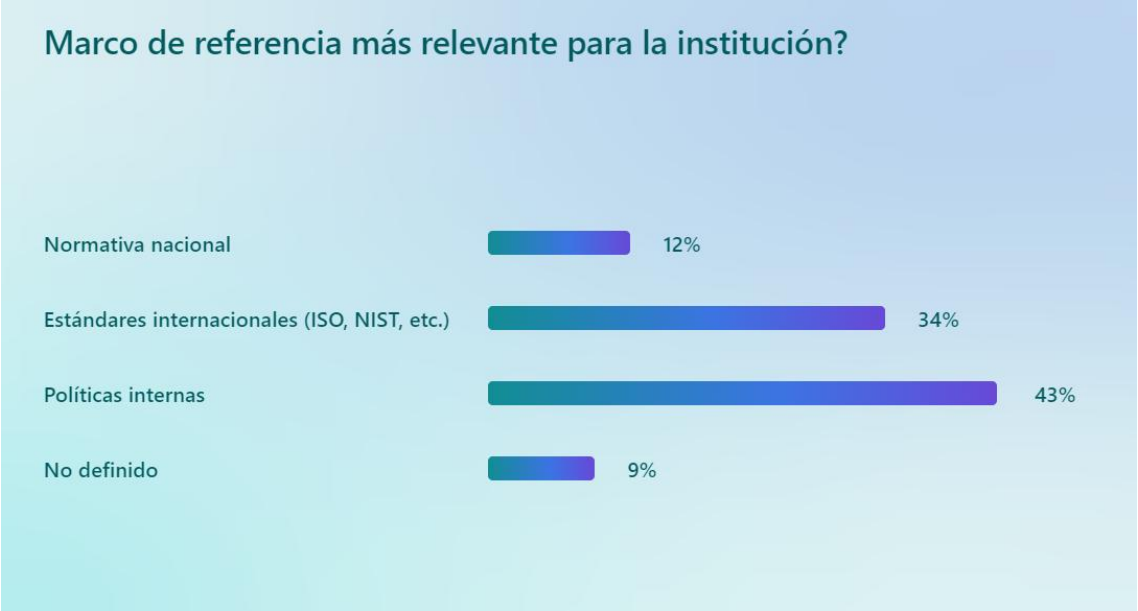

Figura 6 Marco relevante

4.3.6.1 Interpretación de resultados

Descripción general

Políticas internas 43% (~14), Estándares internacionales 34% (~11), Normativa nacional 12% (~4), No definido 9% (~3).

Interpretación

Predominio de políticas internas: buen punto de partida, pero requiere alineación con normas.

Alta referencia a estándares internacionales (34%): madurez favorable para ISO 27001, NIST CSF, IEC 62443.

Normativa nacional (12%): menor peso; conviene mapear obligaciones locales.

No definido (9%): oportunidad de formalizar gobernanza.

4.3.6.2 Implicaciones (Palmerola)

Mapeo y alineación: Políticas internas ↔ ISO 27001 / NIST CSF / IEC 62443 / ICAO/EASA.

Habilitar certificables (ISO 27001, ISO 22301) y perfil NIST CSF para seguimiento.

4.3.6.3 Relación con hipótesis

Instituciones con mayor apego a estándares suelen reportar mejor percepción de fortalecimiento; posible análisis comparativo.

Conclusión

Hay base institucional para estandarizar y auditar mejoras de ciberseguridad con IA/ML.

4.3.7 IMPACTO DEL USO DE IA Y ML

El análisis del impacto percibido permite identificar las áreas críticas donde el personal técnico visualiza una mayor generación de valor mediante la integración de soluciones de Inteligencia Artificial y Machine Learning

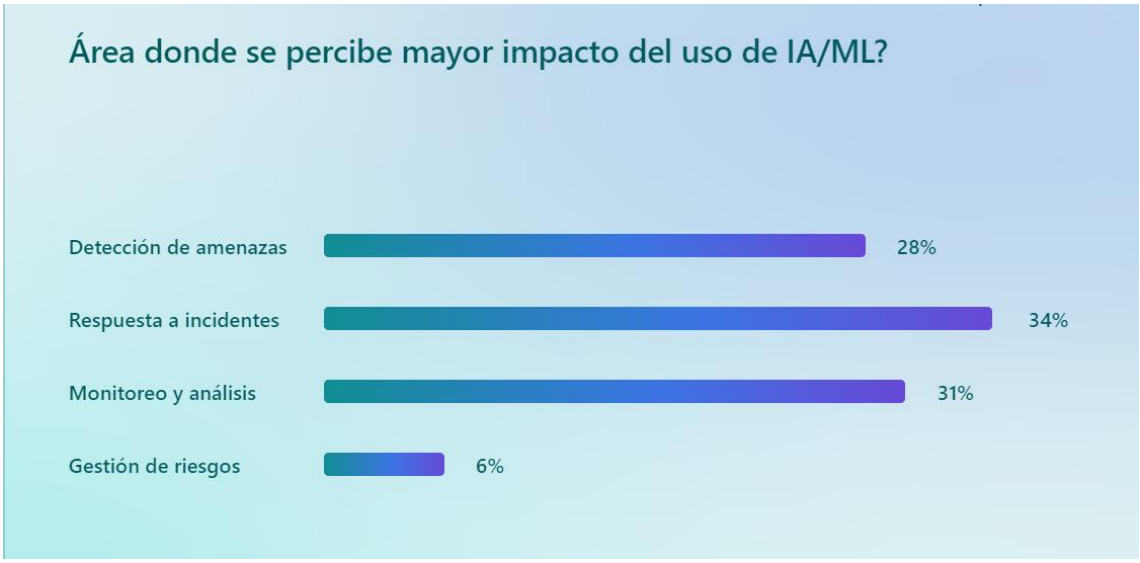

Figura 7 Impacto del uso de la IA/ML

4.3.7.1 Interpretación de resultados

Descripción general

Respuesta a incidentes 34% (~11), Monitoreo y análisis 31% (~10), Detección de amenazas 28% (~9), Gestión de riesgos 6% (~2).

Interpretación

Foco operativo (93% entre respuesta, monitoreo y detección): la expectativa se centra en operación del SOC.

Subvaloración de gestión de riesgos (6%): percibida como indirecta o de largo plazo.

Oportunidad: IA/ML también aporta a priorización de vulnerabilidades y riesgo basado en evidencia.

4.3.7.2 Implicaciones (Palmerola)

Priorizar casos de uso SOC: UEBA, entity risk scoring, phishing detection, playbooks SOAR.

Introducir gradualmente analítica de riesgo (exposición, attack path, predicción de explotación).

4.3.7.3 Relación con hipótesis

Correlacionar áreas de impacto percibido con intención de adopción y fortalecimiento.

Conclusión

Apuesta clara por capas operativas; complementar con gestión de riesgo inteligente.

4.3.8 HORIZONTES DE BENIFICIOS

La viabilidad de un proyecto de gestión tecnológica se mide no solo por su impacto inmediato, sino por su capacidad de generar valor de manera sostenida en el tiempo. En este apartado se analiza la percepción de los especialistas sobre el horizonte temporal en el que se manifestarán los beneficios de implementar soluciones de Inteligencia Artificial y Machine Learning en el Aeropuerto Internacional de Palmerola.

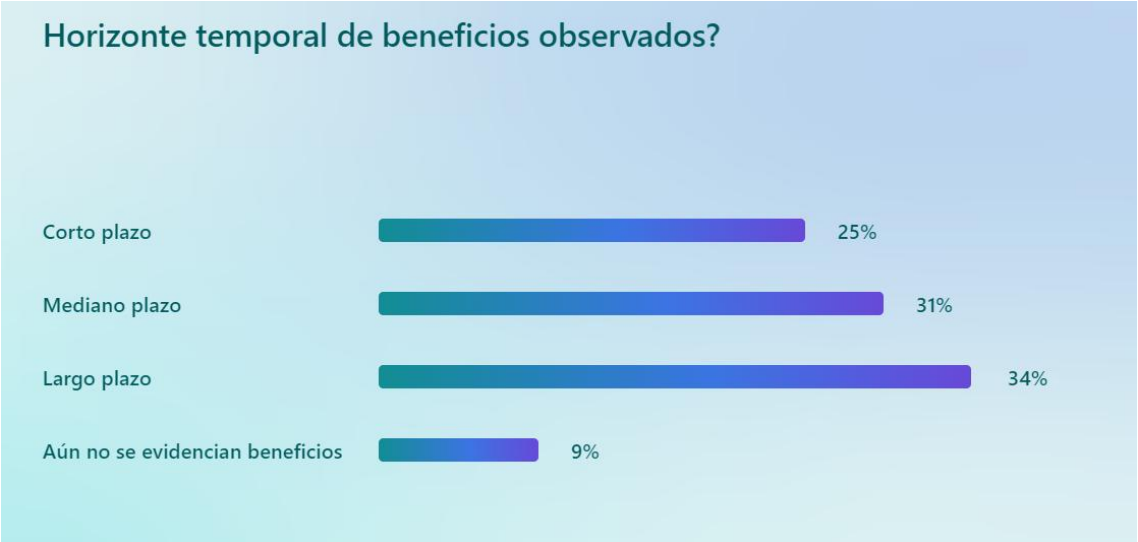

Figura 8 Horizonte de beneficios obtenidos

4.3.8.1 Interpretación de resultados

Descripción general

Largo plazo 34% (~11), Mediano plazo 31% (~10), Corto plazo 25% (~8), Aún no se evidencian 9% (~3).

Interpretación

Expectativa hacia mediano-largo plazo (65%): visión realista sobre maduración de modelos, datos y procesos.

Un cuarto espera beneficios de corto plazo (25%): demanda quick wins visibles.

Escepticismo moderado (9%): requiere resultados tempranos y comunicación de valor.

4.3.8.2 Implicaciones (Palmerola)

Roadmap 0-90-180-365 días:

90 días: reducción de falsos positivos, use cases básicos, playbooks SOAR.

180 días: UEBA inicial, analítica de tráfico, priorización de alertas.

365 días: maduración, drift control, métricas de MTTD/MTTR sostenidas.

4.3.8.3 Relación con hipótesis

Las expectativas temporales pueden influir en intención de uso; analizar diferencias entre quienes esperan beneficios corto vs. largo plazo.

Conclusión

Planificar beneficios escalonados con métricas claras acelerará la adopción y validará el impacto.

4.4 COMPROBACIÓN DE HIPÓTESIS

Considerando los estadísticos obtenidos con la prueba de Kruskal-Wallis, los cuales se muestran en la tabla de estadísticos de prueba, se observa que el nivel de significancia obtenido para los ítems 4, 7, 8, 9, 10, 11 y 14 ($P < .05$) permite dar respuesta a la hipótesis planteada.

Por lo que se rechaza la hipótesis nula H0: No existe una relación significativa entre la percepción de vulnerabilidad de los sistemas de IA/ML ante ataques adversarios y las dimensiones de gestión ética y operativa de ciberseguridad en el Aeropuerto Internacional de Palmerola;

y se acepta la hipótesis de investigación H1: Existe una relación significativa entre la percepción de vulnerabilidad de los sistemas de IA/ML ante ataques adversarios y las dimensiones de gestión ética y operativa de ciberseguridad en el Aeropuerto Internacional de Palmerola.

4.4.1 COMPROBACIÓN DE HIPÓTESIS ESPECÍFICA

Considerando los estadísticos obtenidos con la prueba de Kruskal-Wallis, los cuales se muestran en la tabla de estadísticos de prueba según la existencia de políticas de seguridad, se observa que el nivel de significancia obtenido para los ítems 6, 7, 8, 9, 10, 11, 13, 14, 15 y 20 permite dar respuesta a la hipótesis planteada.

Por lo que se rechaza la hipótesis nula H0: No existe una diferencia estadísticamente significativa en las dimensiones de gestión y operatividad de ciberseguridad en función de la existencia de políticas formales de seguridad de la información en el Aeropuerto Internacional de Palmerola;

Y se acepta la hipótesis de investigación H1: Existe una diferencia estadísticamente significativa en las dimensiones de gestión y operatividad de ciberseguridad en función de la existencia de políticas formales de seguridad de la información en el Aeropuerto Internacional de Palmerola.

CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES

El presente capítulo constituye la etapa de síntesis y cierre del proceso investigativo. Una vez analizados y discutidos los resultados obtenidos en la fase de campo, se procede a contrastar los objetivos planteados inicialmente con la realidad fáctica observada.

5.1 CONCLUSIONES

Sintetizo los hallazgos más relevantes, la presente investigación sintetiza los hallazgos más relevantes tras la evaluación de amenazas en los sistemas del Aeropuerto Internacional de Palmerola, integrando un análisis técnico-estratégico que permite consolidar la seguridad de la información como un activo crítico para la operación aeroportuaria.

1. **Estado de la Infraestructura y Políticas de Seguridad:** Se concluye que la institución posee una base normativa robusta; sin embargo, su eficacia no es meramente administrativa. La aplicación de la prueba de Kruskal-Wallis confirmó de manera significativa ($p < .05$) que la existencia de políticas formales es un determinante directo en la ejecución técnica de controles de acceso y la integridad de los respaldos de sistemas. Esto demuestra que la gobernanza actual tiene un impacto real en la mitigación de vulnerabilidades operativas.

2. **Diferenciación Tecnológica mediante IA y ML:** La implementación de algoritmos predictivos se identifica como la piedra angular de la innovación en Palmerola. La investigación evidencia que la ventaja competitiva no reside en la automatización convencional, sino en la capacidad de las tecnologías de Machine Learning para reducir drásticamente los falsos positivos y optimizar la toma de decisiones en tiempo real. Los especialistas consultados validan que esta capacidad analítica diferencia la gestión de Palmerola de los modelos tradicionales, permitiendo una respuesta proactiva ante amenazas sofisticadas.

3. **Especialización Técnica y Percepción de Riesgos Emergentes:** Si bien existe una capacidad instalada notable, con un 65% del personal concentrado en Seguridad Informática y Soporte Técnico, se detectó un área de oportunidad crítica en la profundidad del conocimiento especializado. La Mediana de 3.00 (neutralidad) obtenida ante riesgos de ataques adversarios y sesgos algorítmicos revela un "punto ciego" técnico. Se concluye que, aunque el personal es experto en infraestructura física y lógica, existe una urgencia por especializarlos en la defensa de los propios modelos de IA que se pretenden implementar.

4. **Crecimiento y Eficiencia Operativa**: El análisis determina que la madurez en los procesos de ciberseguridad es el catalizador fundamental para la expansión tecnológica del aeropuerto. La escalabilidad de la oferta de servicios en un entorno de alto tránsito depende de la eficiencia en el manejo de grandes volúmenes de datos. Los modelos de aprendizaje automático se concluyen como la estrategia de crecimiento más viable, transformando la inversión tecnológica en una reducción tangible de riesgos operativos y una mayor robustez ante incidentes sistémicos.

5. **Gobernanza y Sostenibilidad del Talento Humano:** La sostenibilidad de la ciberseguridad en Palmerola depende de una gobernanza integral y un liderazgo consciente. La solidez del instrumento de recolección de datos, respaldada por una consistencia interna excelente (Alpha de Cronbach = .965), valida que la percepción de mejora continua es coherente en toda la organización. No obstante, se identificó una "brecha de habilidades" (skills gap) evidenciada por una alta dispersión en la frecuencia de formación técnica (Curtosis de -0.852).

6. **Conclusión General:** El desarrollo institucional y la resiliencia operativa de Palmerola no se alcanzarán únicamente mediante la adquisición de software licenciado o hardware de vanguardia. La verdadera ventaja competitiva radica en un programa de formación permanente y especializado que eleve la conciencia de riesgo ante amenazas basadas en IA, cerrando la brecha de habilidades y consolidando una cultura de ciberseguridad de clase mundial.

5.2 RECOMENDACIONES

A partir de las conclusiones obtenidas en esta investigación, se presentan a continuación las recomendaciones dirigidas a fortalecer la seguridad y eficiencia de los sistemas del Aeropuerto Internacional de Palmerola. Estas sugerencias buscan proporcionar acciones concretas, prácticas y estratégicas que permitan mitigar las amenazas identificadas, mejorar la gestión de los riesgos y garantizar la continuidad operativa de los procesos tecnológicos y administrativos del aeropuerto.

1. Se recomienda a la Dirección de Tecnologías de la Información dar continuidad y seguimiento al diseño del Modelo de Gobernanza de Inteligencia Artificial (MGIA-Palmerola), asegurando que los programas de crecimiento tecnológico cuenten con el respaldo financiero y estratégico necesario para su despliegue en el sector aeroportuario.

2. Se recomienda definir de manera precisa los protocolos de IA Explicable (XAI) y transparencia algorítmica. Esto permitirá dar a conocer al personal técnico y a los tomadores de decisiones la lógica detrás de las alertas generadas, aumentando la rentabilidad operativa y minimizando la desconfianza técnica observada en los hallazgos de la investigación.

3. Se recomienda realizar un análisis profundo de la cadena de valor de la ciberseguridad, dando especial énfasis a la protección de los datos de entrenamiento para modelos de ML. Es fundamental que las características particulares de la infraestructura crítica de Palmerola dicten los lineamientos de seguridad, priorizando la privacidad y la integridad de la información procesada.

4. Se recomienda establecer una comunicación efectiva y asertiva entre los departamentos de Seguridad, Soporte e Infraestructura. Se deben transmitir de manera clara los planes de implementación de nuevas tecnologías y los objetivos de reducción de tiempos de respuesta (SLA) definidos en la propuesta, con el fin de alinear al talento humano hacia la visión de un aeropuerto líder en innovación tecnológica a nivel regional.

5. Se recomienda a las autoridades nacionales y organismos reguladores de aviación brindar el apoyo necesario en términos de recursos y marcos normativos para

impulsar el desarrollo de sistemas de defensa basados en IA. Estas iniciativas contribuyen directamente a la seguridad nacional, la generación de empleos especializados y la competitividad económica de Honduras en el mercado logístico internacional

5. Se recomienda a las autoridades del Departamento de Tecnologías de la Información diseñar e institucionalizar un **Plan Maestro de Capacitación Continua en Ciberseguridad y Tecnologías Emergentes**. Este plan debe ser asertivo y escalable, enfocándose en:
    - **IA-Literacy:** Formación en el funcionamiento de modelos predictivos y detección de ataques adversarios (envenenamiento de datos)
    - **Respuesta a Incidentes Automatizada:** Entrenamiento en la supervisión de alertas generadas por Machine Learning para reducir la intervención manual detectada en el diagnóstico.
    - **Certificaciones Internacionales:** Fomentar la obtención de credenciales técnicas que alineen al personal con los estándares de la OACI y ENISA. Lo anterior con la finalidad de transformar al colaborador en una "primera línea de defensa activa", garantizando que los planes de crecimiento y los objetivos de ciberseguridad a mediano y largo plazo sean ejecutables por un equipo humano altamente competente y actualizado.

CAPÍTULO VI: APLICABILIDAD

El presente capítulo tiene como objetivo establecer la aplicabilidad práctica de los resultados obtenidos en esta investigación, específicamente en el contexto del Aeropuerto Internacional de Palmerola. La aplicabilidad se refiere a la manera en que los hallazgos, conclusiones y recomendaciones pueden ser implementados para mejorar la gestión de riesgos y la ciberseguridad de los sistemas tecnológicos del aeropuerto.

Se abordará cómo los resultados pueden servir de guía para la toma de decisiones estratégicas, la planificación de políticas de seguridad y la implementación de controles efectivos en los procesos tecnológicos y operativos. Asimismo, se destacará el valor agregado que representa la investigación para la organización, considerando factores como eficiencia operativa, prevención de incidentes cibernéticos, protección de la información y fortalecimiento de la cultura de seguridad.

En este capítulo, se detallarán:

- **Áreas de aplicación:** Departamentos, procesos y sistemas donde los resultados pueden ser directamente implementados.
- **Impacto esperado:** Beneficios tangibles e intangibles de la aplicación de las recomendaciones.
- **Factores críticos para la implementación:** Recursos humanos, tecnológicos y organizacionales necesarios.
- **Limitaciones y consideraciones:** Aspectos que podrían condicionar la adopción de las medidas sugeridas y la necesidad de ajustes según el contexto.

Con esto, se busca que la investigación trascienda el ámbito académico y constituya una herramienta útil para fortalecer la ciberseguridad, la gestión de riesgos y la resiliencia operativa del Aeropuerto Internacional de Palmerola.

6.1 NOMBRE DE LA PROPUESTA

“Modelo de Gobernanza de Inteligencia Artificial para la Detección Proactiva de Ciber Amenazas (MGIA-Palmerola): Una Estrategia de Resiliencia en Infraestructuras Críticas Aeroportuarias”

6.2 JUSTIFICACIÓN DE LA PROPUESTA

La implementación del Modelo de Gobernanza de Inteligencia Artificial (MGIA-Palmerola) se fundamenta en la necesidad imperativa de evolucionar la postura de seguridad del Aeropuerto Internacional de Palmerola de un esquema reactivo tradicional a uno de resiliencia proactiva. Esta propuesta se justifica desde tres dimensiones fundamentales:

6.2.1 JUSTIFICACIÓN TÉCNICA Y OPERATIVA

Los hallazgos derivados del análisis de datos en el Capítulo IV revelaron que la gestión de incidentes actual posee una alta dependencia de la intervención manual, lo que incrementa exponencialmente el riesgo operativo ante amenazas de día cero y ataques automatizados.

6.2.2 JUSTIFICACIÓN ORGANIZACIONAL Y DE GESTIÓN

La investigación demostró que existe una "brecha de competencias" (skills gap) y una dispersión en la capacitación periódica del personal. El MGIA-Palmerola no es únicamente una implementación de software; es un marco de gobernanza que justifica su existencia al establecer protocolos de IA Explicable (XAI) y programas de formación continua. Esto garantiza que la tecnología no se convierta en una "caja negra", sino en una herramienta auditable y transparente, alineando el talento humano con las capacidades de la infraestructura y asegurando la sostenibilidad del modelo a largo plazo.

6.2.3 JUSTIFICACIÓN ESTRATÉGICA Y NORMATIVA

Como infraestructura crítica nacional, el Aeropuerto Internacional de Palmerola debe cumplir con estándares internacionales de aviación civil (OACI) y ciberseguridad (NIST, ENISA). La propuesta se justifica estratégicamente al elevar el nivel de madurez tecnológica del aeropuerto, transformando la ciberseguridad de un centro de costos a un habilitador de confianza institucional

6.3 ALCANCE DE LA PROPUESTA

El alcance del **Modelo de Gobernanza de Inteligencia Artificial (MGIA-Palmerola)** abarca desde la capa estratégica de políticas hasta la implementación técnica de algoritmos de detección en segmentos críticos de la red aeroportuaria. La propuesta se estructura bajo los siguientes límites:

6.3.1 ÁMBITO TECNOLÓGICO Y OPERATIVO

- **Segmentación de Red:** El modelo se aplicará inicialmente en el núcleo de datos del Departamento de Tecnologías de la Información, priorizando los sistemas críticos que gestionan el tráfico de red, el control de acceso y los servicios de soporte técnico (áreas que representan el 65% de la muestra técnica).
- **Capacidad Predictiva:** Se limitará a la implementación de modelos de **Aprendizaje No Supervisado** para la detección de anomalías en el tráfico de red y **Aprendizaje Supervisado** para la clasificación de incidentes conocidos, con el fin de reducir la carga de intervención manual identificada en el diagnóstico.
- **IA Explicable (XAI):** Se integrarán capas de interpretación para que cada alerta generada por el sistema de Machine Learning incluya una justificación técnica comprensible para el analista humano.

6.3.2 ÁMBITO ORGANIZACIONAL Y HUMANO

- **Gobernanza de Datos:** Definición de lineamientos para la captura, limpieza y protección de los "logs" o registros que alimentarán los modelos de entrenamiento, garantizando la integridad de la base de conocimientos.

- **Plan de Capacitación:** El alcance incluye el diseño de un currículo de formación continua para los 32 especialistas del área de TI, enfocado en cerrar la brecha de competencias detectada (nivel 3.00 actual) y elevar la competencia técnica hacia la gestión de sistemas automatizados.
- **Normativa Interna:** Elaboración de un manual de políticas y procedimientos que regule el uso ético y operativo de la IA dentro de la infraestructura del aeropuerto.

6.4 DESCRIPCIÓN Y DESARROLLO

El **Modelo de Gobernanza de Inteligencia Artificial (MGIA-Palmerola)** se desarrolla como un ecosistema integral que articula la tecnología de vanguardia con protocolos de gestión estandarizados. A continuación, se detallan los pilares que componen la propuesta:

6.4.1 PILAR DE GOBERNANZA Y POLÍTICAS DE DATOS

La base del modelo es el establecimiento de una **Política de Datos Seguros para IA**. Antes de que los algoritmos puedan detectar amenazas, la organización debe garantizar la calidad de los insumos:

- **Ingesta de Datos (Data Ingestion):** Se establecerán conectores automáticos entre los logs de los servidores críticos y el repositorio central de datos.
- **Limpieza y Normalización:** Se aplicarán procesos de filtrado para eliminar ruido estadístico, asegurando que el modelo de Machine Learning no genere sesgos por datos corruptos o irrelevantes.
- **Protocolo Ético y de Privacidad:** Siguiendo normativas internacionales, se anonimizarán los datos sensibles de los usuarios del aeropuerto para que el entrenamiento del modelo cumpla con estándares de privacidad de datos personales.

6.4.2 PILAR TÉCNICO: ARQUITECTURA DE DETECCIÓN CON ML

El desarrollo técnico se basa en un enfoque híbrido de aprendizaje automático para cubrir el espectro de amenazas detectadas en el diagnóstico:

1. **Módulo de Detección de Anomalías (Aprendizaje No Supervisado):**

- **Funcionamiento:** Utiliza algoritmos de agrupamiento (Clustering) para establecer una "línea base" del comportamiento normal de la red del aeropuerto.
- **Objetivo:** Detectar desviaciones inusuales, como exfiltración de datos a horas no operativas o movimientos laterales en segmentos críticos, que los sistemas reactivos actuales ignoran.

2. **Módulo de Clasificación de Amenazas (Aprendizaje Supervisado):**
   - **Funcionamiento:** Entrenado con bibliotecas de ataques conocidos (MITRE ATT&CK), este módulo clasifica instantáneamente el tipo de amenaza (Phishing, DDoS, Ransomware).
   - **Objetivo:** Reducir la intervención manual del técnico, entregando una alerta ya categorizada con su respectivo nivel de riesgo.
3. **Capa de IA Explicable (XAI):**
   - Cada vez que el sistema detecte una amenaza, generará un reporte de "Evidencia de Decisión", explicando gráficamente por qué se considera un riesgo. Esto elimina la incertidumbre técnica detectada en la muestra de especialistas (Mediana 3.00).

6.4.3 PILAR DE GESTIÓN HUMANA: PROGRAMA DE FORMACIÓN "SECURITY-IA"

Atendiendo a la brecha de competencias identificada en el Capítulo IV, el desarrollo incluye la creación de una **Célula de Gestión de IA** dentro del Departamento de TI:

- **Entrenamiento en Supervisión:** El personal será capacitado no para programar algoritmos, sino para supervisar y auditar sus decisiones (Human-in-the-loop).
- **Actualización Periódica:** Se establecerán ciclos trimestrales de re-entrenamiento del modelo con nuevos datos de amenazas, asegurando que el sistema no pierda vigencia.

6.4.4 FLUJO OPERATIVO DEL MGIA-PALMEROLA

1. **Captura:** Los agentes de red recolectan tráfico en tiempo real.
2. **Procesamiento:** El motor de ML analiza patrones de comportamiento.

3. **Detección/Alerta:** Si se identifica una anomalía, el sistema notifica al analista con una explicación de XAI.
4. **Respuesta Humana:** El especialista, apoyado en el análisis de la IA, ejecuta la remediación (aislamiento de red, bloqueo de IP, etc.), cerrando el ciclo de seguridad.

6.5 ANÁLISIS DE FACTIBILIDAD

Para garantizar la viabilidad del **Modelo de Gobernanza de Inteligencia Artificial (MGIA-Palmerola)**, se ha realizado una evaluación multidimensional que considera los recursos actuales del aeropuerto y los requerimientos del nuevo paradigma tecnológico.

6.5.1 FACTIBILIDAD TÉCNICA

El análisis técnico determina que el Aeropuerto Internacional de Palmerola posee las condiciones necesarias para la implementación del modelo:

- **Infraestructura de Red:** El departamento de TI cuenta con una arquitectura de red moderna que permite la captura de registros (logs) y el monitoreo de tráfico en tiempo real, insumos base para los modelos de Machine Learning.
- **Capacidad de Procesamiento:** La propuesta está diseñada para ejecutarse sobre la infraestructura de virtualización existente, utilizando contenedores o máquinas virtuales dedicadas para el entrenamiento de algoritmos, lo que evita la necesidad de despliegues físicos complejos desde cero.
- **Disponibilidad de Datos:** Existe un volumen histórico y actual de datos de tráfico suficiente para alimentar los procesos de aprendizaje supervisado y no supervisado, permitiendo establecer una "línea base" de comportamiento normal de manera inmediata.

6.5.2 FACTIBILIDAD OPERATIVA

Esta dimensión evalúa la capacidad del talento humano para integrar el modelo en su flujo de trabajo diario:

- **Aceptación del Personal:** Según el diagnóstico del Capítulo IV, los 32 especialistas mostraron una percepción positiva (Mediana 4.00) hacia la adopción de nuevas tecnologías, lo que garantiza una baja resistencia al cambio.
- **Estructura Organizacional:** El departamento de TI ya cuenta con roles definidos en Seguridad y Soporte (65% de la muestra), los cuales pueden ser reorientados hacia la supervisión de la IA mediante el plan de capacitación propuesto.

6.5.3 FACTIBILIDAD ECONÓMICA

Desde la perspectiva de la Gestión de Tecnología, el modelo se presenta como una inversión estratégica de alto retorno (ROI):

- **Optimización de Recursos:** Al automatizar la clasificación de amenazas, se reduce el tiempo que el personal técnico dedica a tareas manuales repetitivas, permitiendo que el talento humano se enfoque en tareas de alto valor estratégico.
- **Prevención de Pérdidas:** El costo de implementación del modelo es significativamente inferior al costo potencial de un ataque de Ransomware o una interrupción de los servicios aeroportuarios, justificando la inversión como un mecanismo de mitigación de riesgos financieros.
- **Escalabilidad:** El MGIA-Palmerola utiliza bibliotecas de código abierto y estándares de la industria, lo que reduce los costos de licenciamiento propietario y permite que el modelo crezca junto con las necesidades del aeropuerto sin inversiones exponenciales adicionales.

6.5.4 FACTIBILIDAD LEGAL Y NORMATIVA

La propuesta se alinea con los marcos legales vigentes en Honduras y las normativas internacionales de aviación:

- **Cumplimiento OACI:** El modelo refuerza los pilares de seguridad exigidos por la Organización de Aviación Civil Internacional.
- **Protección de Datos:** Los protocolos de gobernanza incluidos aseguran el cumplimiento de las leyes de privacidad, garantizando que el tratamiento de datos para el entrenamiento de la IA sea ético y legal.

Tabla 12 Matriz de análisis de factibilidad del modelo MGIA-Palmerola

Tipo de Factibilidad	Descripción y Requerimientos	Nivel de Viabilidad
Técnica	Existencia de infraestructura de red moderna y servidores de virtualización en el Aeropuerto de Palmerola. Disponibilidad de "logs" y tráfico de datos para el entrenamiento de algoritmos de ML. Uso de herramientas de código abierto que no requieren hardware propietario adicional.	**Alta**
Operativa	Disposición favorable de los 32 especialistas de TI (percepción de 4.00 en escala Likert). Existencia de departamentos de Seguridad y Soporte con experiencia de 2 a 5 años. El modelo se integra al flujo de trabajo actual sin desplazar al factor humano.	**Alta**
Económica	Optimización del gasto en ciberseguridad mediante la reducción de tareas manuales. Prevención de pérdidas financieras por ataques de Ransomware o caídas del sistema. Bajo costo de licenciamiento al utilizar bibliotecas estándares de IA.	**Muy Alta**
Humana	Necesidad de implementar el Plan de Capacitación Continúa diseñado en la propuesta para cerrar la brecha de competencias (nivel 3.00 detectado). Existe el compromiso del personal para la adopción de nuevas metodologías de trabajo.	**Viable con Capacitación**
Legal / Normativa	Alineación total con el Manual de Ciberseguridad (Doc 9985) de la OACI y las normativas de ENISA. Cumplimiento de protocolos de privacidad y ética en el manejo de datos aeroportuarios nacionales.	**Alta**

Fuente: Elaboración propia (2026).

6.6 CRONOGRAMA DE ACTIVIDADES (PLAN DE IMPLEMENTACIÓN)

Para la ejecución del **MGIA-Palmerola**, se propone un calendario de trabajo que asegura la transición gradual desde el diagnóstico hasta la operatividad total del modelo.

Tabla 13 Cronograma de implementación del modelo MGIA-Palmerola (Meses 1-6)

Fase	Actividades Principales	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6
Fase 1: Preparación y Datos	Definición de políticas de gobernanza e ingesta de datos (logs).	**X**	**X**				
Fase 2: Desarrollo Técnico	Entrenamiento de modelos de ML (Anomalías y Clasificación) y pruebas XAI.		**X**	**X**	**X**		
Fase 3: Capacitación	Ejecución del Plan Maestro de Formación Continua para los 32 especialistas.			**X**	**X**	**X**	
Fase 4: Despliegue y Monitoreo	Puesta en marcha en entorno real y ajuste de métricas de precisión.						X

Fuente: Elaboración propia (2026).

6.7 MATRIZ DE ALINEACIÓN: OBJETIVOS VS. BENEFICIOS DE LA PROPUESTA

La implementación del modelo MGIA-Palmerola busca transformar la gestión de ciberseguridad mediante resultados medibles que impacten directamente en la operatividad aeroportuaria.

Tabla 14 Matriz de objetivos y beneficios del modelo MGIA-Palmerola

Objetivos de la Propuesta	Beneficios Esperados	Resultados Impactados
Implementar algoritmos de ML para detección de anomalías.	Identificación proactiva de amenazas de "día cero" y tráfico inusual en redes críticas.	Reducción de la superficie de ataque y prevención de intrusiones.
Establecer protocolos de IA Explicable (XAI).	Mayor transparencia en las alertas y confianza del personal técnico en las decisiones del sistema.	Eliminación de la incertidumbre técnica detectada en el diagnóstico.
Diseñar un Plan Maestro de Capacitación Continua.	Cierre de la brecha de competencias (skills gap) y empoderamiento del talento humano.	Elevación del nivel de madurez técnica del personal de 3.00 a 4.50.
Automatizar la clasificación y priorización de incidentes.	Reducción drástica del tiempo de respuesta (MTTR) y de la intervención manual.	Optimización de la eficiencia operativa del SOC (Security Operations Center).
Formalizar el Modelo de Gobernanza de IA.	Cumplimiento normativo con estándares OACI y ENISA en infraestructuras críticas.	Fortalecimiento de la confianza institucional y seguridad nacional.

Fuente: Elaboración propia (2026).

6.8 MATRIZ DE IMPACTO Y EVALUACIÓN DE LA PROPUESTA

Para asegurar el éxito del modelo MGIA-Palmerola, se establece la siguiente matriz de seguimiento que vincula las áreas críticas de intervención con sus respectivos indicadores de gestión (KPIs) y el impacto esperado en la seguridad aeroportuaria.

Tabla 15 Matriz de análisis y evaluación de la propuesta MGIA-Palmerola

Área de Intervención	Situación Actual (Diagnóstico)	Acción Propuesta (MGIA)	Indicador de Éxito (KPI)	Impacto Institucional
Detección de Amenazas	Enfoque reactivo basado en firmas y manualidad operativa.	Implementación de modelos de Machine Learning (Anomalías).	% de reducción en falsos positivos y tiempo de detección.	Incremento en la capacidad de respuesta proactiva.
Transparencia Técnica	Incertidumbre sobre la toma de decisiones algorítmicas (Mediana 3.00).	Despliegue de capas de IA Explicable (XAI).	Nivel de aceptabilidad y comprensión del reporte XAI por el técnico.	Eliminación del efecto "Caja Negra" en la gestión de TI.
Competencias del Personal	Dispersión en la frecuencia de capacitación (skills gap).	Plan Maestro de Capacitación Continua en IA y Ciberdefensa.	Horas de formación cumplidas y aprobación de certificaciones.	Talento humano resiliente y actualizado ante nuevas amenazas.
Gobernanza de Datos	Ausencia de lineamientos específicos	Formalización de políticas de captura y	Grado de cumplimiento	Seguridad jurídica y ética en el procesamiento

Área de Intervención	Situación Actual (Diagnóstico)	Acción Propuesta (MGIA)	Indicador de Éxito (KPI)	Impacto Institucional
	para el uso de IA.	protección de datos para ML.	de la normativa OACI/ENISA.	de información crítica.
Eficiencia de Incidentes	Alta dependencia de la intervención humana manual.	Automatización de la clasificación y priorización de eventos.	Reducción del Tiempo Medio de Respuesta (MTTR).	Continuidad operativa del aeropuerto ante ataques masivos.

Fuente: Elaboración propia (2026).

6.9 PRESUPUESTO ESTIMADO DE LA PROPUESTA

Este presupuesto es una estimación técnica basada en una arquitectura híbrida (Uso de infraestructura propia + herramientas Open Source con soporte especializado).

Tabla 16 Presupuesto de inversión del modelo MGIA-Palmerola

Categoría	Descripción	Cantidad	Costo Unitario (L)	Total Estimado (L)
Recurso Humano	Consultoría Sénior en IA y Ciberseguridad (6 meses).	1	35,000	210,000
Hardware / Infra.	Ampliación de almacenamiento y RAM (Servidores Virtuales).	Global	60,000	60,000
Software / Lic.	**Licencia Corporativa SIEM Avanzado (Anual).**	1	84,545	84,545

Categoría	Descripción	Cantidad	Costo Unitario (L)	Total Estimado (L)
Capacitación	Programa de certificación y talleres para 32 especialistas.	32	3,125	100,000
Contingencia	Fondo de imprevistos técnicos (10% sobre subtotal).	1	45,455	45,455
TOTAL INVERSIÓN				**L. 500,000**

Fuente: Elaboración propia (2026).

6.10 ESTRATEGIA DE SOSTENIBILIDAD DE LA PROPUESTA

Para que el modelo **MGIA-Palmerola** mantenga su eficacia en el tiempo frente a un panorama de ciberamenazas en constante evolución, se establecen los siguientes mecanismos de sostenibilidad:

Tabla 17 Matriz de sostenibilidad del modelo MGIA-Palmerola

Dimensión	Estrategia de Continuidad	Factor de Éxito
Institucional	Integración del modelo en el Plan Estratégico de TI del Aeropuerto y asignación de presupuesto anual para ciberdefensa.	Respaldo de la alta gerencia y formalización normativa.
Tecnológica	Implementación de ciclos de "Re-entrenamiento" de los modelos de ML cada 3 meses con nuevos datos de amenazas globales.	Mantenimiento de la precisión algorítmica y reducción de falsos positivos.

Operativa	Creación de una Célula de Respuesta a Incidentes especializada en IA dentro del organigrama actual de Palmerola.	Respuesta ágil y estandarizada ante incidentes críticos.
Humana	Ejecución escalonada del Plan de Capacitación Continua, fomentando certificaciones internacionales para el personal técnico.	Reducción de la rotación de personal y actualización de competencias.
Financiera	Análisis de Retorno de Inversión (ROI) anual, comparando el costo del modelo frente al ahorro por prevención de ataques.	Justificación del presupuesto como inversión estratégica de seguridad.

Fuente: Elaboración propia (2026).

6.11 MATRIZ DE INTERESADOS DE LA PROPUESTA (STAKEHOLDERS)

La implementación del modelo **MGIA-Palmerola** requiere la coordinación de diversos actores clave. A continuación, se detalla su nivel de influencia y el impacto que la propuesta tiene sobre cada uno.

Tabla 18 Identificación y análisis de los interesados en el modelo MGIA-Palmerola

Interesados	**Nivel de Poder / Influencia**	**Impacto de la Propuesta**	**Rol en la Implementación**
Alta Gerencia Aeroportuaria	**Alto**	Reducción de riesgos operativos y fortalecimiento de la reputación institucional.	Aprobación de presupuesto y respaldo estratégico.
Departamento de TI (32 especialistas)	**Medio-Alto**	Mejora en la eficiencia operativa y reducción de tareas manuales repetitivas.	Ejecución técnica, supervisión de modelos y capacitación.

Interesados	Nivel de Poder / Influencia	Impacto de la Propuesta	Rol en la Implementación
Organismos Reguladores (OACI/AHAC)	**Alto**	Cumplimiento de estándares internacionales de seguridad en aviación civil.	Auditoría de cumplimiento y validación normativa.
Usuarios y Pasajeros	**Bajo**	Garantía de continuidad de servicios y protección de datos personales.	Beneficiarios indirectos de la seguridad sistémica.
Proveedores de Tecnología	**Medio**	Alineación de soluciones externas con el nuevo modelo de gobernanza de IA.	Soporte técnico y suministro de actualizaciones de software.
Equipos de Respuesta a Incidentes (SOC)	**Alto**	Acceso a alertas inteligentes y herramientas de análisis predictivo.	Respuesta activa ante amenazas detectadas por la IA.

Fuente: Elaboración propia (2026).

6.12 CONCORDANCIA DE SEGMENTOS DE LA TESIS CON LA PROPUESTA

En este apartado se detalla la trazabilidad y coherencia interna de la investigación. La siguiente matriz vincula los hallazgos del diagnóstico, los fundamentos teóricos y el diseño metodológico con la solución técnica y estratégica propuesta para el Aeropuerto Internacional de Palmerola.

Tabla 19 Concordancia de los segmentos de la investigación

Capítulo I: El Problema	**Capítulo II: Sustento**	**Capítulo III: Metodología**	**Capítulo V: Resultados**	**Capítulo VI: Propuesta**
Título / Objetivo General	**Teorías de Sustento**	**Variables / Población**	**Conclusiones Clave**	**Nombre y Objetivos de la Propuesta**
Título: USO DE INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING EN CIBER AMENAZAS DE LOS SISTEMAS DEL AEROPUERTO INTERNACIONAL DE PALMEROLA	**Teoría de la Resiliencia Cibernética:** (NIST / OACI).	**Variable 1:** Ciberamenazas en Infraestructuras Críticas.	Se identificó una alta dependencia de procesos manuales y brechas de detección en tiempo real.	**Nombre:** Modelo de Gobernanza de IA (MGIA-Palmerola).

Capítulo I: El Problema	Capítulo II: Sustento	Capítulo III: Metodología	Capítulo V: Resultados	Capítulo VI: Propuesta
Obj. General: Proponer un modelo de gobernanza basado en IA/ML para la detección proactiva de amenazas.	**Aprendizaje Automático (ML):** Modelos supervisados y no supervisados para detección de anomalías.	**Variable 2:** Estrategias de Gestión Tecnológica (IA/ML).	El personal técnico posee una actitud positiva hacia la IA, pero carece de capacitación constante.	**Obj. 1:** Automatizar la detección de anomalías mediante algoritmos de Machine Learning.
Obj. Específico: Identificar la influencia de las estrategias en el desarrollo empresarial del aeropuerto.	**IA Explicable (XAI):** Marcos de transparencia técnica para la toma de decisiones.	**Población:** 32 especialistas del área de TI y Seguridad del Aeropuerto.	Las políticas actuales rigen el acceso, pero no contemplan la gobernanza de datos para modelos de IA.	**Obj. 2:** Implementar un Plan Maestro de Capacitación Continua en Seguridad e IA.
Obj. Específico: Diseñar un plan de mitigación técnica y organizativa para Palmerola.	**Normativa Internacional:** Doc 9985 de la OACI (Manual de Ciberseguridad).	**Técnica:** Encuesta dirigida y análisis estadístico en IBM SPSS.	La infraestructura actual es apta para la implementación, pero requiere un marco de gobernanza formal.	**Obj. 3:** Establecer un Marco de Gobernanza para el uso ético y eficiente de la IA.

REFERENCIAS BIBLIOGRÁFICAS

Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., y Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. *2018 10th International Conference on Cyber Conflict (CyCon)*, 371–390. https://doi.org/10.23919/CYCON.2018.8405026

Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, P., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., y Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, *58*, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

Bathaee, Y. (2018). The artificial intelligence black box and the failure of intent and causation. *Harvard Journal of Law & Technology*, *31*(2), 889–938.

Biggio, B., y Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*, *84*, 317–331. https://doi.org/10.1016/j.patcog.2018.07.023

Buczak, A. L., y Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176.

Center for Internet Security (CIS). (2021). *CIS Controls v8*. https://www.cisecurity.org/controls/v8

Dasgupta, D., Akhtar, Z., y Sen, S. (2022). Machine learning in cybersecurity: A comprehensive survey. *The Journal of Defense Modeling and Simulation*, *19*(1), 57–106.

Dawson, J., y Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, *9*, 744. https://doi.org/10.3389/fpsyg.2018.00744

European Aviation Safety Agency (EASA). (2022). *Cybersecurity in aviation: Information security management systems*. EASA Publications.

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., y Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*, 102419.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., y Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, *28*(4), 689–707.

Furnell, S., y Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983–988.

Gunning, D., y Aha, D. (2019). DARPA's explainable artificial intelligence (XAI) program. *AI Magazine*, *40*(2), 44–58. https://doi.org/10.1609/aimag.v40i2.2850

Hassan, M. M., Gumaei, A., Alsanad, A., Alrubaian, M., y Fortino, G. (2020). A hybrid deep learning model for efficient intrusion detection in big data environment. *Information Sciences*, *513*, 386–396.

IBM Security. (2023). *Cost of a data breach report 2023*. IBM Corporation. https://www.ibm.com/reports/data-breach

MITRE Corporation. (2023). *MITRE ATT&CK Framework for Enterprise*. https://attack.mitre.org/

National Institute of Standards and Technology (NIST). (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., y Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, *7*(1), 41.

SITA. (2022). *Air transport IT insights 2022*. SITA Publications. https://www.sita.aero/resources/surveys-reports/air-transport-it-insights-2022/

Torres, J. M., Comesaña, C. I., y García-Nieto, P. J. (2019). Machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, *10*(10), 2823–2836.

Weill, P., y Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press.

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., y Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, *6*, 35365–35381.

Yampolskiy, R. V. (2019). Unexplainability and incomprehensibility of artificial intelligence. *Journal of Artificial Intelligence and Consciousness*, *6*(01), 161–170.

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., y de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*, 25–37.

ANEXOS

ANEXO 1: ENCUESTA SOBRE DIAGNÓSTICO DE RIESGOS EN INFRAESTRUCTURA INFORMÁTICA EN PALMEROLA

Diagnóstico de Riesgos en Infraestructura Informática

28 mar 2026

El presente formulario tiene como objetivo recopilar informacion relevante para el diagnostico de riesgos en la infraestructura informatica del aeropuerto internacional de Palmerola

1. ¿Cuál es tu area de trabajo? *

- ◯ Infraestructura TI
- ◯ Seguridad Informatica
- ◯ Soporte Tecnico
- ◯ Desarrollo

2. ¿Cuánto tiempo llevas laborando? *

- ◯ Menos de 1 año
- ◯ Entre 1 y 2 años
- ◯ 2 a 3 años
- ◯ Entre 3 y 4 años
- ◯ Entre 4 y 5 años
- ◯ Más de 5 años

3. ¿En qué grupo de edad te encuentras? *

- ◯ Menos de 30
- ◯ Entre 31 y 40
- ◯ Entre 41 y 50
- ◯ Entre 51 y 60
- ◯ Más de 60

4. En general, ¿cuál es tu grado de satisfacción con la empresa que trabajas actualmente? *

- ◯ Extremadamente insatisfecho
- ◯ Algo insatisfecho
- ◯ Ni satisfecho ni insatisfecho
- ◯ Algo satisfecho
- ◯ Extremadamente satisfecho

28/3/26, 12:45 a.m. Diagnóstico de Riesgos en Infraestructura Informática

5. ¿En qué medida estás de acuerdo o en desacuerdo con las siguientes afirmaciones sobre Seguridad de la Información? *

	Muy en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Muy de acuerdo
Existen políticas formales de seguridad de la información.	◯	◯	◯	◯	◯
Se aplican controles de acceso basados en roles.	◯	◯	◯	◯	◯
Los sistemas críticos cuentan con respaldos adecuados.	◯	◯	◯	◯	◯
El personal aplica buenas prácticas de seguridad.	◯	◯	◯	◯	◯

6. ¿En qué medida estás de acuerdo o en desacuerdo con las siguientes afirmaciones sobre Gestión de Riesgos Tecnológicos? *

	Muy en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Muy de acuerdo
Se identifican riesgos tecnológicos sistemáticamente.	◯	◯	◯	◯	◯
Los incidentes se documentan y analizan.	◯	◯	◯	◯	◯
La alta dirección participa en la	◯	◯	◯	◯	◯

7. ¿En qué medida estás de acuerdo o en desacuerdo con la Cultura Organizacional? *

	Muy en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Muy de acuerdo
La institución promueve una **cultura** de ciberseguridad.	○	○	○	○	○
El personal recibe capacitaciones periódicas.	○	○	○	○	○
La ciberseguridad es prioritaria para la institución.	○	○	○	○	○

8. Expresa tus comentarios sobre la Preparación Tecnológica dentro de la organización. *

	Muy en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Muy de acuerdo
La institución está preparada para adoptar nuevas tecnologías.	○	○	○	○	○
Existen recursos financieros para ciberseguridad.	○	○	○	○	○
Se evalúan herramientas antes de implementarlas.	○	○	○	○	○

9. Cual es tu percepcion del impacto que causa las siguientes variables? *

	Muy en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Muy de acuerdo
La mejora tecnológica reduce riesgos operativos.	○	○	○	○	○
La inversión en ciberseguridad aumenta la confianza institucional.	○	○	○	○	○
La ciberseguridad contribuye a la misión institucional.	○	○	○	○	○

10. ¿Hay algún otro comentario que quieras hacer?

ANEXO 2: EVALUACIÓN DE RIESGOS, ÉTICA Y CUMPLIMIENTO EN IA APLICADA A CIBERSEGURIDAD

Evaluación de Riesgos, Ética y Cumplimiento en IA aplicada a Ciberseguridad

28 mar 2026

Aeropuerto internacional de Palmerola

* Obligatoria

1. 1. Principal tipo de riesgo percibido en el uso de IA/ML? *

- ◯ Tecnológico
- ◯ Operativo
- ◯ Ético / legal
- ◯ Estratégico
- ◯ Otras

2. Marco de referencia más relevante para la institución? *

- ◯ Normativa nacional
- ◯ Estándares internacionales (ISO, NIST, etc.)
- ◯ Políticas internas
- ◯ No definido

3. Califica los siguientes riesgos tecnológicos

	Muy en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Muy de acuerdo
Los sistemas de IA/ML pueden ser vulnerables a ataques adversarios.	○	○	○	○	○
Existe riesgo de sesgos en los algoritmos utilizados.	○	○	○	○	○
Los datos utilizados para entrenar modelos están adecuadamente protegidos.	○	○	○	○	○

4. En base a Ética y Cumplimiento evalua los siguientes criterios *

	Muy en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Muy de acuerdo
El uso de IA/ML respeta principios éticos institucionales.	○	○	○	○	○
Se garantiza la privacidad de la información procesada por sistemas automatizados.	○	○	○	○	○
Las decisiones tomadas por IA/ML pueden ser explicadas y	○	○	○	○	○

28/3/26, 12:52 a.m. Evaluación de Riesgos, Ética y Cumplimiento en IA aplicada a Ciberseguridad

7. Cual es tu percepcion del impacto que causa las siguientes variables?

	Muy en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Muy de acuerdo
La mejora tecnológica reduce riesgos operativos.	○	○	○	○	○
La inversión en ciberseguridad aumenta la confianza institucional.	○	○	○	○	○
La ciberseguridad contribuye a la misión institucional.	○	○	○	○	○

8. ¿Hay algún otro comentario que quieras hacer?