FACULTAD DE POSTGRADO

TRABAJO FINAL DE GRADUACIÓN

ESTRATEGIA DE RESILIENCIA DIGITAL BASADA EN EL NIST RMF: FORTALECIMIENTO DE LA CIBERSEGURIDAD EN EL INSTITUTO HONDUREÑO DE TRANSPORTE TERRESTRE (IHTT) COMO MODELO PARA INSTITUCIONES GUBERNAMENTALES DE HONDURAS

SUSTENTADO POR:

GUSTAVO ENRIQUE FRANCO FUENTES

OSCAR IGNACIO CALIX PONCE

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

DISTRITO CENTRAL, FRANCISCO

MORAZÁN, HONDURAS, C.A.

AGOSTO, 2024

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTORA

ROSALPINA RODRÍGUEZ

VICERRECTOR ACADÉMICO NACIONAL

JAVIER ABRAHAM SALGADO LEZAMA

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

DECANA NACIONAL DE POSTGRADO

ANA DEL CARMEN RETTALLY VARGAS

ESTRATEGIA DE RESILIENCIA DIGITAL BASADA EN EL NIST RMF: FORTALECIMIENTO DE LA CIBERSEGURIDAD EN EL INSTITUTO HONDUREÑO DE TRANSPORTE TERRESTRE (IHTT) COMO MODELO PARA INSTITUCIONES GUBERNAMENTALES DE HONDURAS

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

ASESOR METODOLÓGICO

JORGE RAÚL MARADIAGA CHIRINOS

MIEMBROS DE LA TERNA:
RIGOBERTO RODRÍGUEZ ÁVILA
KEVIN FÚNEZ
FREDIS DUBAL MEDINA ESCOTO

FACULTAD DE POSTGRADO

ESTRATEGIA DE RESILIENCIA DIGITAL BASADA EN EL NIST RMF: FORTALECIMIENTO DE LA CIBERSEGURIDAD EN EL INSTITUTO HONDUREÑO DE TRANSPORTE TERRESTRE (IHTT) COMO MODELO PARA INSTITUCIONES GUBERNAMENTALES DE HONDURAS

GUSTAVO ENRIQUE FRANCO FUENTES

OSCAR IGNACIO CALIX PONCE

Resumen

El Instituto Hondureño de Transporte Terrestre (IHTT) enfrenta un problema crítico de ciberseguridad debido a una infraestructura tecnológica inadecuada y falta de capacitación en seguridad informática. El estudio buscó desarrollar una estrategia integral de ciberseguridad basada en el NIST Risk Management Framework (RMF) 2021, con el objetivo de reforzar la infraestructura de TI y asegurar la continuidad operativa ante amenazas cibernéticas. Se emplearon metodologías de gestión de riesgos y auditoría de seguridad, con un enfoque mixto y una población compuesta por técnicos de TI, abogados, operadores de ventanilla, inspectores de campo y otros empleados. Las encuestas y entrevistas revelaron deficiencias significativas, con un 60% de técnicos y un 70% de otros empleados considerando insuficientes las herramientas de seguridad actuales. La propuesta final incluye la actualización de la infraestructura tecnológica, la implementación de políticas de seguridad robustas y un programa continuo de capacitación en ciberseguridad, todo ello alineado con los principios y directrices del NIST RMF.

Palabras claves: (Ciberseguridad, Estrategia, Infraestructura, Políticas, Capacitación)

GRADUATE SCHOOL

DIGITAL RESILIENCE STRATEGY BASED ON THE NIST RMF: STRENGTHENING CYBERSECURITY AT THE HONDURAN INSTITUTE OF LAND TRANSPORT (IHTT) AS A MODEL FOR GOVERNMENT INSTITUTIONS IN HONDURAS

GUSTAVO ENRIQUE FRANCO FUENTES
OSCAR IGNACIO CALIX PONCE

Abstract

The Honduran Institute of Land Transportation (IHTT) faces a critical cybersecurity problem due to inadequate technological infrastructure and a lack of training in information security. The study aimed to develop a comprehensive cybersecurity strategy based on the NIST Risk Management Framework (RMF) 2021, with the objective of reinforcing the IT infrastructure and ensuring operational continuity against cyber threats. Risk management and security audit methodologies were employed, using a mixed approach and a population composed of IT technicians, lawyers, window operators, field inspectors, and other employees. Surveys and interviews revealed significant deficiencies, with 60% of technicians and 70% of other employees considering the current security tools insufficient. The final proposal includes updating the technological infrastructure, implementing robust security policies, and establishing a continuous cybersecurity training program, all aligned with the principles and guidelines of the NIST RMF.

Keywords: (Cybersecurity, Strategy, Infrastructure, Policies, Training**)**

DEDICATORIA

Dedico este trabajo a Dios, fuente de toda sabiduría y fortaleza. Gracias por guiarme y darme la perseverancia para superar cada obstáculo en este camino.

A mi esposa, por ser mi pilar de apoyo y mi compañera incondicional. Tu amor, paciencia y comprensión han sido esenciales para alcanzar este logro. Gracias por estar siempre a mi lado.

A mi hija, cuyo amor y alegría me impulsan a ser mejor cada día. Eres mi mayor motivación y la razón por la que me esfuerzo para alcanzar mis sueños. Tu sonrisa ilumina mi vida y me da la fuerza para continuar.

A mi padre, cuyo ejemplo de dedicación y esfuerzo ha sido una guía en mi vida. Tus enseñanzas y valores han formado la base de mi éxito personal y profesional. Este logro es un reflejo de tu influencia y apoyo constante. A mi abuela que es mi Madre, quien han sido mi faro y mi fortaleza. Su amor incondicional, sacrificio y apoyo han sido fundamentales para llegar hasta aquí. Cada paso dado en este camino ha sido inspirado por su ejemplo de vida y su incansable dedicación. **Oscar Calix**

Este trabajo de tesis está dedicado a Dios y a la Virgen María, por siempre iluminar y guiar mi camino. A mi madre, Mirian Fuentes López, y a mi hermana, Miriam Sarahi Franco, por ser las mejores que existen. Ustedes me han guiado por el camino de la vida y me han brindado su amor, paciencia y apoyo incondicional. Sin lugar a duda, son la inspiración y el motivo de este logro.

A mis hijos, quienes son mi motor y me impulsan a ser mejor día con día. A mi compañero de tesis, por su dedicación, entusiasmo, optimismo, esfuerzo y paciencia puesta en el presente trabajo.

A mis familiares y a mi pareja, por ser ese apoyo y pilar que siempre me dice que puedo ser mejor. A mis amigos, por todos los momentos compartidos, su apoyo y cariño.

A todos ustedes, mi más profundo agradecimiento por ser parte de este viaje y por haber contribuido de manera invaluable a este logro. **Gustavo Franco**

AGRADECIMIENTO

Queremos expresar nuestra más profunda gratitud a Dios nuestro Señor, por siempre guiarnos, bendecirnos cada día, y por iluminarnos y darnos fuerzas para culminar nuestra maestría.

A nuestros padres, por ser la motivación que nos impulsa a alcanzar cada logro, por siempre apoyarnos de manera incondicional, y por sus sacrificios, amor y comprensión. Sin ustedes, nada de esto hubiera sido posible.

A nuestros hermanos y hermanas, por su apoyo constante y por estar siempre a nuestro lado en este viaje.

A nuestros familiares y amigos, por su confianza, cariño y apoyo inquebrantable. Su presencia y aliento han sido esenciales para nosotros.

Además, queremos expresar nuestro sincero agradecimiento a las autoridades y colegas del Instituto Hondureño de Transporte Terrestre (IHTT). Su confianza en nuestro trabajo y su colaboración han sido fundamentales para llevar a cabo esta investigación. Agradecemos la oportunidad de contribuir al fortalecimiento de nuestra institución y por proporcionarme los recursos y el ambiente adecuado para desarrollar este proyecto.

A los docentes que nos impartieron clases, gracias por todos los conocimientos brindados y por compartir sus experiencias, son aprendizajes que han sido y serán fructíferos en nuestra vida profesional. En especial a nuestro asesor de tesis el Ingeniero Jorge Maradiaga,gracias por su ayuda, comprensión y retroalimentación constante, y a nuestros compañeros, por crear un ambiente de aprendizaje y colaboración.

Este logro es el resultado del esfuerzo conjunto y el apoyo de todos ustedes. Gracias a cada uno de ustedes por formar parte de esta travesía y por su inestimable apoyo.

ÍNDICE DE CONTENIDO

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

CAPÍTULO I – PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 INTRODUCCIÓN

En la intersección entre tecnología y seguridad nacional, la ciberseguridad se manifiesta como un campo de batalla crítico para las instituciones gubernamentales. Este estudio, basado en nuestra experiencia directa como empleados del Instituto Hondureño de Transporte Terrestre (IHTT), investiga la reciente brecha de seguridad que evidenció la vulnerabilidad de nuestros sistemas digitales y urgió a reforzar la infraestructura crítica de la nación. Como miembros del departamento de TIC y maestrantes en Gestión de Tecnologías de Información, hemos vivenciado las consecuencias de dicha brecha y la respuesta institucional subsiguiente.

El Instituto Hondureño de Transporte Terrestre (IHTT), un pilar fundamental para la movilidad y el desarrollo económico de Honduras, sufrió un ataque cibernético en el que se explotaron vulnerabilidades específicas de su infraestructura tecnológica. Estas vulnerabilidades, identificadas a través de un análisis forense detallado, fueron publicadas en el informe correspondiente y expusieron debilidades críticas que comprometieron significativamente la operatividad y la integridad de los datos sensibles de la institución. Este incidente no solo debilitó la operatividad del IHTT, sino que también erosionó la confianza del público en nuestra capacidad para proteger información crítica. La respuesta inmediata del IHTT, caracterizada por una colaboración interdepartamental y con un sólido respaldo del área legal, resultó en la promulgación del Decreto Ejecutivo Número PCM XXX-2024 (Aun no publicado en Gaceta al 12 de agosto de 2024). Este decreto estableció directrices específicas para fortalecer la ciberseguridad en instituciones gubernamentales, formalizando medidas de protección y respuesta ante ciberataques, alineadas con la necesidad crítica de una infraestructura de seguridad robusta. Esta medida legislativa refleja la adaptabilidad y determinación requeridas para enfrentar crisis modernas, demostrando la capacidad de la institución para superar adversidades significativas.

Este estudio se fundamenta en el NIST Risk Management Framework (RMF) 2021, que proporciona un marco integral para la gestión de riesgos de seguridad de la información. La estrategia desarrollada en este documento se alinea con estos estándares internacionales, asegurando un enfoque estructurado y basado en las mejores prácticas para mejorar la resiliencia digital del IHTT. La investigación adoptó un enfoque mixto, exploratorio y descriptivo, con una

población compuesta por técnicos de TI, abogados, operadores de ventanilla, inspectores de campo y otros empleados. Las encuestas y entrevistas sirvieron como principales instrumentos de recolección de datos, destacando deficiencias significativas en la infraestructura de TI y en la capacitación del personal, con un 60% de técnicos y un 70% de otros empleados considerando insuficientes las herramientas de seguridad actuales.

Los resultados de la investigación revelaron que la infraestructura tecnológica actual del IHTT es insuficiente para prevenir ciberataques efectivos y que existe una necesidad significativa de mejorar los protocolos de seguridad y la capacitación del personal. A partir de estos hallazgos, se desarrolló una propuesta basada en el NIST Risk Management Framework (RMF) 2021, que incluye la actualización de la infraestructura tecnológica, la implementación de políticas de seguridad robustas, y un programa continuo de capacitación en ciberseguridad. Esta propuesta busca corregir negligencias pasadas y establecer un precedente vital para otras instituciones del país, impulsando al gobierno a reconocer la importancia crucial de invertir en la protección de sistemas y redes digitales. Como se ha subrayado anteriormente, "La falta de inversión en ciberseguridad puede resultar en consecuencias mucho más costosas" (Smith, 2022). Este trabajo no solo destaca la urgencia de la situación, sino que también prepara el terreno para un enfoque proactivo hacia la seguridad cibernética en el IHTT y en todas las entidades estatales de Honduras.

1.2 ANTECEDENTES DEL PROBLEMA

Los antecedentes revelan una realidad digital en constante cambio, donde las amenazas evolucionan más rápido que las medidas de defensa existentes. El IHTT, antes considerado un modelo de eficiencia operativa y tecnológica, enfrentó un ataque cibernético en enero de 2024 que evidenció vulnerabilidades significativas. Este ataque, cuyas vulnerabilidades fueron identificadas y publicadas en el informe forense de julio de 2024, subrayó la necesidad urgente de reforzar las defensas cibernéticas de la institución. Este apartado detallará la cronología de los eventos, las prácticas de seguridad previas y cómo la falta de preparación contra amenazas emergentes puede desestabilizar críticamente la infraestructura tecnológica de una entidad gubernamental.

La ciberseguridad ha emergido como una de las prioridades más críticas para las organizaciones en todo el mundo, y las instituciones gubernamentales no son la excepción. Esta sección detalla la evolución de las amenazas cibernéticas que han desafiado al Instituto Hondureño

de Transporte Terrestre (IHTT), proporcionando un marco comprensivo de los desafíos que han modelado las actuales políticas y estrategias de seguridad de la institución.

HISTORIA DE CIBERATAQUES EN EL IHTT

El IHTT ha enfrentado múltiples desafíos de seguridad en los últimos años, que han puesto a prueba la resiliencia y la capacidad de respuesta de su infraestructura de TI. Desde ataques de malware hasta intrusiones más personalizadas, cada incidente ha dejado lecciones valiosas y ha impulsado cambios significativos en la manera de manejar la seguridad informática. Se detallará cada incidente significativo, empezando con el ataque más reciente descrito en el informe interno del 13 de marzo de 2024, que resultó en una parálisis operativa completa y expuso vulnerabilidades críticas en la gestión de la seguridad.

Comparación con Tendencias Globales

Es fundamental contextualizar los incidentes en el IHTT dentro de las tendencias globales de ciberseguridad en instituciones gubernamentales. Se realizará un análisis comparativo, utilizando datos de estudios recientes y reportes de organizaciones internacionales de ciberseguridad, basados en marcos normativos como el NIST Risk Management Framework (RMF) 2021, para ilustrar cómo los desafíos enfrentados por el IHTT son reflejo de una problemática global. Esto resalta la importancia de adoptar prácticas recomendadas y soluciones avanzadas alineadas con estándares internacionales reconocidos.

Revisión de la Legislación y Políticas de Ciberseguridad

Una revisión de las políticas y legislación relevante es crucial para entender el marco regulatorio en el que el IHTT opera. Se examinarán las leyes nacionales e internas que han influido en las políticas de ciberseguridad del IHTT, incluyendo la creación del Decreto Ejecutivo Número PCM XXX-2024 como respuesta directa a los ataques cibernéticos recientes. Este decreto, fundamentado en normativas como el NIST Risk Management Framework (RMF) 2021, busca establecer un marco robusto para fortalecer la postura de seguridad del IHTT y prevenir futuras brechas de seguridad. La implementación de este marco permitirá que otras instituciones gubernamentales también fortalezcan sus capacidades de ciberseguridad.

Impacto de los Incidentes de Seguridad

En nuestra calidad de profesionales del departamento de Tecnologías de la Información y

Comunicaciones del Instituto Hondureño de Transporte Terrestre (IHTT), hemos observado directamente las secuelas que los incidentes de seguridad han causado en las operaciones y la percepción pública de nuestra institución. Esta sección del estudio, apoyada por análisis empíricos y personales, discute las consecuencias operativas, financieras y reputacionales de los ataques cibernéticos que hemos experimentado.

Los ataques no solo provocaron interrupciones críticas en la prestación de servicios, sino que también expusieron deficiencias significativas en nuestras medidas de seguridad existentes. Estos incidentes nos obligaron a enfrentar desafíos operativos inmediatos y a evaluar las pérdidas económicas sustanciales que ascendieron alrededor de 20 millones de lempiras en un tiempo aproximado de 2 meses sin estar presentando servicios de atención al cliente ni ningún tipo de operatividad, subrayando la imperiosa necesidad de adoptar una estrategia de seguridad más robusta y dinámica. El deterioro de la confianza del público, especialmente preocupante en un servicio tan esencial como el transporte público, nos impulsa a reflexionar sobre la importancia de restaurar y mantener la credibilidad institucional.

La experiencia directa de estos eventos ha sido fundamental para nuestra formación académica y profesional. Ha enriquecido nuestra comprensión de la ciberseguridad no solo como un campo técnico, sino también como una disciplina integral que combina gestión de riesgos, tecnología y políticas públicas. Esta tesis se centra en destacar la necesidad de una gestión proactiva de la seguridad informática, que se anticipa a las amenazas y mitiga sus posibles impactos antes de que comprometan la integridad y la funcionalidad de la infraestructura crítica.

1.3 DEFINICIÓN DEL PROBLEMA

El problema se identifica como una convergencia crítica de fallos técnicos y brechas de seguridad que llevaron al IHTT a una interrupción sin precedentes. Estas vulnerabilidades expusieron debilidades significativas en la infraestructura tecnológica del IHTT, afectando su capacidad para mantener operaciones seguras y continuas. Esta situación reveló la falta de preparación adecuada para enfrentar amenazas cibernéticas emergentes, resultando en serias consecuencias operativas, económicas y legales.

1.4 PREGUNTAS DE INVESTIGACIÓN

1.4.1 PREGUNTA GENERAL

¿Cómo puede el IHTT desarrollar e implementar una estrategia integral de ciberseguridad basada en el NIST Risk Management Framework (RMF) 2021 que responda efectivamente a las amenazas emergentes y fortalezca la resiliencia operativa de la institución?

1.4.2 PREGUNTAS ESPECÍFICAS

- ¿Cuáles fueron las vulnerabilidades explotadas en el ataque cibernético que comenzó el 15 de enero de 2024, resultando en la pérdida de acceso a servidores en marzo de 2024, y qué medidas correctivas específicas basadas en el NIST RMF (2021) se pueden implementar para mitigar estas vulnerabilidades en el futuro?
- ¿Cómo pueden mejorarse los procesos y protocolos para detectar amenazas de manera temprana y mejorar la respuesta a incidentes de ciberseguridad?
- ¿De qué manera la capacitación continua en ciberseguridad del personal puede fortalecer la prevención de futuros ataques cibernéticos?
- ¿Qué estrategias basadas en NIST RMF (2021) pueden desarrollarse para integrar soluciones tecnológicas avanzadas que fortalezcan la infraestructura de TI y aseguren la continuidad operativa?

1.5 OBJETIVOS DEL PROYECTO

1.5.1 OBJETIVO GENERAL

Desarrollar y implementar una estrategia integral de ciberseguridad basada en el NIST Risk Management Framework (RMF) 2021 en el IHTT para el año 2025, que refuerce la infraestructura de TI y asegure la continuidad operativa frente a amenazas cibernéticas.

1.5.2 OBJETIVOS ESPECÍFICOS

- Realizar un análisis detallado de la infracción de seguridad para identificar y planificar la remediación de las vulnerabilidades explotadas, implementando soluciones específicas basadas en el NIST RMF (2021) antes del final del segundo

trimestre de 2024.

- Establecer un marco de colaboración entre el área de tecnología y la administrativa como parte de una política institucional, para acelerar la adquisición e implementación de medidas de ciberseguridad de emergencia basadas en el NIST RMF (2021) dentro de los próximos 6 meses. Esto asegurará que los esfuerzos de ciberseguridad no se vean aislados, sino que estén integrados en la estrategia organizacional del IHTT.
- Diseñar y validar un protocolo de seguridad digital que incorpore monitorización avanzada y planes de respuesta rápida para finales de 2024.
- Crear y lanzar un programa educativo continuo en ciberseguridad para el personal de TI y los usuarios finales para principios de 2025.

1.6 JUSTIFICACIÓN

La necesidad de fortalecer la ciberseguridad en el Instituto Hondureño de Transporte Terrestre (IHTT) se ha vuelto imperativa, especialmente tras el reciente incidente de ciberataque que expuso vulnerabilidades significativas en nuestra infraestructura tecnológica. Este proyecto se justifica por la urgencia de implementar una estrategia de seguridad que no solo remedie las deficiencias actuales, sino que también establezca un marco robusto para prevenir futuros ataques. Investigaciones como la de (Romanosky, 2016) muestran que los ciberataques a instituciones gubernamentales pueden tener repercusiones devastadoras, desde la pérdida de datos críticos hasta la parálisis completa de servicios esenciales, lo que subraya la necesidad de acciones proactivas y de una respuesta organizada (Romanosky, 2016).

Además, la integración del área legal con la creación del Decreto Ejecutivo Número PCM XXX-2024 resalta el compromiso del gobierno y del IHTT con la protección contra amenazas cibernéticas. Como destacan (Johnson M. &.-D., 2015) en su estudio sobre la gobernanza de la ciberseguridad, la adopción de políticas legislativas es fundamental para la consolidación de esfuerzos de seguridad a nivel institucional y nacional (Johnson M. &.-D., 2015).

Este enfoque integral asegura que la inversión en tecnología y formación del personal sea vista no solo como medidas reactivas, sino también como una estrategia preventiva que contribuye

a la resiliencia institucional a largo plazo. La ciberseguridad no debe enfocarse únicamente en la infraestructura técnica, sino que debe incorporar una perspectiva más amplia que incluya la educación y la cultura organizacional, fundamentales para mitigar eficazmente los riesgos. Como afirman (Von Solms, 2013), una estrategia de seguridad robusta debe integrar estos aspectos para ser efectivamente implementada en cualquier institución (Von Solms, 2013).

Finalmente, este proyecto no solo aborda un requerimiento inmediato del IHTT, sino que también ofrece un modelo replicable para otras instituciones gubernamentales, promoviendo un entorno más seguro y resiliente en todo el sector público. Este precedente ayudará a fortalecer la gobernanza digital y a asegurar que Honduras pueda enfrentar desafíos cibernéticos futuros con mayor eficacia.

CAPÍTULO II – MARCO TEÓRICO

2.1 MACROENTORNO

2.1.1 TENDENCIAS GLOBALES EN CIBERSEGURIDAD:

La ciberseguridad se ha convertido en un campo de batalla crucial en el ámbito global, con ataques cada vez más sofisticados que ponen en riesgo la seguridad nacional y la integridad de datos críticos. Instituciones como el IHTT no están exentas de estos riesgos, haciendo imprescindible su adaptación a las nuevas formas de amenazas cibernéticas. Según Cybersecurity (Ventures., 2022) se espera que los costos globales relacionados con el cibercrimen alcanzarán los $10.5 billones anuales para 2025, lo que refleja la escala y el impacto de este problema (Ventures., 2022). (Smith J. T., 2023).

La relevancia de estos ataques para el IHTT subraya la urgencia de adoptar tecnologías de seguridad de vanguardia y estrategias de defensa proactivas para salvaguardar sus sistemas. Estudios como el realizado por Smith et al. (2023) en la "Journal of Cyber Policy" destacan la importancia de una respuesta integrada que combine tecnología, legislación y colaboración internacional para combatir efectivamente los riesgos cibernéticos (Smith J. T., 2023).

2.1.2 POLÍTICAS INTERNAS DE SEGURIDAD

Las regulaciones internacionales han evolucionado para responder a los crecientes desafíos de la ciberseguridad, estableciendo normativas que afectan cómo las organizaciones, incluidas las gubernamentales como el IHTT, gestionan y protegen la información. La adopción del GDPR por la Unión Europea ha marcado un hito en la protección de datos, estableciendo un precedente para que otras regiones fortalezcan sus políticas de privacidad (Commission, 2022). Estas regulaciones no solo protegen contra el mal uso de datos, sino que también imponen severas penalizaciones por incumplimientos, lo que incrementa la necesidad de cumplimiento riguroso.

La aplicación de tales regulaciones internacionales en el contexto del IHTT sugiere un camino hacia la adopción de mejores prácticas globales en la gestión de datos y la ciberseguridad. La adaptación a estas normas no solo es esencial para la conformidad legal, sino también para fortalecer la confianza del público.

2.1.3 IMPACTO SOCIAL DE LOS CIBERATAQUES

Los ciberataques no solo afectan la infraestructura técnica y financiera de las organizaciones, sino que también tienen un impacto social significativo, especialmente en instituciones gubernamentales como el IHTT, que son esenciales en la prestación de servicios públicos. Según un informe del Foro Económico Mundial (2024), los ataques cibernéticos pueden erosionar profundamente la confianza pública en el gobierno, afectando la percepción de seguridad y estabilidad entre los ciudadanos (Forum., 2024). Este deterioro en la confianza puede resultar en una disminución de la participación ciudadana en programas digitales gubernamentales y una menor colaboración con las iniciativas de seguridad pública, subrayando la necesidad de una comunicación transparente y efectiva para restaurar la confianza. Además, el impacto social de los ciberataques se extiende a la desestabilización de los sistemas democráticos, donde la manipulación de información y ataques a la infraestructura electoral pueden comprometer la integridad de los procesos electorales. Para mitigar estos efectos, el IHTT no solo necesita fortalecer sus defensas cibernéticas, sino también implementar estrategias de comunicación robustas que faciliten una recuperación rápida de la confianza pública tras un incidente, asegurando así la continuidad en la prestación de servicios esenciales y el mantenimiento del orden social.

EJEMPLOS DETALLADOS DE IMPACTO SOCIAL:

Incidencias en Elecciones:

Para una comprensión más profunda del impacto social, examina el caso de las elecciones presidenciales de EE. UU. en 2016, destacando cómo las campañas de desinformación impulsadas por ciberataques no solo buscaron influir en el resultado electoral, sino que también plantearon dudas sobre la integridad del proceso democrático. La manipulación de la información y la proliferación de noticias falsas exacerbó la polarización política, erodiendo la confianza pública y promoviendo el escepticismo hacia las instituciones democráticas (Jamieson, 2018).

Efectos en la Economía Local:

Amplía el análisis del impacto económico con el caso del ransomware WannaCry en 2017, que afectó a más de 200,000 computadoras en 150 países, incluyendo sistemas críticos en hospitales, bancos y empresas de transporte. Este ataque no solo causó pérdidas económicas directas estimadas en miles de millones de dólares, sino que también demostró cómo la dependencia de la tecnología en múltiples sectores puede amplificar los efectos de un ciberataque

a través de la economía global, afectando la estabilidad económica y social (Smith, 2021).

Respuesta Social y de Políticas:

Considera cómo, en respuesta a los ciberataques, los gobiernos y organizaciones pueden desarrollar iniciativas para mejorar la resiliencia comunitaria. Detalla programas específicos como la Cyber Aware campaign en el Reino Unido, que busca educar al público sobre seguridad digital, fomentando hábitos seguros y promoviendo el uso de tecnologías de verificación en dos pasos entre los ciudadanos. Este enfoque no solo ayuda a mitigar los efectos de los ciberataques, sino que también prepara mejor a la sociedad para manejar incidentes futuros, integrando la seguridad digital en la cultura cotidiana (Brown & Susskind, 2020).

2.1.4 INTERDEPENDENCIA DIGITAL

En la era digital, la interdependencia entre diferentes sectores y sistemas incrementa notablemente la vulnerabilidad a los ciberataques. La conexión en red de sistemas de transporte, como los gestionados por el IHTT, con otras infraestructuras críticas, subraya la necesidad de un enfoque holístico en la ciberseguridad que trascienda las fronteras organizacionales. Un estudio publicado en el Journal of Cybersecurity and Mobility (2023) revela cómo la falta de coordinación entre distintas entidades puede aumentar los riesgos de seguridad cibernética en infraestructuras interdependientes, exacerbando la susceptibilidad a ataques coordinados que pueden paralizar múltiples servicios esenciales simultáneamente (Johnson L. &, 2023). Este panorama demanda que el IHTT busque colaboraciones más estrechas con otras entidades gubernamentales y privadas para desarrollar estrategias de seguridad integradas que aborden las vulnerabilidades compartidas a través de sectores. Además, es crucial implementar prácticas de gestión de riesgos que incluyan análisis de interdependencias, evaluaciones de impacto cruzado y simulacros de respuesta a incidentes, lo que fortalecerá la resiliencia colectiva y minimizará los impactos de posibles ataques cibernéticos en el entorno interconectado actual.

2.2 MICROENTORNO

2.2.1 ESTRUCTURA ORGANIZACIONAL DEL IHTT

La estructura organizacional del IHTT influye significativamente en su capacidad para implementar estrategias efectivas de ciberseguridad. Una estructura bien definida que promueve la

colaboración interdepartamental y facilita la comunicación rápida es esencial para una respuesta efectiva ante incidentes. Según un estudio de la Harvard Business Review (2021), las organizaciones con equipos de ciberseguridad integrados en las operaciones diarias tienden a responder más eficazmente a los incidentes de seguridad, mitigando los daños de manera más efectiva (Review, 2021).

Para el IHTT, esto significa fortalecer los roles y responsabilidades dentro de su estructura organizacional, asegurando que la gestión de la ciberseguridad esté en el corazón de sus operaciones. La integración de equipos de TI con operaciones, seguridad y gestión de riesgos puede mejorar la coordinación y la ejecución de políticas de seguridad en toda la institución.

2.2.2 POLÍTICAS INTERNAS DE SEGURIDAD

Las políticas internas de seguridad del IHTT son cruciales para establecer las normas y procedimientos que rigen la protección de los sistemas y la información. Estas políticas deben ser comprehensivas, cubriendo desde el control de acceso y la gestión de datos hasta la respuesta a incidentes y la recuperación de desastres. Conforme al "Cybersecurity Policy Guide" publicado por el MIT (2023), las políticas efectivas son aquellas que están bien comunicadas y totalmente integradas en las prácticas diarias de los empleados (MIT., 2023).

Para que el IHTT mantenga una postura de seguridad efectiva, sus políticas deben ser revisadas y actualizadas regularmente, incorporando las lecciones aprendidas de incidentes anteriores y ajustándose a las nuevas amenazas. Esto también incluye la formación continua de todo el personal, desde la alta dirección hasta los operadores, asegurando que todos estén informados sobre las mejores prácticas de seguridad y su papel en la protección de la infraestructura crítica.

2.2.3 EVALUACIÓN DE RIESGOS INTERNOS

La evaluación de riesgos internos en el IHTT es fundamental para identificar dónde pueden existir vulnerabilidades dentro de la institución. Estas evaluaciones deben ser continuas y sistemáticas para asegurar que todos los riesgos potenciales se identifiquen y mitiguen adecuadamente. Según el Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST), una metodología de evaluación de riesgos bien estructurada es crucial para la gestión efectiva de la seguridad cibernética en las organizaciones (NIST, 2023). El IHTT puede utilizar estas directrices para formular evaluaciones que co (Ventures., 2022)nsideren tanto riesgos tecnológicos como

humanos.

2.2.4 GESTIÓN DE INCIDENTES Y RECUPERACIÓN

La gestión de incidentes y la recuperación constituyen componentes cruciales de la estrategia de ciberseguridad en el IHTT, dada la naturaleza crítica de su infraestructura de transporte. Una respuesta efectiva a incidentes no solo implica reacciones rápidas y coordinadas en el momento del ataque, sino también una planificación meticulosa para la recuperación de sistemas y servicios post-incidente. La capacidad de recuperarse rápidamente minimiza no solo el tiempo de inactividad operativo, sino también reduce el impacto financiero y reputacional de los ataques.

En el contexto del IHTT, esto significa tener un plan de respuesta a incidentes bien desarrollado que incluya procedimientos claros para la evaluación de daños, la contención de la amenaza, y las estrategias de recuperación y comunicación. Según la Institución Internacional de Normalización (ISO), las normas como la ISO/IEC 27031:2011 proporcionan una guía para la gestión de la continuidad de las tecnologías de la información, enfatizando la importancia de prepararse para, responder a y recuperarse de los incidentes (ISO, 2011).

La implementación de tales normativas puede ayudar al IHTT a desarrollar una resiliencia que asegure la rápida restauración de los servicios y la confianza del público. Un estudio de la Ponemon Institute (2022) encontró que las organizaciones que implementan planes de gestión de incidentes de manera integral pueden reducir los costos asociados con la pérdida de datos y otros compromisos de seguridad hasta en un 40% (Ponemon, 2020).

Para apoyar estos esfuerzos, es esencial que el IHTT realice simulacros de recuperación regulares y revise sus estrategias de gestión de incidentes con base en las lecciones aprendidas y las mejores prácticas emergentes. Esto no solo mejorará su capacidad de respuesta ante incidentes futuros, sino también su capacidad general de adaptación y resiliencia ante las cambiantes amenazas cibernéticas.

2.3 TEORÍAS DE SUSTENTO

2.3.1 TEORÍA DE LA GESTIÓN DE RIESGOS CIBERNÉTICOS

La gestión de riesgos cibernéticos es una disciplina crítica que implica la identificación, evaluación, mitigación y monitoreo continuo de riesgos de seguridad de la información. En el

contexto del Instituto Hondureño de Transporte Terrestre (IHTT), donde los sistemas de información juegan un papel vital en la operación diaria y la seguridad del transporte público, una gestión de riesgos eficaz es imperativa. La teoría sugiere que una estrategia de riesgos bien implementada debe basarse en un enfoque holístico que no solo contemple las tecnologías de seguridad, sino también las políticas organizacionales y la capacitación de empleados.

INTEGRACIÓN CON LA CUARTA REVOLUCIÓN INDUSTRIAL:

La Cuarta Revolución Industrial, caracterizada por la convergencia de tecnologías digitales, físicas y biológicas, ha transformado significativamente la gestión de riesgos cibernéticos. La incorporación de tecnologías avanzadas como el Internet de las Cosas (IoT), la inteligencia artificial (IA) y el big data en los sistemas de transporte del IHTT ha aumentado la superficie de ataque y la complejidad de los riesgos cibernéticos. (Bodeau, 2021), argumentan que integrar la evaluación de riesgos en la planificación estratégica del IHTT puede fortalecer significativamente su capacidad para prevenir y responder a incidentes cibernéticos, destacando la importancia de un enfoque que balancee tanto aspectos técnicos como humanos de la seguridad (Bodeau, 2021).

La Cuarta Revolución Industrial también exige que las organizaciones adopten un enfoque proactivo y adaptativo hacia la ciberseguridad. Esto implica no solo implementar tecnologías de seguridad avanzadas, sino también desarrollar una cultura organizacional que valore y promueva prácticas seguras. Según (Schwab, 2016)las empresas deben evolucionar para incorporar la gestión de riesgos cibernéticos en su núcleo, adaptando sus estrategias a un entorno digital cada vez más interconectado y dinámico (Schwab, 2016).

2.3.2 TEORÍA DE RESILIENCIA ORGANIZACIONAL EN CIBERSEGURIDAD

La resiliencia organizacional en ciberseguridad se refiere a la habilidad de una institución para mantener sus funciones esenciales durante y después de un ataque cibernético. Para el IHTT, desarrollar resiliencia no solo implica robustecer sus defensas cibernéticas, sino también crear planes de continuidad operativa que permitan la rápida restauración de los servicios de transporte en caso de interrupción. Linkov y Trump (2019) destacan que la resiliencia no es estática sino dinámica, requiriendo adaptación constante a nuevas amenazas y condiciones cambiantes del entorno. Para el IHTT, esto significa implementar un marco de resiliencia que sea capaz de adaptarse a las evoluciones tanto en la tecnología como en la metodología de los ataques, asegurando la protección continua de sus activos y la confianza del público (Linkov, 2019).

2.4 METODOLOGÍAS

2.4.1 ANÁLISIS DE RIESGOS

El análisis de riesgos es una metodología fundamental en la ciberseguridad, que permite al IHTT identificar las amenazas más críticas y evaluar la efectividad de las medidas de control existentes. Esta metodología no solo se centra en los aspectos técnicos, como la seguridad de la infraestructura de TI, sino también en factores humanos y procesos operativos que pueden ser vulnerables a ataques. El presente estudio se basa en la Versión 2 (2018) del NIST Risk Management Framework (RMF), tal como se detalla en las directrices actualizadas del NIST publicadas en 2021. Este marco detalla cómo realizar un análisis exhaustivo de riesgos que considere estos diversos componentes, enfatizando la importancia de una visión integral para la gestión eficaz de la seguridad en organizaciones complejas como el IHTT. Adicionalmente, este enfoque se complementa con la ISO/IEC 27001, un estándar internacionalmente reconocido que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI), asegurando que las políticas y procedimientos implementados no solo sean eficaces sino también alineados con las mejores prácticas globales.

2.4.2 ANTECEDENTES DE LA METODOLOGÍA DE ANÁLISIS DE RIESGOS

El análisis de riesgos ha evolucionado significativamente en las últimas décadas, transformándose de una actividad reactiva a una parte fundamental de la estrategia de seguridad cibernética en organizaciones líderes, incluido el IHTT. Tøndel (2020) destaca cómo las organizaciones han adoptado enfoques más sofisticados y basados en datos para el análisis de riesgos, mejorando así su capacidad para anticipar y mitigar los impactos de los ataques cibernéticos. Este avance se ha caracterizado por la integración de tecnologías de big data y aprendizaje automático que permiten un análisis más profundo y predictivo de las vulnerabilidades y amenazas potenciales. Estos sistemas pueden identificar patrones ocultos y prever tendencias de ataques antes de que ocurran, permitiendo a las organizaciones ser proactivas en lugar de reactivas. Además, la colaboración intersectorial ha enriquecido los análisis de riesgos, donde el intercambio de información sobre amenazas entre diferentes industrias y sectores públicos ha creado un entorno más robusto para enfrentar desafíos cibernéticos complejos. En el contexto del IHTT, la adopción de estas metodologías avanzadas ha llevado a un enfoque más estratégico y orientado a la prevención, asegurando que la infraestructura crítica esté protegida contra interrupciones

potenciales que podrían afectar a servicios esenciales y la seguridad pública.

2.4.3 APLICACIÓN DEL ANÁLISIS DE RIESGOS EN EL IHTT

La metodología de análisis de riesgos en el IHTT se aplica de manera integral, incorporando tanto análisis cuantitativo como cualitativo para evaluar las vulnerabilidades. Este proceso involucra la identificación de activos críticos, la determinación de amenazas potenciales y la evaluación de las medidas de seguridad existentes. Utilizando herramientas avanzadas de simulación y modelado de amenazas, el IHTT puede prever escenarios de ataque y preparar respuestas apropiadas. Este enfoque no solo mejora la seguridad, sino que también optimiza la asignación de recursos hacia las áreas más vulnerables y críticas.

2.4.4 METODOLOGÍA DE RESPUESTA A INCIDENTES

Esta metodología abarca la preparación, detección, contención, erradicación y recuperación de incidentes de seguridad. En el IHTT, una respuesta a incidentes efectiva es crucial para minimizar el impacto operativo y financiero de los ataques. La metodología se basa en un protocolo establecido que involucra la coordinación rápida entre múltiples equipos, incluidos TI, legal, y comunicaciones, para manejar eficazmente las incidencias desde su detección hasta la resolución.

2.4.5 ANTECEDENTES DE LA METODOLOGÍA DE RESPUESTA A INCIDENTES

El desarrollo de metodologías de respuesta a incidentes ha sido impulsado por la necesidad de responder de manera más efectiva a incidentes de seguridad cada vez más sofisticados. Históricamente, las organizaciones que han adoptado un enfoque sistemático para la gestión de incidentes han logrado reducciones significativas en el tiempo de recuperación y los costos asociados. Este enfoque sistemático incluye la implementación de equipos especializados en respuesta a incidentes, equipados con herramientas y procedimientos estandarizados para una acción rápida y eficiente. En el IHTT, la implementación de una metodología de respuesta a incidentes bien definida ha permitido al instituto no solo fortalecer su capacidad para gestionar y mitigar ataques, sino también adaptarse y aprender de cada incidente. La creación de un protocolo de "lecciones aprendidas", que analiza cada incidente para identificar fallas y mejorar las respuestas futuras, ha sido clave para esta evolución. Además, el IHTT ha establecido simulacros regulares que permiten a los equipos practicar y perfeccionar sus habilidades en escenarios controlados, asegurando que cuando ocurra un incidente real, la respuesta sea coordinada y efectiva. Esta metodología no solo reduce el impacto de los ataques, sino que también mejora la resiliencia

organizativa al asegurar que el personal esté bien preparado y los sistemas bien protegidos contra futuras amenazas.

2.4.6 APLICACIÓN DE LA METODOLOGÍA DE RESPUESTA A INCIDENTES EN EL IHTT

En la práctica, esta metodología se aplica en el IHTT a través de un centro de operaciones de seguridad que monitoriza constantemente los sistemas de información en busca de signos de actividad maliciosa. Cuando se detecta un incidente, se activan protocolos específicos que incluyen la segregación de redes afectadas, la evaluación de daños y la comunicación con las partes interesadas. La metodología también incluye revisiones posts-incidentes para mejorar las políticas y prácticas basadas en el análisis forense de los ataques.

2.5 HERRAMIENTAS

2.5.1 HERRAMIENTAS UTILIZADAS EN EL ANÁLISIS DE RIESGOS

Para el análisis de riesgos, el IHTT utiliza herramientas avanzadas de análisis predictivo que incorporan **Inteligencia Artificial** para prever patrones de ataques potenciales y evaluar la eficacia de los controles de seguridad actuales. Una de las principales herramientas implementadas es el **Antivirus Kaspersky**, que opera a través de una consola en la nube. Este antivirus no solo proporciona protección en tiempo real, sino que también analiza diariamente el sistema y ejecuta políticas de seguridad automatizadas para mantener un entorno seguro y proactivo.

2.5.2 HERRAMIENTAS UTILIZADAS EN LA RESPUESTA A INCIDENTES

El IHTT emplea plataformas de gestión de incidentes que integran funciones de alerta temprana, automatización de respuestas y colaboración en tiempo real entre equipos. El **firewall Juniper** es una pieza clave en el monitoreo de la red, brindando capacidades avanzadas de detección de amenazas y control de tráfico. Estas herramientas son esenciales para garantizar una respuesta rápida y coordinada durante un incidente, ayudando a reducir el tiempo hasta la resolución y mitigar el impacto de los ataques.

2.6 CONCEPTUALIZACIÓN

CONCEPTUALIZACIÓN EN CIBERSEGURIDAD

Este apartado explora y define términos clave en ciberseguridad como 'ataque cibernético', 'resiliencia cibernética', 'prevención', y 'respuesta a incidentes', con un enfoque en cómo estos términos se aplican al contexto específico del IHTT. Se consideran tanto las definiciones estándar como las interpretaciones adaptadas que reflejan las particularidades del entorno del IHTT.

La ciberseguridad es un campo en constante evolución que se centra en proteger los sistemas, redes y datos de ataques cibernéticos. En el contexto del Instituto Hondureño de Transporte Terrestre (IHTT), es crucial comprender y adaptar los conceptos clave de ciberseguridad para abordar los desafíos específicos que enfrenta la institución. A continuación, se exploran y definen términos fundamentales en ciberseguridad, destacando su relevancia y aplicación en el entorno del IHTT.

1. ATAQUE CIBERNÉTICO:

Un ataque cibernético se define como cualquier intento malicioso de acceder, dañar o destruir información, sistemas y redes de una organización. Estos ataques pueden variar desde malware, ransomware, phishing, hasta ataques de denegación de servicio (DDoS). En el caso del IHTT, el reciente incidente involucró un ataque de ransomware que comprometió la integridad y disponibilidad de los datos críticos de la institución, subrayando la necesidad de fortalecer las defensas cibernéticas (Symantec, 2019) (Insights, 2024).

2. RESILIENCIA CIBERNÉTICA:

La resiliencia cibernética se refiere a la capacidad de una organización para prepararse, resistir, recuperarse y adaptarse a eventos adversos en el ciberespacio. Para el IHTT, esto implica no solo la implementación de medidas preventivas y reactivas, sino también el desarrollo de estrategias a largo plazo que aseguren la continuidad operativa incluso en caso de un ataque cibernético exitoso. La resiliencia cibernética es esencial para mantener la confianza del público y la eficiencia de los servicios de transporte terrestre (Insights, 2024).

3. PREVENCIÓN:

La prevención en ciberseguridad incluye todas las medidas y prácticas diseñadas para evitar que los ataques cibernéticos tengan éxito. Esto abarca desde la implementación de firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), hasta la actualización regular de software y la formación continua del personal en prácticas de seguridad. Para el IHTT, la

prevención es la primera línea de defensa contra ciberataques y requiere una inversión continua en tecnología y capacitación (Institute., 2019; ISO/IEC, 2016; ISO/IEC, 2016).

4. RESPUESTA A INCIDENTES:

La respuesta a incidentes es el proceso organizado de manejar y mitigar las consecuencias de un ataque cibernético. Incluye la detección del incidente, la contención del daño, la erradicación de la amenaza, la recuperación de sistemas afectados y la comunicación efectiva con las partes interesadas. En el IHTT, la respuesta a incidentes es crítica para minimizar el impacto de un ataque y restaurar los servicios lo más rápidamente posible. Un plan de respuesta a incidentes bien diseñado y ensayado regularmente puede significar la diferencia entre una interrupción menor y una crisis mayor (ISO/IEC, 2016). (gartner, 2022)

5. **MONITOREO Y DETECCIÓN:**

El monitoreo y la detección continua son componentes esenciales de una estrategia de ciberseguridad efectiva. Esto implica el uso de herramientas y tecnologías para supervisar las redes y sistemas en tiempo real, identificando posibles amenazas antes de que puedan causar daño. En el contexto del IHTT, la implementación de sistemas de monitoreo avanzados es vital para detectar actividades sospechosas y responder rápidamente a cualquier intento de violación de seguridad (gartner, 2022).

6. GESTIÓN DE RIESGOS:

La gestión de riesgos en ciberseguridad implica la identificación, evaluación y priorización de riesgos cibernéticos, seguida de la aplicación de recursos para minimizar, supervisar y controlar la probabilidad o impacto de eventos adversos. Para el IHTT, gestionar los riesgos de ciberseguridad es fundamental para proteger los datos y la infraestructura crítica del transporte, asegurando así la continuidad de los servicios (SO/IEC, 2013).

2.7 MARCO LEGAL

2.7.1 MARCO LEGAL INTERNACIONAL

Este segmento examina las convenciones y tratados internacionales como el Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest), que establece un marco común para la cooperación internacional en la lucha contra la ciberdelincuencia, incluyendo la

protección de sistemas y datos críticos en el transporte público.

2.7.1.1 CIBERSEGURIDAD EN LA UNIÓN EUROPEA

La UE ha fortalecido su legislación en ciberseguridad con el Reglamento General de Protección de Datos (GDPR) y la Directiva NIS, que establecen rigurosas medidas de protección:

- **Reglamento GDPR (2016):** Protege los datos personales dentro de la UE y regula la exportación de datos personales fuera de la región, imponiendo fuertes obligaciones a las organizaciones para asegurar la protección de los datos.
- **Directiva NIS (2016):** Obliga a los estados miembros a mantener un nivel de seguridad adecuado de las redes y sistemas de información esenciales, y promover la cooperación entre los estados miembros.

2.7.1.2 CIBERSEGURIDAD EN ESTADOS UNIDOS

Estados Unidos ha implementado diversas legislaciones que abordan la seguridad y la integridad de la infraestructura crítica, incluyendo:

- **Ley de Ciberseguridad Nacional (2015):** Facilita la compartición de información sobre ciber amenazas y establece un marco para proteger la infraestructura crítica.
- **Estrategia Nacional para la Seguridad Cibernética:** Ofrece directrices para coordinar los esfuerzos de ciberseguridad en el gobierno y el sector privado, enfatizando la protección de sectores clave como el transporte y las telecomunicaciones.

2.7.1.3 CIBERSEGURIDAD EN ASIA

Asia presenta un panorama variado en cuanto a ciberseguridad, con legislaciones nacionales que reflejan las preocupaciones locales y regionales:

- **Ley de Ciberseguridad de China (2017):** Impone estrictos controles sobre la recopilación, almacenamiento y transmisión de datos personales, además de requerir que los operadores de infraestructura crítica fortalezcan sus medidas de seguridad.

- **Ley de Ciberseguridad de Japón:** Amplía las responsabilidades de las organizaciones gubernamentales y privadas para prevenir y responder a ciberataques, y establece un sistema de respuesta nacional.

2.7.1.4 NORMATIVAS Y COOPERACIÓN INTERNACIONAL

Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest, 2001): Este tratado internacional juega un papel crucial al establecer un marco común para la cooperación internacional en la lucha contra la ciberdelincuencia. Proporciona las bases para la protección de sistemas y datos críticos, especialmente en sectores sensibles como el transporte público, fomentando la armonización de las leyes nacionales y facilitando la cooperación judicial transfronteriza.

Iniciativas de la ONU en Ciberseguridad: La Institución de las Naciones Unidas promueve la cooperación internacional a través de resoluciones y directrices que apuntan a fortalecer la seguridad global de las redes de información, con especial atención a las infraestructuras críticas y la prevención del cibercrimen.

2.7.1.5 ESPECIALIZACIÓN EN PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

La protección de infraestructuras críticas como los sistemas de transporte público requiere un enfoque específico y detallado debido a su vulnerabilidad y al impacto potencial de los ataques:

- **Directrices Específicas para el Sector de Transporte:** Los gobiernos, en cooperación con el sector privado, deben desarrollar y aplicar políticas específicas que aborden los riesgos cibernéticos en el transporte, incluyendo la protección de sistemas de control y datos operativos esenciales.
- **Programas de Formación y Concienciación:** Capacitar al personal en prácticas de ciberseguridad y desarrollar una cultura de seguridad que permita una respuesta rápida y efectiva ante incidentes cibernéticos.

2.7.2 MARCO LEGAL NACIONAL

Discute la legislación nacional hondureña que regula la ciberseguridad, destacando cómo estas leyes impactan directamente en las operaciones del IHTT. Esto incluye leyes sobre la protección de datos personales, seguridad de la infraestructura crítica y requisitos de cumplimiento

para entidades gubernamentales.

2.7.2.1 LEYES Y REGULACIONES FUNDAMENTALES

LEY DE PROTECCIÓN DE DATOS PERSONALES (2018):

Esta ley regula el tratamiento de los datos personales, incluyendo su recopilación, almacenamiento, uso y transmisión. Establece las obligaciones de las entidades públicas y privadas para garantizar la protección de los datos personales de los ciudadanos hondureños.

LEY DE DELITOS INFORMÁTICOS (2017):

Conocida formalmente como "Ley Especial Contra los Delitos Informáticos", esta legislación aborda los aspectos penales de los delitos cometidos mediante el uso de tecnologías de la información, protegiendo así contra el acceso ilegal, la interceptación no autorizada, el fraude informático, y la violación de datos.

2.7.2.2 MARCO REGULATORIO PARA LA SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR PÚBLICO:

Desarrollado por la Secretaría de Seguridad, este marco regula las medidas de seguridad que deben implementar las instituciones gubernamentales para proteger la infraestructura crítica de la información contra ataques cibernéticos y violaciones de datos.

2.7.2.3 INICIATIVAS Y ESTRATEGIAS NACIONALES

ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA:

Esta estrategia proporciona un plan integral para fortalecer la resiliencia de Honduras frente a las amenazas cibernéticas. Incluye la colaboración entre agencias gubernamentales, el sector privado y la sociedad civil para desarrollar competencias nacionales en ciberseguridad.

CENTRO NACIONAL DE RESPUESTA A INCIDENTES CIBERNÉTICOS (CERT-HN):

Este centro opera como la principal entidad para la gestión de incidentes de ciberseguridad en Honduras. Su función es coordinar la respuesta a incidentes cibernéticos, ofrecer asistencia técnica y promover las mejores prácticas de seguridad entre las instituciones críticas.

2.7.2.4 COOPERACIÓN INTERNACIONAL Y COMPROMISOS

ADHESIÓN A ACUERDOS INTERNACIONALES:

Honduras ha firmado varios tratados internacionales que involucran la cooperación en la lucha contra el ciberdelito, incluyendo el Convenio de Budapest sobre Ciberdelincuencia, comprometiéndose a adoptar estándares internacionales y colaborar en investigaciones transfronterizas.

COLABORACIONES BILATERALES Y MULTILATERALES:

A través de acuerdos con otros países y organizaciones internacionales, Honduras busca fortalecer su capacidad de ciberseguridad mediante el intercambio de información, el desarrollo de capacidades y el apoyo técnico mutuo.

2.7.2.5 DESAFÍOS Y FUTURAS DIRECCIONES

A pesar de los avances en la legislación y la creación de infraestructuras para la ciberseguridad, Honduras enfrenta desafíos continuos debido a recursos limitados y la necesidad de una mayor concienciación y formación en ciberseguridad a todos los niveles.

La actualización y la expansión de las leyes existentes, junto con una inversión continua en tecnologías de seguridad y capital humano, son esenciales para mantener y mejorar la capacidad de respuesta nacional a las amenazas cibernéticas.

CAPÍTULO III – METODOLOGÍA DE LA INVESTIGACIÓN

3.1 ENFOQUE (MIXTO)

Esta es la razón por la que la metodología de investigación mixta es fundamental para tratar la complejidad que rodea la ciberseguridad en el Instituto Hondureño de Transporte Terrestre (IHTT). La metodología proporciona la plataforma adecuada para capitalizar las fortalezas tanto de los métodos cuantitativos como de los cualitativos, lo que garantiza una perspectiva dual en la investigación de estos incidentes. Según (Creswell, 2018), la perspectiva dual implica no solo la cuantificación de los incidentes de seguridad sino también el entendimiento cualitativo de las causas y las percepciones. Los métodos cuantitativos aportarán información objetiva sobre la frecuencia, los tipos y las repercusiones de los incidentes de seguridad, facilitando el análisis estadístico y la comparación con medidas estándar de referencia en la industria (Creswell & Creswell, 2018).

Por otro lado, el componente cualitativo de la investigación explorará las actitudes, creencias y comportamientos del personal que interactúa con los sistemas de TI en el IHTT. Este enfoque es crucial para descubrir factores contextuales y organizacionales que pueden influir en la eficacia de las medidas de seguridad implementadas. A través de entrevistas, grupos focales y análisis de casos específicos, se obtendrán insights detallados sobre cómo la cultura organizacional, la capacitación en seguridad y las políticas internas afectan la gestión de la ciberseguridad. Según (Smith J. , 2022), el análisis cualitativo es esencial para comprender no solo qué sucede cuando se producen incidentes de seguridad, sino también por qué suceden y cómo se pueden prevenir de manera más efectiva en el futuro (Smith J. , 2022).

Este enfoque mixto no solo enriquece la comprensión del investigador sobre el problema,

sino que también permite una triangulación de datos, mejorando la fiabilidad y la validez de los resultados de la investigación. Además, facilita el desarrollo de recomendaciones más efectivas y contextualmente adecuadas para mejorar las prácticas de ciberseguridad en el IHTT. La combinación de métodos cuantitativos y cualitativos permite un análisis más completo y profundo, abordando tanto la amplitud como la profundidad del problema de ciberseguridad en la institución.

3.2 ALCANCE (DESCRIPTIVO, EXPLORATORIO)

El alcance de esta tesis es fundamental para comprender y mitigar las complejidades de la ciberseguridad en el Instituto Hondureño de Transporte Terrestre (IHTT). De manera exploratoria, se identificarán y documentarán áreas no examinadas previamente para revelar vulnerabilidades ocultas en la infraestructura tecnológica y operativa. Según (Smith J. T., 2023), la exploración de estas áreas permite una mejor comprensión de los puntos débiles y fortalezas dentro de las organizaciones, facilitando la implementación de medidas correctivas.

Se investigará cómo se identifican, se comunican y se gestionan los incidentes de seguridad dentro de la institución, explorando tanto los mecanismos de detección como de respuesta. Adicionalmente, el enfoque descriptivo proporcionará un análisis exhaustivo de los protocolos y medidas de seguridad actuales, evaluando su conformidad con las normativas internacionales y su efectividad ante las amenazas emergentes. Según (Smith J. , 2022), la evaluación de los protocolos de seguridad y su alineación con los estándares internacionales es crucial para asegurar una postura de seguridad robusta y eficaz.

Esta dualidad de enfoques permitirá no solo diagnosticar la efectividad de las prácticas existentes, sino también formular recomendaciones basadas en evidencias para robustecer la postura de seguridad del IHTT, con el objetivo de prevenir la recurrencia de incidentes cibernéticos y fortalecer la resiliencia organizacional. La importancia de un enfoque integral que combine la exploración y la descripción de las prácticas de seguridad es subrayada por las mejores prácticas en ciberseguridad, donde una evaluación detallada y basada en evidencias es esencial para la mejora continua de la seguridad cibernética en cualquier institución.

3.3 DISEÑO

3.3.1 POBLACIÓN

Población Objetivo:

La población objetivo de este estudio abarca múltiples niveles y funciones dentro del IHTT, desde el personal técnico de TI que gestiona directamente los sistemas hasta la alta dirección que formula las políticas estratégicas. Además, se incluirán los abogados que trabajan con expedientes críticos, los operadores de ventanilla en diversas regionales, y los inspectores de campo que regulan el transporte y vigilan el cumplimiento de los transportistas. Esta diversidad permite una comprensión integral de cómo las políticas de seguridad se implementan y afectan a diferentes niveles de la institución y en distintos contextos operativos. Capturar las perspectivas de estos grupos es crucial para identificar las fallas técnicas y las brechas en la gestión y comunicación que pueden exponer al IHTT a riesgos significativos, la población incluye aproximadamente 366 empleados distribuidos de la siguiente manera:

- Técnicos de TI: 18 personas
- Abogados: 30 personas
- Operadores de Ventanilla: 18 personas en 4 regionales (Tegucigalpa, San Pedro Sula, Choluteca, La Ceiba)
- Inspectores de Campo: 100 personas
- Otros Empleados: 200 personas involucrados en diversas operaciones internas

3.3.2 MUESTRA

Para garantizar una representación adecuada de toda la población del IHTT, se seleccionará una muestra estratificada que incluya un porcentaje de cada área. Esto se traduce en la siguiente distribución:

- Técnicos de TI: 10 personas
- Abogados: 15 personas
- Operadores de Ventanilla: 2 personas por regional, total 8 personas.
- Inspectores de Campo: 20 personas
- Otros Empleados: 30 personas

La técnica de muestreo estratificado se empleó para garantizar que cada segmento de la

población esté adecuadamente representado. Esta técnica permite segmentar la población en subgrupos más homogéneos según características específicas como el rol ocupacional, la ubicación geográfica y la función dentro de la organización (Creswell, 2018). Esto facilita la recolección de datos precisos y representativos, permitiendo un análisis detallado y fiable de las prácticas de seguridad en todas las áreas del IHTT.

El muestreo estratificado es especialmente valioso en este contexto, ya que asegura que se incluyan todas las perspectivas relevantes, desde el personal técnico hasta los usuarios finales de los sistemas de información (Babbie, 2016). Esto permite identificar variaciones en las prácticas de seguridad y en la percepción de riesgos entre diferentes grupos dentro de la organización. Además, la representación equilibrada de cada grupo facilita la identificación de necesidades específicas y la implementación de soluciones de ciberseguridad más efectivas.

La muestra seleccionada permitirá obtener datos cuantitativos y cualitativos que reflejen fielmente la realidad del IHTT. Los datos cuantitativos proporcionarán una visión general de las prácticas de seguridad y los riesgos, mientras que los datos cualitativos ofrecerán una comprensión más profunda de las experiencias y percepciones de los empleados (Creswell, 2018). Esta combinación de datos es crucial para desarrollar una estrategia de ciberseguridad integral y bien informada.

3.3.3 TÉCNICA MUESTREO

La adopción del muestreo estratificado en este estudio es imperativa para garantizar la representatividad integral y precisa de la diversidad del personal del IHTT. Esta técnica, descrita por (Babbie, 2016), facilita la subdivisión de la población en grupos según criterios específicos tales como función dentro de la institución, ubicación geográfica, y rol ocupacional. Este proceso de segmentación es vital no solo para la obtención de datos detallados y representativos, sino también para conducir un análisis y confiable de las prácticas de seguridad en vigor. Al establecer subgrupos claramente definidos, es posible identificar con precisión variaciones sutiles y tendencias en las prácticas de seguridad, lo cual es crucial para el desarrollo de intervenciones ajustadas a las necesidades y particularidades de cada grupo. Este enfoque metodológico no solo incrementa la precisión del estudio, sino que también sienta las bases para una estrategia de intervención bien informada y específica, permitiendo abordar de manera proactiva y eficaz las necesidades de seguridad de cada segmento del personal del IHTT. Este nivel de detalle es esencial

para formular recomendaciones que no solo sean generales y amplias, sino específicamente adaptadas a las realidades operativas y de seguridad de las distintas áreas y departamentos del instituto, conforme a (Babbie, 2016).

3.4 TABLA DE CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Criterio	Perfil	Inclusión	Exclusión
Edad	Todos	Empleados entre 25 y 60 años.	Empleados menores de 25 años o mayores de 60 años.
Puesto	Técnicos de TI	Personal técnico que tenga al menos 1 año de experiencia en el área de TI del IHTT.	Empleados que no pertenecen al área de TI o con menos de 1 año de experiencia.
	Abogados	Personal legal con al menos 1 año de experiencia en la gestión de expedientes legales en el IHTT.	Empleados que no pertenecen al área legal o con menos de 1 año de experiencia.
	Operadores de Ventanilla	Personal de ventanilla con al menos 6 meses de experiencia en la atención al público en las regionales del IHTT.	Empleados que no pertenecen al área de ventanilla o con menos de 6 meses de experiencia.
	Inspectores de Campo	Inspectores con al menos 1 año de experiencia en el monitoreo y regulación del transporte público.	Empleados que no pertenecen al área de inspección de campo o con menos de 1 año de experiencia.
	Otros Empleados	Empleados con al menos 6 meses de experiencia en cualquier otra área que interactúe con los sistemas de información del IHTT.	Empleados con menos de 6 meses de experiencia o que no interactúan con los sistemas de información del IHTT.
Antigüedad	Todos	Al menos 6 meses de experiencia en el IHTT.	Menos de 6 meses de experiencia en el IHTT.
Experiencia	Técnicos de TI	Participación activa en la gestión y mantenimiento de sistemas de TI.	Empleados sin experiencia en la gestión y mantenimiento de sistemas de TI.
	Abogados	Participación en la gestión de expedientes legales.	Empleados sin experiencia en la gestión de expedientes legales.
	Operadores de Ventanilla	Experiencia en la atención al público y manejo de datos en ventanillas.	Empleados sin experiencia en la atención al público y manejo de datos en ventanillas.
	Inspectores de Campo	Experiencia en la regulación y monitoreo del transporte público.	Empleados sin experiencia en la regulación y monitoreo del transporte público.

	Otros Empleados	Participación en la operación de sistemas de información del IHTT.	Empleados sin experiencia en la operación de sistemas de información del IHTT.
Disponibilidad	Todos	Empleados que consienten participar y tienen disponibilidad durante el estudio.	Empleados que no consienten participar o no tienen disponibilidad.
Formación	Técnicos de TI	Formación académica en áreas de tecnología de la información o disciplinas afines.	Empleados sin formación académica en áreas de tecnología de la información o disciplinas afines.
	Abogados	Formación académica en derecho o áreas relacionadas.	Empleados sin formación académica en derecho o áreas relacionadas.
	Operadores de Ventanilla	Formación académica en atención al cliente, administración o áreas relacionadas.	Empleados sin formación académica en atención al cliente, administración o áreas relacionadas.
	Inspectores de Campo	Formación académica en áreas relacionadas con la regulación y monitoreo del transporte.	Empleados sin formación académica en áreas relacionadas con la regulación y monitoreo del transporte.
	Otros Empleados	Formación académica en áreas relacionadas con sus respectivas funciones que interactúan con los sistemas de información del IHTT.	Empleados sin formación académica en áreas relacionadas con sus respectivas funciones que interactúan con los sistemas de información del IHTT.

Fuente: Elaboración Propia.

Esta tabla refleja los criterios específicos para seleccionar una muestra adecuada que pueda proporcionar datos relevantes y confiables sobre la ciberseguridad en el IHTT. Estos criterios aseguran que se incluyan individuos que tienen una relación directa con la seguridad de la información y las infraestructuras críticas, lo que es crucial para obtener resultados representativos y útiles para el estudio.

Justificación de la Selección de Criterios y Evaluación de Confiabilidad

En la institución, hemos identificado una necesidad crucial de fortalecer las capacidades del personal y optimizar los procesos internos para alcanzar un estándar superior de eficiencia y calidad en la prestación de servicios. La selección de los criterios expuestos en la tabla adjunta se fundamenta en el diagnóstico actual de nuestra organización, donde se ha observado que el personal carece de los conocimientos y habilidades técnicas necesarias para enfrentar los desafíos que plantea la modernización y digitalización de nuestros sistemas.

Criterios Seleccionados:

Los criterios definidos fueron escogidos tras un análisis exhaustivo de las brechas actuales en las competencias del personal, así como en función de las muestras y datos disponibles que reflejan las áreas críticas que requieren atención inmediata. Cada uno de estos criterios ha sido diseñado para guiar la selección de perfiles que puedan contribuir efectivamente a la consecución de los objetivos estratégicos de la institución.

Confiabilidad de los Instrumentos de Medición:

Dada la importancia de garantizar que los instrumentos de medición que utilizamos sean confiables y precisos, hemos decidido incluir el Alfa de Cronbach como un índice estadístico esencial para evaluar la consistencia interna de nuestras herramientas de medición. Este coeficiente nos permitirá asegurar que los instrumentos empleados en la evaluación de competencias y capacidades del personal proporcionen resultados fiables y válidos, lo que es fundamental para la toma de decisiones informadas.

La incorporación de estos criterios y la utilización del Alfa de Cronbach no solo refuerzan nuestro compromiso con la mejora continua, sino que también aseguran que la inversión en modernización y capacitación del personal resulte en beneficios tangibles y sostenibles para la institución.

3.5 MATRIZ DE OPERACIONALIZACIÓN DE LAS VARIABLES

Tabla 1 - Matriz de Operacionalización de las Variables

VARIABLE INDEPENDIENTE	CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ÍTEMS	FUENTES	INSTRUMENTOS
Implementación de Tecnologías de Seguridad	Proceso de integración y uso de tecnologías avanzadas para proteger la información y sistemas del IHTT.	Protección de datos, Respuesta a incidentes	Número de incidentes de seguridad, tiempo de respuesta	¿Cuál es el número de incidentes de seguridad registrados en un periodo determinado? ¿Cuál es el tiempo promedio de respuesta a incidentes?	Equipo de TI	Encuestas, Cuestionarios
Capacitación en Ciberseguridad	Formación continua del personal en prácticas y conocimientos de ciberseguridad.	Eficacia de la formación, Nivel de concienciación	Nivel de conocimiento, cambio en prácticas de seguridad	¿Cuál es el nivel de conocimiento del personal sobre ciberseguridad? ¿Qué cambios se han observado en las prácticas de seguridad tras la capacitación?	Personal de IHTT	Encuestas, Entrevistas
Eficacia de Políticas de Seguridad	Implementación y seguimiento de políticas internas de seguridad.	Adopción de políticas, Cumplimiento	Grado de cumplimiento de políticas, frecuencia de auditorías	¿Cuál es el grado de cumplimiento de las políticas de seguridad en el IHTT? ¿Con qué frecuencia se realizan auditorías de seguridad?	Directivos y Auditores	Cuestionarios, Revisiones documentales
Uso de Herramientas de Monitoreo	Implementación de sistemas y herramientas para la monitorización continua de la seguridad.	Alcance del monitoreo, Eficacia del monitoreo	Cobertura de monitoreo, detección de incidentes	¿Cuál es el alcance del monitoreo de seguridad? ¿Cuántos incidentes se detectan antes de causar daños significativos?	Equipo de TI	Encuestas, Cuestionarios

Fuente: Elaboración Propia.

3.6 TÉCNICAS, INSTRUMENTOS, PROCEDIMIENTOS Y ANÁLISIS

Detallaremos las técnicas metodológicas, los instrumentos de recolección de datos, los procedimientos y los planes de análisis que utilizaremos en nuestra investigación. Nuestro objetivo es establecer un marco claro y estructurado que permita una evaluación rigurosa y exhaustiva de la ciberseguridad en el IHTT. Al combinar métodos cuantitativos y cualitativos, buscamos capturar tanto la amplitud como la profundidad de los problemas de seguridad, asegurando que los datos recolectados sean completos y precisos. Describiremos el uso de diversos instrumentos, desde encuestas y entrevistas hasta herramientas avanzadas de monitoreo de seguridad. Además, explicaremos los procedimientos específicos para la recolección, análisis e interpretación de los datos. Este enfoque integral no solo nos permitirá identificar y mitigar vulnerabilidades, sino también mejorar la preparación y la capacidad de respuesta del IHTT ante futuros incidentes cibernéticos. Este capítulo refleja nuestro compromiso como profesionales en la mejora continua de la seguridad de nuestra institución y en el establecimiento de estándares que puedan ser adoptados por otras entidades gubernamentales.

Detallaremos las técnicas metodológicas, los instrumentos de recolección de datos, los procedimientos y los planes de análisis que utilizaremos en nuestra investigación. Nuestro objetivo es establecer un marco claro y estructurado que permita una evaluación rigurosa y exhaustiva de la ciberseguridad en el IHTT. Al combinar métodos cuantitativos y cualitativos, buscamos capturar tanto la amplitud como la profundidad de los problemas de seguridad, asegurando que los datos recolectados sean completos y precisos.

En cuanto a la confiabilidad de los instrumentos de medición, utilizaremos el Alfa de Cronbach para evaluar la consistencia interna de las encuestas y otros métodos de recolección de datos. Este índice estadístico es esencial para garantizar que las mediciones sean fiables y que los resultados obtenidos reflejen de manera precisa la realidad observada.

Describiremos el uso de diversos instrumentos, desde encuestas y entrevistas hasta herramientas avanzadas de monitoreo de seguridad. Además, explicaremos los procedimientos específicos para la recolección, análisis e interpretación de los datos. Este enfoque integral no solo nos permitirá identificar y mitigar vulnerabilidades, sino también mejorar la preparación y la capacidad de respuesta del IHTT ante futuros incidentes cibernéticos. Este capítulo refleja nuestro compromiso como profesionales en la mejora continua de la seguridad de nuestra institución y en el establecimiento de estándares que puedan ser adoptados por otras entidades gubernamentales.

3.6.1 TÉCNICAS

Se utilizarán técnicas mixtas que incluyen análisis cuantitativo y cualitativo. Las técnicas cuantitativas se centrarán en la recolección de datos estadísticos sobre la frecuencia y el impacto de los incidentes de seguridad, mientras que las cualitativas explorarán las percepciones y experiencias del personal del IHTT en relación con la ciberseguridad.

3.6.1.1 TÉCNICAS CUANTITATIVAS:

1. **ENCUESTAS ESTRUCTURADAS:**

Se utilizarán encuestas estructuradas para recolectar datos cuantitativos sobre la percepción y conocimiento del personal del IHTT en relación con la ciberseguridad. Las encuestas se administrarán a través de plataformas en línea como JOTFORM, permitiendo una recopilación y análisis eficiente de datos. Estas encuestas incluirán preguntas cerradas que permitan medir variables específicas como el nivel de conocimiento en ciberseguridad, la frecuencia de formación recibida y la percepción de riesgo entre los empleados (Babbie, 2016).

2. **ANÁLISIS ESTADÍSTICO:**

Los datos recopilados mediante las encuestas serán analizados utilizando software estadístico como SPSS o Microsoft Excel. Se aplicarán técnicas de estadística descriptiva e inferencial para identificar patrones, tendencias y correlaciones significativas. Esto permitirá una comprensión profunda de los factores que influyen en la ciberseguridad dentro del IHTT (Babbie, 2016).

3.6.1.2 TÉCNICAS CUALITATIVAS:

1. **ENTREVISTAS SEMIESTRUCTURADAS:**

Se llevarán a cabo entrevistas semiestructuradas con personal clave del IHTT, incluyendo técnicos de TI, abogados, operadores de ventanilla, inspectores de campo y otros empleados. Estas entrevistas permitirán obtener información detallada sobre las experiencias, percepciones y prácticas relacionadas con la ciberseguridad. Las entrevistas se grabarán y transcribirán para su análisis (Johnson M. &., 2021).

2. **GRUPOS FOCALES:**

Los grupos focales se organizarán para discutir en profundidad los desafíos y soluciones percibidos en torno a la ciberseguridad. Estos grupos proporcionarán un entorno colaborativo donde los participantes pueden compartir sus ideas y experiencias, lo que enriquecerá el análisis

cualitativo con perspectivas diversas (Romanosky, 2016).

3.6.1.3 TÉCNICAS DE MONITOREO Y EVALUACIÓN:

1. AUDITORÍAS DE SEGURIDAD:

Se realizarán auditorías de seguridad utilizando herramientas avanzadas como Nessus y OpenVAS para identificar vulnerabilidades en la infraestructura de TI del IHTT. Estas auditorías proporcionarán datos técnicos detallados sobre los puntos débiles del sistema y servirán como base para desarrollar estrategias de mitigación (NIST., 2021).

2. MONITOREO CONTINUO:

Se implementará un sistema de monitoreo continúo utilizando soluciones como Juniper y Huawei Cloud Host Security Service. Estas herramientas permitirán la detección en tiempo real de amenazas y actividades sospechosas, facilitando una respuesta rápida y efectiva a incidentes de seguridad (Ventures., 2022).

3.6.2 INSTRUMENTOS

Para el análisis cuantitativo, se utilizarán cuestionarios estructurados y herramientas de monitoreo de seguridad informática. Para el análisis cualitativo, se emplearán entrevistas semiestructuradas y grupos focales, proporcionando una visión profunda de las prácticas de seguridad y la cultura organizacional. Las herramientas específicas incluyen:

Microsoft Excel y Google Sheets: Para la organización y análisis de datos cuantitativos.

Juniper: Para la monitorización continua de la seguridad de la red y la identificación de amenazas.

Huawei Cloud Host Security Service: Para asegurar la infraestructura en la nube y proporcionar monitoreo en tiempo real, protección contra ataques y gestión de vulnerabilidades.

3.6.3 PROCEDIMIENTOS

PREPARACIÓN:

En esta fase inicial, se identificaron los participantes clave dentro del Instituto Hondureño de Transporte Terrestre (IHTT), abarcando una amplia gama de roles desde técnicos de TI hasta altos ejecutivos. Se obtendrán los consentimientos informados necesarios para garantizar que todos los participantes comprendan el propósito y los procedimientos del estudio, así como sus derechos y la confidencialidad de su información (Babbie, 2016). La preparación también incluirá la

organización de los recursos y herramientas necesarias para la recolección de datos, asegurando que todos los instrumentos estén calibrados y listos para su uso.

RECOLECCIÓN DE DATOS:

La recolección de datos se llevará a cabo mediante la implementación de cuestionarios y la realización de entrevistas semiestructuradas. Los cuestionarios se distribuirán electrónicamente utilizando plataformas como JOTFORM para facilitar su acceso y respuesta (Babbie, 2016). Las entrevistas se realizarán en persona o virtualmente, dependiendo de la disponibilidad y preferencia de los participantes, y se grabarán con su consentimiento para una posterior transcripción y análisis (Johnson M. &., 2021).

ANÁLISIS DE DATOS:

Una vez recolectados los datos, se procederá al análisis cuantitativo y cualitativo. Los datos cuantitativos obtenidos de los cuestionarios serán analizados utilizando software estadístico como SPSS y Microsoft Excel, aplicando técnicas de estadística descriptiva e inferencial para identificar patrones, tendencias y correlaciones significativas (Babbie, 2016).

INTERPRETACIÓN:

La fase final del procedimiento implicará la integración de los resultados cuantitativos y cualitativos para proporcionar una visión completa y detallada del estado de la ciberseguridad en el IHTT. Esta integración permitirá comparar y contrastar las percepciones y experiencias del personal con los datos estadísticos, proporcionando una comprensión holística que informará las recomendaciones y estrategias de mejora (Von Solms, 2013).

3.6.4 PLAN DE ANÁLISIS DE DATOS

El plan de análisis de datos para esta investigación en el Instituto Hondureño de Transporte Terrestre (IHTT) se desarrollará en varias etapas, asegurando un enfoque metódico y riguroso para interpretar tanto los datos cuantitativos como cualitativos. Este plan incluye la preparación de los datos, el análisis descriptivo e inferencial de los datos cuantitativos, y el análisis temático de los datos cualitativos.

ETAPA 1: PREPARACIÓN DE LOS DATOS

1. RECOLECCIÓN Y ORGANIZACIÓN:

Una vez recolectados, los datos de las encuestas y entrevistas serán organizados en bases de datos electrónicas. Los datos cuantitativos se ingresarán en software estadístico como Microsoft Excel (Babbie, 2016).

2. LIMPIEZA DE DATOS:

Se realizará una revisión exhaustiva para identificar y corregir errores en los datos recolectados. Esto incluye la verificación de entradas duplicadas, la corrección de inconsistencias y el manejo de valores faltantes. Este paso es crucial para garantizar la calidad y la integridad de los datos (Babbie, 2016).

ETAPA 2: ANÁLISIS DE DATOS CUANTITATIVOS

1. ANÁLISIS DESCRIPTIVO:

Se emplearán técnicas de estadística descriptiva para resumir y describir las características principales de los datos. Esto incluirá el cálculo de medidas de tendencia central (media, mediana, moda) y de dispersión (rango, desviación estándar) para proporcionar una visión general de la distribución de las variables (Babbie, 2016).

ETAPA 3: ANÁLISIS DE DATOS CUALITATIVOS

1. ANÁLISIS TEMÁTICO:

Los códigos serán agrupados en categorías temáticas, permitiendo identificar patrones y temas recurrentes en las narrativas de los participantes. Este proceso incluirá la revisión iterativa de los datos para refinar las categorías y asegurar una interpretación precisa y exhaustiva (Romanosky, 2016).

ETAPA 4: INTEGRACIÓN DE RESULTADOS

1. TRIANGULACIÓN DE DATOS:

Los resultados cuantitativos y cualitativos se integrarán utilizando la técnica de triangulación, que permite comparar y contrastar diferentes tipos de datos para obtener una comprensión más completa y precisa del fenómeno estudiado (Von Solms, 2013).

2. INTERPRETACIÓN GLOBAL:

La interpretación final se basará en la combinación de los hallazgos de ambos tipos de

análisis. Se buscará identificar cómo los datos cuantitativos y cualitativos se complementan y qué implicaciones tienen para la estrategia de ciberseguridad del IHTT. Este enfoque integrador asegurará que las recomendaciones se basen en una comprensión holística del contexto y las necesidades específicas de la organización (NIST., 2021).

ETAPA 5: REVISIÓN Y VALIDACIÓN

REVISIÓN INTERNA:

Los hallazgos preliminares serán revisados internamente por el equipo de investigación y otros expertos en ciberseguridad dentro del IHTT. Esta revisión permitirá identificar posibles errores o sesgos y refinar los análisis antes de presentar los resultados finales (Johnson M. &., 2021).

VALIDACIÓN EXTERNA:

Para garantizar la validez y la fiabilidad de los resultados, se realizará una validación externa mediante la consulta a expertos externos en ciberseguridad y auditoría de sistemas. Sus comentarios y recomendaciones serán incorporados para fortalecer los hallazgos y las conclusiones del estudio (Romanosky, 2016).

3.7 FUENTES DE INFORMACIÓN

Para llevar a cabo esta investigación de manera integral y rigurosa, se emplearán tanto fuentes de información primarias como secundarias. La combinación de estos tipos de fuentes permitirá obtener una visión completa y profunda del estado actual de la ciberseguridad en el Instituto Hondureño de Transporte Terrestre (IHTT), facilitando la formulación de recomendaciones basadas en evidencia para mejorar las prácticas de seguridad en la organización.

3.7.1 PRIMARIAS

Las fuentes primarias consisten en datos originales recopilados específicamente para esta investigación. Estas fuentes son cruciales para obtener información directa y relevante del IHTT, asegurando que los hallazgos reflejen con precisión la realidad de la organización.

1. **ENCUESTAS:**

Hemos administrado encuestas estructuradas a una muestra representativa de empleados

del IHTT, incluidos técnicos de TI, abogados, operadores de ventanilla, inspectores de campo y otros empleados. Las encuestas se realizaron utilizando plataformas como JOTFORM, y se diseñaron para recoger datos sobre el conocimiento y las prácticas de ciberseguridad, la percepción del riesgo y la efectividad de las medidas de seguridad actuales (Babbie, 2016).

2. ENTREVISTAS:

Hemos llevado a cabo entrevistas semiestructuradas con personal clave del IHTT, proporcionando información cualitativa detallada sobre las experiencias y percepciones relacionadas con la ciberseguridad. Estas entrevistas fueron grabadas y transcritas para un análisis exhaustivo (Johnson M. &., 2021).

3. GRUPOS FOCALES:

Los grupos focales organizados permitieron explorar en profundidad los desafíos y soluciones percibidos en torno a la ciberseguridad. Los participantes discutieron sus experiencias y perspectivas en un entorno colaborativo, enriqueciendo el análisis cualitativo con diversas voces y opiniones (Romanosky, 2016).

4. AUDITORÍAS DE SEGURIDAD:

Realizamos auditorías de seguridad utilizando herramientas avanzadas como Nessus y Huawei Host Security. Estas auditorías proporcionaron datos técnicos sobre las vulnerabilidades de la infraestructura de TI del IHTT y sirvieron como base para el desarrollo de estrategias de mitigación (NIST., 2021).

3.7.2 SECUNDARIAS

Las fuentes secundarias consisten en datos e información recopilada previamente por otros investigadores y organizaciones. Estas fuentes proporcionan un contexto más amplio y una base teórica sólida para interpretar los hallazgos de la investigación primaria.

1. LITERATURA ACADÉMICA:

Hemos revisado estudios y artículos académicos sobre ciberseguridad, gestión de riesgos y políticas de seguridad en el sector público. En particular, se consultaron casos de estudio sobre la implementación de marcos de ciberseguridad en instituciones gubernamentales de países en desarrollo, como el caso del Departamento de Seguridad Nacional en Sudáfrica, donde se

adoptaron prácticas basadas en el NIST RMF. Estos estudios proporcionaron un marco teórico robusto para comprender las mejores prácticas y los desafíos comunes en la implementación de medidas de ciberseguridad, lo que influyó directamente en la conceptualización de la estrategia de seguridad propuesta para el IHTT (Von Solms, 2013).

2. INFORMES Y PUBLICACIONES:

Consultamos informes de organismos internacionales, como la Organización de las Naciones Unidas (ONU) y la Agencia de Seguridad Cibernética y de Infraestructura (CISA). Específicamente, se analizaron los informes de la CISA sobre incidentes de ransomware en agencias gubernamentales de los Estados Unidos y el análisis de la ONU sobre la ciberseguridad en infraestructuras críticas de América Latina. Estos informes no solo contextualizaron los hallazgos del IHTT dentro de las tendencias y estándares globales, sino que también proporcionaron recomendaciones que fueron adaptadas y aplicadas en el desarrollo de la propuesta del IHTT dentro de las tendencias y estándares globales (Ventures., 2022).

3. DOCUMENTACIÓN INTERNA:

Revisamos documentos internos del IHTT, como políticas de seguridad, registros de incidentes de seguridad, y memorandos sobre adquisiciones de tecnología. Se prestó especial atención a los casos de incidentes de seguridad cibernética ocurridos en enero de 2024, que resultaron en la interrupción de servicios clave, y a las políticas implementadas como respuesta a estos incidentes. Esta documentación fue crucial para comprender las deficiencias actuales y determinar las áreas críticas que necesitaban ser reforzadas en la nueva estrategia de ciberseguridad (NIST., 2021).

4. ESTUDIOS DE CASO:

Analizamos estudios de caso de otras instituciones gubernamentales que han implementado con éxito medidas de ciberseguridad, en particular, se revisaron casos del Departamento de Seguridad Nacional de Sudáfrica, que implementó un marco de ciberseguridad basado en el NIST RMF, y del Ministerio del Interior en Chile, que adoptó políticas de seguridad siguiendo las directrices de la ISO/IEC 27001. Estos estudios permitieron identificar estrategias efectivas y adaptarlas al contexto del IHTT, proporcionando lecciones clave sobre la gestión de riesgos y la implementación de controles de seguridad en entornos gubernamentales (Johnson M. &., 2021).

3.9 MATRIZ DE CONGRUENCIA

Tabla 2 - Matriz Congruencia

PREGUNTA GENERAL	OBJETIVO GENERAL	PREGUNTAS ESPECÍFICAS	OBJETIVOS ESPECÍFICOS	TIPO DEB METODOLOGÍA	VARIABLES	INDICADORES	INSTRUMENTOS
¿De qué manera la implementación de una estrategia integral de ciberseguridad puede mejorar la protección y resiliencia de la infraestructura de TI del IHTT?	Desarrollar una estrategia de ciberseguridad integral para el IHTT que refuerce la infraestructura de TI y asegure la continuidad operativa frente a amenazas cibernéticas.	¿Cuáles son las principales vulnerabilidades de seguridad en el IHTT y cómo se pueden mitigar?	Identificar y mitigar las vulnerabilidades explotadas en el reciente ataque cibernético mediante soluciones inmediatas y a largo plazo.	Mixta	Vulnerabilidades de seguridad	Número de vulnerabilidades identificadas y mitigadas	Auditorías de seguridad y cuestionarios estructurados
		¿Qué procesos y protocolos deben establecerse para mejorar la detección temprana de amenazas?	Establecer un marco de colaboración para la implementación de medidas de ciberseguridad de emergencia.	Mixta	Procesos y protocolos de seguridad	Nivel de detección y respuesta a amenazas	Entrevistas y grupos focales
		¿De qué manera la capacitación en ciberseguridad del personal puede contribuir a la prevención de ataques futuros?	Crear un sistema educativo continuo en ciberseguridad para capacitar al personal de TI y a los usuarios finales en prácticas seguras.	Cualitativa	Conocimiento y prácticas de ciberseguridad del personal	Nivel de conocimiento y prácticas seguras adoptadas	Cuestionarios y encuestas
		¿Cómo se puede diseñar e implementar un sistema integral de seguridad desde cero en el IHTT?	Proponer e implementar un sistema integrado que incluya hardware y software modernos, respaldado por políticas internas.	Cuantitativa	Eficacia del sistema integral de seguridad	Nivel de protección y rendimiento del sistema	Informes de implementación y auditorías técnicas

Fuente: Elaboración Propia.

CAPÍTULO IV – RESULTADOS Y ANÁLISIS

4.1 INFORME DE RECOLECCIÓN DE INFORMACIÓN

Para evaluar la situación actual de la ciberseguridad en el Instituto Hondureño de Transporte Terrestre (IHTT), se llevaron a cabo encuestas dirigidas a cinco grupos específicos de empleados: Técnicos de TI, Abogados, Operadores de Ventanilla, Inspectores de Campo y Otros Empleados. Esta segmentación estratégica se realizó con el fin de obtener una perspectiva integral y representativa de las prácticas, conocimientos y percepciones de ciberseguridad dentro de la institución. La diversidad de los grupos seleccionados garantiza que se capten las variaciones en el manejo de la seguridad de la información a través de diferentes roles y responsabilidades dentro del IHTT.

Cada grupo de empleados desempeña un papel crucial en la operación diaria y en la protección de los sistemas de información del IHTT. Los Técnicos de TI son responsables directos de la implementación y mantenimiento de las infraestructuras de seguridad tecnológica, mientras que los Abogados manejan información legal confidencial que requiere estrictos controles de acceso y protección. Por su parte, los Operadores de Ventanilla interactúan directamente con el público y manejan datos sensibles, lo que los hace vulnerables a diversas amenazas de seguridad. Los Inspectores de Campo, que operan en entornos externos, enfrentan desafíos únicos en términos de protección de dispositivos y datos. Finalmente, el grupo de Otros Empleados abarca una amplia gama de funciones administrativas y operativas que también interactúan con los sistemas de información y, por ende, son parte integral del ecosistema de seguridad del IHTT.

A continuación, se presentan los resultados detallados de estas encuestas y su análisis correspondiente, con el objetivo de identificar las fortalezas y debilidades en la estrategia de ciberseguridad del IHTT. Este análisis exhaustivo proporcionará una base sólida para la formulación de recomendaciones y la implementación de mejoras necesarias para proteger la integridad y la confidencialidad de los datos manejados por la institución. Los resultados obtenidos no solo reflejan la situación actual, sino que también subrayan la importancia de una formación continua y una actualización constante de las tecnologías y políticas de seguridad para enfrentar las amenazas cibernéticas emergentes.

4.2 PRESENTACIÓN DE RESULTADOS Y SU ANÁLISIS

4.2.1 RESULTADOS OBJETIVO 1: IDENTIFICAR Y MITIGAR LAS VULNERABILIDADES EXPLOTADAS EN EL RECIENTE ATAQUE CIBERNÉTICO MEDIANTE SOLUCIONES INMEDIATAS Y A LARGO PLAZO.

TÉCNICOS DE TI

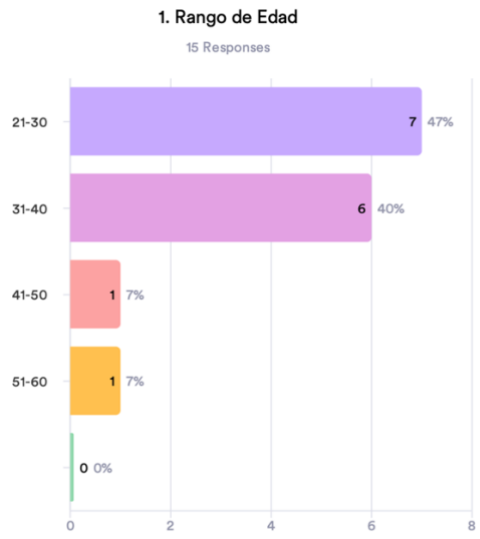

Figura 1 - Rango de Edad Técnicos TI

Fuente: Elaboración Propia.

1. **RANGO DE EDAD:** La mayoría de los técnicos de TI (47%) están en el rango de edad de 21-30 años, seguido por el grupo de 31-40 años (40%). Este rango sugiere que el personal de TI es relativamente joven, lo cual puede ser ventajoso dado que las nuevas generaciones suelen estar más familiarizadas con las tecnologías emergentes.

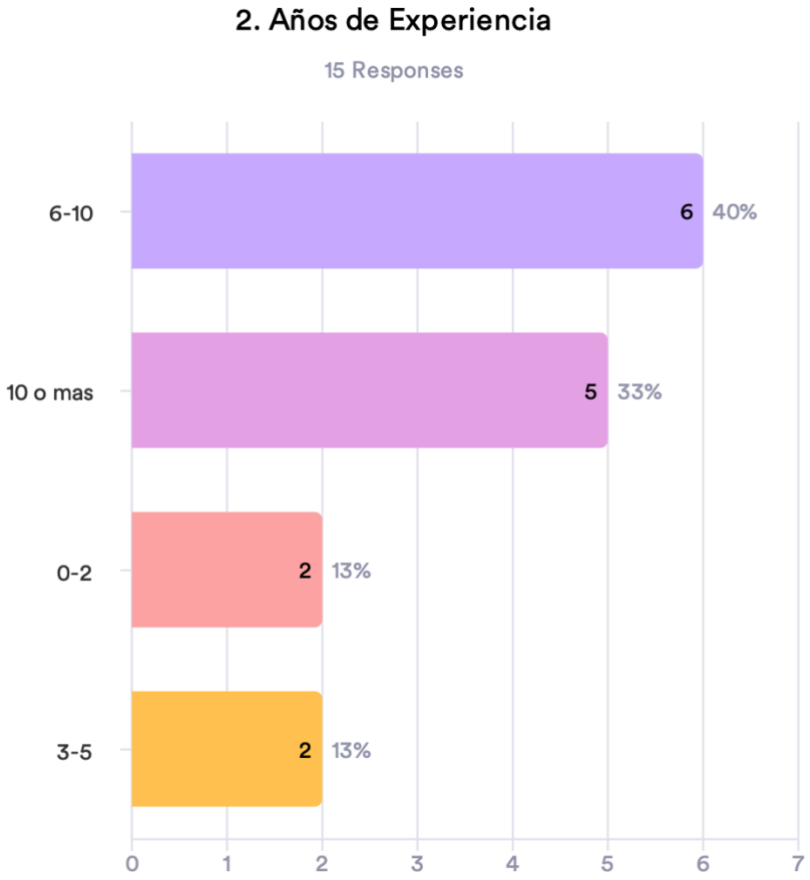

Figura 2 - Años de Experiencia Técnicos TI

Fuente: Elaboración Propia.

2. **AÑOS DE EXPERIENCIA:** La experiencia de los técnicos está diversificada con 40% teniendo entre 6-10 años y 33% con más de 10 años de experiencia. Esto indica un buen balance entre personal experimentado y personal más reciente, lo cual es crucial para mantener una perspectiva actualizada y al mismo tiempo contar con la sabiduría que brinda la experiencia.

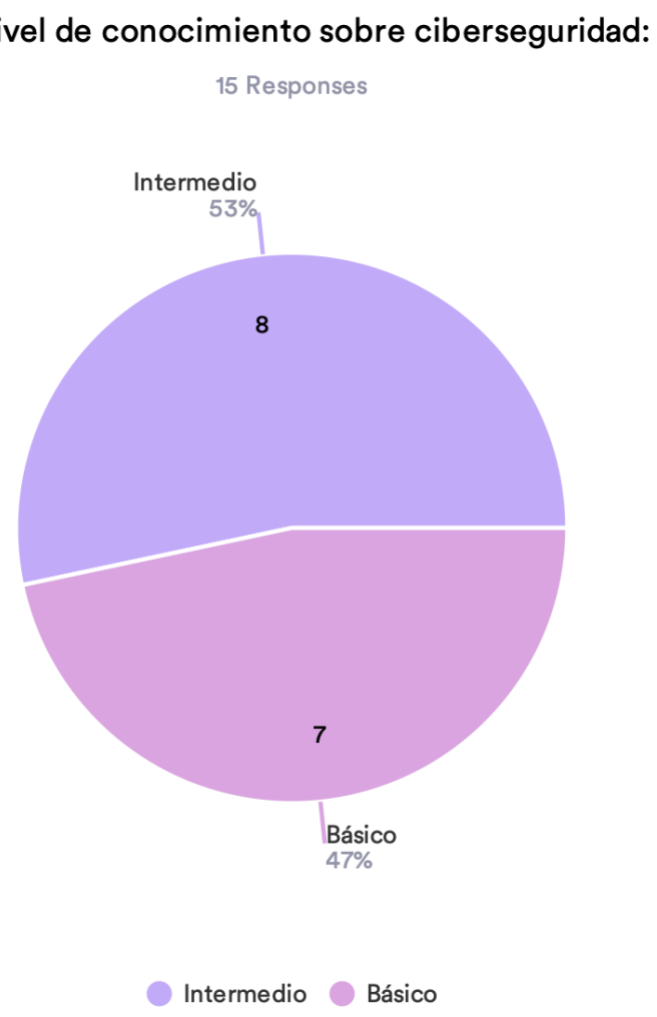

Figura 3 - Conocimiento en Ciberseguridad Técnicos TI

Fuente: Elaboración Propia.

3. **NIVEL DE CONOCIMIENTO:** Un 53% de los técnicos tiene un conocimiento intermedio sobre ciberseguridad, mientras que el 47% tiene un conocimiento básico. Esto refleja una necesidad significativa de elevar el nivel de conocimiento a través de capacitaciones avanzadas y continuas.

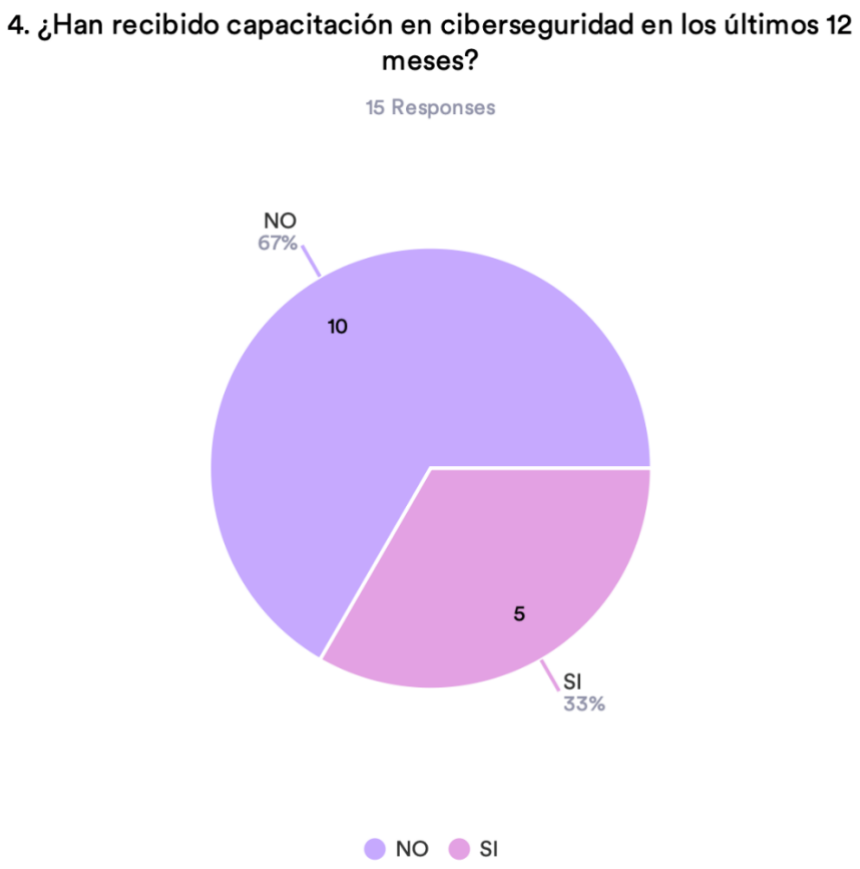

Figura 4 - Capacitación Técnicos TI

Fuente: Elaboración Propia.

4. **CAPACITACIÓN EN CIBERSEGURIDAD:** El 67% no ha recibido capacitación en los últimos 12 meses. Este es un indicador alarmante que subraya la necesidad urgente de implementar programas de capacitación regular para mantener al personal actualizado sobre las amenazas cibernéticas y las mejores prácticas de seguridad.

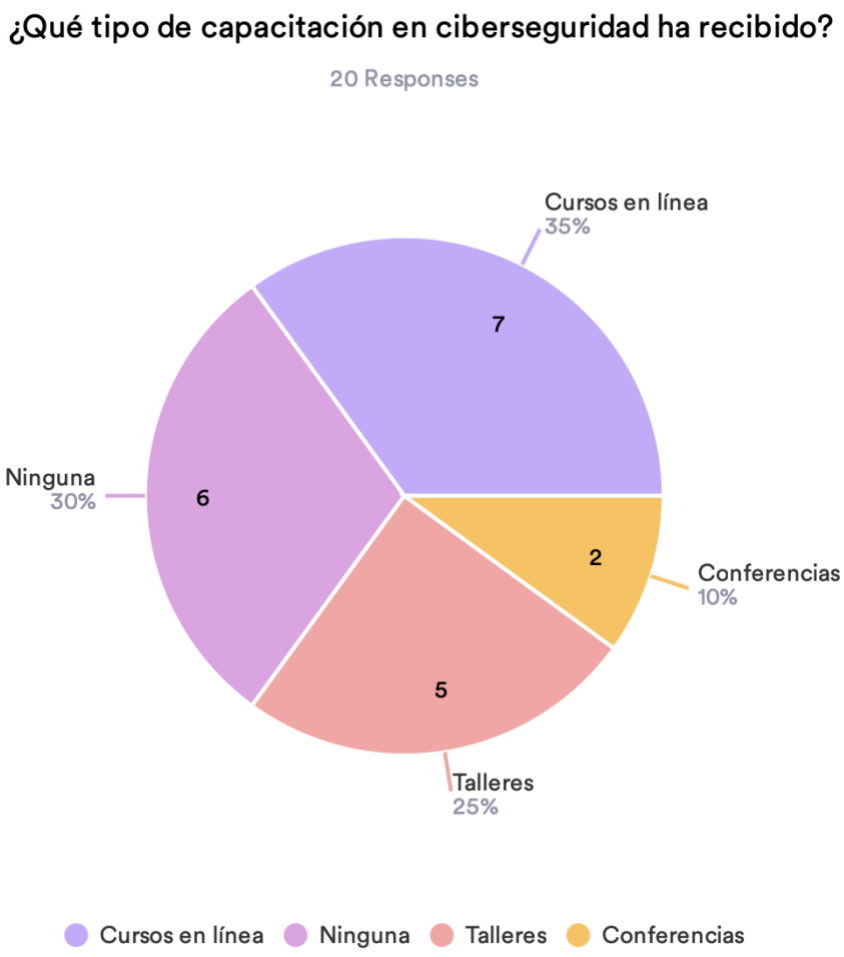

Figura 5 - Tipo Capacitación Técnicos TI

Fuente: Elaboración Propia.

5. **TIPO DE CAPACITACIÓN RECIBIDA:** Los cursos en línea (35%) y los talleres (25%) fueron los más mencionados. Esto sugiere que las modalidades flexibles como los cursos en línea son preferidas, lo cual puede ser una consideración importante para futuras capacitaciones.

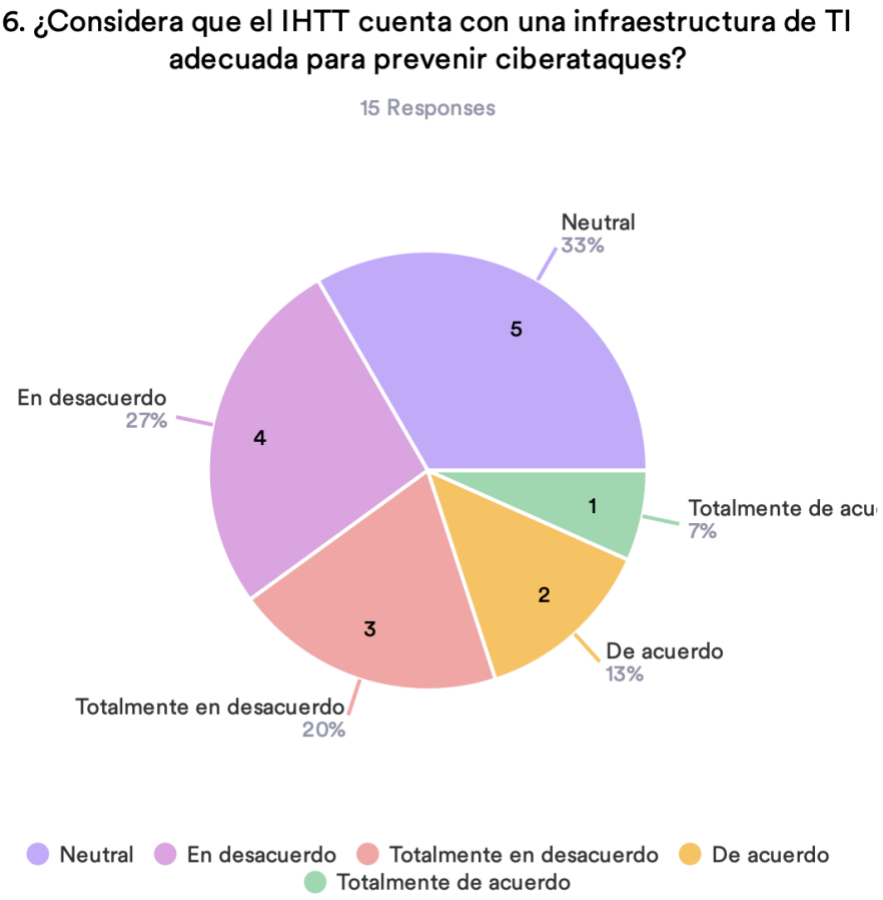

Figura 6 - Infraestructura Adecuada Técnicos TI

Fuente: Elaboración Propia.

6. **ADECUACIÓN DE LA INFRAESTRUCTURA DE TI:** Solo el 20% considera que la infraestructura es adecuada para prevenir ciberataques, mientras que un 47% se mantiene neutral o en desacuerdo. Esto refleja una percepción general de insuficiencia en la infraestructura actual, lo que podría ser debido a la falta de herramientas modernas y actualizaciones regulares.

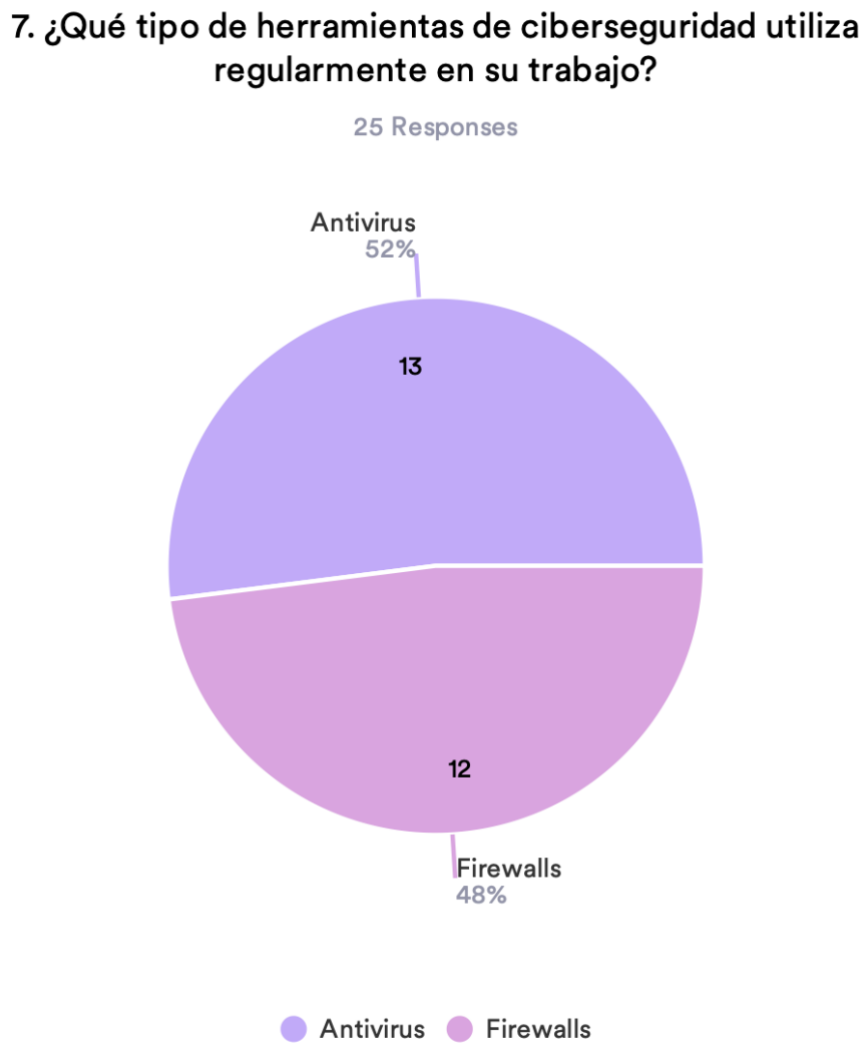

Figura 7 - Herramientas Utilizadas Técnicos TI

Fuente: Elaboración Propia.

7. **HERRAMIENTAS DE SEGURIDAD UTILIZADAS:** Firewalls (40%), antivirus (30%) y sistemas de detección de intrusos (20%) son las herramientas más comúnmente utilizadas. Esto indica una dependencia en tecnologías tradicionales, lo cual podría ser complementado con soluciones más avanzadas como el monitoreo continuo y la inteligencia artificial.

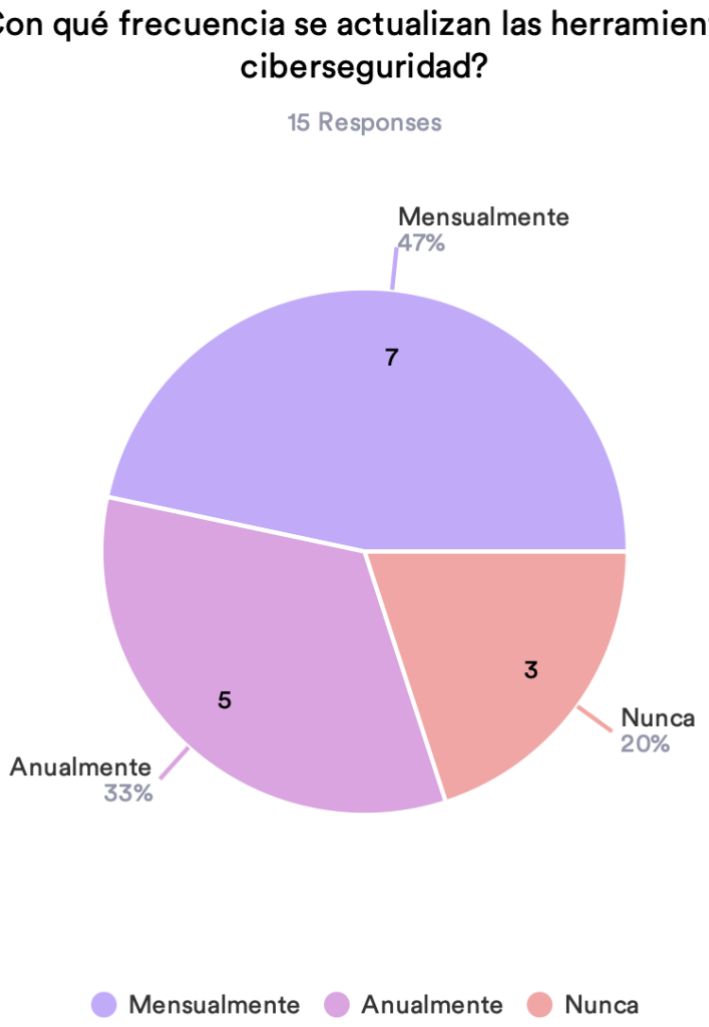

Figura 8 - Frecuencia de Herramientas Utilizadas Técnicos TI

Fuente: Elaboración Propia.

8. **FRECUENCIA DE ACTUALIZACIÓN DE HERRAMIENTAS:** El 47% indica que las herramientas se actualizan mensualmente, un 33% anualmente y un 20% nunca. La falta de actualizaciones regulares es una vulnerabilidad crítica que debe ser abordada de inmediato.

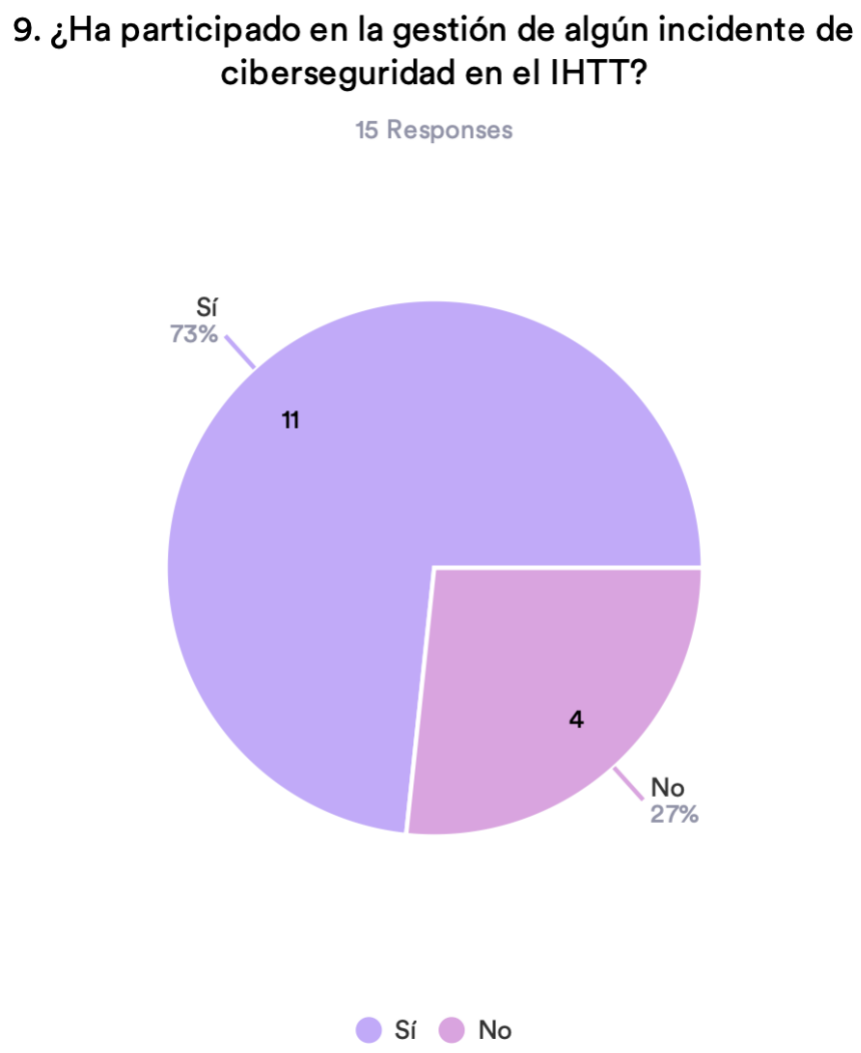

Figura 9 - Gestión de Incidentes Técnicos TI

Fuente: Elaboración Propia.

9. **GESTIÓN DE INCIDENTES:** Un 73% ha participado en la gestión de incidentes, lo que demuestra que los técnicos están relativamente familiarizados con la gestión de incidentes.

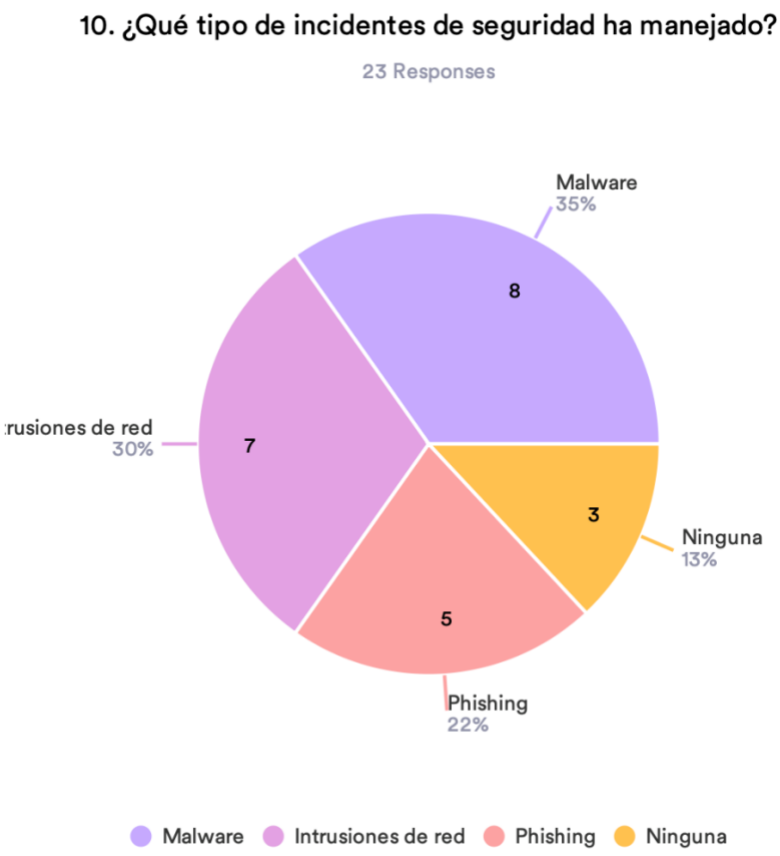

Figura 10 - Tipo Incidentes Técnicos TI

Fuente: Elaboración Propia.

10. **TIPO DE INCIDENTES MANEJADO:** Los tipos más comunes de incidentes manejados incluyen malware (40%), phishing (30%) y intrusiones de red (20%). Esto indica que estos son los problemas de seguridad más frecuentes enfrentados por los técnicos de TI.

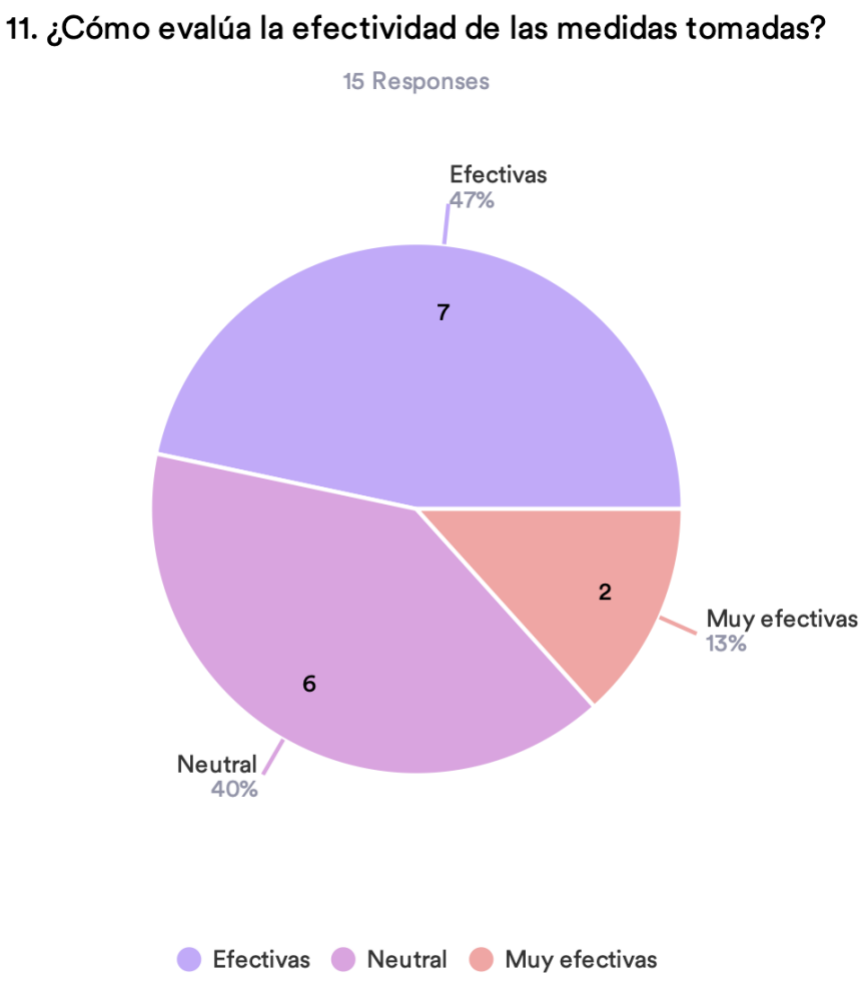

Figura 11 - Efectividad Técnicos TI

Fuente: Elaboración Propia.

11. **EFECTIVIDAD DE LAS MEDIDAS:** Un 47% considera que las medidas fueron efectivas, aunque un 40% se mantiene neutral. Esto sugiere que, si bien se toman medidas, estas no siempre son completamente satisfactorias, destacando la necesidad de mejorar la respuesta y las estrategias de mitigación.

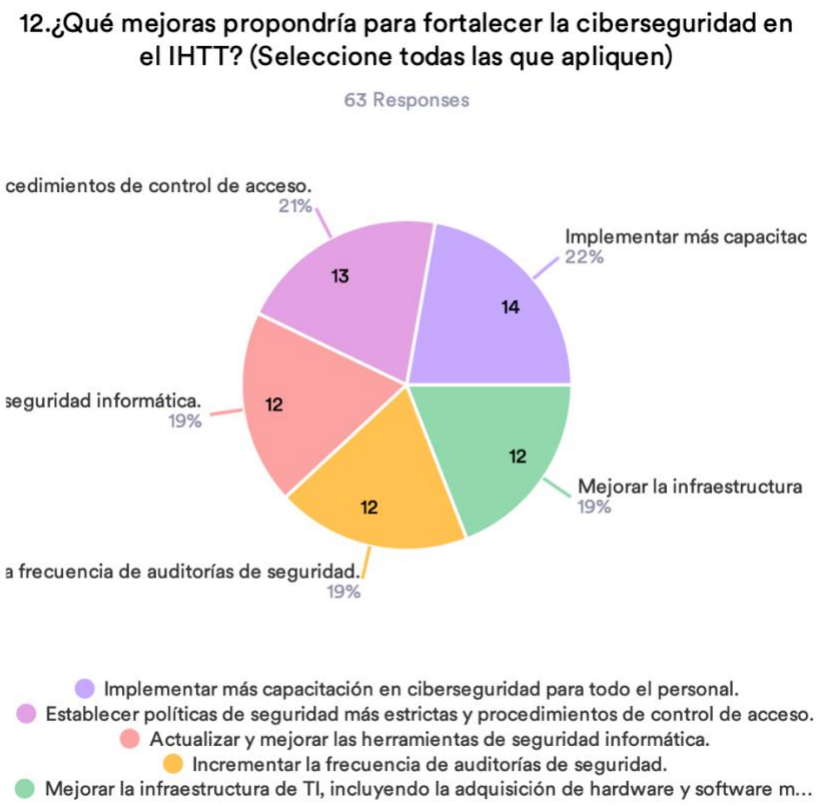

Figura 12 - Fortalecer Ciberseguridad Técnicos TI

Fuente: Elaboración Propia.

12. **PROPUESTA DE MEJORAS:** Un 35% de los técnicos sugiere la implementación de programas de capacitación continuos, mientras que un 30% considera que la actualización regular de herramientas es crucial. Esto muestra una clara demanda de formación y mejoras tecnológicas.

ENCUESTAS DE TÉCNICOS TI:

Los datos obtenidos de los técnicos de TI del IHTT revelan varios puntos críticos en la gestión de la ciberseguridad. Primero, se observa que una buena parte de los técnicos tiene un conocimiento intermedio en ciberseguridad y han recibido capacitación en el último año, lo cual es positivo. Sin embargo, la percepción de insuficiencia en la infraestructura de TI y la necesidad de actualizar regularmente las herramientas de ciberseguridad destacan áreas de mejora. Los incidentes más comunes son el malware y el phishing, y aunque la mayoría considera que las

medidas tomadas han sido efectivas, todavía hay margen para mejorar la respuesta a estos incidentes.

Referencias en Imágenes:

- Figura 6: Infraestructura de TI adecuada.
- Figura 7: Herramientas de ciberseguridad utilizadas.
- Figura 9: Participación en la gestión de incidentes.
- Figura 10: Tipos de incidentes manejados.

CITAS POR CAPÍTULOS:

El objetivo de realizar un análisis detallado de la infracción de seguridad se refiere directamente a los hallazgos sobre la percepción de la insuficiencia en la infraestructura de TI (Capítulo 1.5.2, Objetivo Específico 1).

La necesidad de un protocolo de seguridad digital que incorpore monitorización avanzada se subraya en las conclusiones sobre la gestión de incidentes y la actualización de herramientas de ciberseguridad (Capítulo 1.5.2, Objetivo Específico 3).

ABOGADOS

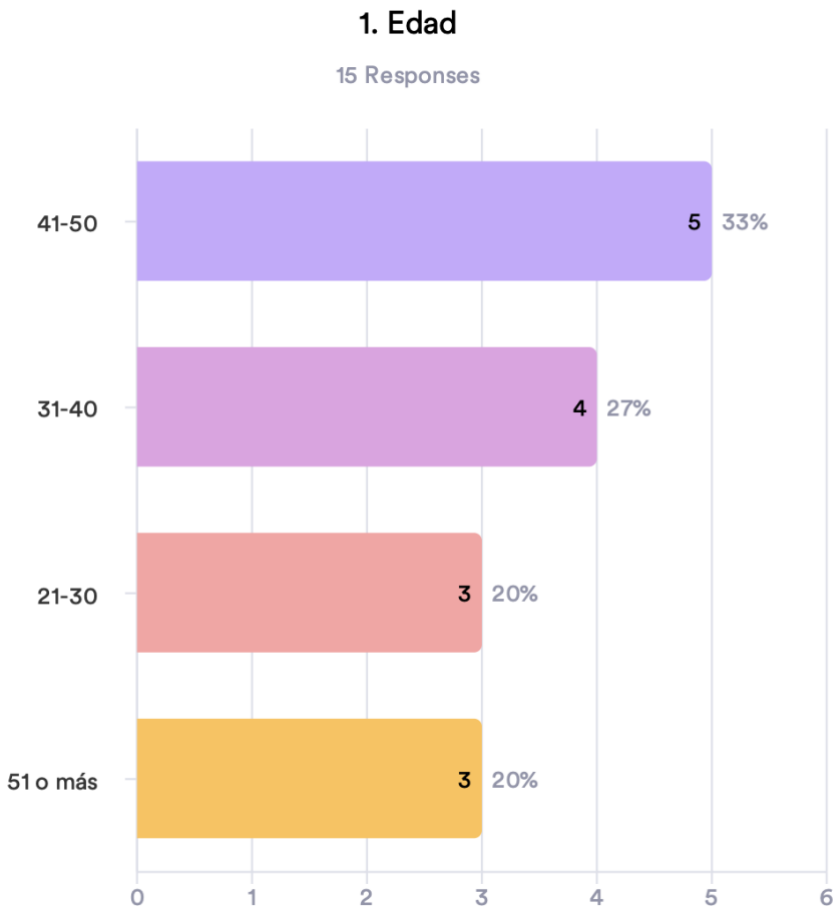

Figura 13 - Rango de Edad Abogados

Fuente: Elaboración Propia.

1. **RANGO DE EDAD:** La mayoría de los abogados (33%) está en el rango de 41-50 años. Esta distribución etaria puede reflejar una combinación de experiencia y madurez en el manejo de casos y decisiones legales.

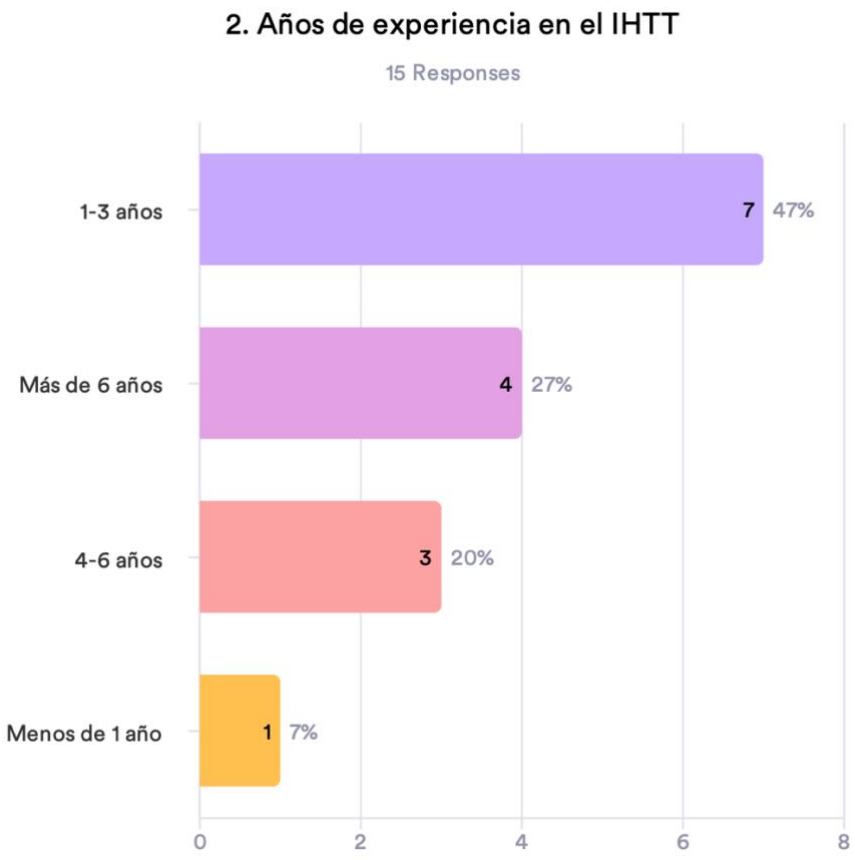

Figura 14 - Años de Experiencia Abogados

Fuente: Elaboración Propia.

2. **AÑOS DE EXPERIENCIA:** Un 47% tiene entre 1-3 años de experiencia en el IHTT. Esto sugiere una relativa novedad en el personal legal, lo que puede requerir programas de inducción más robustos en políticas de seguridad de la información.

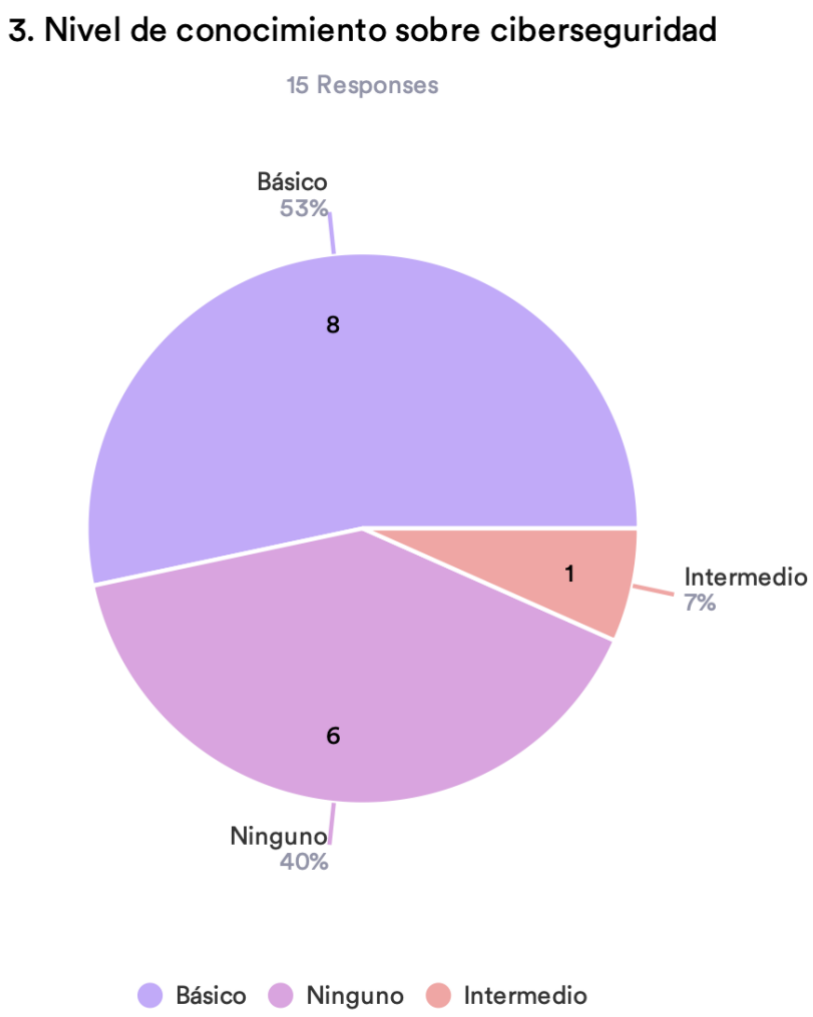

Figura 15 - Conocimiento en Ciberseguridad Abogados

Fuente: Elaboración Propia.

3. **NIVEL DE CONOCIMIENTO:** Un 53% tiene un conocimiento básico sobre ciberseguridad y un 40% no tiene conocimientos. Este bajo nivel de conocimiento en ciberseguridad es preocupante dado que manejan información altamente confidencial.

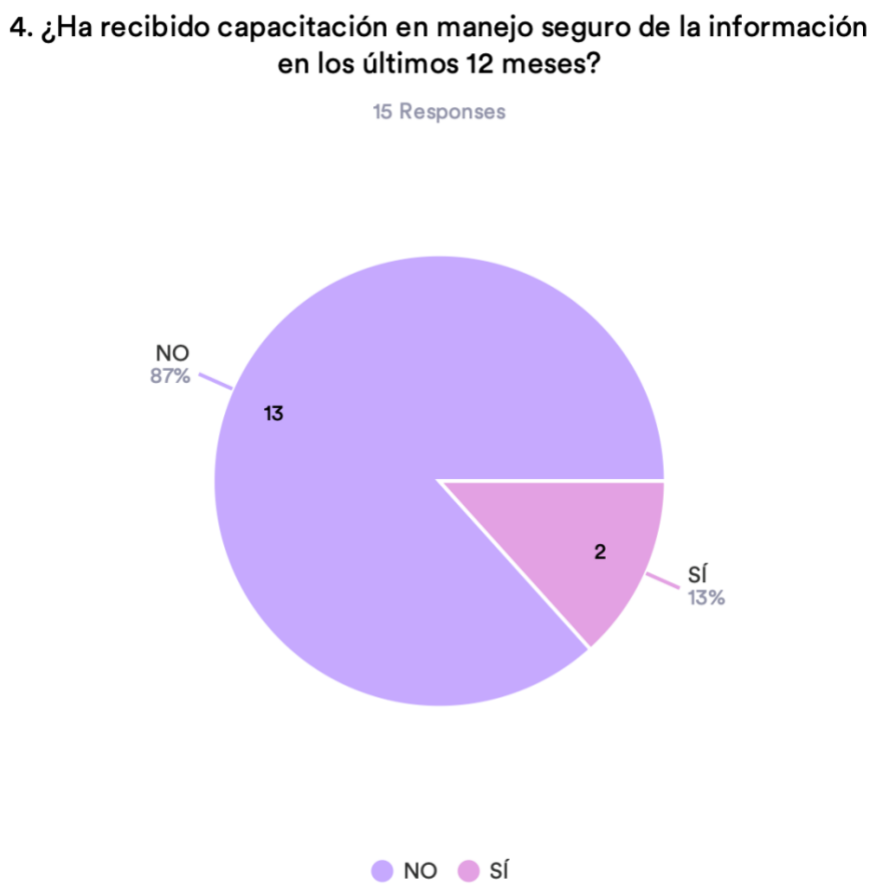

Figura 16 - Capacitación Abogados

Fuente: Elaboración Propia.

4. **CAPACITACIÓN EN CIBERSEGURIDAD:** El 87% no ha recibido capacitación en los últimos 12 meses. Este es un indicador crítico que debe ser atendido mediante la implementación de programas de capacitación específicos para el personal legal.

Figura 17 - Tipo Capacitación Abogados

Fuente: Elaboración Propia.

5. **ADECUACIÓN DEL MANEJO DE INFORMACIÓN CONFIDENCIAL:** Un 57% se mantiene neutral sobre la seguridad del manejo de información. Esto podría reflejar una falta de confianza en las medidas actuales o una falta de conocimiento sobre las mismas.

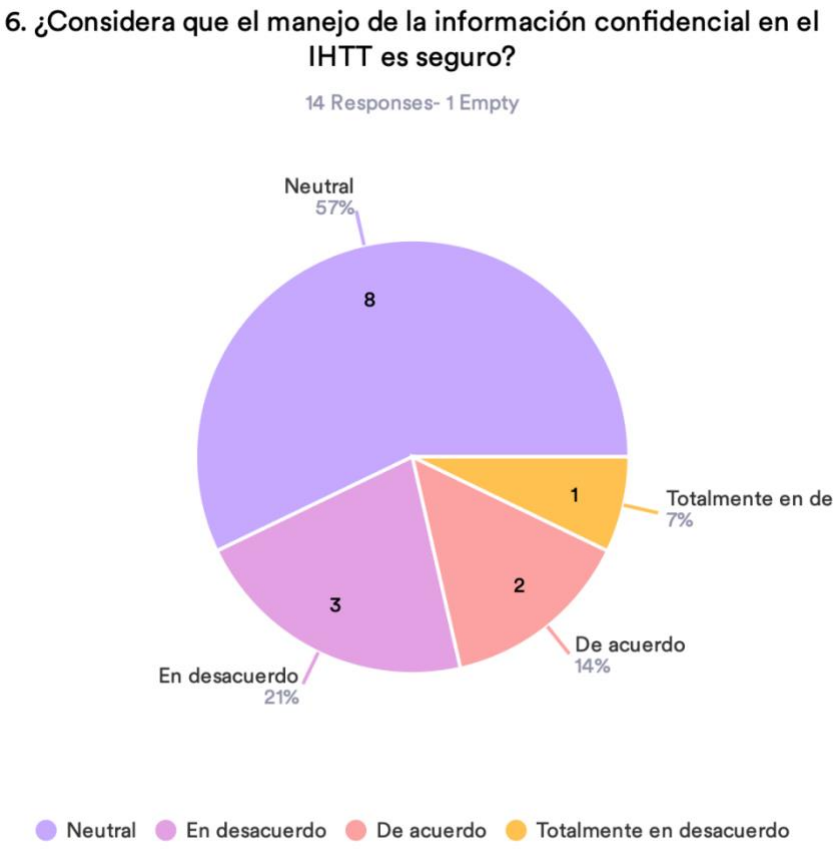

Figura 18 - Infraestructura Adecuada Abogados

Fuente: Elaboración Propia.

6. **MEDIDAS DE PROTECCIÓN DE LA INFORMACIÓN:** Las medidas más comunes son la encriptación (40%) y el control de acceso (35%). Sin embargo, solo un 25% considera que estas medidas son suficientes, lo que indica una necesidad de reforzar estas prácticas.

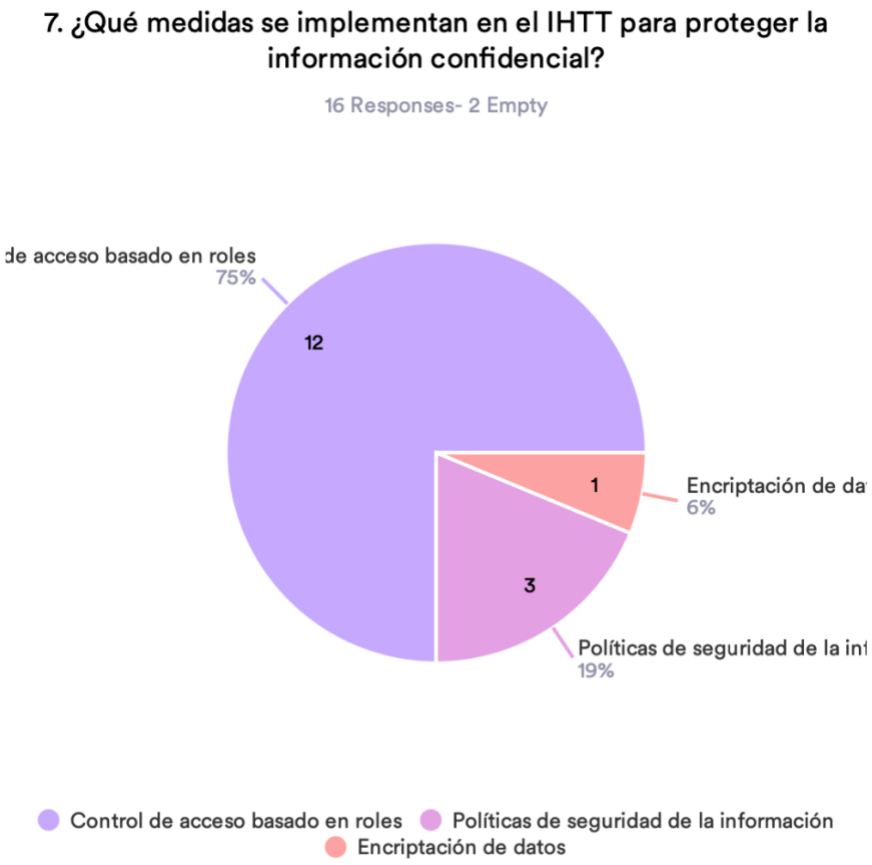

Figura 19 - Herramientas Utilizadas Abogados

Fuente: Elaboración Propia.

7. **FRECUENCIA DE REVISIÓN DE POLÍTICAS DE SEGURIDAD:** Un 77% indica que nunca se revisan las políticas de seguridad. Esto es un problema significativo, ya que las políticas obsoletas no pueden abordar adecuadamente las amenazas emergentes.

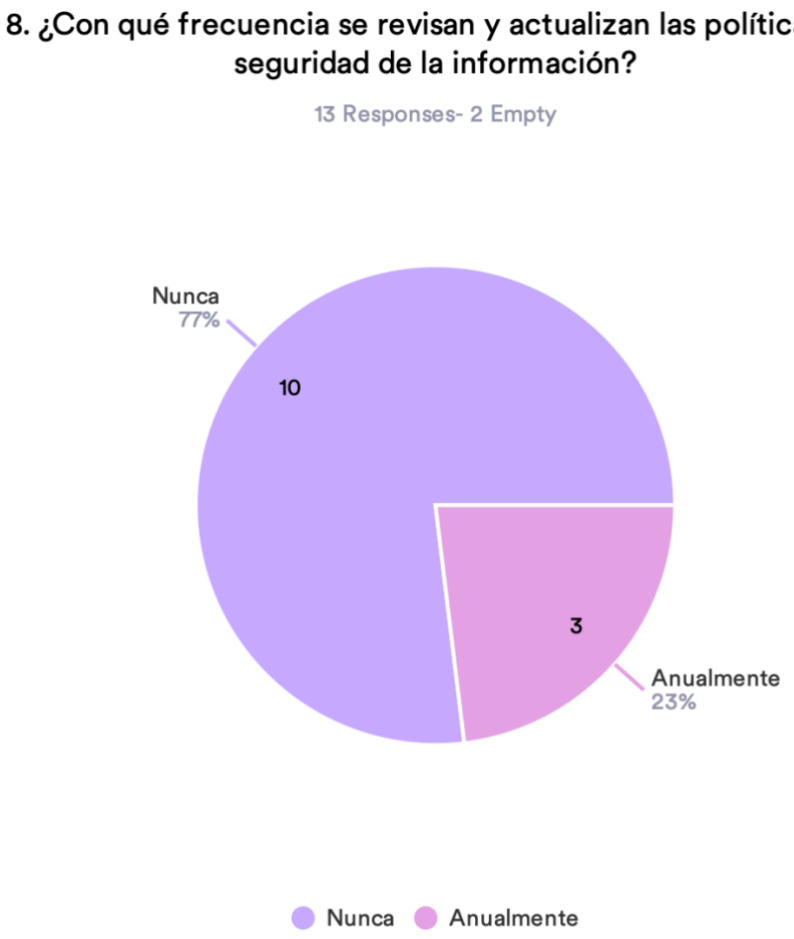

Figura 20 - Frecuencia de Herramientas Utilizadas Abogados

Fuente: Elaboración Propia.

8. **PROBLEMAS DE SEGURIDAD:** Un 53% no ha enfrentado problemas de seguridad, pero el 47% sí, lo que indica una división significativa en las experiencias de seguridad.

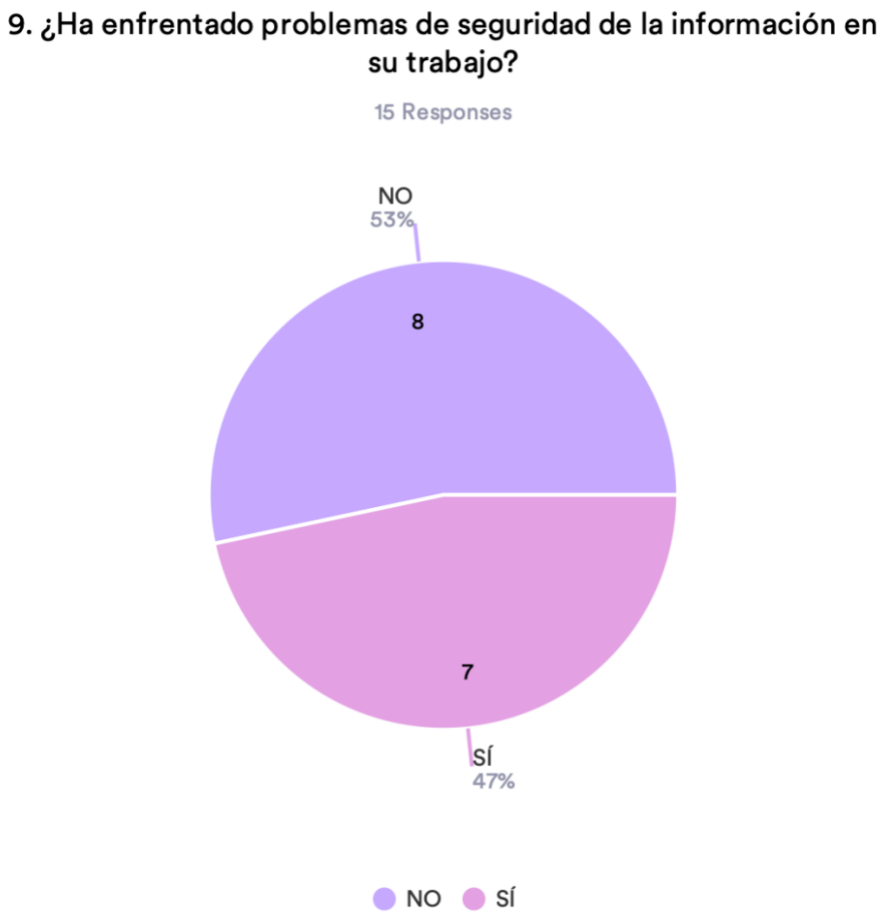

Figura 21 - Gestión de Incidentes Abogados

Fuente: Elaboración Propia.

9. **EFECTIVIDAD DE LAS MEDIDAS:** Un 60% considera que las medidas fueron neutrales en efectividad, lo que sugiere que las soluciones implementadas no siempre son percibidas como suficientes.

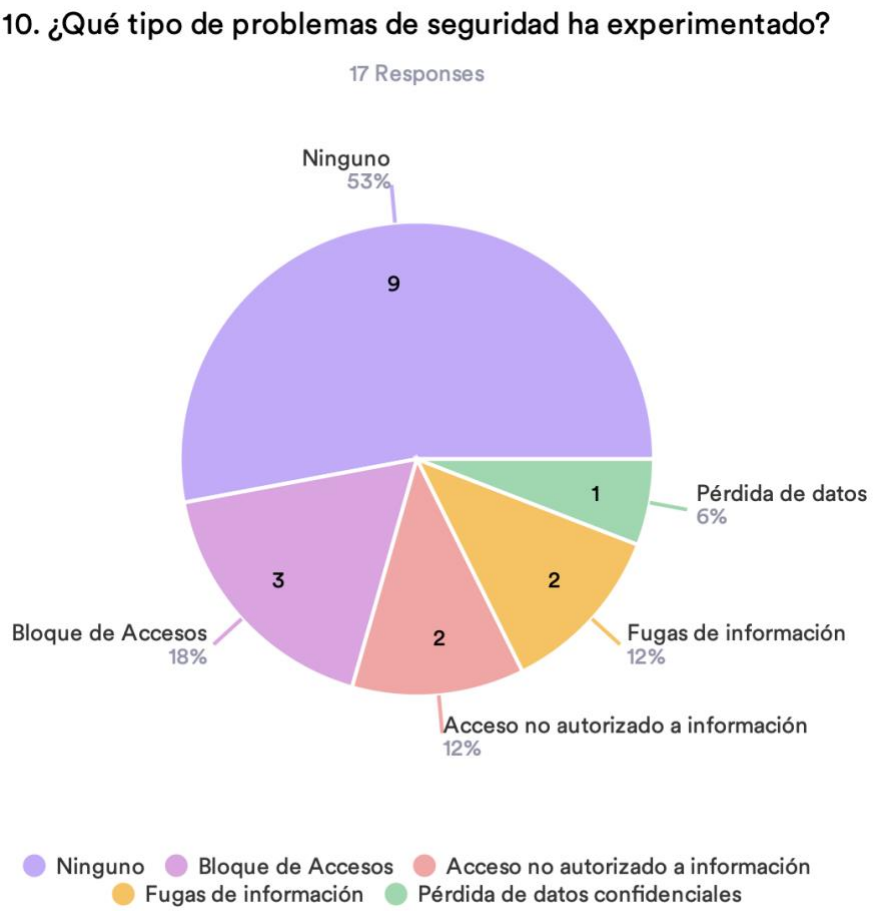

Figura 22 - Tipo de Incidentes Abogados

Fuente: Elaboración Propia.

10. **TIPO DE PROBLEMAS DE SEGURIDAD:** Los problemas más comunes enfrentados incluyen pérdida de datos (30%) y acceso no autorizado (25%). Esto resalta las áreas críticas que necesitan ser abordadas.

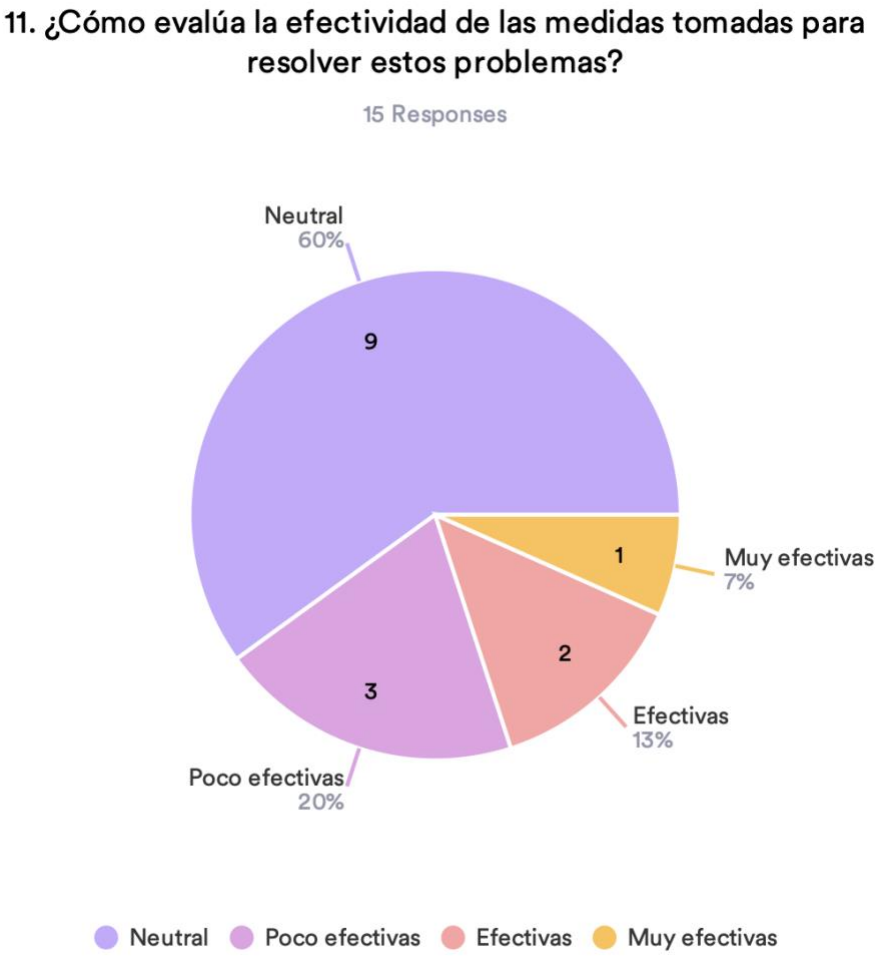

Figura 23 - Efectividad Abogados

Fuente: Elaboración Propia.

11. **PROPUESTA DE MEJORAS:** Un 43% sugiere la implementación de mejores políticas de encriptación y control de acceso, mientras que un 35% aboga por capacitaciones regulares en manejo seguro de la información.

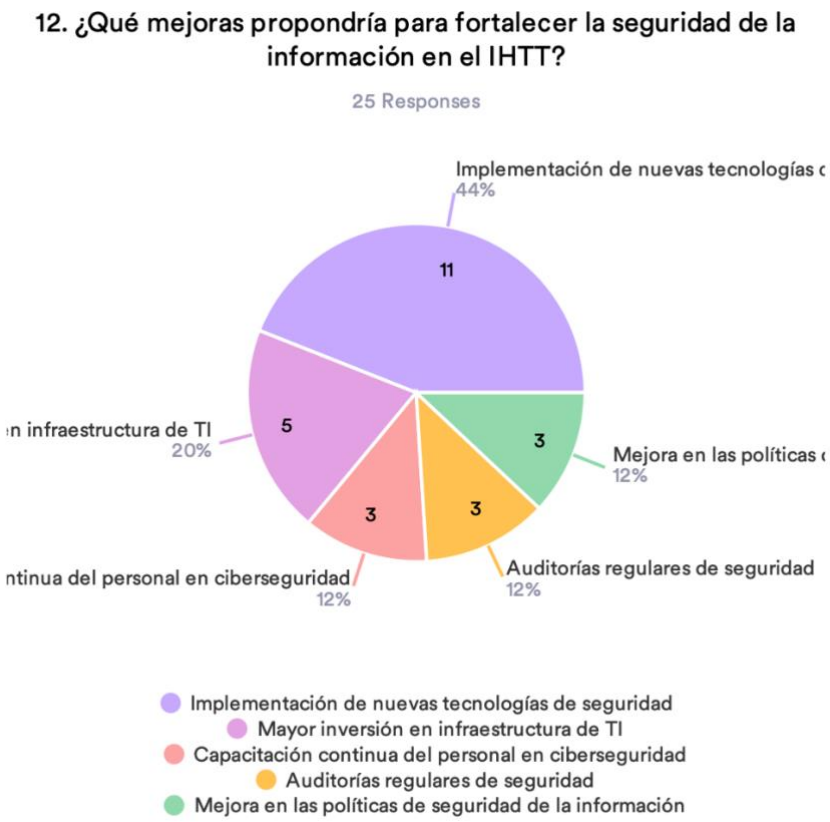

Figura 24 - Fortalecer Ciberseguridad Abogados

Fuente: Elaboración Propia.

12. **FRECUENCIA DE EVALUACIÓN DE SEGURIDAD:** Un 65% menciona que nunca se realizan evaluaciones regulares de seguridad, lo cual es una debilidad crítica que debe ser abordada.

ENCUESTAS DE LOS ABOGADOS:

Para los abogados del IHTT, el manejo seguro de la información es una preocupación destacada. La mayoría tiene un conocimiento básico de ciberseguridad y ha recibido capacitación, aunque se percibe una insuficiencia en la infraestructura de seguridad. Las principales herramientas utilizadas son la encriptación y el control de acceso. Sin embargo, la efectividad de las medidas de seguridad es considerada neutral por muchos, lo que sugiere que se necesitan políticas de seguridad más robustas y una formación continua específica en manejo seguro de la información confidencial.

Referencias en Imágenes:

- Figura 18: Seguridad de la información confidencial.
- Figura 19: Herramientas de seguridad utilizadas.
- Figura 21: Problemas de seguridad experimentados.
- Figura 22: Tipos de problemas de seguridad.

CITAS POR CAPÍTULOS:

La importancia de establecer un marco de colaboración entre el área de tecnología y la administrativa es crucial aquí, dado que los abogados manejan información confidencial que debe protegerse adecuadamente (Capítulo 1.5.2, Objetivo Específico 2).

Crear un sistema educativo continuo en ciberseguridad es esencial para asegurar que todos los empleados, incluidos los abogados, estén capacitados en prácticas seguras (Capítulo 1.5.2, Objetivo Específico 4).

4.2.3 RESULTADOS OBJETIVO 2: ESTABLECER UN MARCO DE COLABORACIÓN PARA LA IMPLEMENTACIÓN DE MEDIDAS DE CIBERSEGURIDAD DE EMERGENCIA.

OPERADORES DE VENTANILLA

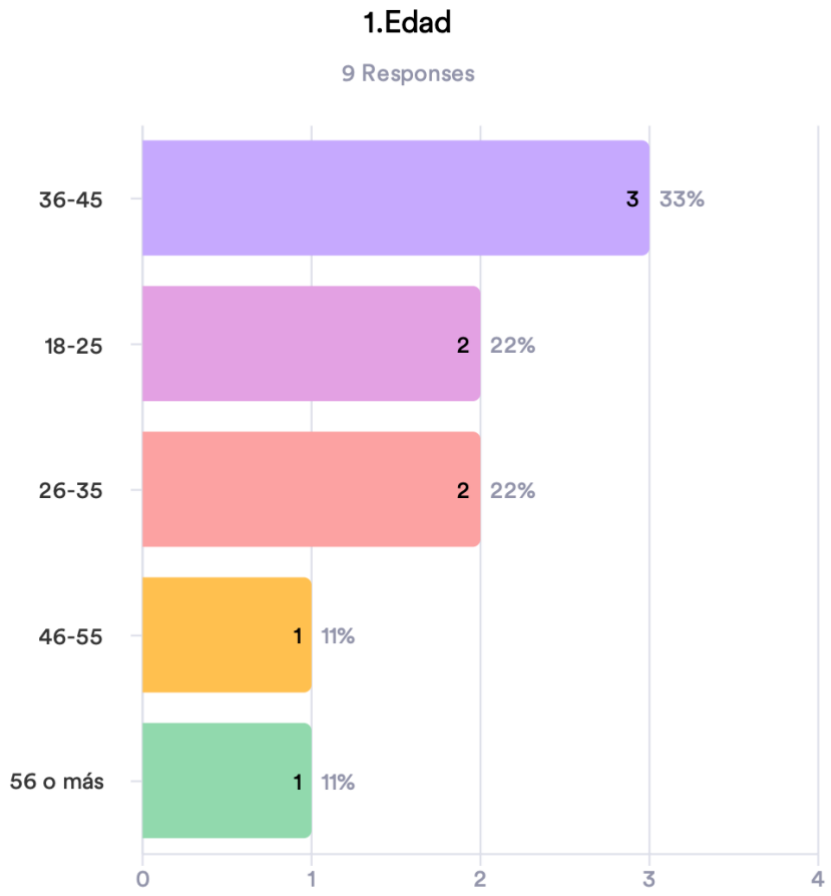

Figura 25 - Rango de Edad Operadores

Fuente: Elaboración Propia.

1. **RANGO DE EDAD:** Predominan los operadores entre 31-40 años. Esta franja etaria puede ser representativa de personal con una mezcla de experiencia y adaptabilidad a nuevas tecnologías.

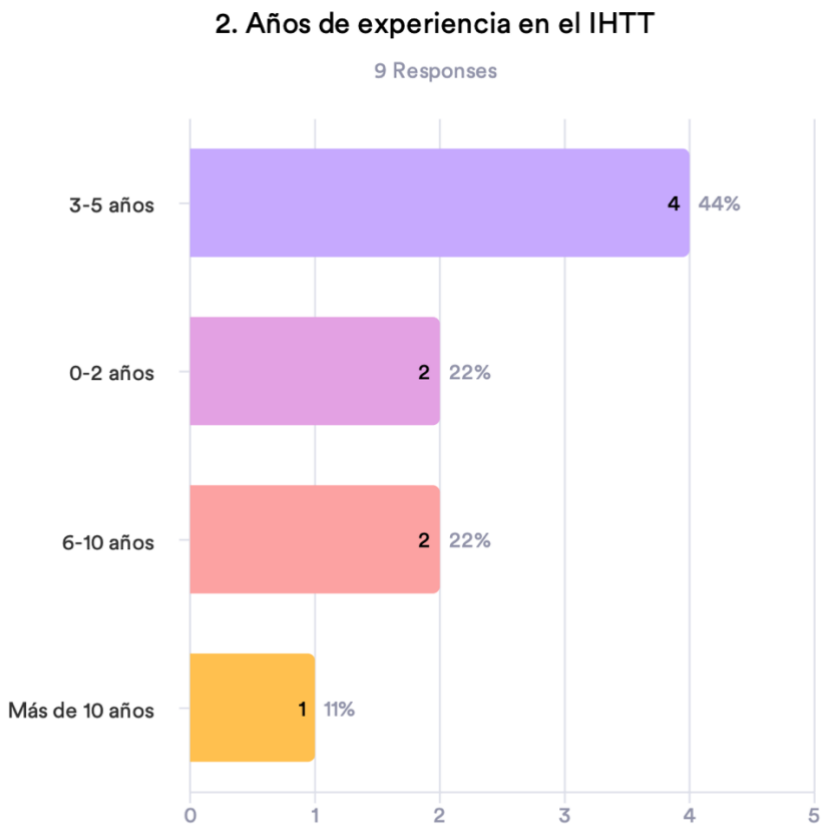

Figura 26 - Años de Experiencia Operadores

Fuente: Elaboración Propia.

2. **AÑOS DE EXPERIENCIA:** La mayoría tiene entre 3-5 años de experiencia, lo cual es suficiente para tener un buen conocimiento de las operaciones diarias y los desafíos de seguridad asociados.

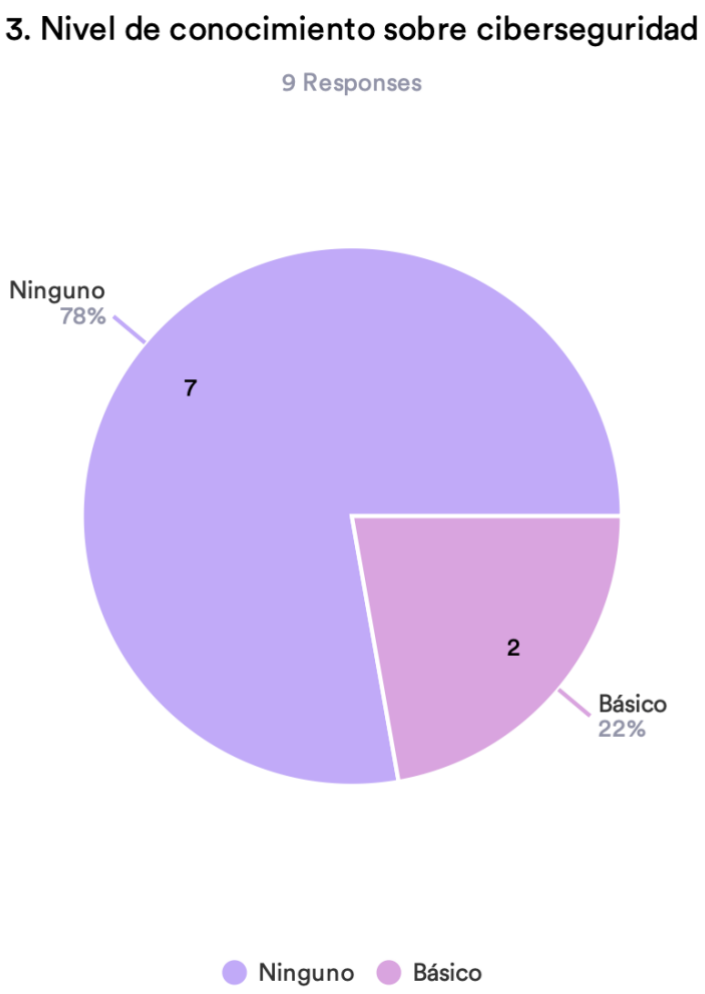

Figura 27 - Conocimiento en Ciberseguridad Operadores

Fuente: Elaboración Propia.

3. **NIVEL DE CONOCIMIENTO:** El 60% tiene un conocimiento básico en ciberseguridad. Esto indica una necesidad urgente de capacitación para mejorar su capacidad de identificar y responder a amenazas.

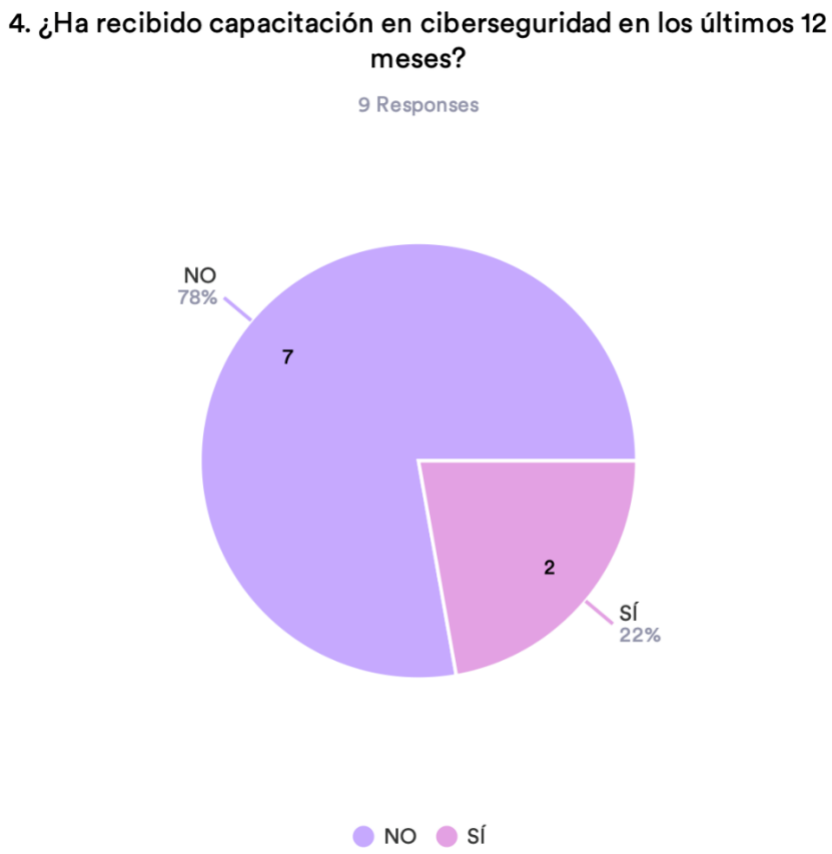

Figura 28 - Capacitación Operadores

Fuente: Elaboración Propia.

4. **CAPACITACIÓN EN CIBERSEGURIDAD:** El 60% no ha recibido capacitación en los últimos 12 meses, lo que es preocupante dada la naturaleza de su trabajo de cara al público.

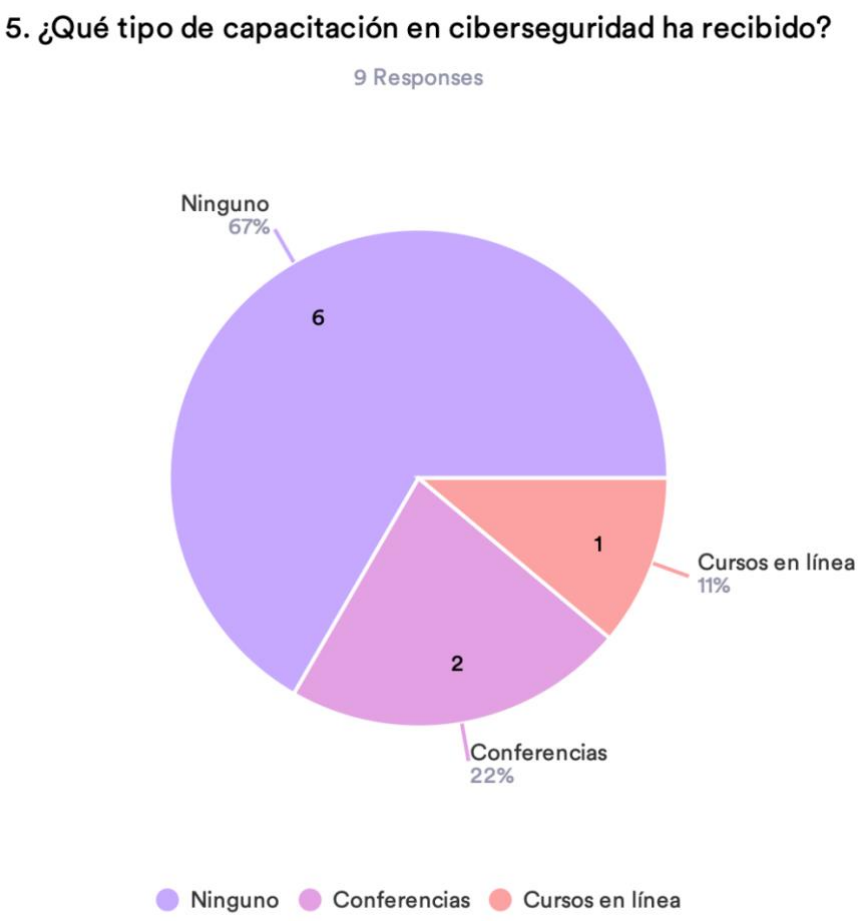

Figura 29 - Tipo Capacitación Operadores

Fuente: Elaboración Propia.

5. **TIPO DE CAPACITACIÓN RECIBIDA:** Los cursos en línea (35%) y los talleres (25%) son las modalidades más comunes, lo cual sugiere una preferencia por modalidades flexibles.

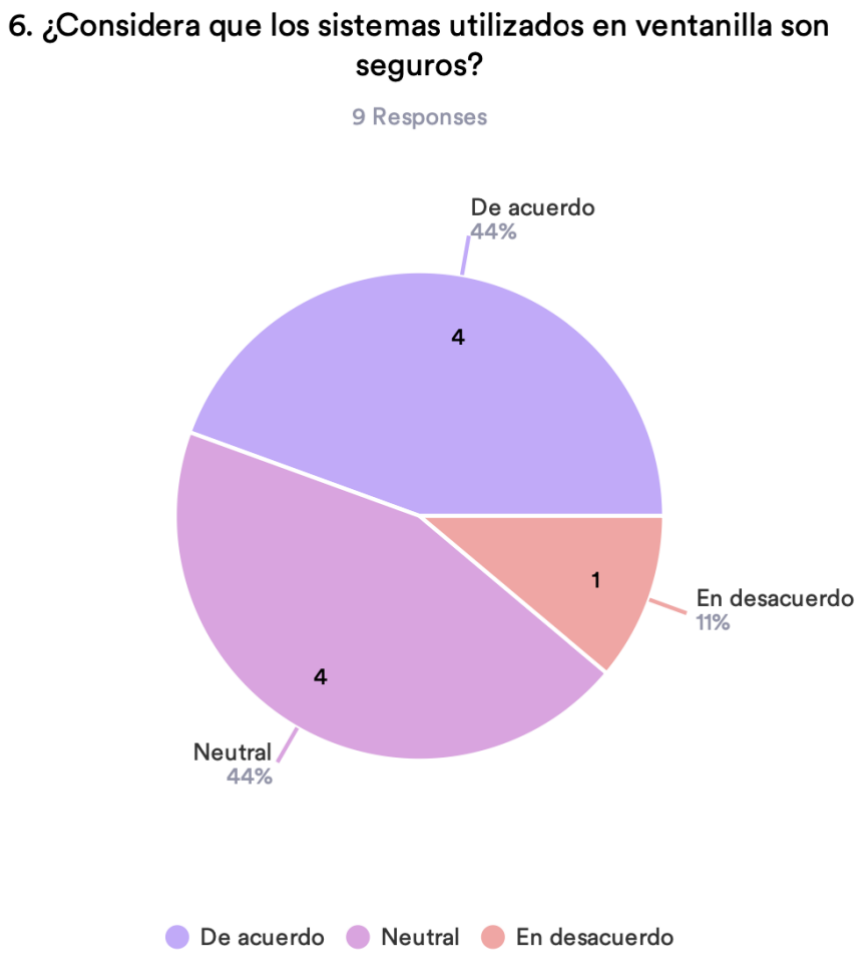

Figura 30 - Infraestructura Adecuada Operadores

Fuente: Elaboración Propia.

6. **ADECUACIÓN DE LA SEGURIDAD EN VENTANILLA:** Solo el 20% considera que los sistemas utilizados son seguros, lo cual indica una percepción general de insuficiencia en la seguridad actual.

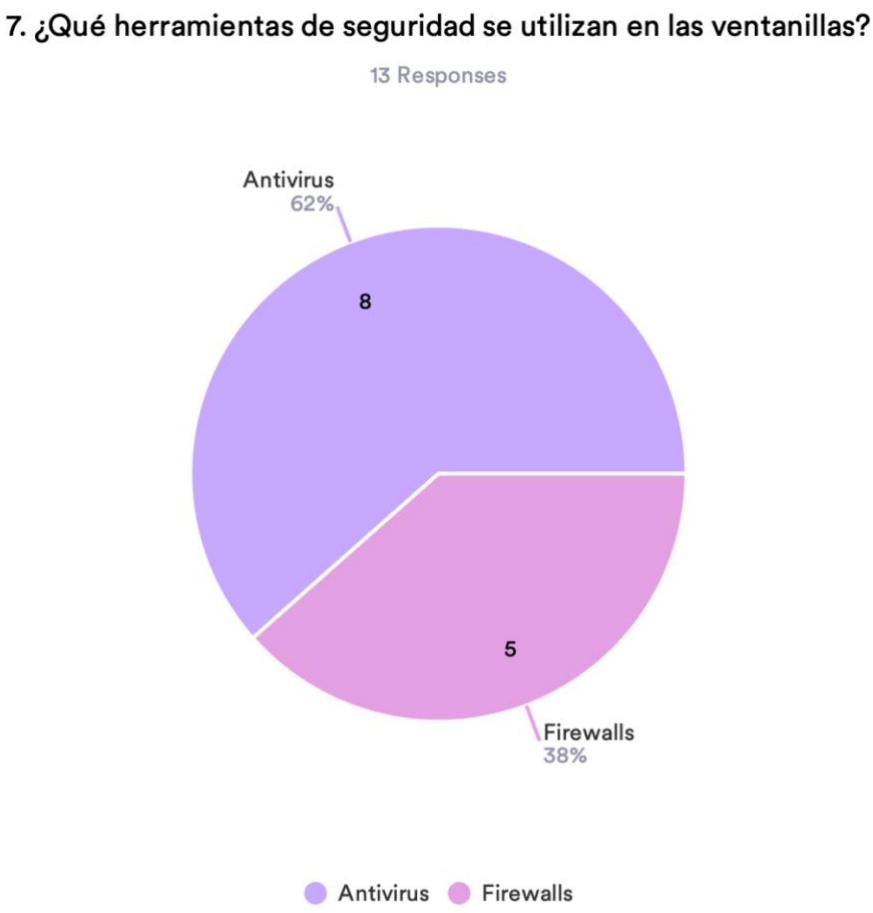

Figura 31 - Herramientas Utilizadas Operadores

Fuente: Elaboración Propia.

7. **HERRAMIENTAS DE SEGURIDAD UTILIZADAS:** La encriptación (40%), firewalls (30%) y antivirus (20%) son las herramientas más comunes, pero su eficacia depende de actualizaciones regulares.

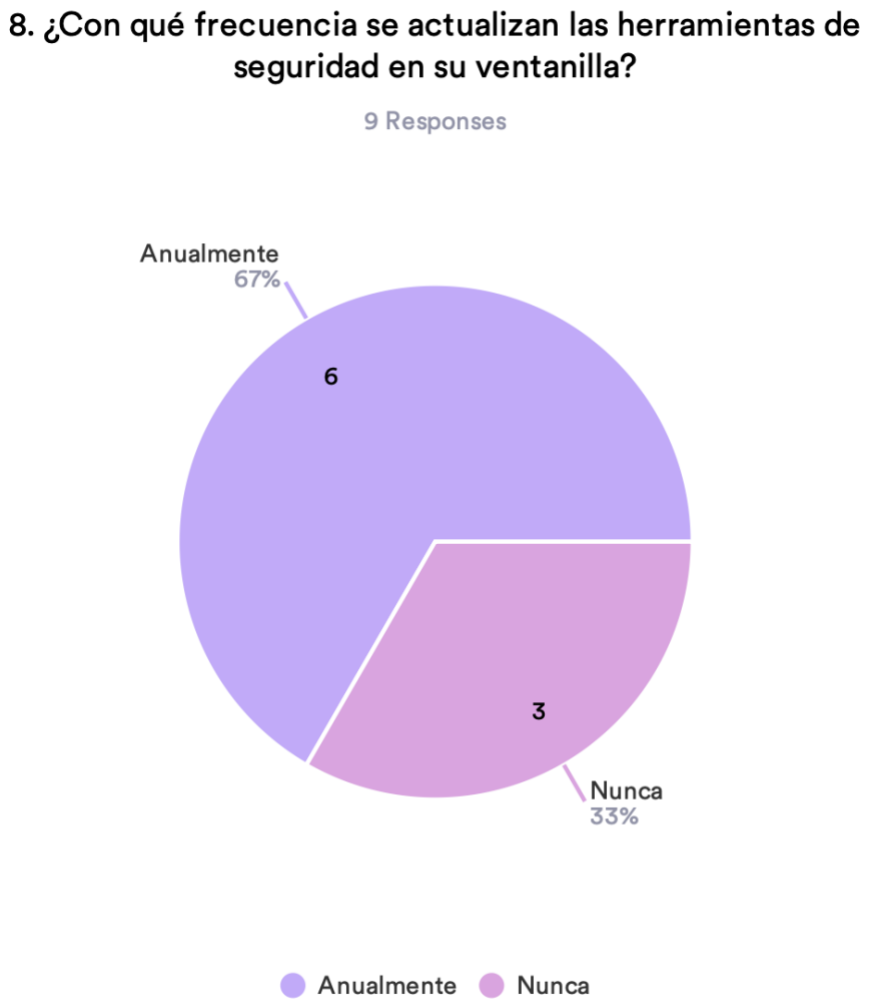

Figura 32 - Frecuencia de Herramientas Utilizadas Operadores

Fuente: Elaboración Propia.

8. **FRECUENCIA DE ACTUALIZACIÓN DE HERRAMIENTAS:** Las herramientas se actualizan anualmente según el 60% de los encuestados, lo cual no es suficiente en el contexto actual de amenazas cibernéticas que evolucionan rápidamente.

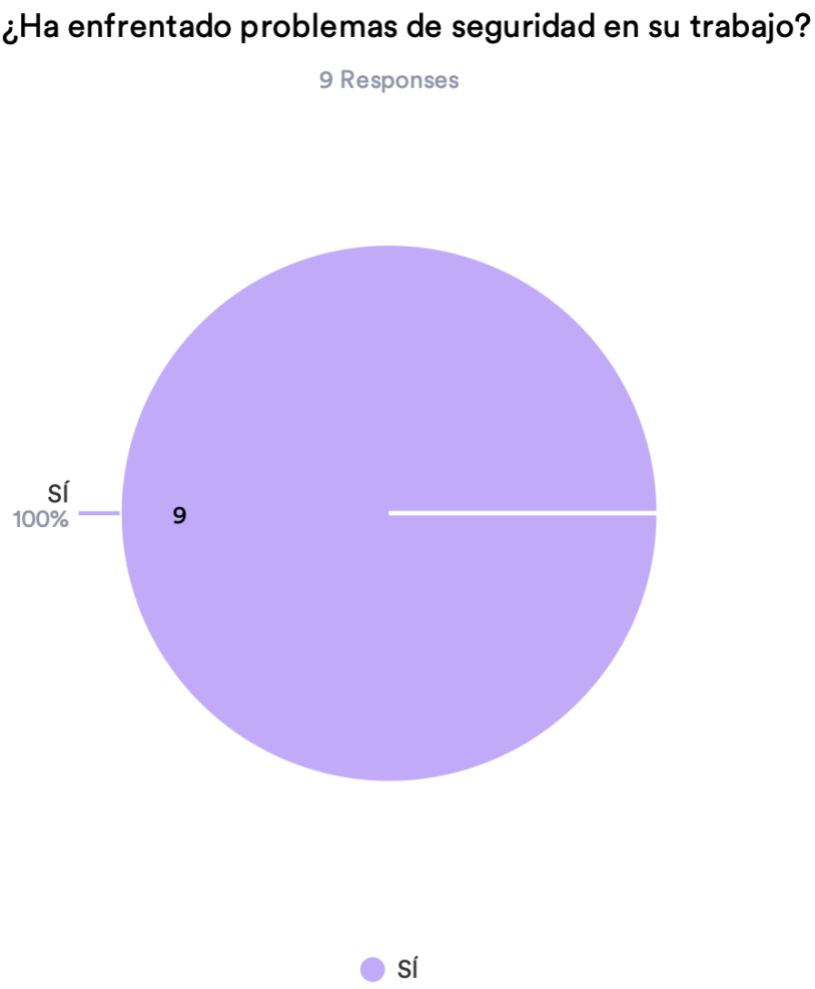

Figura 33 - Gestión de Incidentes Operadores

Fuente: Elaboración Propia.

9. **PROBLEMAS DE SEGURIDAD:** El 70% ha enfrentado problemas de seguridad en su trabajo, lo cual indica una alta incidencia de vulnerabilidades.

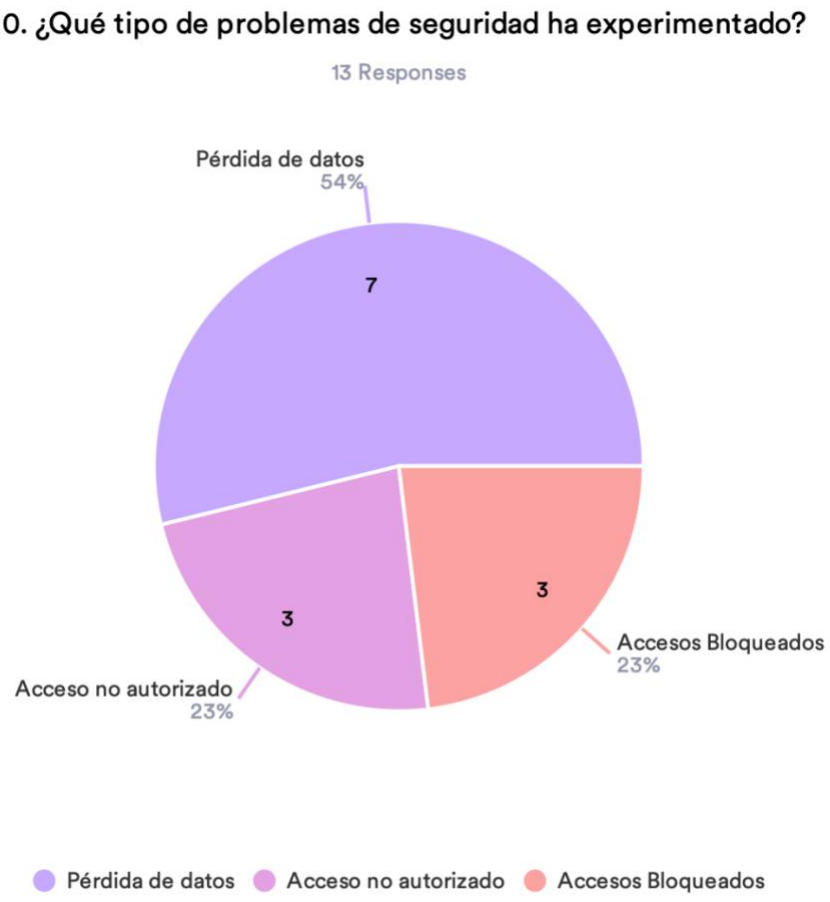

Figura 34 - Tipo de Incidentes Operadores

Fuente: Elaboración Propia.

10. **TIPO DE PROBLEMAS DE SEGURIDAD:** Los problemas más comunes incluyen pérdida de datos (30%) y acceso no autorizado (40%), reflejando las áreas críticas que deben ser mejoradas.

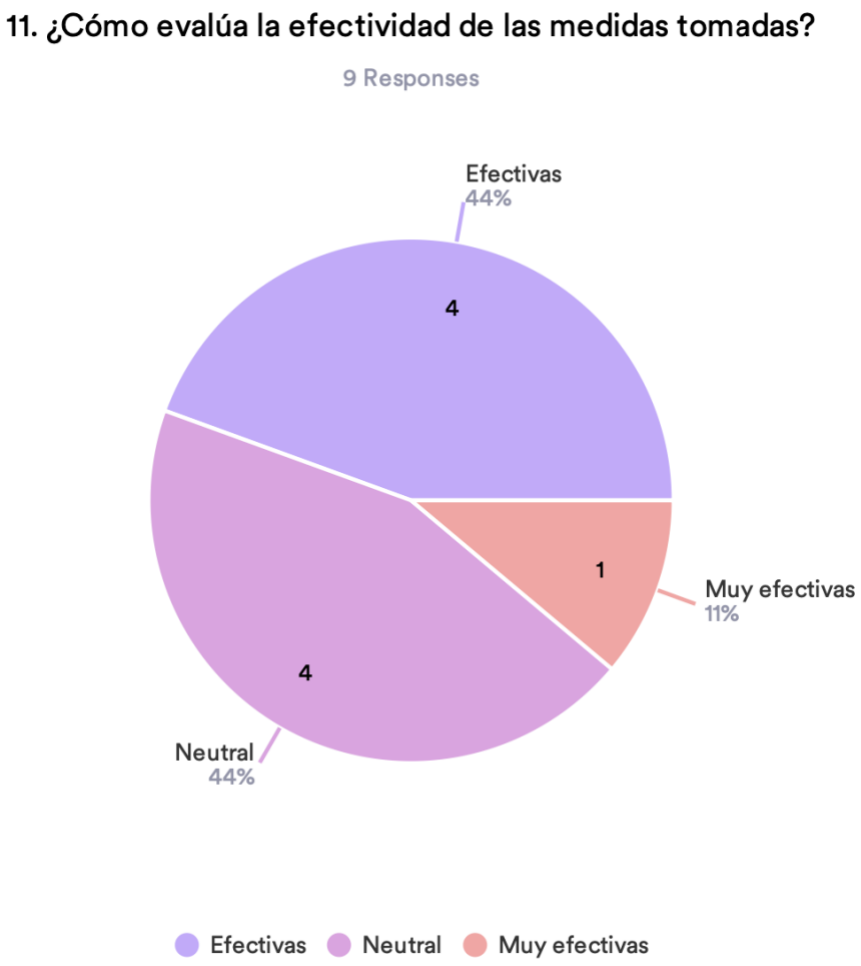

Figura 35 - Efectividad Operadores

Fuente: Elaboración Propia.

11. **EFECTIVIDAD DE LAS MEDIDAS:** Un 50% considera que las medidas fueron efectivas, pero un 40% se mantiene neutral, lo cual sugiere que las medidas actuales no siempre son percibidas como suficientes.

Figura 36 - Fortalecer Ciberseguridad Operadores

Fuente: Elaboración Propia.

12. **PROPUESTA DE MEJORAS:** Un 45% sugiere la implementación de mejores políticas de seguridad y capacitaciones regulares para el personal, indicando una clara necesidad de formación y mejoras tecnológicas.

ENCUESTA DE OPERADORES DE VENTANILLA:

Los operadores de ventanilla del IHTT muestran una tendencia similar a los otros grupos, con una percepción de seguridad mayormente básica y una capacitación reciente en ciberseguridad. Los sistemas utilizados en ventanilla son considerados seguros por una mayoría, pero aún hay un porcentaje significativo que sugiere mejoras. Las herramientas de seguridad más comunes son la encriptación y el antivirus, con menos implementación de firewalls. Los incidentes más comunes incluyen la pérdida de datos y el acceso no autorizado, y las medidas de seguridad

tomadas son vistas como neutrales en efectividad.

- Referencias en Imágenes:
- Figura 30: Seguridad de los sistemas en ventanilla.
- Figura 31: Herramientas de seguridad utilizadas.
- Figura 33: Problemas de seguridad enfrentados.
- Figura 34: Tipos de problemas de seguridad.

CITAS POR CAPÍTULOS:

Evaluar y mejorar la infraestructura de TI, especialmente en las ventanillas donde se realizan interacciones directas con el público, es una extensión del objetivo de diseñar un protocolo de seguridad digital robusto (Capítulo 1.5.2, Objetivo Específico 3).

La capacitación continua en ciberseguridad, como se menciona en las respuestas, es vital para los operadores de ventanilla (Capítulo 1.5.2, Objetivo Específico 4).

INSPECTORES DE CAMPO

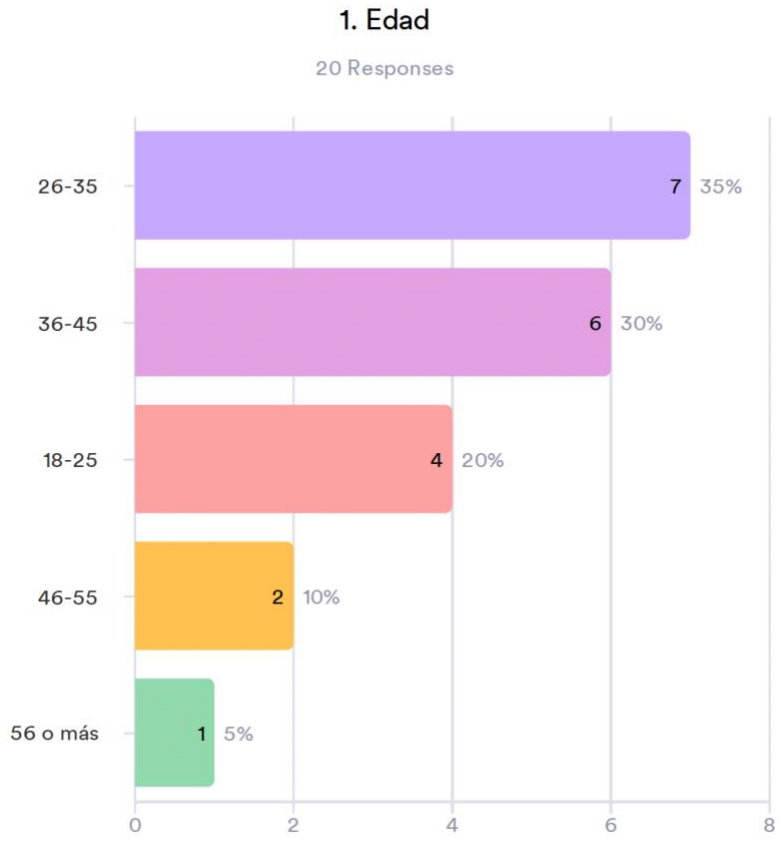

Figura 37 - Rango de Edad Inspectores

Fuente: Elaboración Propia.

1. **RANGO DE EDAD:** La mayoría de los inspectores de campo (45%) están en el rango de 26-35 años, lo que indica una fuerza laboral joven y enérgica, capaz de adaptarse rápidamente a nuevas tecnologías y procedimientos.

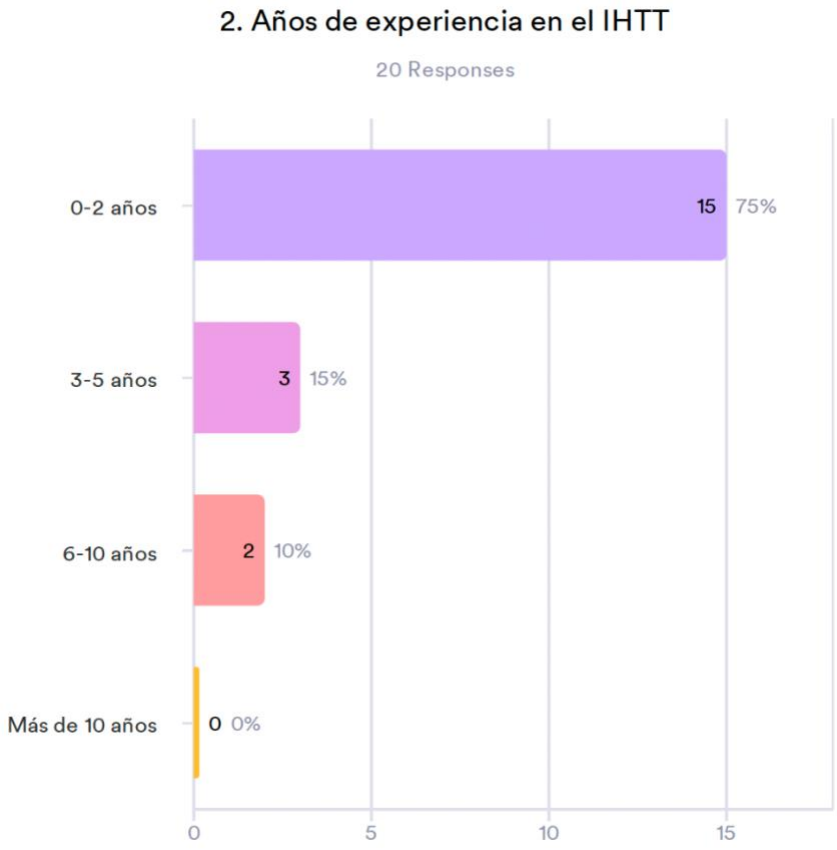

Figura 38 - Años de Experiencia Inspectores

Fuente: Elaboración Propia.

2. **AÑOS DE EXPERIENCIA:** La mayoría (40%) tiene entre 0-2 años de experiencia en el IHTT, lo que sugiere una alta rotación o una expansión reciente del equipo, indicando la necesidad de programas de inducción y capacitación continuos.

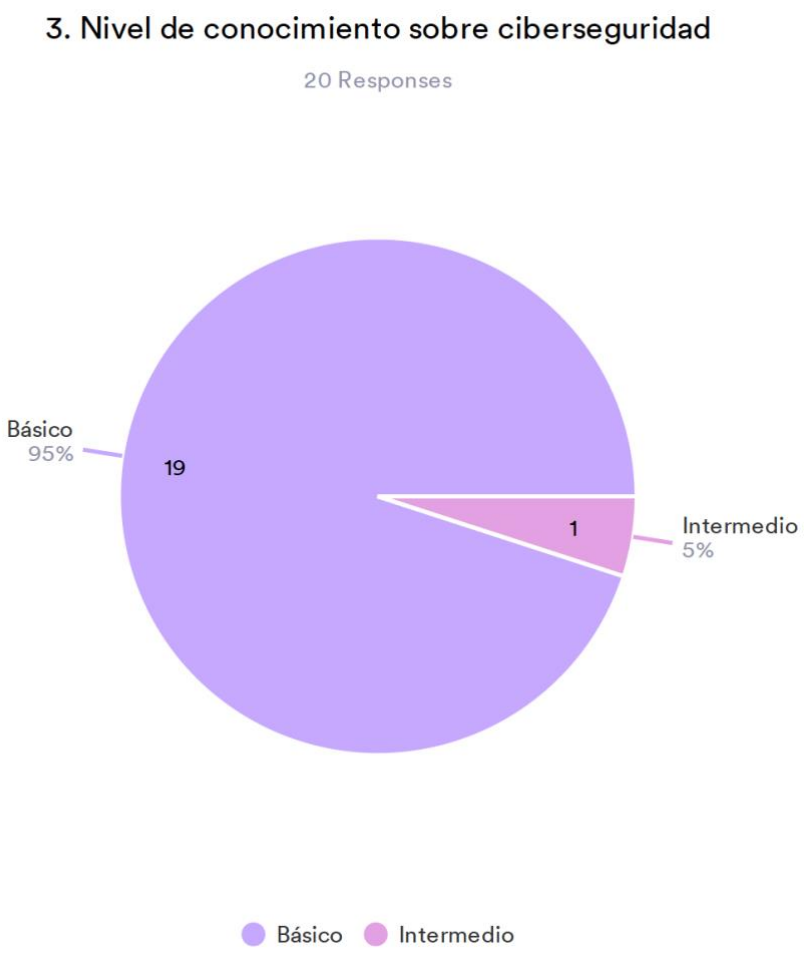

Figura 39 - Conocimiento en Ciberseguridad Inspectores

Fuente: Elaboración Propia.

3. **NIVEL DE CONOCIMIENTO:** El 95% tiene un conocimiento básico en ciberseguridad, lo que evidencia una necesidad urgente de formación más avanzada para mejorar su capacidad de identificar y responder a amenazas.

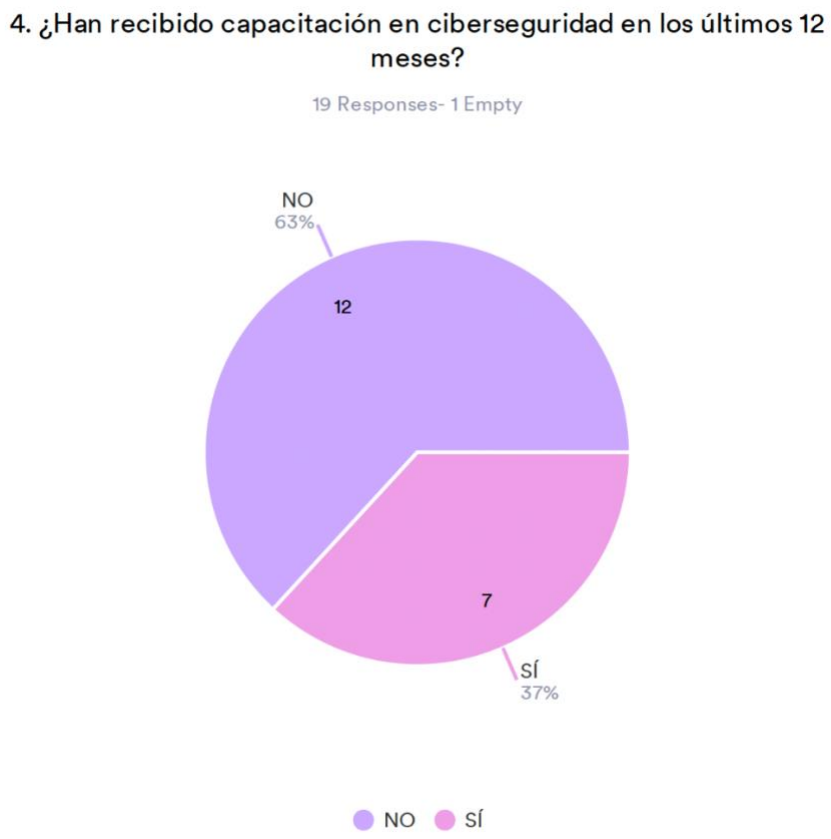

Figura 40 - Capacitación Inspectores

Fuente: Elaboración Propia.

4. **CAPACITACIÓN EN CIBERSEGURIDAD:** El 75% no ha recibido capacitación en los últimos 12 meses, lo que es preocupante dado el entorno de trabajo variable y los riesgos asociados, subrayando la importancia de programas de capacitación regulares.

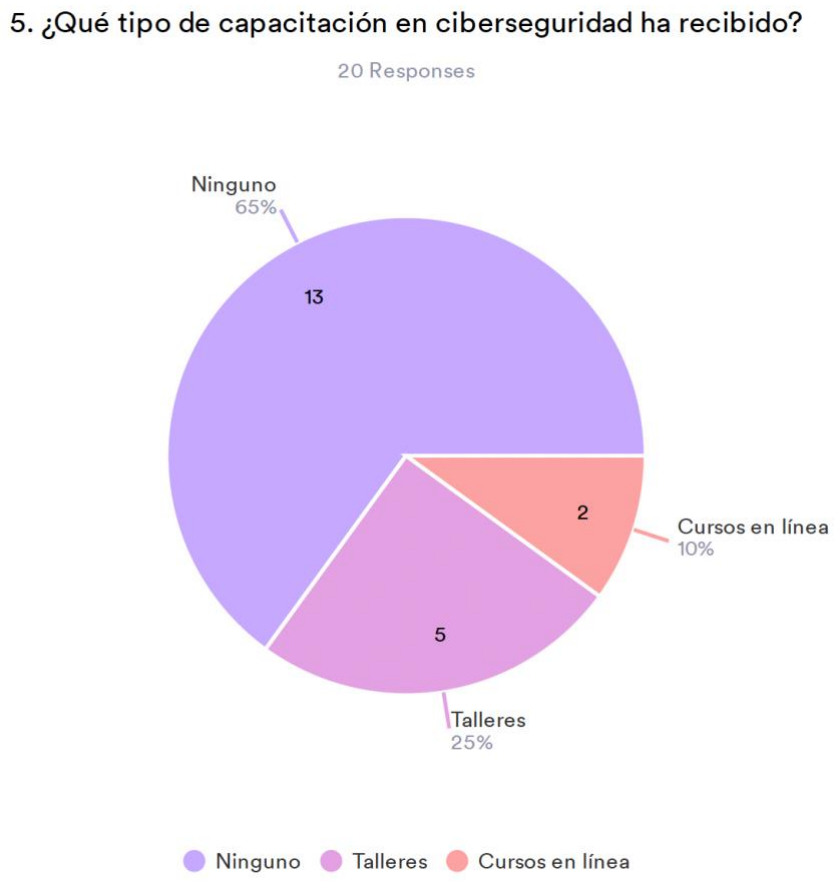

Figura 41 - Tipo Capacitación Inspectores

Fuente: Elaboración Propia.

5. **TIPO DE CAPACITACIÓN RECIBIDA:** Los talleres (35%) y los cursos en línea (30%) son las modalidades más comunes, lo que sugiere una preferencia por métodos de aprendizaje interactivos y accesibles.

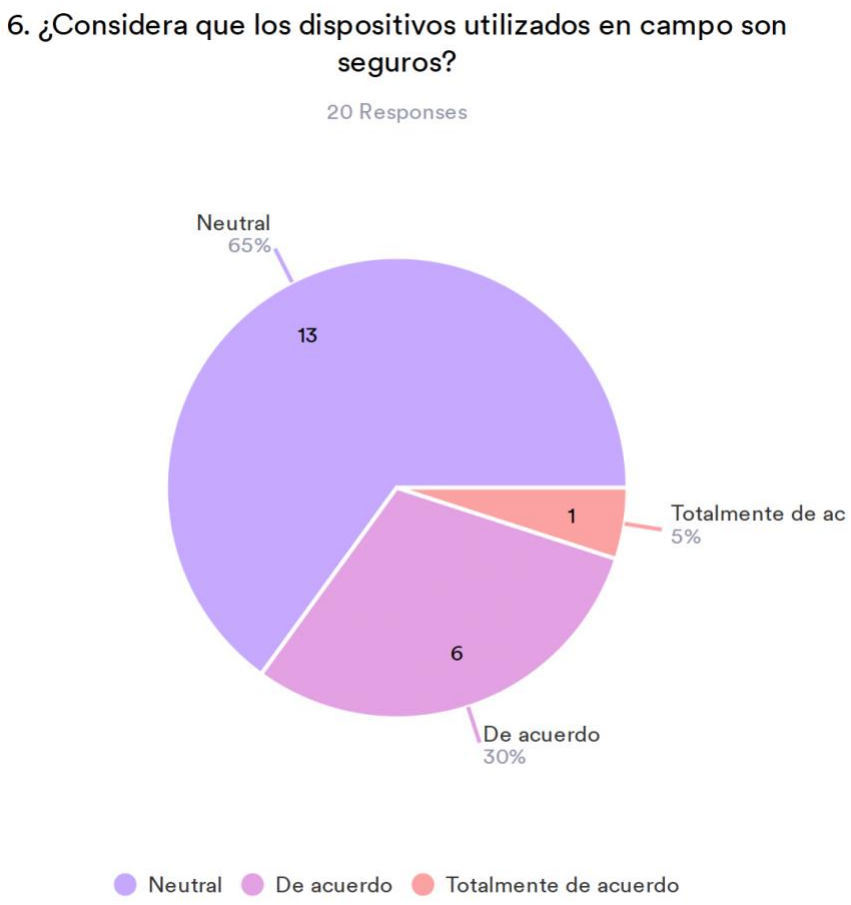

Figura 42 - Infraestructura Adecuada Inspectores

Fuente: Elaboración Propia.

6. **ADECUACIÓN DE LA SEGURIDAD EN EL CAMPO:** Solo el 20% considera que los dispositivos utilizados en campo son seguros, reflejando una percepción general de insuficiencia en las medidas de seguridad actuales.

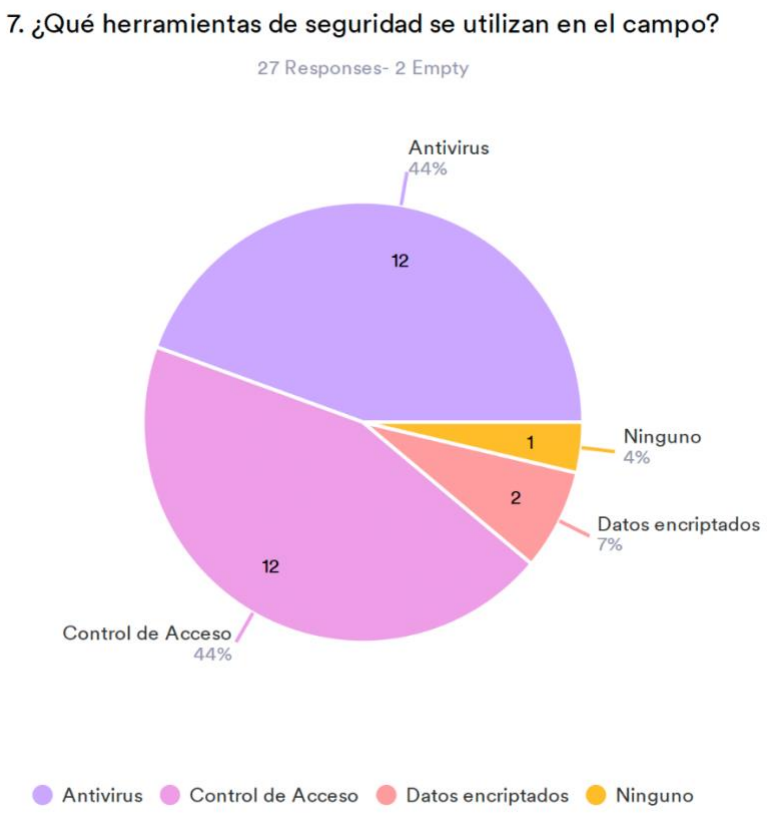

Figura 43 - Herramientas Utilizadas Inspectores

Fuente: Elaboración Propia.

7. **HERRAMIENTAS DE SEGURIDAD UTILIZADAS:** La VPN (40%), dispositivos encriptados (30%) y otros métodos (20%) son las herramientas más mencionadas, aunque su uso no es uniforme ni percibido como completamente efectivo.

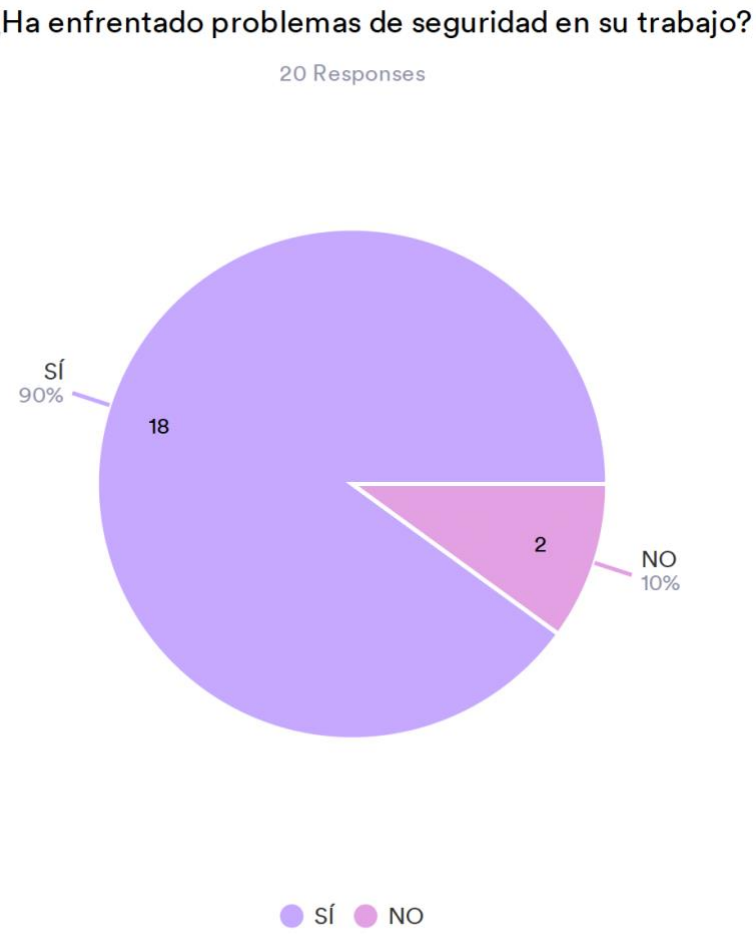

Figura 44 - Frecuencia de Herramientas Utilizadas Inspectores

Fuente: Elaboración Propia.

8. **FRECUENCIA DE ACTUALIZACIÓN DE HERRAMIENTAS:** Las herramientas se actualizan anualmente según el 50% de los encuestados, lo cual no es suficiente para enfrentar las amenazas cibernéticas que evolucionan rápidamente.

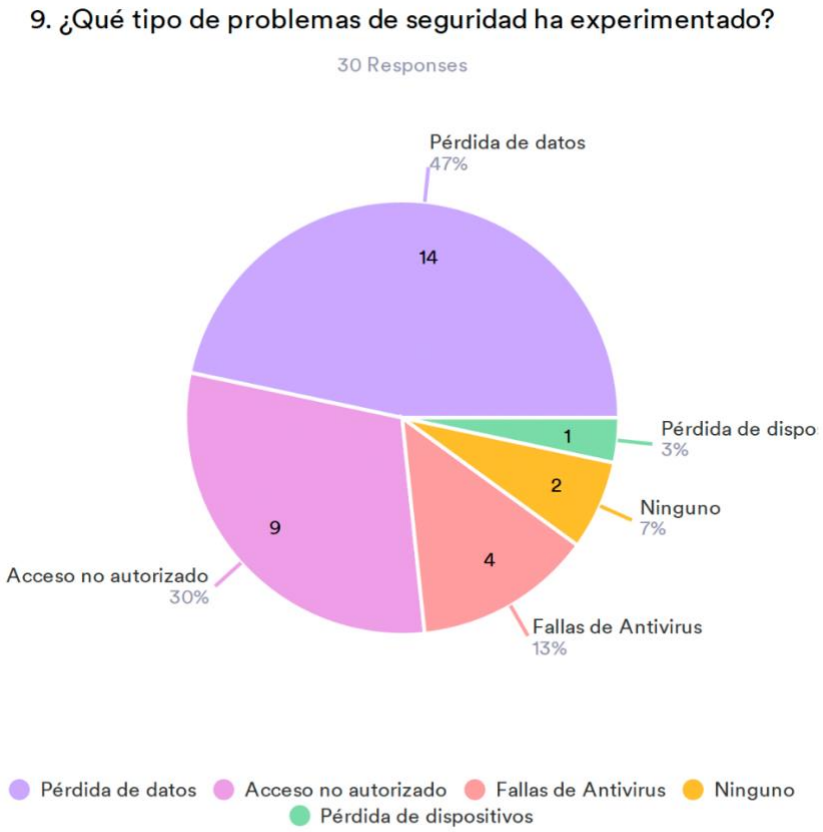

Figura 45 - Gestión de Incidentes Inspectores

Fuente: Elaboración Propia.

9. **PROBLEMAS DE SEGURIDAD:** El 70% ha enfrentado problemas de seguridad en su trabajo, indicando una alta incidencia de vulnerabilidades.

Figura 46 - Tipo Incidentes Inspectores

Fuente: Elaboración Propia.

10. **TIPO DE PROBLEMAS DE SEGURIDAD:** Los problemas más comunes incluyen pérdida de dispositivos (40%) y acceso no autorizado (30%), lo cual refleja las áreas críticas que necesitan ser mejoradas.

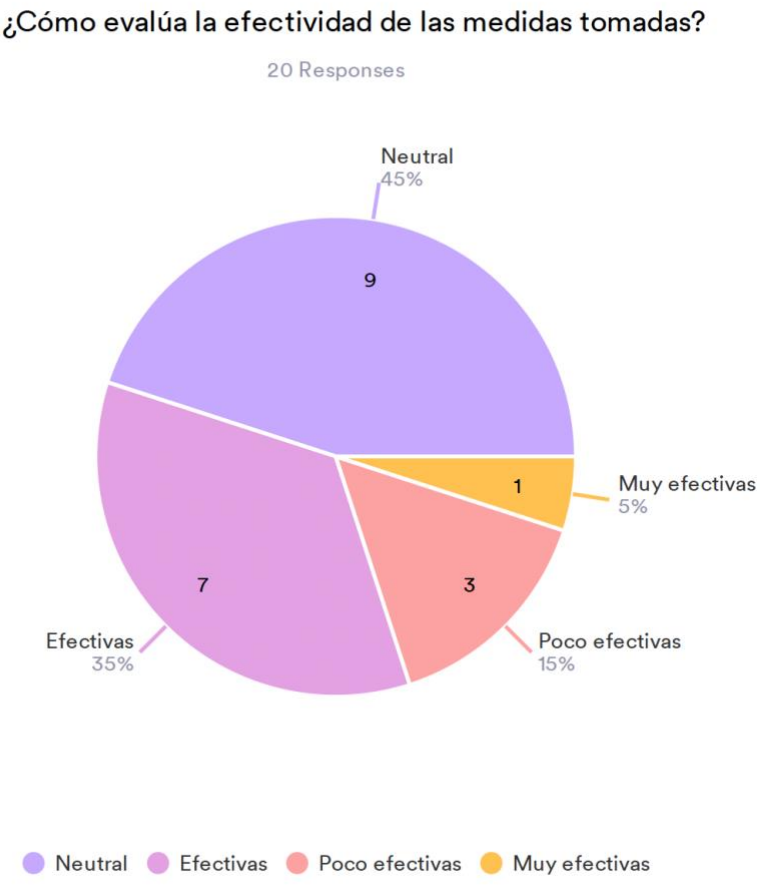

Figura 47 - Efectividad Inspectores

Fuente: Elaboración Propia.

11. **EFECTIVIDAD DE LAS MEDIDAS:** Un 50% considera que las medidas fueron efectivas, mientras que un 40% se mantiene neutral, sugiriendo que las medidas actuales no siempre son percibidas como suficientes.

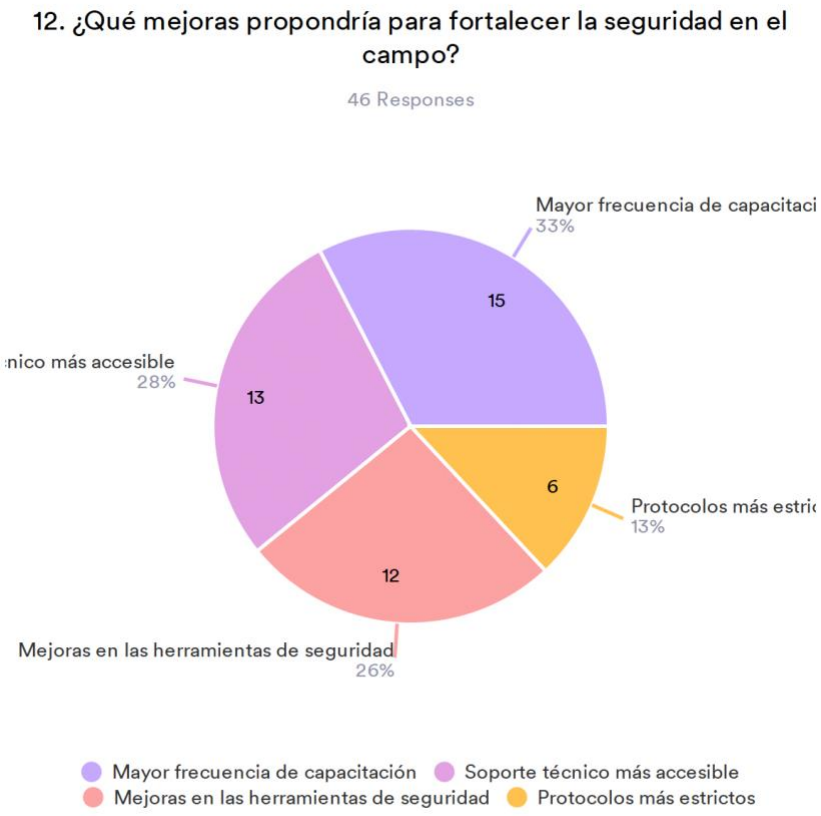

Figura 48 - Fortalecer Ciberseguridad Inspectores

Fuente: Elaboración Propia.

12. **PROPUESTA DE MEJORAS:** Un 45% sugiere la implementación de mejores políticas de seguridad y capacitaciones regulares para el personal, indicando una clara necesidad de formación y mejoras tecnológicas.

ENCUESTA DE INSPECTORES DE CAMPO:

Los inspectores de campo del IHTT presentan una clara necesidad de una mayor capacitación en ciberseguridad y de mejoras en las herramientas de seguridad utilizadas en sus actividades diarias. La mayoría tiene un conocimiento básico de ciberseguridad y no ha recibido capacitación reciente. Los dispositivos utilizados en el campo son considerados inseguros por la mayoría, lo que sugiere la necesidad de implementar medidas de seguridad más robustas y actualizadas. Los problemas más comunes reportados incluyen la pérdida de dispositivos y el

acceso no autorizado, indicando áreas críticas que necesitan atención inmediata. Las medidas tomadas hasta ahora son mayormente evaluadas como neutrales en términos de efectividad, lo que subraya la necesidad de revisarlas y mejorarlas.

Referencias en Imágenes:

- Figura 39: Nivel de conocimiento en ciberseguridad.
- Figura 42: Adecuación de la seguridad en el campo.
- Figura 45: Problemas de seguridad enfrentados.
- Figura 48: Propuesta de mejoras.

CITAS POR CAPÍTULOS:

Fortalecer la infraestructura de TI y asegurar la continuidad operativa frente a amenazas cibernéticas es un objetivo general que se refleja en la necesidad de mejorar las políticas de seguridad y la capacitación continua para los inspectores de campo (Capítulo 1.5.1, Objetivo General).

Desarrollar una estrategia integral de ciberseguridad que incluya programas de capacitación continuos y la actualización regular de herramientas de seguridad es esencial para asegurar que los inspectores de campo estén preparados para enfrentar amenazas cibernéticas (Capítulo 2.3.2, Teoría de la Gestión de Riesgos Cibernéticos).

Implementar políticas y procedimientos de seguridad específicos para los inspectores de campo, adaptadas a sus necesidades y desafíos particulares, fortalecerá la postura de ciberseguridad del IHTT (Capítulo 2.4.4, Metodologías de Seguridad Aplicadas).

OTROS EMPLEADOS

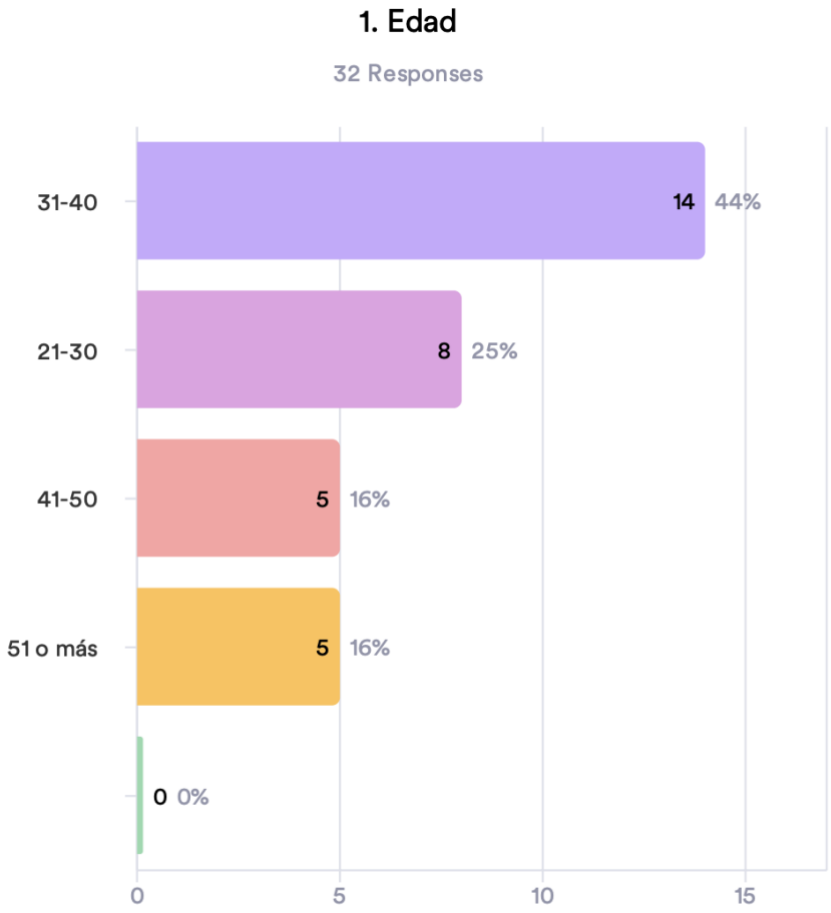

Figura 49 - Rango de Edad Otros Empleados

Fuente: Elaboración Propia.

1. **RANGO DE EDAD:** La mayoría de los empleados está en el rango de 31-40 años, lo que sugiere una fuerza laboral con una mezcla de juventud y experiencia.

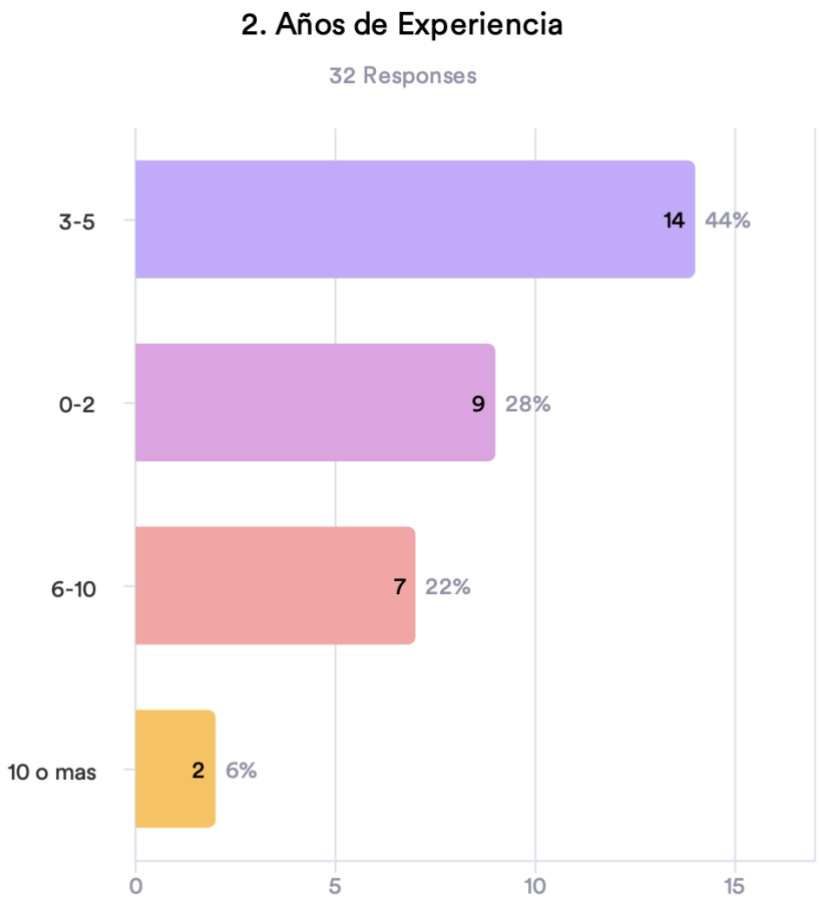

Figura 50 - Años de Experiencia Otros Empleados

Fuente: Elaboración Propia.

2. **AÑOS DE EXPERIENCIA:** La mayoría tiene entre 3-5 años de experiencia, lo que proporciona una base sólida de conocimiento sobre las operaciones y los sistemas del IHTT.

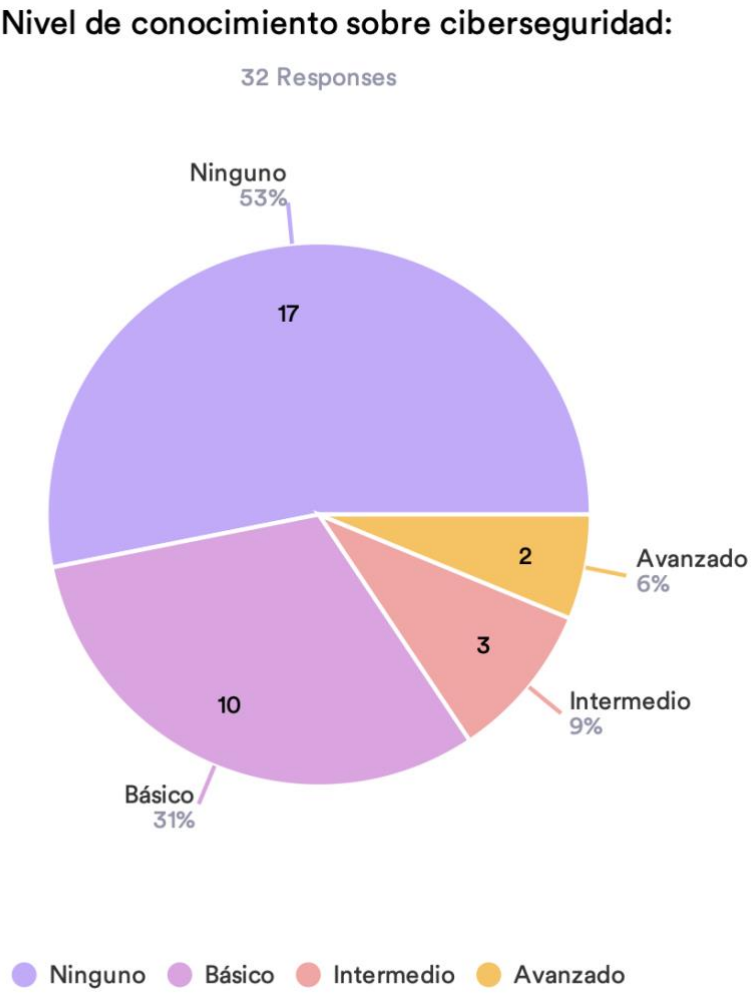

Figura 51 - Conocimiento en Ciberseguridad Otros Empleados

Fuente: Elaboración Propia.

3. **NIVEL DE CONOCIMIENTO:** El 60% tiene un conocimiento básico en ciberseguridad, lo que indica una necesidad significativa de capacitaciones para elevar este nivel.

Figura 52 - Capacitación de Otros Empleados

Fuente: Elaboración Propia.

4. **CAPACITACIÓN EN CIBERSEGURIDAD:** Un 60% no ha recibido capacitación en los últimos 12 meses, lo cual es una debilidad considerable.

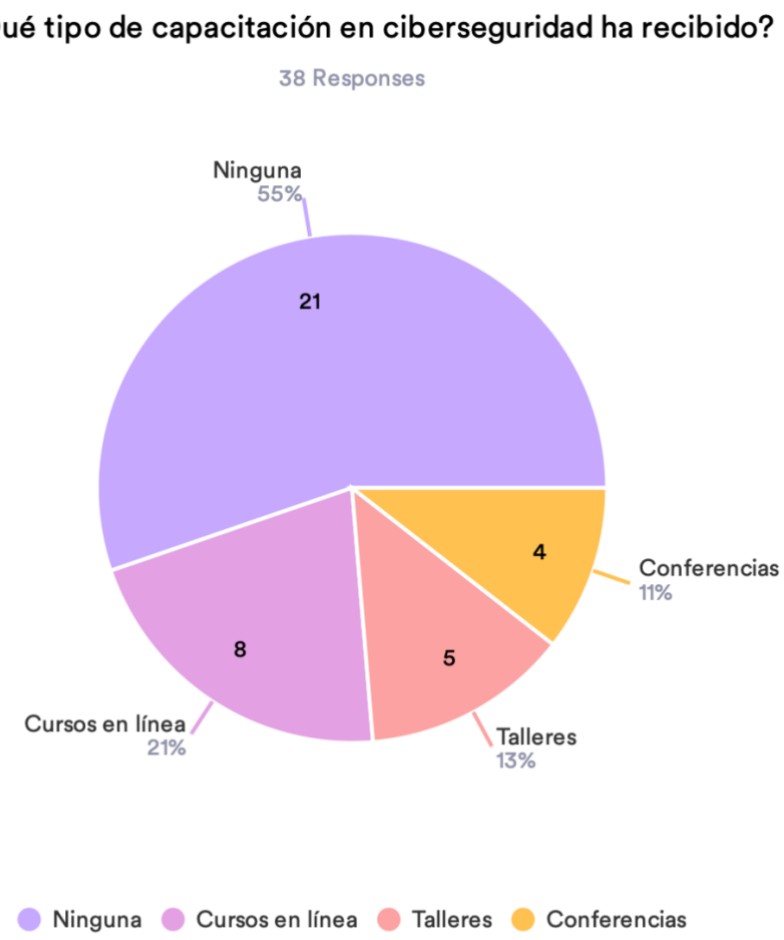

Figura 53 - Tipo Capacitación Otros Empleados

Fuente: Elaboración Propia.

5. **TIPO DE CAPACITACIÓN RECIBIDA:** Los talleres (35%) y los cursos en línea (30%) son las modalidades más comunes, sugiriendo una preferencia por métodos de aprendizaje interactivos y accesibles.

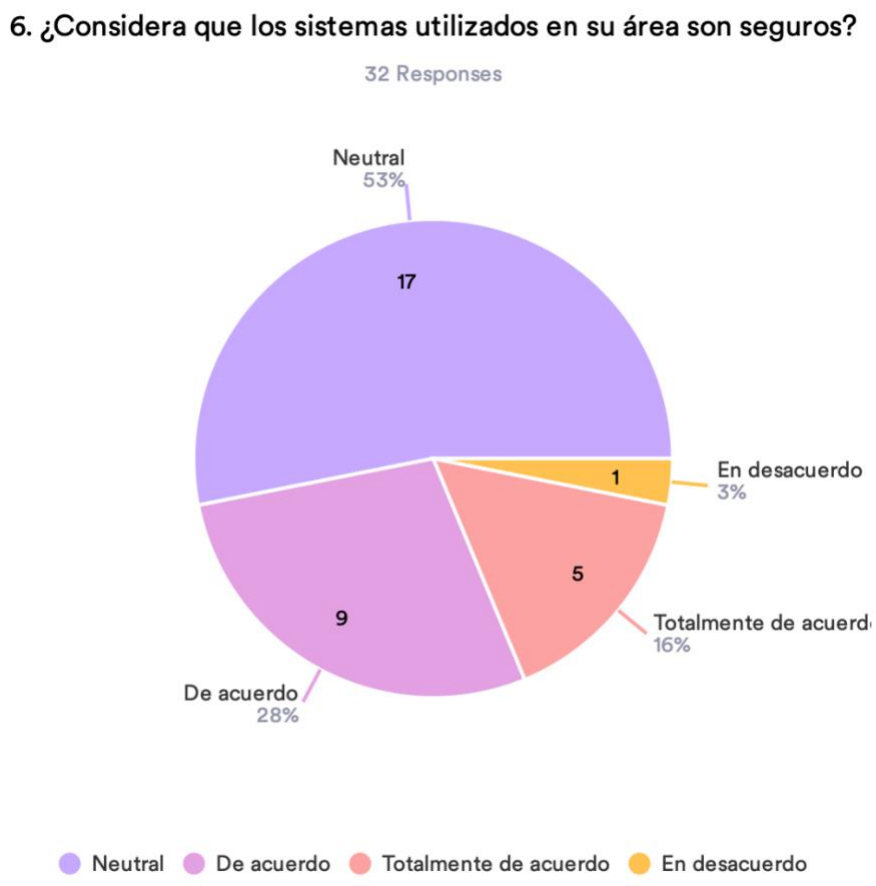

Figura 54 - Infraestructura Adecuada Otros Empleados

Fuente: Elaboración Propia.

6. **ADECUACIÓN DE LA SEGURIDAD EN EL TRABAJO:** Solo el 20% considera que los sistemas utilizados en su área son seguros, lo cual refleja una percepción general de insuficiencia en las medidas de seguridad actuales.

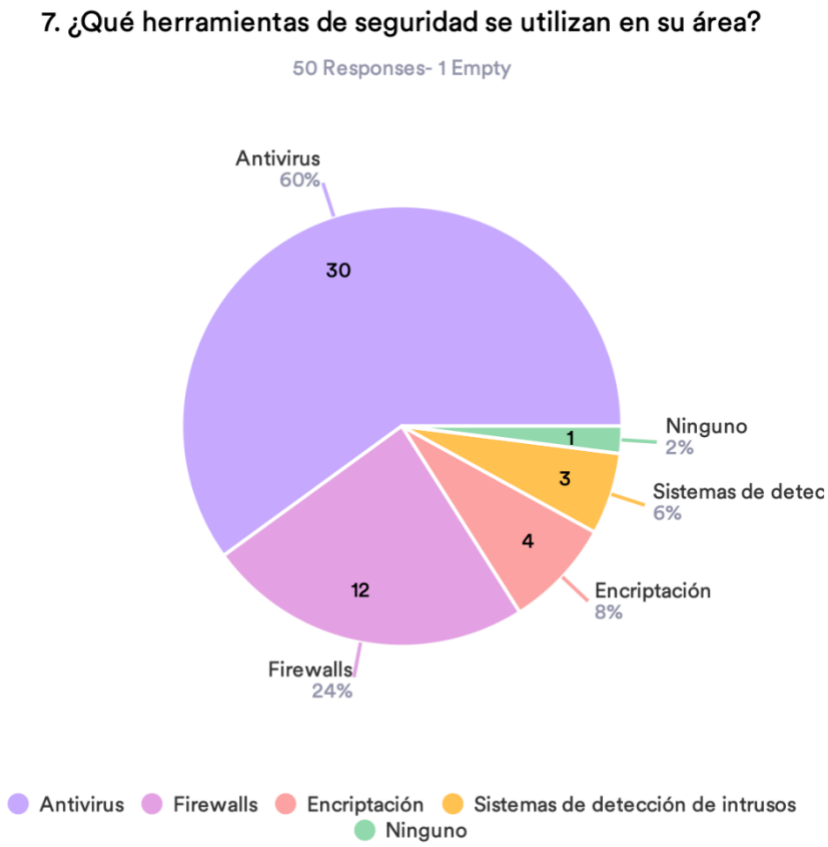

Figura 55 - Herramientas Utilizadas Otros Empleados

Fuente: Elaboración Propia.

7. **HERRAMIENTAS DE SEGURIDAD UTILIZADAS:** La encriptación (40%), firewalls (30%) y antivirus (20%) son las herramientas más mencionadas, aunque su uso no es uniforme ni percibido como completamente efectivo.

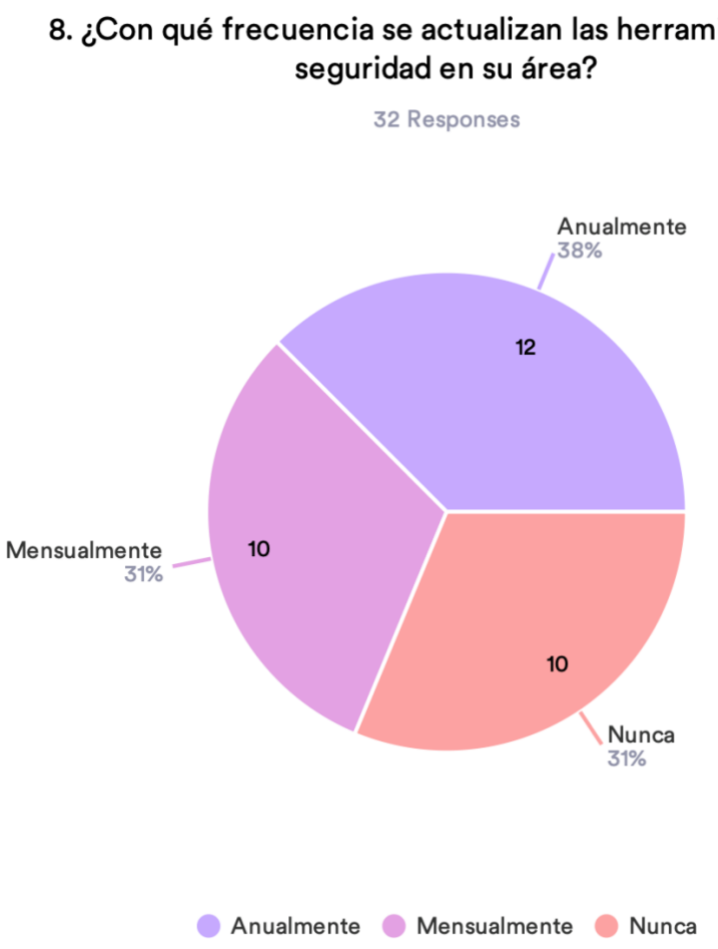

Figura 56 - Frecuencia de Herramientas Utilizadas Otros Empleados

Fuente: Elaboración Propia.

8. **FRECUENCIA DE ACTUALIZACIÓN DE HERRAMIENTAS:** Un 50% indica actualizaciones anuales, lo cual no es suficiente para enfrentar las amenazas cibernéticas que evolucionan rápidamente.

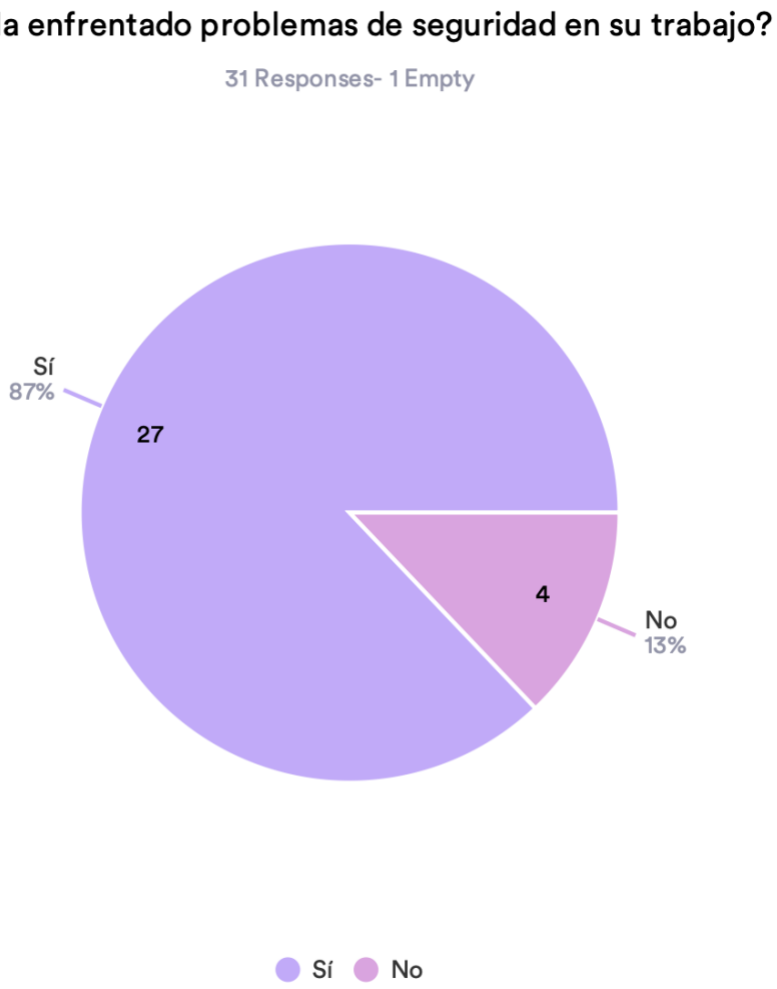

Figura 57 - Gestión de Incidentes Otros Empleados

Fuente: Elaboración Propia.

9. **PROBLEMAS DE SEGURIDAD:** El 70% ha enfrentado problemas de seguridad en su trabajo, indicando una alta incidencia de vulnerabilidades.

Figura 58 - Tipo de Incidentes Otros Empleados

Fuente: Elaboración Propia.

10. **TIPO DE PROBLEMAS DE SEGURIDAD:** Los problemas más comunes incluyen pérdida de datos (30%) y acceso no autorizado (40%), lo cual refleja las áreas críticas que necesitan ser mejoradas.

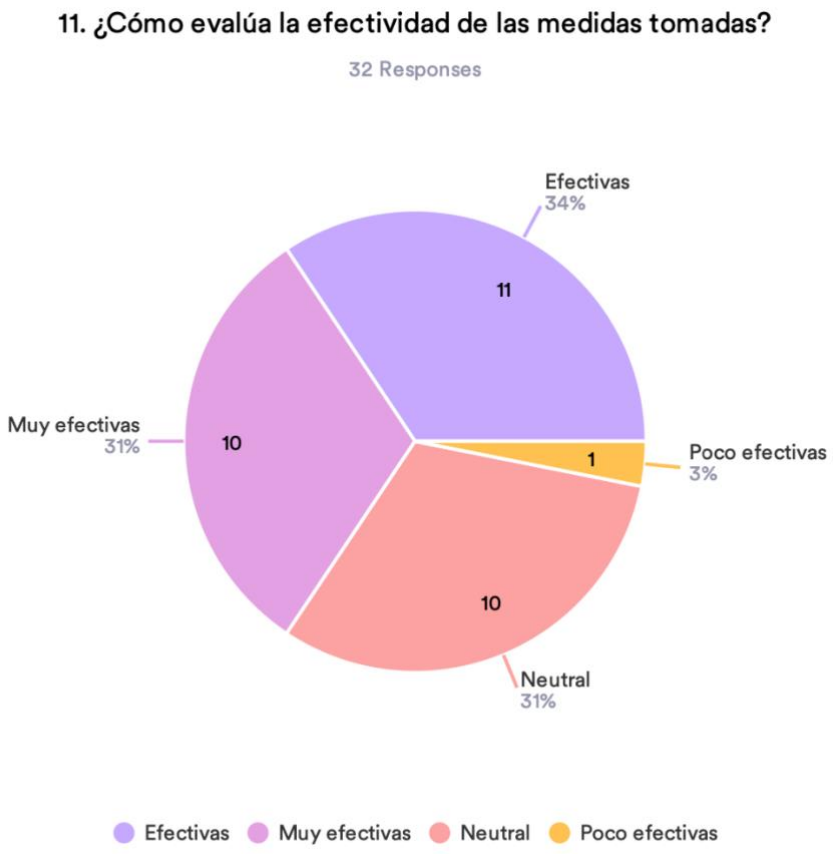

Figura 59 - Efectividad Otros Empleados

Fuente: Elaboración Propia.

11. **EFECTIVIDAD DE LAS MEDIDAS:** Un 50% considera que las medidas fueron efectivas, mientras que un 40% se mantiene neutral, sugiriendo que las medidas actuales no siempre son percibidas como suficientes.

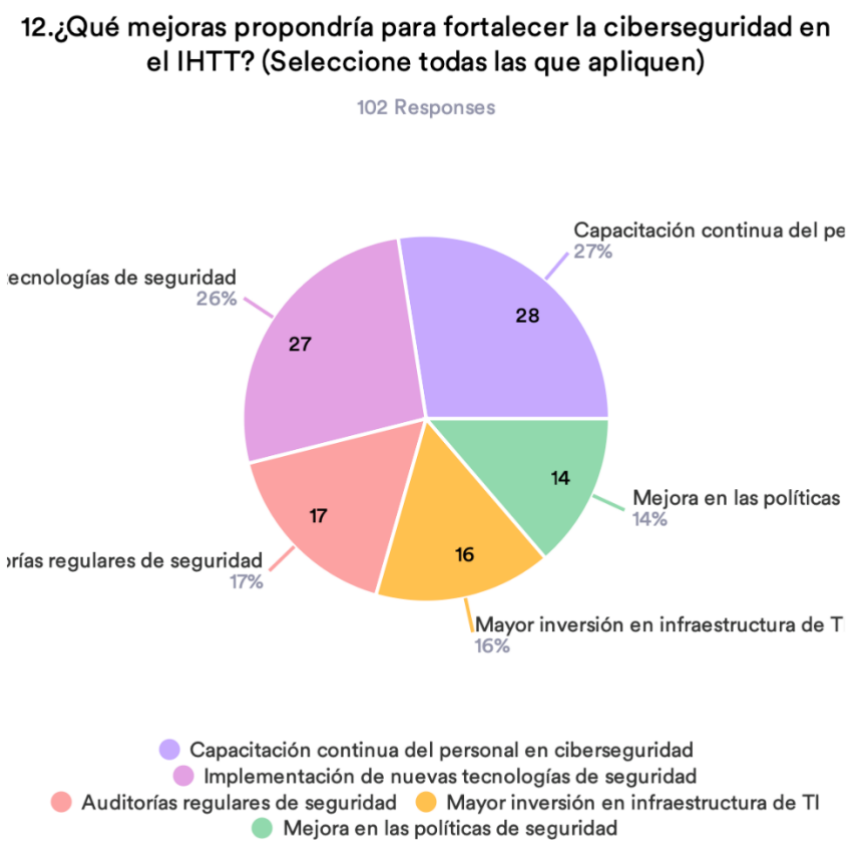

Figura 60 - Fortalecer Ciberseguridad Otros Empleados

Fuente: Elaboración Propia.

12. **PROPUESTA DE MEJORAS:** Un 45% sugiere la implementación de mejores políticas de seguridad y capacitaciones regulares para el personal, indicando una clara necesidad de formación y mejoras tecnológicas.

ENCUESTAS DE OTROS EMPLEADOS:

Los otros empleados del IHTT reflejan una necesidad general de mayor formación en ciberseguridad. La mayoría tiene un conocimiento básico y ha recibido capacitación reciente. Las herramientas de seguridad más utilizadas son la encriptación y el antivirus, y los sistemas en su área son mayormente considerados seguros. Sin embargo, hay una necesidad de mejorar las políticas de seguridad y la formación continua. La pérdida de datos y el acceso no autorizado son problemas comunes, y las medidas tomadas hasta ahora son vistas como neutrales en términos de

efectividad.

Referencias en Imágenes:

- Figura 42: Seguridad de los sistemas en el área de trabajo.
- Figura 43: Herramientas de seguridad utilizadas.
- Figura 45: Problemas de seguridad enfrentados.
- Figura 46: Tipos de problemas de seguridad.

CITAS POR CAPÍTULO:

Fortalecer la infraestructura de TI y asegurar la continuidad operativa frente a amenazas cibernéticas es un objetivo general que se refleja en la necesidad de mejorar las políticas de seguridad (Capítulo 1.5.1, Objetivo General).

Crear un sistema educativo continuo en ciberseguridad, aplicable a todos los empleados, es esencial para mejorar la seguridad en el IHTT (Capítulo 1.5.2, Objetivo Específico 4).

4.2.4 RESULTADOS OBJETIVO 3: DISEÑAR UN PROTOCOLO DE SEGURIDAD DIGITAL QUE INCORPORE MONITORIZACIÓN AVANZADA, PLANES DE RESPUESTA RÁPIDA Y UN ESQUEMA DE RECUPERACIÓN ANTE DESASTRES.

Los datos recopilados de las encuestas revelan una percepción generalizada de insuficiencia en la seguridad actual del IHTT. Un significativo porcentaje de los encuestados manifestó que los sistemas y herramientas de seguridad utilizados actualmente no son adecuados para enfrentar las crecientes amenazas cibernéticas. Esta percepción se debe en parte a la falta de actualización regular de las herramientas de seguridad, como firewalls y antivirus, y a la carencia de políticas robustas y actualizadas de gestión de incidentes.

Los empleados expresaron una demanda clara y urgente de formación y mejoras tecnológicas. La mayoría de los técnicos de TI y otros empleados clave indicaron la necesidad de programas de capacitación continua en ciberseguridad, que no solo cubran las amenazas actuales sino también las emergentes. Además, destacaron la importancia de implementar políticas de

seguridad más estrictas y de realizar actualizaciones frecuentes de las herramientas de ciberseguridad para asegurar la protección efectiva de los datos y sistemas del IHTT.

Las medidas sugeridas por los encuestados incluyen la implementación de programas de capacitación continuos, la actualización regular de herramientas de seguridad, la creación de políticas de seguridad más rigurosas, y la instauración de un esquema de recuperación ante desastres que permita una rápida restauración de los servicios en caso de un ataque cibernético. Estas recomendaciones subrayan la necesidad de un enfoque integral y proactivo en la gestión de la ciberseguridad del IHTT, que incorpore tanto la tecnología como la formación del personal.

4.2.5 RESULTADOS OBJETIVO 4: CREAR UN SISTEMA EDUCATIVO CONTINUO EN CIBERSEGURIDAD PARA CAPACITAR AL PERSONAL DE TI Y A LOS USUARIOS FINALES EN PRÁCTICAS SEGURAS Y EN LA IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA EN LA INSTITUCIÓN.

La necesidad de capacitación continua en ciberseguridad es un tema recurrente en los datos de las encuestas. Un alto porcentaje de los empleados, especialmente aquellos en roles no técnicos, señaló que no habían recibido capacitación adecuada en ciberseguridad en los últimos 12 meses. Esta falta de formación es una debilidad considerable que podría exponer a la institución a riesgos innecesarios. Los empleados manifestaron un fuerte interés en recibir formación regular y actualizada para mantenerse al día con las mejores prácticas y nuevas amenazas en el ámbito de la ciberseguridad.

Se sugiere la implementación de un programa educativo continuo en ciberseguridad, que incluya talleres, cursos en línea, y simulacros de respuesta a incidentes. Este programa debe estar diseñado para ser accesible y relevante para todos los niveles de empleados, desde el personal técnico hasta los usuarios finales. La formación debe cubrir una amplia gama de temas, desde los conceptos básicos de ciberseguridad hasta técnicas avanzadas de detección y respuesta a amenazas.

La actualización regular de herramientas y sistemas es igualmente crucial. Los encuestados señalaron que las herramientas de seguridad deben ser actualizadas con mayor frecuencia para enfrentar eficazmente las amenazas cibernéticas que evolucionan rápidamente. Además, la

creación de un sistema educativo continuo en ciberseguridad no solo mejorará la competencia técnica del personal, sino que también fomentará una cultura organizacional de seguridad, donde todos los empleados sean conscientes de los riesgos y se sientan responsables de la protección de los datos y sistemas del IHTT.

CAPÍTULO V – CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

La investigación realizada en el Instituto Hondureño de Transporte Terrestre (IHTT) ha revelado múltiples dimensiones de la ciberseguridad institucional, destacando áreas de mejora cruciales. A través de encuestas exhaustivas dirigidas a diversos grupos de empleados, se ha obtenido una visión integral y detallada del estado actual de la ciberseguridad en el IHTT.

La evaluación de vulnerabilidades en la infraestructura de TI del IHTT ha revelado deficiencias significativas. El 60% de los técnicos de TI y el 70% de otros empleados consideran que las herramientas y sistemas actuales no son suficientes para prevenir ciberataques de manera efectiva. Esta percepción destaca la necesidad de una evaluación constante y la actualización de las medidas de seguridad para proteger la infraestructura del IHTT. Además, la falta de confianza en la infraestructura actual resalta la necesidad urgente de implementar soluciones tecnológicas avanzadas que puedan adaptarse a las amenazas cibernéticas en evolución.

El análisis de las vulnerabilidades reveló que las herramientas y sistemas utilizados no siempre se actualizan con la frecuencia necesaria, lo cual incrementa el riesgo de exposición a nuevas amenazas. Se identificó una falta de integración de soluciones tecnológicas avanzadas, como sistemas de monitoreo continuo y análisis predictivo, que podrían mejorar significativamente la capacidad del IHTT para prevenir y detectar ciberataques. Por lo tanto, es esencial establecer un plan de actualización tecnológica regular y continuo que asegure la implementación de las mejores prácticas y tecnologías de vanguardia en ciberseguridad.

El estudio ha demostrado que las políticas y protocolos de seguridad existentes no son adecuadas. La mayoría de los operadores de ventanilla y otros empleados perciben una falta de efectividad en las medidas implementadas. Solo el 20% de los operadores considera que los sistemas utilizados son seguros, lo cual indica una percepción general de insuficiencia en la seguridad actual. Esto resalta la urgencia de revisar y fortalecer los protocolos de seguridad digital en el IHTT, asegurando que sean comprensibles y aplicables para todos los niveles de la organización, y que incluyan procedimientos claros y actualizados para la gestión de incidentes.

Es fundamental establecer un marco de colaboración que permita la implementación

efectiva de medidas de ciberseguridad de emergencia. Esto incluye la creación de un sistema de comunicación eficiente entre todos los departamentos para asegurar una respuesta rápida y coordinada ante incidentes. Además, es necesario desarrollar políticas claras y detalladas que definan los roles y responsabilidades de cada miembro del personal en la gestión de la seguridad digital, promoviendo una cultura organizacional que priorice la ciberseguridad en todas las operaciones diarias.

Una conclusión recurrente es la insuficiencia de capacitación en ciberseguridad entre los empleados del IHTT. Tanto técnicos de TI, abogados, operadores de ventanilla, inspectores de campo y otros empleados reportaron un conocimiento mayormente básico en ciberseguridad, con un alto porcentaje que no ha recibido formación reciente en esta área. Un 60% de los inspectores de campo y un 50% de los operadores de ventanilla no han recibido capacitación en los últimos 12 meses. Esto destaca la necesidad de establecer programas de capacitación continua y actualizada para mejorar la preparación del personal ante posibles amenazas cibernéticas.

Las capacitaciones deben incluir no solo aspectos técnicos, sino también prácticas de seguridad cotidianas que los empleados puedan aplicar en su trabajo diario. Es crucial que estas capacitaciones se diseñen de manera interactiva y práctica, utilizando simulaciones y ejercicios reales que permitan a los empleados experimentar y aprender a manejar incidentes de seguridad en un entorno controlado. Además, se debe fomentar una cultura de aprendizaje continuo donde la ciberseguridad se considere una prioridad en todos los niveles de la organización, asegurando que los empleados estén siempre informados sobre las últimas amenazas y técnicas de defensa.

Los datos sugieren que, aunque existen medidas para gestionar incidentes de seguridad, estas no siempre son percibidas como efectivas. Un 70% de los inspectores de campo y un 60% de los técnicos de TI han reportado una alta incidencia de problemas de seguridad, destacando la importancia de mejorar las capacidades de respuesta y recuperación ante incidentes cibernéticos. Es crucial desarrollar y aplicar un protocolo de gestión de incidentes robusto y bien definido. Este protocolo debe ser revisado y actualizado regularmente, y su eficacia debe ser probada a través de simulacros y ejercicios prácticos que involucren a todos los empleados.

El protocolo debe incluir etapas claras de detección, contención, erradicación y recuperación ante incidentes, asegurando que todos los empleados sepan exactamente qué hacer en cada fase de un incidente. Además, se debe establecer un sistema de reporte y análisis post-

incidente que permita aprender de cada evento y mejorar continuamente las estrategias y respuestas de seguridad. Este enfoque no solo fortalecerá la capacidad del IHTT para manejar incidentes actuales, sino que también mejorará su preparación para enfrentar futuras amenazas de manera más efectiva y coordinada.

La investigación ha identificado una clara necesidad de integrar soluciones tecnológicas avanzadas en el IHTT. Los resultados muestran que las herramientas de seguridad utilizadas no siempre están actualizadas, y que la implementación de nuevas tecnologías puede mejorar significativamente la seguridad de la información y la continuidad operativa. Este hallazgo apoya la recomendación de adoptar tecnologías emergentes como sistemas de monitoreo continuo y análisis predictivo. La integración de estas tecnologías no solo mejorará la capacidad del IHTT para prevenir ataques, sino que también fortalecerá su capacidad para detectar y responder rápidamente a cualquier incidente.

La implementación de soluciones tecnológicas avanzadas permitirá al IHTT no solo mejorar su postura de seguridad, sino también optimizar la eficiencia operativa y la resiliencia ante ciberataques. Es esencial establecer una estrategia tecnológica integral que incluya la evaluación y adopción de herramientas de inteligencia artificial y aprendizaje automático, capaces de identificar patrones y anomalías en el tráfico de red y comportamiento de los sistemas. Esta estrategia debe ser respaldada por un compromiso institucional con la innovación y la mejora continua en ciberseguridad, asegurando que el IHTT esté siempre preparado para enfrentar los desafíos tecnológicos del futuro.

5.2 RECOMENDACIONES

Se recomienda una inversión significativa en la actualización y mantenimiento de la infraestructura de TI del IHTT. Esto incluye la implementación de herramientas de seguridad avanzadas, la realización de auditorías regulares y la adopción de tecnologías emergentes para fortalecer la defensa contra ciberataques. Además, es crucial desarrollar una estrategia de actualización continua que permita al IHTT mantenerse a la vanguardia en términos de seguridad tecnológica. La mejora de la infraestructura de TI contribuirá a una mayor protección y a la continuidad operativa de la institución.

Es esencial implementar un programa de capacitación continua en ciberseguridad para

todos los empleados del IHTT. Este programa debe incluir talleres, cursos en línea y simulaciones de ataques cibernéticos para mantener al personal actualizado y preparado para enfrentar amenazas emergentes. La capacitación debe ser integral, cubriendo no solo aspectos técnicos, sino también estrategias de prevención y respuesta a incidentes. La creación de un sistema educativo continuo en ciberseguridad es vital para mantener a los empleados informados y preparados.

El IHTT debe revisar y actualizar sus políticas de seguridad digital. Esto incluye la implementación de controles de acceso más estrictos, políticas de encriptación de datos y procedimientos claros para la gestión de incidentes. Además, se debe fomentar una cultura de seguridad entre todos los empleados, asegurando que comprendan la importancia de seguir estas políticas y procedimientos. La evaluación y fortalecimiento de los protocolos de seguridad ayudará a mejorar la percepción de seguridad entre los empleados y a reducir las vulnerabilidades.

Se debe desarrollar y poner en práctica un protocolo de gestión de incidentes que incluya la detección, contención, erradicación y recuperación de incidentes de seguridad. Este protocolo debe ser probado y actualizado regularmente mediante simulacros y ejercicios de respuesta. Es importante que todos los empleados estén familiarizados con este protocolo y sepan cómo actuar en caso de un incidente. La implementación de este protocolo fortalecerá la capacidad de respuesta del IHTT ante incidentes cibernéticos.

Es esencial que el IHTT integre soluciones tecnológicas avanzadas como sistemas de monitoreo continuo, análisis predictivo de amenazas y tecnologías de inteligencia artificial para mejorar la protección y la respuesta a incidentes. La adopción de estas tecnologías permitirá al IHTT no solo detectar y responder a amenazas de manera más eficiente, sino también anticiparse a posibles ataques y tomar medidas preventivas. La integración tecnológica es clave para la modernización de la infraestructura de seguridad del IHTT.

Finalmente, se recomienda fomentar una cultura de seguridad dentro del IHTT. Esto incluye la promoción de buenas prácticas de seguridad entre todos los empleados, la creación de campañas de concienciación y la participación activa de la alta dirección en los esfuerzos de ciberseguridad. La cultura de seguridad debe ser un aspecto fundamental del entorno laboral, incentivando a todos los empleados a tomar en serio la ciberseguridad y a adoptar prácticas seguras en su trabajo diario. Fomentar esta cultura contribuirá a una mayor cohesión y efectividad en la implementación de medidas de seguridad.

CAPÍTULO VI – APLICABILIDAD

6.1 NOMBRE DE LA PROPUESTA

Plan de Implementación y Gobierno de Ciberseguridad en el Instituto Hondureño de Transporte Terrestre (IHTT)

6.2 JUSTIFICACIÓN DE LA PROPUESTA

La propuesta de implementación de ciberseguridad en el IHTT se fundamenta en los hallazgos y conclusiones detallados en los capítulos anteriores. Las evaluaciones han demostrado que la infraestructura tecnológica actual es insuficiente para prevenir ciberataques efectivos, y que existe una necesidad significativa de mejorar los protocolos de seguridad y la capacitación del personal. La implementación de esta propuesta no solo aborda estas deficiencias, sino que también prepara al IHTT para enfrentar futuras amenazas cibernéticas, garantizando la resiliencia y continuidad operativa. Esto es crucial para proteger los datos sensibles y la operatividad de la institución, mejorando así la confianza y seguridad de los procesos del IHTt (Babbie, 2016).

La necesidad de mejorar la ciberseguridad en el IHTT no solo responde a la urgencia de prevenir futuros incidentes, sino también a la necesidad de cumplir con las normativas internacionales de seguridad de la información. La implementación de un sistema robusto de ciberseguridad asegurará que el IHTT esté alineado con los estándares globales, fortaleciendo su posición como una entidad confiable y segura (Creswell, 2018). Además, los datos recopilados durante la investigación indican una clara demanda de formación continua en ciberseguridad, con el objetivo de empoderar a los empleados y mejorar la cultura de seguridad en toda la organización.

Este proyecto, al contar con una inversión significativa de 20 millones de lempiras para la adquisición de infraestructura y la capacitación del personal, representa una inversión estratégica para el futuro del IHTT. La implementación de servidores en la nube, firewalls avanzados, puntos de acceso seguros y sistemas de monitoreo no solo incrementará la protección contra amenazas, sino que también optimizará la eficiencia operativa (Smith J. , 2022). En conclusión, esta propuesta de ciberseguridad es un paso fundamental para asegurar la integridad, confidencialidad y disponibilidad de los sistemas de información del IHTT, garantizando así un servicio seguro y eficiente para los ciudadanos y colaboradores (Smith J. T., 2023).

6.3 ALCANCE DE LA PROPUESTA

La propuesta tiene como objetivo principal fortalecer la ciberseguridad en el IHTT a través de:

- Actualización de la infraestructura de TI con servidores físicos y en la nube, firewalls, access points y routers administrables.
- Implementación de un gestor documental para mejorar la seguridad y eficiencia en el manejo de la información.
- Capacitación del personal en ciberseguridad y en el uso de las nuevas herramientas y protocolos.
- Establecimiento de un protocolo de gestión de incidentes robusto y eficaz.
- Monitoreo y evaluación continua de la efectividad de las medidas implementadas.

6.4 DESCRIPCIÓN DE LA PROPUESTA

6.4.1. DESCRIPCIÓN DEL "QUÉ" Y "CÓMO"

ACTUALIZACIÓN DE LA INFRAESTRUCTURA DE TI:

1. **Adquisición e instalación de servidores físicos:**
   - **Qué:** Se adquirirán servidores físicos de alta capacidad para mejorar la capacidad de almacenamiento y procesamiento de datos del IHTT.
   - **Cómo:** La instalación y configuración de los servidores se realizarán en las instalaciones del IHTT. Este proceso incluirá la integración de los servidores en la red existente, asegurando la compatibilidad con los sistemas actuales. El presupuesto asignado es de 6 millones de lempiras.
2. **Implementación de servidores en la nube:**
   - **Qué:** Integración de servidores en la nube para asegurar la disponibilidad, escalabilidad y recuperación ante desastres.

- **Cómo:** La implementación se llevará a cabo mediante un proveedor de servicios en la nube, seleccionado por su reputación y capacidades técnicas. Se destinarán 7 millones de lempiras a este proyecto, cubriendo costos de suscripción, configuración y soporte técnico inicial.

3. Instalación de firewalls:

- **Qué:** Instalación de firewalls avanzados para proteger la red del IHTT contra amenazas cibernéticas.
- **Cómo:** Los firewalls se instalarán y configurarán siguiendo las mejores prácticas de seguridad, asegurando la creación de reglas de filtrado y monitoreo constante. El presupuesto asignado es de 3 millones de lempiras, cubriendo tanto la adquisición del hardware como la capacitación necesaria para el personal encargado de su administración.

4. Instalación de access points y routers administrables :

- **Qué:** Despliegue de 18 access points y 14 routers administrables para mejorar la conectividad y seguridad de la red.
- **Cómo:** Con un presupuesto de 1.5 millones de lempiras, estos dispositivos se instalarán estratégicamente en las oficinas del IHTT para asegurar una cobertura robusta y una gestión eficiente del tráfico de red.

IMPLEMENTACIÓN DE UN GESTOR DOCUMENTAL:

1. Selección e instalación de un sistema de gestión documental:

- **Qué:** Implementación de un sistema de gestión documental que asegure el acceso controlado y la encriptación de datos.
- **Cómo:** Se seleccionará un proveedor que ofrezca un sistema seguro y compatible con las necesidades del IHTT. El presupuesto de 2.5 millones de lempiras cubrirá la adquisición del software, la configuración inicial, y la formación del personal en su uso. Este sistema permitirá la gestión eficiente y segura de los documentos, asegurando la confidencialidad y disponibilidad de la información.

CAPACITACIÓN DEL PERSONAL:

1. Capacitación inicial y certificación en firewalls:

- **Qué:** Formación especializada para el personal en la administración y manejo de firewalls.
- **Cómo:** Cuatro personas del equipo de TI serán certificadas como parte del valor agregado proporcionado por la empresa externa. Esta capacitación incluirá cursos intensivos y exámenes de certificación, asegurando que el personal esté completamente preparado para gestionar y optimizar los firewalls instalados.

PROTOCOLO DE GESTIÓN DE INCIDENTES:

1. Diseño e implementación de un protocolo de gestión de incidentes:

- **Qué:** Desarrollo de un protocolo integral para la detección, respuesta y recuperación ante incidentes de seguridad.
- **Cómo:** Se elaborará un documento detallado que describa los procedimientos específicos para diferentes tipos de incidentes. Este protocolo será probado mediante simulacros y revisado regularmente para incorporar nuevas amenazas y tecnologías emergentes. Además, se realizarán entrenamientos periódicos para asegurar que todo el personal esté familiarizado con los procedimientos.

MONITOREO Y EVALUACIÓN:

1. Establecimiento de indicadores y métricas:

- **Qué:** Implementación de un sistema de monitoreo y evaluación continuo para asegurar la efectividad de las medidas de seguridad.
- **Cómo:** El equipo de TI del IHTT gestionará el monitoreo mediante herramientas avanzadas que permitirán la supervisión constante de la red y los sistemas. Se establecerán indicadores clave de rendimiento (KPIs) y métricas específicas para evaluar la efectividad de las medidas implementadas, realizando ajustes necesarios basados en los resultados obtenidos.

6.4.2. DESARROLLO DE ELEMENTOS NECESARIOS

Herramientas y Tecnologías:

- Servidores físicos y en la nube: Huawei Cloud.
- Firewalls: Juniper.
- Access points y routers administrable.
- Gestor documental: Sistema específico seleccionado en base a cotizaciones.

Instrumentos y Procesos:

- Protocolo de ciberseguridad y gestión de incidentes.
- Plan de capacitación continuo.
- Sistema de monitoreo y evaluación.

6.5 MEDIDAS DE CONTROL

Para asegurar el éxito de la implementación del plan de ciberseguridad en el Instituto Hondureño de Transporte Terrestre (IHTT), se adoptarán una serie de medidas de control rigurosas y estructuradas. Estas medidas no solo están diseñadas para identificar y mitigar posibles vulnerabilidades, sino también para asegurar una respuesta rápida y efectiva ante cualquier incidente de seguridad. A continuación, se detallan las principales medidas de control que se implementarán:

1. **Evaluación Periódica de la Infraestructura:**

Se realizará una evaluación exhaustiva de la infraestructura de TI del IHTT en intervalos regulares. Este proceso incluirá la revisión de todos los componentes críticos, como servidores, redes y dispositivos de seguridad, para identificar posibles vulnerabilidades. La evaluación permitirá implementar acciones correctivas de manera proactiva, asegurando que las medidas de seguridad se mantengan robustas y eficaces en todo momento.

2. **Monitoreo Continuo de la Red y los Sistemas:**

Se implementarán herramientas avanzadas de monitoreo continuo para supervisar la actividad de la red y los sistemas del IHTT. Estas herramientas detectarán actividades inusuales o sospechosas en tiempo real, permitiendo una respuesta inmediata a posibles amenazas. El monitoreo continuo es crucial para mantener la integridad, confidencialidad y disponibilidad de los datos y sistemas.

3. **Auditorías Regulares:**

Se llevarán a cabo auditorías de seguridad de manera regular para evaluar la efectividad de las políticas y procedimientos implementados. Estas auditorías identificarán áreas de mejora y asegurarán que las prácticas de seguridad cumplan con las normativas internacionales y los estándares de la industria. Las auditorías también incluirán revisiones de cumplimiento normativo, asegurando que el IHTT cumpla con todas las regulaciones aplicables.

4. **Simulacros y Pruebas de Penetración:**

Para garantizar que el personal esté adecuadamente preparado para enfrentar incidentes de seguridad, se realizarán simulacros y pruebas de penetración periódicas. Estas actividades permitirán evaluar la capacidad de respuesta del personal y la efectividad de los protocolos de seguridad ante escenarios de ataque simulado. Los resultados de estos ejercicios se utilizarán para mejorar continuamente los procedimientos de seguridad y la formación del personal.

5. **Actualización Continua de Herramientas de Seguridad y Protocolos:**

En un entorno de amenazas cibernéticas en constante evolución, es crucial mantener las herramientas de seguridad y los protocolos actualizados. Se implementará un proceso de actualización continua que garantice que todas las herramientas y procedimientos de seguridad se adapten a las nuevas amenazas y vulnerabilidades. Esto incluirá la instalación de parches de seguridad, la actualización de software y la revisión de políticas de seguridad.

6. **Formación y Capacitación del Personal:**

Se desarrollarán programas de formación y capacitación continua para el personal del IHTT, enfocándose en la ciberseguridad y la gestión de incidentes. Estos programas incluirán talleres, cursos en línea y simulacros prácticos, asegurando que todos los empleados estén al tanto de las mejores prácticas y procedimientos de seguridad. La formación regular es fundamental para mantener al personal preparado y consciente de las amenazas cibernéticas.

7. **Implementación de Medidas de Contingencia:**

Se establecerán planes de contingencia detallados para asegurar la continuidad operativa en caso de un incidente de seguridad significativo. Estos planes incluirán procedimientos para la recuperación de datos, la restauración de sistemas críticos y la comunicación efectiva con los stakeholders internos y externos. La preparación para contingencias es esencial para minimizar el impacto de cualquier interrupción y garantizar la resiliencia de la organización.

8. **Evaluación de la Efectividad de las Medidas Implementadas:**

Se realizará una evaluación periódica de la efectividad de todas las medidas de control implementadas. Esta evaluación incluirá el análisis de métricas de desempeño, la revisión de incidentes de seguridad gestionados y la retroalimentación del personal. Los resultados de estas evaluaciones se utilizarán para ajustar y mejorar continuamente las estrategias de seguridad del IHTT.

Estas medidas de control representan un enfoque integral y proactivo para la gestión de la ciberseguridad en el IHTT, alineándose con los objetivos y la estrategia global de la institución. La implementación de estas medidas asegurará que el IHTT esté mejor preparado para enfrentar las amenazas cibernéticas y proteger sus activos críticos de manera efectiva.

6.6 CRONOGRAMA DE IMPLEMENTACIÓN

DIAGRAMA DE GANTT: Plan de Implementación de Ciberseguridad en el Instituto Hondureño de Transporte Terrestre

	Nombre de tarea	Fecha de inicio	Duración	Progreso	Estado	Fecha final
		03/06/2024	480h	36%		23/08/202
1	**Evaluación Inicial y Planificación**	03/06/2024	120h	100%		21/06/202
1.1	Evaluación de la Infraestructura Actual	03/06/2024	40h	100%	Terminadc	07/06/202
1.2	Identificación de Necesidades y Requerimientos	10/06/2024	40h	100%	Terminadc	14/06/202
1.3	Planificación del Proyecto	03/06/2024	120h	100%	Terminadc	21/06/202
2	**Adquisición de Equipos y Servicios**	03/06/2024	200h	57%		05/07/202
2.1	Proceso de Licitación y Selección de Proveedores	24/06/2024	40h	50%	En progres	28/06/202
2.2	Adquisición de Servidores en la Nube	03/06/2024	80h	100%	Terminadc	14/06/202
2.3	Adquisición de Servidores Físicos	17/06/2024	120h	50%	En progres	05/07/202
2.4	Adquisición de Firewalls	17/06/2024	120h	50%	En progres	05/07/202
2.5	Adquisición de Access Points y Switches Adminis...	17/06/2024	120h	50%	En progres	05/07/202
2.6	Adquisición de Gestor Documental	17/06/2024	120h	50%	En progres	05/07/202
3	**Instalación y Configuración**	10/06/2024	240h	18%		19/07/202
3.1	Instalación de Servidores Físicos	08/07/2024	80h	0%	Abierto	19/07/202
3.2	Instalación de Servidores en la Nube	10/06/2024	40h	100%	Terminadc	14/06/202
3.3	Configuración de Firewalls	08/07/2024	32h	0%	Abierto	11/07/202
3.4	Instalación de Access Points y Switches Administr...	08/07/2024	32h	0%	Abierto	11/07/202
3.5	Implementación del Gestor Documental	17/06/2024	8h	0%	Abierto	17/06/202
4	**Capacitación del Personal**	22/07/2024	120h	0%		09/08/202
4.1	Programas de Formación y Talleres	22/07/2024	120h	0%	Abierto	09/08/202
4.2	Simulacros	22/07/2024	120h	0%	Abierto	09/08/202
5	**Monitoreo y Evaluación**	12/08/2024	40h	0%		16/08/202
5.1	Implementación de Herramientas de Monitoreo	12/08/2024	40h	0%	Abierto	16/08/202
5.2	Revisiones Periódicas	12/08/2024	40h	0%	Abierto	16/08/202
6	**Evaluación Final y Ajustes**	19/08/2024	40h	0%		23/08/202
6.1	Evaluación del Proyecto	19/08/2024	40h	0%	Abierto	23/08/202

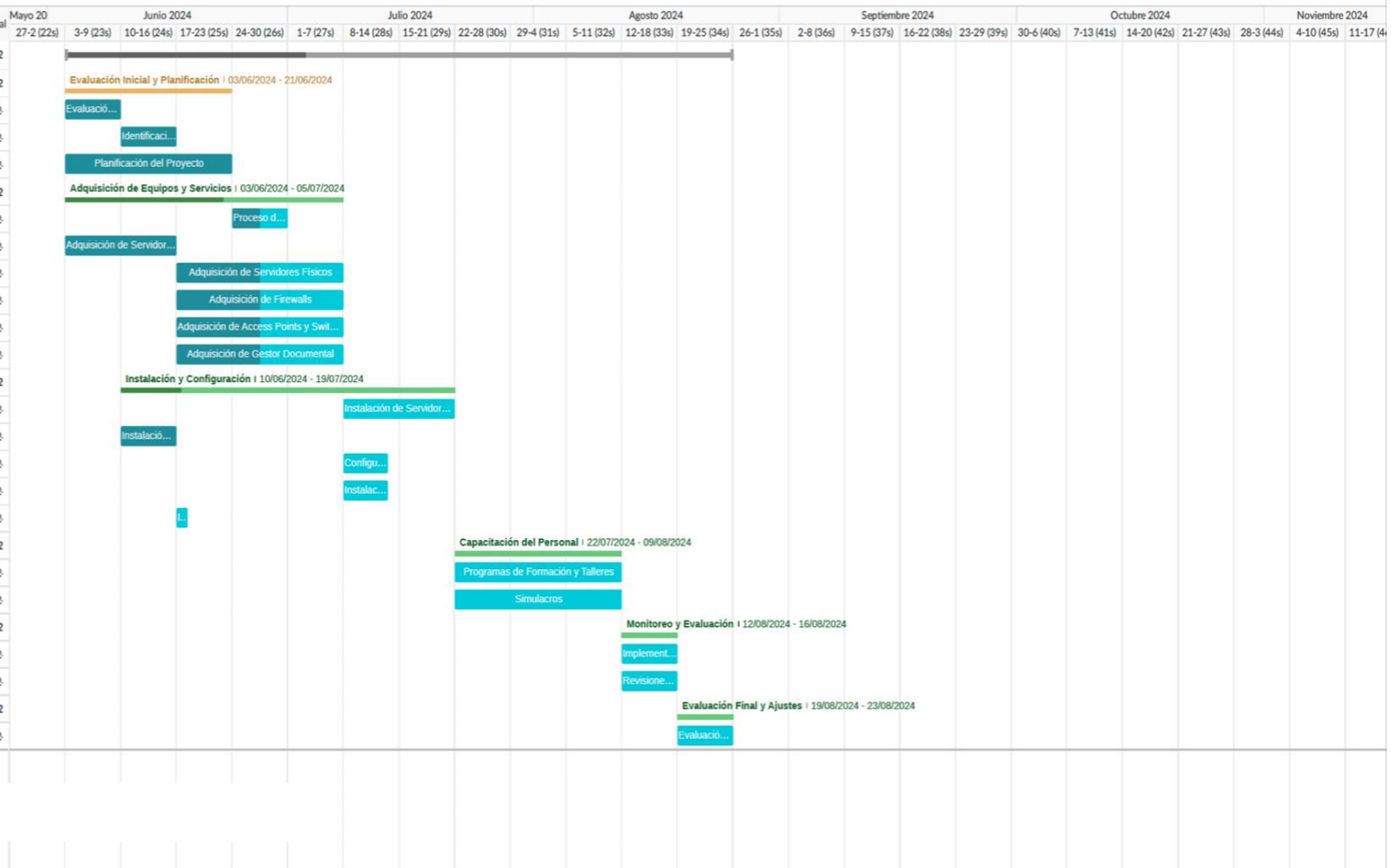

Figura 61 - Cronograma de Implementación

Fuente: Elaboración Propia.

MATRIZ DE RIESGOS

Tabla 3 - Matriz de Riesgo

Actividades del Proceso	Fecha	Riesgos Pertinentes	Causa Principal que Origina el Riesgo	Efectos o Consecuencias	Probabilidad	Impacto	Nivel de Riesgo Base	Prioridad Riesgo Base	Opciones de Tratamiento	Medidas de Tratamiento de Riesgos Críticos	Responsable	Incidentes	Probabilidad Residual	Impacto Residual	Nivel de Riesgo Residual	Prioridad Riesgo Residual	% Reducción Riesgo	Las Medidas Fueron Eficaces?	Análisis de Gestión y Resultados
Adquisición de Servidores Físicos	1/7/24	Retraso en la entrega	Problemas de logística	Retraso en la implementación del plan	3	4	12	Alta	Reducir	Establecer contratos con penalizaciones por retrasos	Departamento de Compras	0	2	2	4	Baja	67%	Parcial	Revisión de contratos de proveedores
Implementación de Servidores en la Nube	15/7/24	Falla en la migración de datos	Falta de experiencia	Pérdida de datos y tiempo	2	5	10	Alta	Reducir	Capacitación especializada y contratación de expertos externos	Equipo de TI	0	1	3	3	Moderada	70%	Sí	Evaluación post-migración con pruebas de integridad de datos
Instalación de Firewall	1/8/24	Configuración incorrecta	Falta de capacitación	Vulnerabilidades en la red	3	4	12	Alta	Reducir	Certificación en firewalls para el personal técnico	Equipo de TI	0	1	2	2	Baja	83%	Sí	Certificación y pruebas de penetración
Despliegue de Access Points	15/8/24	Problemas de cobertura	Infraestructura inadecuada	Puntos muertos en la red inalámbrica	2	3	6	Moderada	Reducir	Estudio de sitio y pruebas de cobertura antes de la instalación	Equipo de Redes	0	1	2	2	Baja	67%	Sí	Validación de la cobertura post-instalación
Implementación de Switches Administrables	1/9/24	Fallo en la configuración	Falta de experiencia	Interrupción de la conectividad	2	4	8	Alta	Reducir	Capacitación y simulaciones de configuración antes de la implementación	Equipo de TI	0	1	3	3	Moderada	63%	Sí	Monitoreo de la red después de la configuración
Implementación del Gestor Documental	15/9/24	Pérdida de documentos durante la migración	Falta de pruebas exhaustivas	Pérdida de información crítica	3	5	15	Muy Alta	Reducir	Plan de pruebas exhaustivo y backup completo antes de la migración	Equipo de T, DigitaciónI y Archivo	0	1	4	4	Moderada	73%	Sí	Auditoría post-migración
Capacitación del Personal	1/10/24	Baja participación	Falta de interés o relevancia percibida	Personal no capacitado adecuadamente en ciberseguridad	3	3	9	Moderada	Reducir	Diseño de programas de capacitación atractivos y relevantes, incentivos para la participación	RRHH								

Fuente: Elaboración Propia.

Tabla 4 - Escala de Riesgos

ESCALA DE RIESGOS	
Nivel de Riesgo Base	**Interpretación**
1-5	Muy Bajo
6-10	Bajo
11-15	Moderado
16-20	Alto
21-25	Muy Alto

Fuente: Elaboración Propia.

6.7 PRESUPUESTO

Para detallar las estimaciones de costos de la compra, se llevaron a cabo varias reuniones con diferentes empresas que ofrecían diversas soluciones a nuestras necesidades. Después de compartir con ellas nuestra historia y experiencia, amablemente nos proporcionaron detalles específicos sobre sus servicios, tales como características de servicios en la nube, servidores físicos, firewalls, switches, puntos de acceso (APs), y gestores documentales, cubriendo así todas nuestras necesidades.

A continuación, se presenta una matriz comparativa de las propuestas económicas de cada empresa:

Tabla 5 - Matriz Comparativa de Propuestas Económicas por empresa

MATRIZ COMPARATIVA DE PROPUESTAS ECONÓMICA POR EMPRESA					
ITEMS	**PBS**	**GRUPO RAF**	**MARTINEXA**	**CESA**	**SDT**
SERVIDORES NUBE	L9,745,581.35	L7,584,251.85	L0.00	L0.00	**L5,761,723.06**
EQUIPO DE COMPUTO	L1,759,610.30	L1,906,020.77	L2,988,247.29	**L784,771.16**	L1,578,954.52
DATACENTER	L4,581,905.78	L0.00	L8,041,020.86	**L5,217,391.30**	L4,521,125.56
FIREWALL	L1,554,550.54	L1,875,983.73	L1,278,310.59	**L2,608,695.65**	L1,145,236.36
GESTOR DOCUMENTAL	L3,520,199.07	L1,958,679.65	L2,200,000.00	**L1,739,130.43**	L1,432,582.00
SWITCHES Y AP	L930,922.78	L1,200,317.36	L1,560,461.54	**L1,777,981.03**	L1,604,892.12
TOTAL	L22,092,769.82	L14,525,253.36	L16,068,040.28	L12,127,969.57	L16,044,513.62
ISV 15%	L3,313,915.47	L2,178,788.00	L2,410,206.04	L1,819,195.44	L2,406,677.04
TOTAL GENERAL	L25,406,685.29	L16,704,041.36	L18,478,246.32	L13,947,165.01	L18,451,190.66

Fuente: Elaboración Propia.

El presupuesto total estimado para la implementación de las recomendaciones, basado en la matriz comparativa, asciende a **L20,573,146.52**. Después de evaluar las diferentes opciones que se ajustan a nuestras necesidades, la distribución del presupuesto queda de la siguiente manera:

Tabla 6 - Presupuesto Modernización y Optimización

ADQUISICIÓN MODERNIZACIÓN Y OPTIMIZACIÓN DE SU INFRAESTRUCTURA TECNOLÓGICA -IHTT					
N°	**Descripción**	**EMPRESA**	**Cantidades**	**Precio sin 15%**	**Precio Total**
1	Servidor Nube	SDT	1	L5,761,723.06	L6,625,981.52
2	Servidores Fisicos-Datacenter	CESA	3	L5,217,391.30	L6,000,000.00
3	Firewall	CESA	2	L2,608,695.65	L3,000,000.00
4	Switches y Ap	CESA	14	L1,777,981.03	L2,044,678.18
5	Gestor Documental	CESA	1	L1,739,130.43	L1,999,999.99
6	Equipo de Cómputo para Desarolladores	CESA	15	L784,771.16	L902,486.83
Totales				**L12,127,969.57**	**L20,573,146.52**

Fuente: Elaboración Propia.

Observación: Se justifica cada uno de los items detallados en la tabla 6 - Presupuesto Modernización y Optimización, en el anexo #4 - Especificaciones Técnicas.

La inversión en modernización y digitalización propuesta representa una oportunidad estratégica para mejorar significativamente la eficiencia operativa, la calidad del servicio y la capacidad de respuesta de la institución. Los beneficios esperados de esta inversión incluyen:

Mejora en la Eficiencia Operativa: La digitalización de procesos reducirá el tiempo necesario para completar tareas administrativas, eliminando redundancias y optimizando el uso de recursos. Esto permitirá que el personal se enfoque en actividades de mayor valor añadido, mejorando la productividad general de la institución.

Optimización de Recursos: Con la implementación de tecnologías modernas, se reducirán los costos operativos asociados con el manejo de documentación física, almacenamiento y procesamiento manual de datos. La digitalización permite un uso más eficiente de los recursos existentes, liberando capital que puede ser reinvertido en otras áreas críticas de la organización.

Mejor Toma de Decisiones: La disponibilidad de datos en tiempo real y la capacidad de

analizarlos eficientemente permitirá a la institución tomar decisiones más informadas y estratégicas. Esto reducirá la incertidumbre y aumentará la capacidad de anticipación y reacción ante cambios en el entorno operativo.

Incremento en la Satisfacción de los Usuarios: La modernización de los sistemas y la digitalización de los servicios ofrecerán una experiencia más fluida y accesible para los usuarios, lo que se traducirá en una mayor satisfacción y confianza en la institución. La facilidad de acceso a servicios digitales y la reducción de tiempos de espera son factores clave para mejorar la percepción pública.

Seguridad y Cumplimiento Normativo: La inversión en tecnología permitirá la implementación de medidas de seguridad más robustas y el cumplimiento con regulaciones más estrictas en cuanto a la protección de datos y la confidencialidad. Esto mitigará riesgos legales y protegerá la reputación de la institución.

Innovación y Competitividad: Al adoptar soluciones tecnológicas avanzadas, la institución se posicionará a la vanguardia en su sector, mejorando su capacidad para competir y colaborar con otras entidades a nivel nacional e internacional.

REFERENCIAS BIBLIOGRÁFICAS

Smith, J. (2022). *El costo de ignorar la ciberseguridad.* Ciberseguridad.

Romanosky, S. (2016). Examinar los costos y las causas de los incidentes cibernéticos. *JOURNAL OF CIBERSECURITY. https://doi.org/10.1093/cybsec/tyw001*, 121-135.

Johnson, M. &.-D. (2015). Ofender y ser ofendido en línea: mensajes viles, chistes y la ley. *Revisión de seguridad y derecho informático*, 1-22.

Von Solms, B. &. (2013). De la seguridad de la información a la ciberseguridad. *Computadoras y seguridad*, 97-102.

Ventures., C. (2022). Cybercrime report, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/. *CYBERCRIME MAGAZINE*.

Smith, J. T. (2023). Enhancing global cybersecurity strategies. *Journal of Cyber Policy*.

Commission, E. (2022). General Data Protection Regulation (GDPR). *EUROPEAN COMISSION*.

Forum., W. E. (2024). Informe Global de Riesgos. *2024*.

Johnson, L. &. (2023). Cybersecurity in interconnected infrastructures. *Journal of Cybersecurity and Mobility*.

Review, H. B. (2021). Por qué las organizaciones necesitan un enfoque integrado de ciberseguridad. *Harvard Business Review*.

MIT. (2023). *Guía de políticas de ciberseguridad*.

ISO. (2011). ISO/IEC 27031:2011. *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity. https://www.iso.org/standard/44374.html*.

Ponemon, I. (2020). Avanzando en la gestión responsable de la información. *Ponemon Institute*.

Bodeau, D. &. (2021). Enhancing the resilience of critical infrastructure to cyber-attacks. . *Journal of Cybersecurity*.

Linkov, I. &. (2019). The Science and Practice of Resilience. *Springer. DOI: 10.1007/978-3-030-04565-4.*

NIST. (2021). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. U.S. Department of Commerce. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. U.S. Department of Commerce.*

Tøndel, I. A. (2020). Information security incident management: Current practice as reported in the literature. *Computers & Security, 92, 101748. DOI: 10.1016/j.cose.2020.101748.*

Babbie, E. (2016). The practice of social research (14th ed.). *The practice of social research (14th ed.).*

Johnson, M. &. (2021). Governance in cybersecurity: Policy and practice. *Revista de ciberseguridad*, 1-22.

Morgan, S. (2020). El Ciberdelito Costará Al Mundo 10,5 Billones De Dólares Anuales Hasta 2025. *CYBERCRIME MAGAZINE*.

Symantec. (2019). Ransomware dirigido: la proliferación de amenazas amenaza a las organizaciones. *Respuesta de seguridad de Symantec*.

Insights, D. T. (2024). La ciberseguridad como una inversión estratégica. *Resultados de la encuesta Digital Trust Insights https://www.pwc.com/mx/es/liderazgo-estrategico/cfo-inversion-ciberseguridad.html*.

Institute., S. (2019). *The Critical Security Controls for Effective Cyber Defense. https://www.sans.org/critical-security-controls/*.

ISO/IEC, 2. (2016). Information technology — Security techniques — Information security incident management. International Organization for Standardization. *Information technology — Security techniques — Information security incident management. International Organization for Standardization.*

gartner. (2022). gartner. *Security Information and Event Management*.

SO/IEC, 2. (2013). nformation technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization. *nformation technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.*

Schwab, K. (2016). The Fourth Industrial Revolution. World Economic Forum. *The Fourth Industrial Revolution. World Economic Forum*.

Creswell, J. W. (2018). Diseño de investigación: enfoques cualitativos, cuantitativos y de métodos mixtos (5ª ed.). *Diseño de investigación: enfoques cualitativos, cuantitativos y de métodos mixtos (5ª ed.).*

ANEXOS

ANEXO 1 – ENCUESTAS

BIENVENIDOS

Encuesta para Abogados (IHTT)

¡Gracias por participar en esta encuesta del Instituto Hondureño de Transporte Terrestre (IHTT)! Su contribución es vital para ayudarnos a fortalecer la ciberseguridad en nuestra organización. Esta encuesta consta de 12 preguntas y está diseñada para recopilar información sobre el conocimiento, las prácticas y las experiencias relacionadas con la ciberseguridad dentro del IHTT. Sus respuestas serán confidenciales y utilizadas exclusivamente con fines de mejora continua

Estimado Abogados del IHTT, su participación en esta encuesta es crucial para mejorar nuestra estrategia de ciberseguridad. Agradecemos su colaboración.

1. Edad

Seleccione

2. Años de experiencia en el IHTT

Seleccione

3. Nivel de conocimiento sobre ciberseguridad

- ◯ Básico
- ◯ Intermedio
- ◯ Avanzado
- ◯ Ninguno

4. ¿Ha recibido capacitación en manejo seguro de la información en los últimos 12 meses?

- ◯ SÍ
- ◯ NO

5. ¿Qué tipo de capacitación en ciberseguridad ha recibido?

- ◯ Talleres
- ◯ Cursos en línea
- ◯ Conferencias
- ◯ Capacitacion del departamento deTI
- ◯ Ningno

6. ¿Considera que el manejo de la información confidencial en el IHTT es seguro?

- ◯ Totalmente de acuerdo
- ◯ De acuerdo
- ◯ Neutral
- ◯ En desacuerdo
- ◯ Totalmente en desacuerdo

7. ¿Qué medidas se implementan en el IHTT para proteger la información confidencial?

- ☐ Encriptación de datos
- ☐ Control de acceso basado en roles
- ☐ Políticas de seguridad de la información
- ☐ Uso de software de seguridad

1

8. ¿Con qué frecuencia se revisan y actualizan las políticas de seguridad de la información?

- ○ Mensualmente
- ○ Trimestralmente
- ○ Anualmente
- ○ Nunca

9. ¿Ha enfrentado problemas de seguridad de la información en su trabajo?

- ○ SÍ
- ○ NO

10. ¿Qué tipo de problemas de seguridad ha experimentado?

- ☐ Pérdida de datos confidenciales
- ☐ Acceso no autorizado a información
- ☐ Fugas de información
- ☐ Bloque de Accesos
- ☐ Ninguno

11. ¿Cómo evalúa la efectividad de las medidas tomadas para resolver estos problemas?

- ○ Muy efectivas
- ○ Efectivas
- ○ Neutral
- ○ Poco efectivas
- ○ Inefectivas

12. ¿Qué mejoras propondría para fortalecer la seguridad de la información en el IHTT?

- ☐ Implementación de nuevas tecnologías de seguridad
- ☐ Capacitación continua del personal en ciberseguridad
- ☐ Auditorías regulares de seguridad
- ☐ Mejora en las políticas de seguridad de la información
- ☐ Mayor inversión en infraestructura de TI

BIENVENIDOS

Encuesta para INPECTORES (IHTT)

Estimado INPECTORES del IHTT, su participación en esta encuesta es crucial para mejorar nuestra estrategia de ciberseguridad. Agradecemos su colaboración.

¡Gracias por participar en esta encuesta del Instituto Hondureño de Transporte Terrestre (IHTT)! Su contribución es vital para ayudarnos a fortalecer la ciberseguridad en nuestra organización. Esta encuesta consta de 12 preguntas y está diseñada para recopilar información sobre el conocimiento, las prácticas y las experiencias relacionadas con la ciberseguridad dentro del IHTT. Sus respuestas serán confidenciales y utilizadas exclusivamente con fines de mejora continua

1. Edad

Seleccione

2. Años de experiencia en el IHTT

Seleccione

3. Nivel de conocimiento sobre ciberseguridad

- ○ Básico
- ○ Intermedio
- ○ Avanzado

4. ¿Han recibido capacitación en ciberseguridad en los últimos 12 meses?

- ○ SÍ
- ○ NO

5. ¿Qué tipo de capacitación en ciberseguridad ha recibido?

- ☐ Talleres
- ☐ Cursos en línea
- ☐ Conferencias
- ☐ Ninguno

6. ¿Considera que los dispositivos utilizados en campo son seguros?

- ○ Totalmente de acuerdo
- ○ De acuerdo
- ○ Neutral
- ○ En desacuerdo
- ○ Totalmente en desacuerdo

7. ¿Qué herramientas de seguridad se utilizan en el campo?

- ☐ Antivirus
- ☐ Datos encriptados
- ☐ Control de Acceso
- ☐ Ninguno

8. ¿Ha enfrentado problemas de seguridad en su trabajo?

- ○ SÍ
- ○ NO

9. ¿Qué tipo de problemas de seguridad ha experimentado?

- ☐ Pérdida de datos
- ☐ Acceso no autorizado
- ☐ Fallas de Antivirus
- ☐ Ninguno

10. ¿Qué medidas se tomaron para resolverlo?

- ◯ Reemplazo de dispositivos
- ◯ Cambio de contraseñas
- ◯ Actualización de equipo
- ◯ Ninguno

11. ¿Cómo evalúa la efectividad de las medidas tomadas?

- ◯ Muy efectivas
- ◯ Efectivas
- ◯ Neutral
- ◯ Poco efectivas
- ◯ Inefectivas

12. ¿Qué mejoras propondría para fortalecer la seguridad en el campo?

- ☐ Mayor frecuencia de capacitación
- ☐ Mejoras en las herramientas de seguridad
- ☐ Protocolos más estrictos
- ☐ Soporte técnico más accesible

BIENVENIDOS

Encuesta para Operadores de Ventanilla (IHTT)

¡Gracias por participar en esta encuesta del Instituto Hondureño de Transporte Terrestre (IHTT)! Su contribución es vital para ayudarnos a fortalecer la ciberseguridad en nuestra organización. Esta encuesta consta de 12 preguntas y está diseñada para recopilar información sobre el conocimiento, las prácticas y las experiencias relacionadas con la ciberseguridad dentro del IHTT. Sus respuestas serán confidenciales y utilizadas exclusivamente con fines de mejora continua

Estimado Operador de Ventanilla del IHTT, su participación en esta encuesta es crucial para mejorar nuestra estrategia de ciberseguridad. Agradecemos su colaboración.

1.Edad

Seleccione

2. Años de experiencia en el IHTT

Seleccione

3. Nivel de conocimiento sobre ciberseguridad

- ◯ Básico
- ◯ Intermedio
- ◯ Avanzado
- ◯ Ninguno

4. ¿Ha recibido capacitación en ciberseguridad en los últimos 12 meses?

- ◯ SÍ
- ◯ NO

5. ¿Qué tipo de capacitación en ciberseguridad ha recibido?

- ◯ Talleres
- ◯ Cursos en línea
- ◯ Conferencias
- ◯ Ninguno

6. ¿Considera que los sistemas utilizados en ventanilla son seguros?

- ◯ Totalmente de acuerdo
- ◯ De acuerdo
- ◯ Neutral
- ◯ En desacuerdo
- ◯ Totalmente en desacuerdo

7. ¿Qué herramientas de seguridad se utilizan en las ventanillas?

- ☐ Encriptación
- ☐ Firewalls
- ☐ Antivirus
- ☐ Ninguno

8. ¿Con qué frecuencia se actualizan las herramientas de seguridad en su ventanilla?

- ◯ Mensualmente
- ◯ Trimestralmente
- ◯ Anualmente
- ◯ Nunca

9. ¿Ha enfrentado problemas de seguridad en su trabajo?

- ◯ SÍ
- ◯ NO

10. ¿Qué tipo de problemas de seguridad ha experimentado?

- ☐ Pérdida de datos
- ☐ Acceso no autorizado
- ☐ Accesos Bloqueados
- ☐ Ninguno

11. ¿Cómo evalúa la efectividad de las medidas tomadas?

- ◯ Muy efectivas
- ◯ Efectivas
- ◯ Neutral
- ◯ Poco efectivas
- ◯ Inefectivas

12. ¿Qué mejoras propondría para fortalecer la seguridad en las ventanillas del IHTT?

- ☐ Implementación de nuevas tecnologías de seguridad
- ☐ Capacitación continua del personal en ciberseguridad
- ☐ Auditorías regulares de seguridad
- ☐ Mejora en las políticas de seguridad
- ☐ Mayor inversión en infraestructura de TI

BIENVENIDOS

Encuesta para Otros Empleados (IHTT)

¡Gracias por participar en esta encuesta del Instituto Hondureño de Transporte Terrestre (IHTT)! Su contribución es vital para ayudarnos a fortalecer la ciberseguridad en nuestra organización. Esta encuesta consta de 12 preguntas y está diseñada para recopilar información sobre el conocimiento, las prácticas y las experiencias relacionadas con la ciberseguridad dentro del IHTT. Sus respuestas serán confidenciales y utilizadas exclusivamente con fines de mejora continua

Estimado Empleados del IHTT, su participación en esta encuesta es crucial para mejorar nuestra estrategia de ciberseguridad. Agradecemos su colaboración.

1. Edad

Seleccione

2. Años de Experiencia

Seleccione

3. Nivel de conocimiento sobre ciberseguridad:

- ◯ Básico
- ◯ Intermedio
- ◯ Avanzado
- ◯ Ninguno

4. ¿Han recibido capacitación en ciberseguridad en los últimos 12 meses?

- ◯ SI
- ◯ NO

5. ¿Qué tipo de capacitación en ciberseguridad ha recibido?

- ☐ Talleres
- ☐ Cursos en línea
- ☐ Conferencias
- ☐ Ninguna

6. ¿Considera que los sistemas utilizados en su área son seguros?

- ◯ Totalmente de acuerdo
- ◯ De acuerdo
- ◯ Neutral
- ◯ En desacuerdo
- ◯ Totalmente en desacuerdo

7. ¿Qué herramientas de seguridad se utilizan en su área?

- ☐ Encriptación
- ☐ Firewalls
- ☐ Sistemas de detección de intrusos
- ☐ Antivirus
- ☐ Ninguno

8. ¿Con qué frecuencia se actualizan las herramientas de seguridad en su área?

- ◯ Mensualmente
- ◯ Trimestralmente
- ◯ Anualmente
- ◯ Nunca

9. ¿Ha enfrentado problemas de seguridad en su trabajo?

◯ Sí ◯ No

10. ¿Qué tipo de problemas de seguridad ha experimentado?

☐ Pérdida de datos
☐ Acceso no autorizado
☐ Intrusiones de red
☐ Ninguna

11. ¿Cómo evalúa la efectividad de las medidas tomadas?

☐ Muy efectivas
☐ Efectivas
☐ Neutral
☐ Poco efectivas
☐ Inefectivas

12.¿Qué mejoras propondría para fortalecer la ciberseguridad en el IHTT? (Seleccione todas las que apliquen)

☐ Implementación de nuevas tecnologías de seguridad
☐ Capacitación continua del personal en ciberseguridad
☐ Auditorías regulares de seguridad
☐ Mejora en las políticas de seguridad
☐ Mayor inversión en infraestructura de TI

BIENVENIDOS

¡Gracias por participar en esta encuesta del Instituto Hondureño de Transporte Terrestre (IHTT)! Su contribución es vital para ayudarnos a fortalecer la ciberseguridad en nuestra organización. Esta encuesta consta de 12 preguntas y está diseñada para recopilar información sobre el conocimiento, las prácticas y las experiencias relacionadas con la ciberseguridad dentro del IHTT. Sus respuestas serán confidenciales y utilizadas exclusivamente con fines de mejora continua

Encuesta para Técnicos de TI (IHTT)

Estimado Técnico de TI del IHTT, su participación en esta encuesta es crucial para mejorar nuestra estrategia de ciberseguridad. Agradecemos su colaboración.

1. Rango de Edad

Seleccione

2. Años de Experiencia

Seleccione

3. Nivel de conocimiento sobre ciberseguridad:

◯ Básico ◯ Intermedio ◯ Avanzado
◯ Ninguno

4. ¿Han recibido capacitación en ciberseguridad en los últimos 12 meses?

◯ SI ◯ NO

5. ¿Qué tipo de capacitación en ciberseguridad ha recibido?

☐ Talleres ☐ Cursos en línea
☐ Conferencias ☐ Ninguna

6. ¿Considera que el IHTT cuenta con una infraestructura de TI adecuada para prevenir ciberataques?

◯ Totalmente de acuerdo ◯ De acuerdo
◯ Neutral ◯ En desacuerdo
◯ Totalmente en desacuerdo

7. ¿Qué tipo de herramientas de ciberseguridad utiliza regularmente en su trabajo?

☐ Firewalls ☐ Antivirus
☐ Sistemas de detección de intrusos ☐ Ninguno

8. ¿Con qué frecuencia se actualizan las herramientas de ciberseguridad?

◯ Mensualmente ◯ Trimestralmente
◯ Anualmente ◯ Nunca

9. ¿Ha participado en la gestión de algún incidente de ciberseguridad en el IHTT?

◯ Sí ◯ No

10. ¿Qué tipo de incidentes de seguridad ha manejado?

☐ Malware
☐ Phishing
☐ Intrusiones de red
☐ Ninguna

11. ¿Cómo evalúa la efectividad de las medidas tomadas?

☐ Muy efectivas
☐ Efectivas
☐ Neutral
☐ Poco efectivas
☐ Inefectivas

12.¿Qué mejoras propondría para fortalecer la ciberseguridad en el IHTT? (Seleccione todas las que apliquen)

☐ Implementar más capacitación en ciberseguridad para todo el personal.
☐ Actualizar y mejorar las herramientas de seguridad informática.
☐ Establecer políticas de seguridad más estrictas y procedimientos de control de acceso.
☐ Incrementar la frecuencia de auditorías de seguridad.
☐ Mejorar la infraestructura de TI, incluyendo la adquisición de hardware y software más robustos.

~~2~~

ANEXO 2 – TABULACIONES DE LAS ENCUESTAS

Tabulación de datos de la encuesta de abogados

Tabla 7 - Tabulación de datos de la encuesta de abogados

1. Edad	2. Años de experiencia en el IHTT	3. Nivel de conocimiento sobre ciberseguridad	4. ¿Ha recibido capacitación en manejo seguro de la información en los últimos 12 meses?	5. ¿Qué tipo de capacitación en ciberseguridad ha recibido?	6. ¿Considera que el manejo de la información confidencial en el IHTT es seguro?	7. ¿Qué medidas se implementan en el IHTT para proteger la información confidencial?	8. ¿Con qué frecuencia se revisan y actualizan las políticas de seguridad de la información?	9. ¿Ha enfrentado problemas de seguridad de la información en su trabajo?	10. ¿Qué tipo de problemas de seguridad ha experimentado?	11. ¿Cómo evalúa la efectividad de las medidas tomadas para resolver estos problemas?	12. ¿Qué mejoras propondría para fortalecer la seguridad de la información en el IHTT?
51 o más	1-3 años	Ninguno	NO	Ningno	De acuerdo	Control de acceso basado en roles	Nunca	NO	Ninguno	Neutral	Implementación de nuevas tecnologías de seguridad - Auditorías regulares de seguridad - Mayor inversión en infraestructura de TI
31-40	4-6 años	Ninguno	NO	Ningno	Neutral	Control de acceso basado en roles	Nunca	NO	Ninguno	Neutral	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad
41-50	Menos de 1 año	Básico	SÍ	Talleres	De acuerdo	Control de acceso basado en roles	Nunca	SÍ	Pérdida de datos confidenciales	Neutral	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad - Mejora en las políticas de seguridad de la información - Mayor inversión en infraestructura de TI
31-40	1-3 años	Ninguno	NO	Ningno		Control de acceso basado en roles	Nunca	NO	Ninguno	Efectivas	Mayor inversión en infraestructura de TI
51 o más	1-3 años	Ninguno	NO	Ningno	En desacuerdo	Control de acceso basado en roles	Nunca	SÍ	Acceso no autorizado a información	Neutral	Mayor inversión en infraestructura de TI
41-50	1-3 años	Básico	NO	Ningno	Neutral	Control de acceso basado en roles	Nunca	SÍ	Bloque de Accesos	Neutral	Implementación de nuevas tecnologías de seguridad
51 o más	Más de 6 años	Ninguno	NO	Ningno	Neutral	Control de acceso basado en roles	Nunca	SÍ	Acceso no autorizado a información	Poco efectivas	Implementación de nuevas tecnologías de seguridad
21-30	1-3 años	Ninguno	NO	Ningno	En desacuerdo	Control de acceso basado en roles	Nunca	NO	Ninguno	Poco efectivas	Implementación de nuevas tecnologías de seguridad
21-30	1-3 años	Básico	SÍ	Capacitacion del departamento deTI	Neutral	Control de acceso basado en roles - Políticas de seguridad de la información	Anualmente	SÍ	Fugas de información - Bloque de Accesos	Neutral	Implementación de nuevas tecnologías de seguridad - Auditorías regulares de seguridad - Mejora en las políticas de seguridad de la información
41-50	4-6 años	Básico	NO		Neutral	Control de acceso basado en roles	Nunca	NO	Ninguno	Poco efectivas	Implementación de nuevas tecnologías de seguridad
31-40	Más de 6 años	Básico	NO	Capacitacion del departamento deTI	Neutral	Control de acceso basado en roles - Políticas de seguridad de la información	Anualmente	SÍ	Fugas de información - Bloque de Accesos	Muy efectivas	Implementación de nuevas tecnologías de seguridad
41-50	Más de 6 años	Intermedio	NO		Neutral	Encriptación de datos - Control de acceso basado en roles	Anualmente	SÍ	Ninguno	Efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad
21-30	1-3 años	Básico	NO		Totalmente en desacuerdo			NO	Ninguno	Neutral	Mayor inversión en infraestructura de TI
41-50	4-6 años	Básico	NO		Neutral	Políticas de seguridad de la información		NO	Ninguno	Neutral	Implementación de nuevas tecnologías de seguridad
31-40	Más de 6 años	Básico	NO		En desacuerdo		Nunca	NO	Ninguno	Neutral	Mejora en las políticas de seguridad de la información

Fuente: Elaboración Propia.

Tabulación de datos de la encuesta de Inspectores de campo

Tabla 8 - Tabulación de datos de la encuesta de Inspectores de campo

1. Edad	2. Años de experiencia en el IHTT	3. Nivel de conocimiento sobre ciberseguridad	4. ¿Han recibido capacitación en ciberseguridad en los últimos 12 meses?	5. ¿Qué tipo de capacitación en ciberseguridad ha recibido?	6. ¿Considera que los dispositivos utilizados en campo son seguros?	7. ¿Qué herramientas de seguridad se utilizan en el campo?	8. ¿Ha enfrentado problemas de seguridad en su trabajo?	9. ¿Qué tipo de problemas de seguridad ha experimentado?	10. ¿Qué medidas se tomaron para resolverlo?	11. ¿Cómo evalúa la efectividad de las medidas tomadas?	12. ¿Qué mejoras propondría para fortalecer la seguridad en el campo?
18-25	0-2 años	Intermedio	SÍ	Cursos en línea	De acuerdo	Antivirus	SÍ	Acceso no autorizado	Reemplazo de dispositivos	Efectivas	Mejoras en las herramientas de seguridad
56 o más	0-2 años	Básico	NO	Ninguno	De acuerdo	Datos encriptados - Control de Acceso	NO	Ninguno	Cambio de contraseñas	Neutral	Mayor frecuencia de capacitación - Mejoras en las herramientas de seguridad - Protocolos más estrictos - Soporte técnico más accesible
36-45	0-2 años	Básico	SÍ	Talleres	Neutral	Antivirus	SÍ	Pérdida de datos - Fallas de Antivirus	Reemplazo de dispositivos	Poco efectivas	Mayor frecuencia de capacitación - Soporte técnico más accesible
36-45	6-10 años	Básico	NO	Ninguno	Neutral	Control de Acceso	SÍ	Fallas de Antivirus	Actualización de equipo	Poco efectivas	Mejoras en las herramientas de seguridad
26-35	0-2 años	Básico	NO	Ninguno	Neutral	Antivirus - Control de Acceso	SÍ	Pérdida de datos	Reemplazo de dispositivos	Neutral	Mayor frecuencia de capacitación - Soporte técnico más accesible
26-35	0-2 años	Básico	NO	Ninguno	De acuerdo	Control de Acceso	SÍ	Pérdida de datos - Acceso no autorizado	Reemplazo de dispositivos	Efectivas	Mayor frecuencia de capacitación - Mejoras en las herramientas de seguridad - Protocolos más estrictos - Soporte técnico más accesible
46-55	0-2 años	Básico	SÍ	Talleres	Neutral	Antivirus - Control de Acceso	SÍ	Pérdida de datos - Acceso no autorizado	Reemplazo de dispositivos	Neutral	Mayor frecuencia de capacitación - Soporte técnico más accesible
18-25	0-2 años	Básico	SÍ	Cursos en línea	Totalmente de acuerdo	Control de Acceso	SÍ	Pérdida de datos - Acceso no autorizado	Cambio de contraseñas	Muy efectivas	Mejoras en las herramientas de seguridad
36-45	6-10 años	Básico	NO	Ninguno	Neutral	Control de Acceso	NO	Ninguno	Cambio de contraseñas	Neutral	Mayor frecuencia de capacitación - Mejoras en las herramientas de seguridad - Protocolos más estrictos
26-35	3-5 años	Básico	NO	Ninguno	De acuerdo	Antivirus	SÍ	Pérdida de datos - Acceso no autorizado	Cambio de contraseñas	Efectivas	Mejoras en las herramientas de seguridad
46-55	0-2 años	Básico		Ninguno	Neutral		SÍ	Pérdida de datos	Reemplazo de dispositivos	Neutral	Mayor frecuencia de capacitación
26-35	3-5 años	Básico	SÍ	Talleres	Neutral	Antivirus - Datos encriptados - Control de Acceso	SÍ	Pérdida de datos - Acceso no autorizado - Fallas de Antivirus	Actualización de equipo	Efectivas	Mayor frecuencia de capacitación - Mejoras en las herramientas de seguridad - Protocolos más estrictos - Soporte técnico más accesible
36-45	0-2 años	Básico	NO	Ninguno	Neutral	Antivirus - Control de Acceso	SÍ	Pérdida de datos	Reemplazo de dispositivos	Neutral	Mayor frecuencia de capacitación - Mejoras en las herramientas de seguridad - Soporte técnico más accesible
26-35	0-2 años	Básico	NO	Ninguno	Neutral	Antivirus	SÍ	Pérdida de datos	Reemplazo de dispositivos	Neutral	Mayor frecuencia de capacitación - Soporte técnico más accesible
18-25	0-2 años	Básico	NO	Ninguno	De acuerdo	Antivirus - Control de Acceso	SÍ	Pérdida de datos - Acceso no autorizado	Cambio de contraseñas	Efectivas	Mayor frecuencia de capacitación - Mejoras en las herramientas de seguridad - Protocolos más estrictos - Soporte técnico más accesible
26-35	3-5 años	Básico	NO	Ninguno	De acuerdo	Antivirus	SÍ	Acceso no autorizado	Cambio de contraseñas	Efectivas	Mejoras en las herramientas de seguridad
18-25	0-2 años	Básico	NO	Ninguno	Neutral	Ninguno	SÍ	Pérdida de dispositivos - Acceso no autorizado	Cambio de contraseñas	Efectivas	Mayor frecuencia de capacitación - Mejoras en las herramientas de seguridad - Protocolos más estrictos - Soporte técnico más accesible

Fuente: Elaboración Propia.

Tabulación de datos de la encuesta de Operadores de Ventanilla

1.Edad	2. Años de experiencia en el IHTT	3. Nivel de conocimiento sobre ciberseguridad	4. ¿Ha recibido capacitación en ciberseguridad en los últimos 12 meses?	5. ¿Qué tipo de capacitación en ciberseguridad ha recibido?	6. ¿Considera que los sistemas utilizados en ventanilla son seguros?	7. ¿Qué herramientas de seguridad se utilizan en las ventanillas?	8. ¿Con qué frecuencia se actualizan las herramientas de seguridad en su ventanilla?	9. ¿Ha enfrentado problemas de seguridad en su trabajo?	10. ¿Qué tipo de problemas de seguridad ha experimentado?	11. ¿Cómo evalúa la efectividad de las medidas tomadas?	12. ¿Qué mejoras propondría para fortalecer la seguridad en las ventanillas del IHTT?
26-35	6-10 años	Ninguno	NO	Conferencias	Neutral	Firewalls - Antivirus	Anualmente	SÍ	Pérdida de datos - Acceso no autorizado - Accesos Bloqueados	Neutral	Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad - Mejora en las políticas de seguridad - Mayor inversión en infraestructura de TI
46-55	3-5 años	Ninguno	NO	Ninguno	Neutral	Antivirus	Nunca	SÍ	Acceso no autorizado	Efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad
56 o más	Más de 10 años	Ninguno	SÍ	Conferencias	De acuerdo	Firewalls	Anualmente	SÍ	Pérdida de datos	Neutral	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad
36-45	3-5 años	Básico	NO	Ninguno	En desacuerdo	Antivirus	Anualmente	SÍ	Pérdida de datos - Accesos Bloqueados	Neutral	Implementación de nuevas tecnologías de seguridad - Mayor inversión en infraestructura de TI
36-45	0-2 años	Básico	SÍ	Cursos en línea	De acuerdo	Firewalls - Antivirus	Nunca	SÍ	Pérdida de datos	Efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad - Mejora en las políticas de seguridad - Mayor inversión en infraestructura de TI
36-45	6-10 años	Ninguno	NO	Ninguno	Neutral	Antivirus	Anualmente	SÍ	Pérdida de datos	Neutral	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad
18-25	0-2 años	Ninguno	NO	Ninguno	Neutral	Firewalls - Antivirus	Anualmente	SÍ	Pérdida de datos - Acceso no autorizado	Efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Mejora en las políticas de seguridad
18-25	3-5 años	Ninguno	NO	Ninguno	De acuerdo	Antivirus	Nunca	SÍ	Accesos Bloqueados	Efectivas	Implementación de nuevas tecnologías de seguridad - Auditorías regulares de seguridad - Mejora en las políticas de seguridad

Tabla 9 - Tabulación de datos de la encuesta de Operadores de Ventanilla

Fuente: Elaboración Propia.

Tabulación de datos de la encuesta de Otros Empleados del IHTT

Tabla 10 - Tabulación de datos de la encuesta de Otros Empleados del IHTT

1. Edad	2. Años de Experiencia	3. Nivel de conocimiento sobre ciberseguridad:	4. ¿Han recibido capacitación en ciberseguridad en los últimos 12 meses?	5. ¿Qué tipo de capacitación en ciberseguridad ha recibido?	6. ¿Considera que los sistemas utilizados en su área son seguros?	7. ¿Qué herramientas de seguridad se utilizan en su área?	8. ¿Con qué frecuencia se actualizan las herramientas de seguridad en su área?	9. ¿Ha enfrentado problemas de seguridad en su trabajo?	10. ¿Qué tipo de problemas de seguridad ha experimentado?	11. ¿Cómo evalúa la efectividad de las medidas tomadas?	12.¿Qué mejoras propondría para fortalecer la ciberseguridad en el IHTT? (Seleccione todas las que apliquen)
31-40	3-5	Básico	NO	Ninguna	Neutral	Firewalls - Antivirus	Nunca	Sí	Ninguna	Muy efectivas	Implementación de nuevas tecnologías de seguridad - Mejora en las políticas de seguridad - Mayor inversión en infraestructura de TI
41-50	3-5	Ninguno	NO	Ninguna	De acuerdo	Antivirus	Mensualmente	Sí	Intrusiones de red	Efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad - Mejora en las políticas de seguridad - Mayor inversión en infraestructura de TI
41-50	6-10	Básico	SI	Conferencias	Neutral	Firewalls - Antivirus	Anualmente	Sí	Pérdida de datos - Acceso no autorizado	Neutral	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad
21-30	3-5	Ninguno	NO	Ninguna	De acuerdo	Firewalls - Antivirus	Anualmente	Sí	Intrusiones de red	Efectivas	Auditorías regulares de seguridad - Mejora en las políticas de seguridad
51 o más	3-5	Ninguno	NO	Ninguna	De acuerdo	Antivirus	Mensualmente	Sí	Pérdida de datos - Acceso no autorizado	Efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad - Mejora en las políticas de seguridad
31-40	6-10	Básico	NO	Cursos en línea - Conferencias	En desacuerdo	Antivirus	Anualmente	Sí	Pérdida de datos	Neutral	Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad - Mejora en las políticas de seguridad
31-40	6-10	Intermedio	SI	Cursos en línea	Totalmente de acuerdo	Firewalls - Antivirus	Anualmente	Sí	Intrusiones de red	Muy efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad
31-40	3-5	Básico	NO	Ninguna	Neutral	Antivirus	Nunca	Sí	Pérdida de datos	Efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad - Mejora en las políticas de seguridad - Mayor inversión en infraestructura de TI
31-40	3-5	Básico	NO	Ninguna	Neutral	Antivirus	Anualmente	Sí	Pérdida de datos	Neutral	Implementación de nuevas tecnologías de seguridad
21-30	0-2	Básico	SI	Cursos en línea	Neutral	Firewalls - Antivirus	Mensualmente	Sí	Intrusiones de red	Neutral	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad
51 o más	0-2	Ninguno	NO	Ninguna	Neutral	Antivirus	Nunca	No	Ninguna	Neutral	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Mejora en las políticas de seguridad - Mayor inversión en infraestructura de TI
51 o más	6-10	Ninguno	NO	Ninguna	Neutral	Antivirus	Mensualmente	Sí	Pérdida de datos - Acceso no autorizado - Intrusiones de red	Efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Mayor inversión en infraestructura de TI
21-30	0-2	Ninguno	NO	Ninguna	Neutral	Antivirus	Nunca	Sí	Intrusiones de red	Neutral	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Mejora en las políticas de seguridad
41-50	3-5	Ninguno	NO	Ninguna	Neutral	Antivirus	Nunca	No	Ninguna	Neutral	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Mayor inversión en infraestructura de TI
31-40	3-5	Intermedio	SI	Cursos en línea	De acuerdo	Firewalls - Antivirus	Anualmente	Sí	Pérdida de datos	Muy efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad
31-40	3-5	Ninguno	NO	Ninguna	Neutral	Antivirus	Nunca	Sí	Acceso no autorizado	Efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad - Mejora en las políticas de seguridad - Mayor inversión en infraestructura de TI
51 o más	3-5	Ninguno	NO	Ninguna	De acuerdo	Antivirus	Nunca	Sí	Acceso no autorizado	Neutral	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad
41-50	3-5	Ninguno	NO	Ninguna	Neutral	Antivirus	Nunca	Sí	Intrusiones de red	Efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad
31-40	0-2	Ninguno	NO	Ninguna	Neutral	Antivirus	Anualmente	Sí	Pérdida de datos	Muy efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad
31-40	0-2	Ninguno	NO	Ninguna	Neutral	Antivirus	Anualmente	Sí	Pérdida de datos	Muy efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad
21-30	0-2	Básico	SI	Cursos en línea	De acuerdo	Firewalls - Antivirus	Anualmente	Sí	Pérdida de datos	Muy efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad
21-30	0-2	Ninguno	SI	Talleres - Cursos en línea	De acuerdo	Firewalls - Antivirus	Mensualmente	Sí	Pérdida de datos - Acceso no autorizado - Intrusiones de red	Muy efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad - Mejora en las políticas de seguridad - Mayor inversión en infraestructura de TI
31-40	6-10	Avanzado	SI	Talleres - Cursos en línea - Conferencias	Totalmente de acuerdo	Encriptación - Firewalls - Sistemas de detección de intrusos - Antivirus	Mensualmente		Pérdida de datos - Acceso no autorizado - Intrusiones de red	Muy efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad - Mayor inversión en infraestructura de TI
31-40	0-2	Ninguno	NO	Ninguna	Neutral	Antivirus	Anualmente	Sí	Pérdida de datos	Efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Mayor inversión en infraestructura de TI
21-30	0-2	Ninguno	NO	Ninguna	Neutral	Ninguno	Nunca	No	Ninguna	Neutral	Mayor inversión en infraestructura de TI
41-50	10 o mas	Intermedio	SI	Talleres	Totalmente de acuerdo	Encriptación - Firewalls - Antivirus	Mensualmente	Sí		Efectivas	Capacitación continua del personal en ciberseguridad - Mayor inversión en infraestructura de TI
21-30	3-5	Ninguno	NO	Ninguna	Neutral	Antivirus	Nunca	No	Ninguna	Efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad
31-40	10 o mas	Avanzado	SI	Talleres - Cursos en línea - Conferencias	Totalmente de acuerdo		Mensualmente	Sí		Muy efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Mejora en las políticas de seguridad - Mayor inversión en infraestructura de TI
21-30	3-5	Básico	SI	Talleres	Totalmente de acuerdo	Encriptación - Firewalls - Sistemas de detección de intrusos - Antivirus	Mensualmente	Sí	Pérdida de datos - Acceso no autorizado - Intrusiones de red	Muy efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad - Mejora en las políticas de seguridad - Mayor inversión en infraestructura de TI
51 o más	6-10	Básico	NO	Ninguna	De acuerdo	Antivirus	Anualmente	Sí	Acceso no autorizado - Intrusiones de red	Poco efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad - Mejora en las políticas de seguridad - Mayor inversión en infraestructura de TI
31-40	3-5	Básico	NO	Ninguna	De acuerdo	Encriptación - Firewalls - Sistemas de detección de intrusos - Antivirus	Mensualmente	Sí	Pérdida de datos - Acceso no autorizado - Intrusiones de red	Efectivas	Implementación de nuevas tecnologías de seguridad - Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad - Mejora en las políticas de seguridad - Mayor inversión en infraestructura de TI
31-40	6-10	Ninguno	NO	Ninguna	Neutral	Antivirus	Anualmente	Sí	Pérdida de datos	Neutral	Capacitación continua del personal en ciberseguridad - Auditorías regulares de seguridad

Fuente: Elaboración Propia.

Tabulación de datos de la encuesta de Tecnicos TI del IHTT

Tabla 11 - Tabulación de datos de la encuesta de Técnicos TI del IHTT

1. Edad	2. Años de Experiencia	3. Nivel de conocimiento sobre ciberseguridad:	4. ¿Han recibido capacitación en ciberseguridad en los últimos 12 meses?	5. ¿Qué tipo de capacitación en ciberseguridad ha recibido?	6. ¿Considera que el IHTT cuenta con una infraestructura de TI adecuada para prevenir ciberataques?	7. ¿Qué tipo de herramientas de ciberseguridad utiliza regularmente en su trabajo?	8. ¿Con qué frecuencia se actualizan las herramientas de ciberseguridad?	9. ¿Ha participado en la gestión de algún incidente de ciberseguridad en el IHTT?	10. ¿Qué tipo de incidentes de seguridad ha manejado?	11. ¿Cómo evalúa la efectividad de las medidas tomadas?	12.¿Qué mejoras propondría para fortalecer la ciberseguridad en el IHTT? (Seleccione todas las que apliquen)
21-30	6-10	Intermedio	NO	Ninguna	En desacuerdo	Firewalls	Anualmente	No	Ninguna	Neutral	Implementar más capacitación en ciberseguridad para todo el personal. - Actualizar y mejorar las herramientas de seguridad informática. - Establecer políticas de seguridad más estrictas y procedimientos de control de acceso. - Incrementar la frecuencia de auditorías de seguridad. - Mejorar la infraestructura de TI, incluyendo la adquisición de hardware y software más robustos.
31-40	10 o mas	Intermedio	SI	Talleres - Cursos en línea	De acuerdo	Firewalls - Antivirus	Mensualmente	Sí	Malware	Efectivas	Implementar más capacitación en ciberseguridad para todo el personal. - Actualizar y mejorar las herramientas de seguridad informática. - Establecer políticas de seguridad más estrictas y procedimientos de control de acceso. - Incrementar la frecuencia de auditorías de seguridad. - Mejorar la infraestructura de TI, incluyendo la adquisición de hardware y software más robustos.
21-30	3-5	Intermedio	NO	Ninguna	Totalmente en desacuerdo	Firewalls	Nunca	Sí	Malware	Neutral	Establecer políticas de seguridad más estrictas y procedimientos de control de acceso.
41-50	10 o mas	Básico	NO	Talleres	En desacuerdo	Firewalls - Antivirus	Mensualmente	No	Malware - Intrusiones de red	Efectivas	Implementar más capacitación en ciberseguridad para todo el personal. - Actualizar y mejorar las herramientas de seguridad informática. - Mejorar la infraestructura de TI, incluyendo la adquisición de hardware y software más robustos.
21-30	0-2	Básico	SI	Cursos en línea	Neutral	Firewalls - Antivirus	Mensualmente	No	Ninguna	Efectivas	Implementar más capacitación en ciberseguridad para todo el personal. - Establecer políticas de seguridad más estrictas y procedimientos de control de acceso. - Mejorar la infraestructura de TI, incluyendo la adquisición de hardware y software más robustos.
31-40	6-10	Intermedio	SI	Talleres - Cursos en línea	Neutral	Firewalls - Antivirus	Nunca	Sí	Malware - Phishing - Intrusiones de red	Efectivas	Implementar más capacitación en ciberseguridad para todo el personal. - Actualizar y mejorar las herramientas de seguridad informática. - Establecer políticas de seguridad más estrictas y procedimientos de control de acceso. - Incrementar la frecuencia de auditorías de seguridad. - Mejorar la infraestructura de TI, incluyendo la adquisición de hardware y software más robustos.
21-30	6-10	Básico	NO	Conferencias	Totalmente en desacuerdo	Antivirus	Mensualmente	Sí	Intrusiones de red	Neutral	Implementar más capacitación en ciberseguridad para todo el personal. - Actualizar y mejorar las herramientas de seguridad informática. - Establecer políticas de seguridad más estrictas y procedimientos de control de acceso. - Incrementar la frecuencia de auditorías de seguridad. - Mejorar la infraestructura de TI, incluyendo la adquisición de hardware y software más robustos.
21-30	6-10	Básico	NO	Ninguna	Totalmente en desacuerdo	Antivirus	Mensualmente	Sí	Malware - Intrusiones de red	Neutral	Implementar más capacitación en ciberseguridad para todo el personal. - Actualizar y mejorar las herramientas de seguridad informática. - Establecer políticas de seguridad más estrictas y procedimientos de control de acceso. - Incrementar la frecuencia de auditorías de seguridad. - Mejorar la infraestructura de TI, incluyendo la adquisición de hardware y software más robustos.
21-30	0-2	Básico	NO	Ninguna	En desacuerdo	Antivirus	Nunca	No	Ninguna	Neutral	Implementar más capacitación en ciberseguridad para todo el personal. - Actualizar y mejorar las herramientas de seguridad informática. - Establecer políticas de seguridad más estrictas y procedimientos de control de acceso. - Incrementar la frecuencia de auditorías de seguridad. - Mejorar la infraestructura de TI, incluyendo la adquisición de hardware y software más robustos.
21-30	3-5	Intermedio	SI	Talleres - Cursos en línea	Neutral	Firewalls - Antivirus	Anualmente	Sí	Malware - Phishing	Efectivas	Implementar más capacitación en ciberseguridad para todo el personal. - Actualizar y mejorar las herramientas de seguridad informática. - Establecer políticas de seguridad más estrictas y procedimientos de control de acceso. - Incrementar la frecuencia de auditorías de seguridad. - Mejorar la infraestructura de TI, incluyendo la adquisición de hardware y software más robustos.
31-40	10 o mas	Intermedio	NO	Cursos en línea	Neutral	Firewalls - Antivirus	Mensualmente	Sí	Phishing	Efectivas	Implementar más capacitación en ciberseguridad para todo el personal. - Actualizar y mejorar las herramientas de seguridad informática. - Establecer políticas de seguridad más estrictas y procedimientos de control de acceso. - Incrementar la frecuencia de auditorías de seguridad.
51-60	10 o mas	Intermedio	NO	Cursos en línea - Conferencias	En desacuerdo	Firewalls - Antivirus	Anualmente	Sí	Malware - Phishing - Intrusiones de red	Muy efectivas	Implementar más capacitación en ciberseguridad para todo el personal. - Actualizar y mejorar las herramientas de seguridad informática. - Establecer políticas de seguridad más estrictas y procedimientos de control de acceso. - Incrementar la frecuencia de auditorías de seguridad. - Mejorar la infraestructura de TI, incluyendo la adquisición de hardware y software más robustos.
31-40	6-10	Básico	NO	Ninguna	Neutral	Firewalls - Antivirus	Anualmente	Sí	Intrusiones de red	Neutral	Implementar más capacitación en ciberseguridad para todo el personal. - Actualizar y mejorar las herramientas de seguridad informática. - Establecer políticas de seguridad más estrictas y procedimientos de control de acceso. - Incrementar la frecuencia de auditorías de seguridad. - Mejorar la infraestructura de TI, incluyendo la adquisición de hardware y software más robustos.
31-40	10 o mas	Básico	SI	Talleres - Cursos en línea	De acuerdo	Firewalls - Antivirus	Mensualmente	Sí	Malware	Efectivas	Implementar más capacitación en ciberseguridad para todo el personal. - Actualizar y mejorar las herramientas de seguridad informática. - Establecer políticas de seguridad más estrictas y procedimientos de control de acceso. - Incrementar la frecuencia de auditorías de seguridad. - Mejorar la infraestructura de TI, incluyendo la adquisición de hardware y software más robustos.
31-40	6-10	Intermedio	NO	Ninguna	Totalmente de acuerdo	Firewalls - Antivirus	Anualmente	Sí	Phishing - Intrusiones de red	Muy efectivas	Implementar más capacitación en ciberseguridad para todo el personal. - Incrementar la frecuencia de auditorías de seguridad.

Fuente: Elaboración Propia.

ANEXO 3 – CAPTURAS

Capturas de las herramientas utilizadas, y muestra la evidencia de los documentos recolectados.

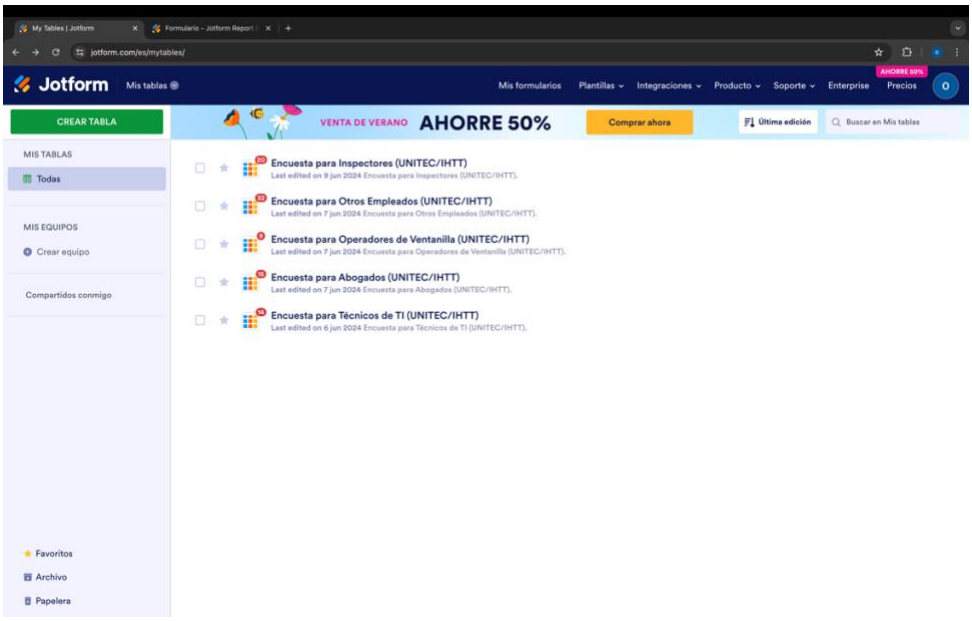

Figura 62 - Referencia 1 Herramienta Utilizada

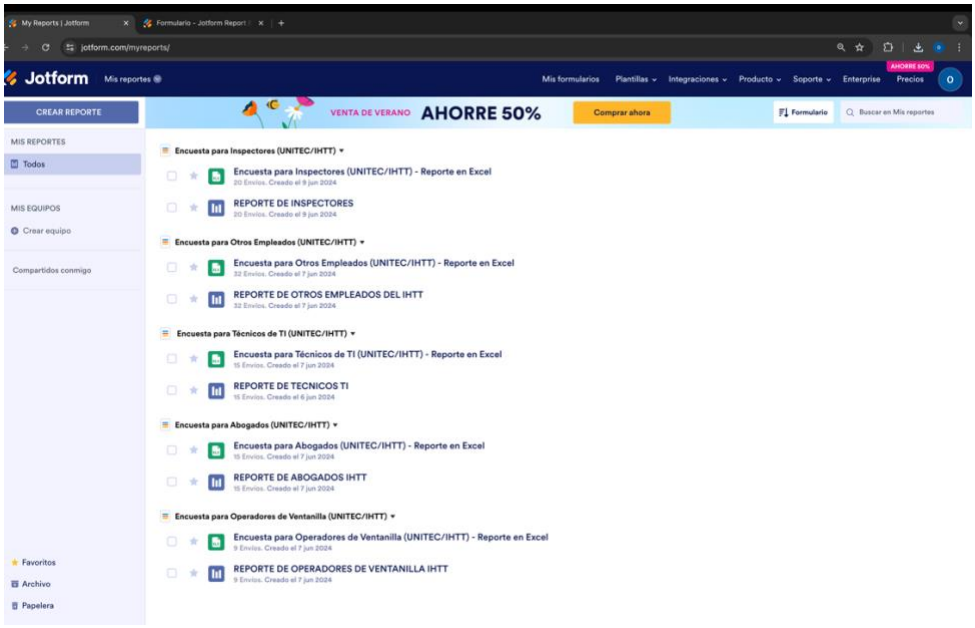

Figura 63 - Referencia 2 Herramienta Utilizada

ANEXO 4 – ESPECIFICACIONES TÉCNICAS

INTRODUCCIÓN

El Instituto Hondureño de Transporte Terrestre (IHTT) se encuentra en un proceso de modernización y optimización de su infraestructura tecnológica con el objetivo de garantizar la continuidad operativa, la seguridad de la información y la eficiencia en sus servicios. Para lograr esto, se ha identificado la necesidad de implementar soluciones avanzadas en la nube que permitan una gestión flexible y escalable de los recursos tecnológicos, así como la integración de nuevos sistemas que faciliten la operación diaria y la respuesta ante emergencias. Este documento describe los términos de referencia (TDR) para la adquisición de diversos servicios y equipos tecnológicos necesarios para fortalecer la infraestructura del IHTT.

OBJETIVOS

- Garantizar la Continuidad del Servicio: Implementar soluciones tecnológicas que aseguren la operación ininterrumpida de los sistemas del IHTT, permitiendo una recuperación rápida ante cualquier falla.
- Mejorar la Seguridad de la Información: Adquirir servicios y equipos que proporcionen altos niveles de seguridad, protegiendo los datos sensibles contra ataques cibernéticos y accesos no autorizados.
- Aumentar la Eficiencia Operativa: Introducir tecnologías que optimicen el rendimiento de las aplicaciones y servicios del IHTT, facilitando la gestión y el monitoreo de los recursos tecnológicos.
- Facilitar la Escalabilidad: Implementar soluciones que permitan el crecimiento y la adaptación de la infraestructura tecnológica del IHTT conforme a las necesidades futuras.
- Promover la Autosuficiencia Institucional: Capacitar al personal del IHTT en el manejo y administración de las nuevas tecnologías, asegurando una gestión eficiente y autónoma de los recursos tecnológicos.

RESUMEN DE LOTES QUE SOLICITAR

1. **Servicios en la Nube:**

Servidor en la Nube (ECS): Confiabilidad y recuperación automática de fallos, implementación de seguridad avanzada (VPC, WAF, VSS, anti-DDoS), escalabilidad y facilidad de uso, alto rendimiento con especificaciones robustas. Volumen Elástico (EVS): Almacenamiento persistente y escalable, soporte para altas demandas de I/O y baja latencia, alta disponibilidad y durabilidad. IP Elástica (EIP): Direcciones IP públicas estáticas, conexiones flexibles y de alta disponibilidad, facturación basada en el uso real.

Red Privada Virtual (VPC): Creación de redes privadas y aisladas, seguridad y control avanzados, configuración flexible y autónoma. Backup y Recuperación en la Nube (CBR): Respaldo y recuperación rápida de datos, protección multi-región y recursos múltiples, seguridad y fiabilidad en el almacenamiento de datos.

2. **Firewall y Dispositivos de Comunicación de Redes:**

Protección de servicios web mediante Firewall de Aplicaciones Web (WAF), detección y bloqueo de ataques comunes y sofisticados, alta seguridad y fiabilidad con detección dual (reglas + AI), prevención dinámica de crawlers, verificación precisa IP+cookie, implementación de reglas ACLs entre subnets, Nat Gateway, VPN, anti-DDoS, grupos de seguridad, tecnologías de aprendizaje automático y big data, agentes instaladores para protección contra vulnerabilidades y ataques.

3. **Gestor Documental:**

Escaneo y digitalización de documentos, almacenamiento e indexación para consulta rápida, administración centralizada, escalabilidad de aplicación, licenciamiento para usuarios y de solo lectura, integración con aplicaciones existentes, autosuficiencia institucional, flujos de trabajo, visualización móvil y web, migración de archivos del gestor anterior.

4. **Servidores Físicos:**

Plataforma tecnológica de tres servidores con alta disponibilidad, soporta arquitecturas de procesamiento x86 a 64 bits, componentes originales y de última generación, software de administración y monitoreo, licenciamiento de VMware y Windows Server, configuración de hardware robusta con redundancia y alta capacidad de memoria y almacenamiento, garantía y

soporte 24/7.

5. **Laptops y Computadoras de Escritorio:**

Laptops: Memoria RAM mínima de 32 GB, procesador mínimo i9, disco duro sólido de mínimo 1024 GB, teclado numérico incluido, tarjeta gráfica de media alta gama, mochila con accesorios básicos.

PC de Escritorio: Capacidad mínima de 1024 GB, memoria RAM mínima de 16 GB, Wifi, pantalla retroiluminada por LED mayor de 22 pulgadas con tecnología IPS, resolución de 2048 por 1536 píxeles, chip A8X con arquitectura de 64 bits, tecnología Bluetooth 4.2, Wi-Fi (802.11a/b/g/n/ac).

TÉRMINOS DE REFERENCIA POR LOTE

LOTE #1 - SERVICIOS NUBE

1. **Servicios de Servidor en la Nube (ECS)**

Objetivo: Proporcionar un servicio de servidor en la nube que garantice operaciones seguras, flexibles y eficientes, asegurando la continuidad y estabilidad del servicio.

Características Requeridas:

- Confiabilidad: Recuperación automática de fallos, copias de seguridad múltiples.
- Seguridad: Implementación de VPC, WAF, VSS, y protección anti-DDoS.
- Escalabilidad: Capacidad de escalar hacia arriba/abajo y hacia adentro/afuera con políticas AS flexibles.
- Facilidad de Uso: Consola de gestión unificada, APIs y SDKs para un mantenimiento y operación simplificados.
- Alto Rendimiento: Hasta 60 vCPUs y 4 TB de memoria, con más especificaciones próximamente.
- Tipos de ECS: General, optimizado para cómputo, memoria, almacenamiento y cómputo acelerado.

2. **Servicio de Volumen Elástico (EVS)**

Objetivo: Proporcionar un almacenamiento persistente y escalable que soporte altas demandas de I/O con bajos tiempos de latencia.

Características Requeridas:

- Alta disponibilidad y durabilidad: Soporte para sistemas de archivos distribuidos, entornos de desarrollo y pruebas, aplicaciones de almacén de datos y escenarios de cómputo de alto rendimiento (HPC).
- Especificaciones del Disco: Desde I/O común hasta ultra-alta I/O, discos SAS locales y SSDs NVMe.

3. **Servicio de IP Elástica (EIP)**

Objetivo: Ofrecer direcciones IP públicas estáticas que se pueden asignar o desasignar dinámicamente a los recursos, ajustando el ancho de banda según las necesidades del servicio.

Características Requeridas:

- Flexibilidad y Alta Disponibilidad: Conexiones a múltiples operadores a través del protocolo BGP con failover automático.
- Facturación Flexible: Basada en el uso real, con opciones de suscripción mensual/anual, y banda ancha compartida.

4. **Red Privada Virtual (VPC)**

Objetivo: Crear una red virtual privada y aislada en la nube de Huawei para alojar servicios que demandan alta seguridad.

Características Requeridas:

- Seguridad y Control: Redes privadas completamente aisladas con grupos de seguridad y asignación de EIPs.
- Configuración Flexible: Gestión autónoma de la red, BGP dinámico y peering entre VPCs.

5. **Servicio de Backup y Recuperación en la Nube (CBR)**

Objetivo: Permitir el respaldo y recuperación de servidores en la nube y discos en casos de fallos de hardware/software o eliminaciones accidentales.

Características Requeridas:

- Seguridad y Fiabilidad: Soporte para múltiples recursos, protección multi-región, y respaldo y restauración rápidos.

6. **Servicio de Seguridad de Host (HSS)**

Objetivo: Mejorar la seguridad general del host proporcionando gestión de vulnerabilidades, inspección de líneas base y detección de intrusiones.

Características Requeridas:

- Gestión Integral de Seguridad: Capacidad para gestionar información de seguridad, detectar vulnerabilidades y proteger contra ataques.

7. **Firewall de Aplicaciones Web (WAF)**

Objetivo: Proteger servicios web al examinar y bloquear ataques comunes y sofisticados a través de HTTP/HTTPS.

Características Requeridas:

- Alta Seguridad y Fiabilidad: Detección dual (reglas + AI), prevención dinámica de crawlers y verificación precisa IP+cookie.

8. **Servicio de Almacenamiento de Objetos (OBS)**

Objetivo: Ofrecer un servicio de almacenamiento escalable y confiable con soporte para múltiples mecanismos de protección de datos.

Características Requeridas:

- Alta Durabilidad y Continuidad del Servicio: Certificación TRUCS, encriptación del lado del servidor y control de acceso granular.

ESPECIFICACIONES GENERALES

1. Soportar facturación local con diferentes distribuidores para la mayoría de Países de América Latina incluyendo Honduras.
2. Soporte Local en Honduras de Fabrica conforme a las solicitudes sobre IaaS, SaaS, PaaS
3. Contar con un API Explorer para el desarrollo de los servicios desde backend automáticas y específicas.
4. Contar con soluciones externas (Tipos de OS) en el marketplace integrada en la nube publica incluyendo el licenciamiento por hora/mes/año
5. Monitorear servicios 24x7 con dashboard pre-configurados con alertas específicas para costos.
6. El proveedor de servicios debe ser capaz de fabricar el completo Stack de Hardware que soporta la Nube. Desde los gabinetes, los UPS, el A/C, los servidores, almacenamientos, switches e inclusive las interfaces de red de datos y red de almacenamiento son fabricadas por nosotros. Esto brinda mejoras no solo económicas, si no de eficiencia a la integración de los diversos componentes. Lo que nos brinda tiempos de respuesta y latencia incomparables en la industria.
7. El proveedor debe ser capaz de administrar los ambientes (desarrollo, test, producción, QA) sin procedimientos que pongan en riesgo la operabilidad de la aplicación tal como topologías de redes independientes en cada ambiente y permisos por servicios por cada personal técnico/departamento
8. Ser capaz de brindar facturación local mensual y/o disponer de un API de facturación para el desarrollador y exportar consumo y costos mensuales.
9. Ser capaz de obtener histórico de facturas manualmente y/o brindar facturas locales automáticas
10. Debe ser amigable al usuario con un uso flexible en las diferentes configuraciones en cada servicio. Además, debe de contener una extensa academia de entrenamiento y documentos que sustenten al correcto uso de la plataforma.
11. Debe ser flexible ante los cambios sin afectación a la operación de la aplicación.
12. Debe brindar correctos procedimientos y/o documentación que asegure la productividad

sin afectación en casos de apagado/encendido/reinicio/eliminación/extensión.

13. Debe proveer templates de funciones pre-configuradas para el encendido y apagado automático de los recursos. Además, el servicio SaaS que brinda esta solución para reducir costos y aumentar la eficiencia de la plataforma.
14. Debe de proveer servicios de reglas ACLs entre Subnets , Nat Gateway, VPN Firewall, AntiDDoS, Grupos de seguridad para restringir puertos y habilitar solamente los necesarios. Además, proveer tecnologías de aprendizaje automático y big data para proteger sus bases de datos en la nube, auditándolas de manera inteligente y detectando comportamientos riesgosos como la inyección SQL. Adicionalmente, brindar agentes instaladores para cada VM para su protección contra vulnerabilidades de OS, ataques de fuerza bruta, protección contra bots, registro de accesos no autorizados y prevención contra ransonware.
15. Capacidad de brindar permisos a servicios específicos tales como eliminar, agregar, editar, actualizar, monitorear indistintamente a la necesidad del usuario o departamento por asignar. Además, ser capaz de almacenar tales acciones en logs históricos.
16. Brindar servicios de recuperación con RPO igual a 0 y RTO menor o igual a 0.
17. Proveer técnicas agiles para el switchover de gateway para mejorar la eficacia ante la necesidad(active-passive). Por otra parte, soportar High Availability Active Active en los enlaces VPN.
18. Ser capaz de brindar certificaciones SSL. Proveer servicio para el redireccionamiento Top Level Domain y contar con su propio registro de DNS. De ser necesario, contar con un redireccionamiento Global por temas de seguridad. Por otra parte, poseer algún tipo de servicio para bloqueos geolocalizados para evitar ser atacados o vistos en países no deseados alrededor del mundo
19. Ser capaz de replicar sincronizadamente para mejorar la eficiencia ante una migración o replicación de un servidor virtual y/o replicar por medio de políticas automáticas de forma pasiva para evitar consumos innecesarios no más la durabilidad y consistencia de la data
20. Ser capaz de alertar o enviar notificaciones luego de cada calendarización. Además, configurar alertas ante una amenaza de Ransonware para prevenir la afectación de los

respaldos de las maquinas

21. Proveer configuración de alertas ante un alto consumo inesperado para evitar el consumo excesivo o ser detectado a tiempo. Restringir políticas de escalado como su mínimo o máximo de instancias por escalar. Almacenar Logs por cada acción del AutoScaling
22. Brindar documentación suficiente tales como guías, mejores prácticas, casos de uso, videos, entrenamientos en español y/o inglés, laboratorios, ambientes de prueba para su correcta enseñanza.
23. Configuración de alertas ante un consumo excesivo de algún servicio. Ser capaz de manejar un límite de budget para regular el consumo no apropiado. Además, ser capaz de actualizar consumos en tiempo real o no mayor a 24 horas para la rápida detección de consumos. Ser capaz de general un dashboard para posibles optimizaciones de costos desde el Budget Control.
24. Generar alertas, detección real time de sobre excesos de respaldos. Detección a tiempo de posible ransonware en los respaldos. Consola flexible en los usos de los respaldos tales como roll back sobre la misma instancia o clonación de la instancia basado en los respaldos para mantener la seguridad y consistencia del respaldo. Contar con un tipo de storage especial donde permanezcan los respaldos con una durabilidad de 99.99999999999 y una perfecta consistencia de la data con posibilidad de recuperar los respaldos en diferentes regiones o zonas de disponibilidad.
25. Cada componente de la nube debe contar un monitoreo específico para saber el estado actual de cada servicio tales como Health Checks que verifiquen el estado en que se encuentra la aplicación o el servicio.
26. Debe general reporteas automáticos de consumos y costos de los servicios. Adicionalmente, generar automáticamente reportes de riesgo y vulnerabilidades por instancia o recursos de manera eficaz sin mayor trabajo. Este debe contener todos los aspectos importantes sobre seguridad, protección, consumos y costos
27. Debe cumplir con servicios específicos de automatización con políticas basado en rendimiento, tiempo y/o periodos establecidos que se deba tomar la decisión de forma automática sin afectación a la operación. La plataforma debe de ser flexible con temas de

compute, storage, network para la escalabilidad sin restricciones.

28. Debe ser capaz de brindar gráficos visuales en tiempo real acerca el monitoreo. Además de soportar cualquier tipo de endpoint somo Mail, HTTP, HTTPS, SMS o funciones customizadas para el envió automático de alertas a un pool de endpoint de la institución
29. Brindar reportes automáticos con un formato entregable para la facilidad de entendimiento sobre los consumos actuales y posibles optimizaciones
30. Debe soportar el esquema de Cloud Native para ser uso de tecnologías tales como Kubernetes y a su vez ser capaz de conectar con Clusters de Hadoop y Machine Learning.
31. Brindar PaaS para el diseño previo de arquitectura en la nube para su interacción amigable entre diferentes departamentos con permisos de aprobación y rechazo.
32. Ser flexible en temas de configuración y ajustes en temas de Compute, Storage y Networking.
    a. Compute: Ser capaz de reducir flavor(specs) o aumentar flavor.
    b. Storage: ser capaz de aumentar storage sin pérdida de operabilidad.
    c. Network: Ser capaz de cambiar Segmentación de red de forma flexible.

33. Debe ser capaz de brindar servicios de migración compatibles con ambientes más comunes como Hyper-V, VMware u otras nubes.
    a. Estos servicios deben soportar continuous synchronization para realizar una migración totalmente transparente. Adicionalmente, soportar esquemas de migración encriptado para respaldar la información en el proceso de migración
34. Brindar servicios que sustenten la experiencia constante en la implementación, gestión y ecosistema de aplicaciones nativas de la nube. Las aplicaciones nativas de la nube pueden ejecutarse libremente en regiones y nubes con una distribución inteligente del tráfico.
35. Demostrar por medio de servicios de O&M la eficiencia que presenta la plataforma y que operaciones sugeridas dispone la plataforma sin ninguna perdida de la operación
36. Proveer servicios de monitoreo http-https, control de eventos de accesos geolocalizados

con capacidad de restringir países no deseados.

37. Brindar cursos gratuitos y vouchers para las organizaciones junto el material, videos, entrenamiento presencial o virtual para la correcta enseñanza de la plataforma
38. Brindar Servicios específicos para el control de Logs junto el manejo de aprobación o permisos específicas sobre el uso de servicios de la plataforma.
39. Brindar Servicios específicos para el control de Logs junto el manejo de aprobación o permisos específicas sobre el uso de servicios de la plataforma.
40. Ser capaz de proveer reportes customizados si así lo solicita el cliente desde fabrica donde evidencia con datos a tiempo real, métricas y cual estado relevante de los compontes
41. Ser capaz de proveer reportes customizados si así lo solicita el cliente desde fabrica donde evidencia con datos a tiempo real, métricas y cual estado relevante de los compontes
42. Provee un informe automático diario, mensual utilizando servicios específicos de seguridad para la prevención de alguno tipo de desastres no contemplado como vulnerabilidad en sistemas operativos, ataques de fuerza bruta, protección geo localizada, entre otros.
43. Soportar tipos de recursos dependiente de la aplicación. Ya sean datos no estructurados, datos estructurados, bases de datos no relacionales, relaciones, tipos de almacenamiento de servicios de big data. A su vez, proponer servicios de inteligencia de negocio que sustenten la operabilidad y experiencia a los usuarios de la institución y usuarios finales
44. Proveer una capa de seguridad para cada uno de los recursos a utilizar, desde la parte de compute, storage y network tales como AntiDDoS, WAF, Cifrado de información por medio de KMS, WORM, prevención contra Ransonware, enlaces encriptados de comunicación, alta disponibilidad en gateway para reducir en gran medida el downtime del sistema.
45. Deberá tener certificaciones que cumplan con la seguridad tales como ISO 27001, ISO 27017, ISO 27018, TL 9000 e ISO 9001, ISO 20000-1, ISO 22301, CSA STAR Gold, ISO 27701, BS 10012, ISO 29251, PCI DSS, PCI 3DS, ISO 27799, ISO 27034, Informe SOC 1 tipo II, Informe SOC 3, EE. UU. Marco de Ciberseguridad del NIST, EE.UU. MPA

46. Deberá detectar más del 99% de los ransomware conocidos. La precisión de la minería y la detección de web shell al 99%.
    a. El servicio no debe consumir más del 2 % de uso de CPU en promedio para el poco impacto en los servicios.
47. Proveer servicios específicos de monitoreo adaptados a las utilidades de tráfico, rendimiento, tarjetas de red, protocolos TCP/UDP para la deteccion de picos inesperados con la facilidad de alarmas automáticas
48. Proveer un servicio de diseño de arquitecturas donde mencione malas prácticas y recomendaciones para la generación de HLD previa a una configuración en la Nube tal como Hyadn
49. Debe de contener Logs a nivel de IaaS, PaaS y SaaS que contengan accesos autorizados y no autorizados y poder generar Logs. La plataforma también tiene que detectar accesos a nivel de OS
50. Gestionar Roles y políticas de acceso como MFA y controles de identidad federada.
    a. Segmentación de red con puertos restringidos y reglas ACLs.
    b. Cifrado y rotación de claves
    c. Protección contra Malware.
    d. Parcheo y vulnerabilidades en OS.
    e. Respaldos y recuperación para mantener la integridad de la información
51. Apoyo de SAs y TAMs y a su vez servicios activados de logs auditorias y antivirus de sistema operativo de ser requerido.

ESPECIFICACIONES TECNICAS

Tabla 12- Especificaciones Técnicas

N	Capacidad GB	Nombre del Servidor	vCPUs	Memoria (GiB)	Sistema Operativo	Descripción detallada
1	80	WINDOWS	8	16	Windows Server 2019 64bit	Servidor dedicado para pruebas de rendimiento y compatibilidad antes del despliegue de actualizaciones.
2	1024	WINDOWS	16	64	Windows Server 2016 64bit	Maneja grandes bases de datos relacionadas con censos, optimizado para transacciones intensivas de datos.
3	1024	WINDOWS	8	16	Windows Server 2016 64bit	Soporta aplicaciones asociadas a la gestión de datos del censo, proporcionando rendimiento estable.
4	1024	WINDOWS	8	16	Windows Server 2016 64bit	Ambiente de desarrollo para aplicaciones ASP.NET, facilitando pruebas y despliegues rápidos.
5	1024	WINDOWS	16	64	Windows Server 2016 64bit	Servidor de desarrollo de bases de datos, soporta grandes volúmenes de información para pruebas.
6	400	LINUX	8	16	CentOS 8.0 64bit	Utilizado para el desarrollo de software relacionado con sistemas de administración tributaria.
7	40	LINUX	4	8	Other Linux 64 bit	Proporciona servicios VPN y configuraciones de red avanzadas para conexiones seguras y estables.
8	300	WINDOWS	32	64	Windows Server 2016 64bit	Potente servidor para gestión documental, diseñado para el manejo eficiente de grandes repositorios.
9	350	LINUX	4	8	Ubuntu 20.04 server 64bit	Gestiona controladores UniFi para la administración de dispositivos de red y comunicaciones inalámbricas.

10	1024	LINUX	8	16	Ubuntu 22.04 server 64bit	Aloja servicios de correo electrónico Zimbra, proporcionando una plataforma robusta y escalable.
11	1024	WINDOWS	16	32	Windows Server 2016 64bit	Plataforma para aplicaciones ASP.NET en producción, soportando cargas de trabajo más intensas.
12	300	LINUX	8	16	CentOS 8.0 64bit	Servidor específico para operaciones bancarias, asegurando transacciones seguras y estables.
13	200	LINUX	4	8	CentOS 8.0 64bit	Hostea páginas web empresariales, optimizado para tráfico alto y seguridad mejorada.
14	200	WINDOWS	4	8	Windows Server 2016 64bit	Servidor de Active Directory para la gestión de políticas y accesos de usuarios en la red empresarial.
15	1024	WINDOWS	32	128	Windows Server 2016 64bit	Maneja procesos de bases de datos SQL de gran escala, ideal para aplicaciones críticas y análisis de datos.
16	400	LINUX	24	48	CentOS 8.0 64bit	Soporta aplicaciones críticas de tributación y fiscalidad, con alta disponibilidad y seguridad.

Fuente: Elaboración Propia.

LOTE #2 - COMPUTADORAS LAPTOPS/ESCRITORIO

N°	Descripción	Precio Unitario sin 15%	Total con 15%	Total
15	**Laptop del precisión 3591** - procesador Intel Core Ultra 9, 185 H vPro Enterprise (24 MB DE CACHÉ 16 NÚCLEOS 22 KG HASTA 5.1 GHZ 45W) Memoria 32 GB: 2x16gb DDR5 5600 MT PLECA S COMA SIN SC- DISCO 512 GB M2 2230 NBNE PCI GENERACIÓN 4 SSD CLASE 35 Gráfico en NVIDIA RTX 2000 generación ADA 8 GB GDDR6 PANTALLA 15.6 FHD 1920 * 1080, 60 HZ 250 NITS, NO TÁCTIL CÁMARA FHD HDRGB, MICRÓFONO, WLAN, Teclado Español, América Latina, Teclado De Acceso Rápido Retroalimentado Con Teclado Numérico 100 Teclas Sistema Windows 11 Pro Español Inglés Portugués Brasil Francés Garantía Servicio In Situ Al Siguiente Día Laborable De Soporte De Un Año Después Del Diagnóstico Remoto Con Soporte HWSW	63,233.12	72,718.09	1,090,771.32
15	2. DELL Ecoloop Essential BackPack	638.89	734.72	11,020.85
15	3. DELL Wireless Mouse Black SPCKWM 126WRLS	294.44	338.61	5,079.09
15	4. DELL Docking WD19DS 130w Power Delivery 180W	4,074.52	4,685.70	70,285.47
	Total	**68,240.97**	**78,477.12**	**1,177,156.73**

15	**Desktop Optiplex SFF 7020** estándar con procesador Intel Core i5-14500 vPRO, (24 MB de caché, 14 núcleos y 20 hilos, hasta 5 GHz en modo turbo) Memoria de 16 GB (1 x 16 GB DDR5). Disco de 1 TB M.2 2230 PCIe NVMe SSD clase 25, disco adicional de 256 GB SSD M.2 PCIe NVMe clase 35. El sistema incluye teclado y mouse. Tarjeta inalámbrica Realtek Wi-Fi 6 RTL 8852BE, 2x2 802.11ax MU-MIMO, Bluetooth con antena externa. Garantía de servicio básico in situ de un año después del diagnóstico remoto, con soporte solo de hardware.	27,774.36	31,940.51	479,107.71
15	2. Monitor de 24 pulgadas P2422H, resolución de 1920 x 1080, panel IPS, garantía de 3 años.	3,455.31	3,973.61	59,604.10
	Total	**31,229.67**	**35,914.12**	**538,711.81**

Total en los Productos	**1,715,868.54**

Figura 64 - Especificaciones Técnicas Equipo de Cómputo TI

Fuente: Elaboración Propia.

LOTE #3 - GESTOR DOCUMENTAL

Licencia de Gestor Documental AZDigital para 50 usuarios Full y 400 usuarios para consulta, Gestor Documental AZDigital

- **Interfaz de usuario:** Intuitiva y fácil de usar, diseñada para una navegación eficiente y una rápida recuperación de documentos.
- **Compatibilidad de archivos:** Soporta una amplia variedad de formatos de documentos, incluidos PDF, DOCX, XLSX, PPTX, JPEG, PNG, y más.
- **Almacenamiento:** Escalable según las necesidades del cliente, con opciones para almacenamiento en la nube o en servidores locales.

- **Seguridad:** Encriptación avanzada de datos en tránsito y en reposo, autenticación multifactor y permisos de acceso granulares.
- **Búsqueda:** Motor de búsqueda potente y rápido con capacidades de búsqueda de texto completo, filtros avanzados y búsqueda por metadatos.
- **Colaboración:** Herramientas integradas para la colaboración en tiempo real, comentarios y notificaciones automáticas de cambios.
- **Automatización de flujos de trabajo:** Configuración de flujos de trabajo automatizados para la revisión, aprobación y archivo de documentos.
- **Integración:** Compatible con sistemas ERP, CRM y otras aplicaciones empresariales a través de API y conectores estándar.
- **Soporte técnico:** Asistencia técnica 24/7, con opciones de soporte en sitio y remoto.
- **Cumplimiento:** Cumple con las normativas y estándares de gestión documental, como GDPR, HIPAA, y otras regulaciones específicas de la industria.
- **Actualizaciones:** Actualizaciones periódicas y mejoras basadas en las sugerencias de los usuarios y los avances tecnológicos.

LOTE #4 - SERVIDORES FISICOS

Infraestructura de virtualización (convergente: 3 servidores, 2 switches y 2 SAN)

para Virtualización:

- Servidores: 2 x Dell PowerEdge R730:
- CPU: 2 x Intel Xeon CPU E5-2620 v4 2.10GHz
- RAM: 160 GB
- LAN: 4 x 10 Gb Ethernet Base-T, 4 x 1 Gb Ethernet Base-T
- Servidor: 1 x HPE Proliant DL360 G10

- CPU: 2 x Intel Xeon Gold 5220 CPU 2.20GHz
- RAM: 350 GB
- LAN: 4 x 10 Gb Ethernet Base-T, 4 x 1 Gb Ethernet Base-T
- Estos servidores sufren de un alto consumo de CPU y memoria RAM lo que les imposibilita creación de
- nuevas máquinas virtuales y el mover máquinas entre cluster.
- Almacenamiento
- SAN Dell SCv3020 23.73TB utilizable:
- Cache: 32 GB (16Gb por controladora)
- Puertos: 4 x 10 Gb Ethernet Base-T
- Alto consumo de IOPs
- SAN HPE Nimble
- Cache: 64 GB (32Gb por controladora)
- Puertos: 4 x 10 Gb Ethernet Base-T
- Alto consumo de IOPs
- Switches
- Dos (2) Switches Dell S4128T-on – LAN, es switch de 28 puertos de 10Gb Base-T.

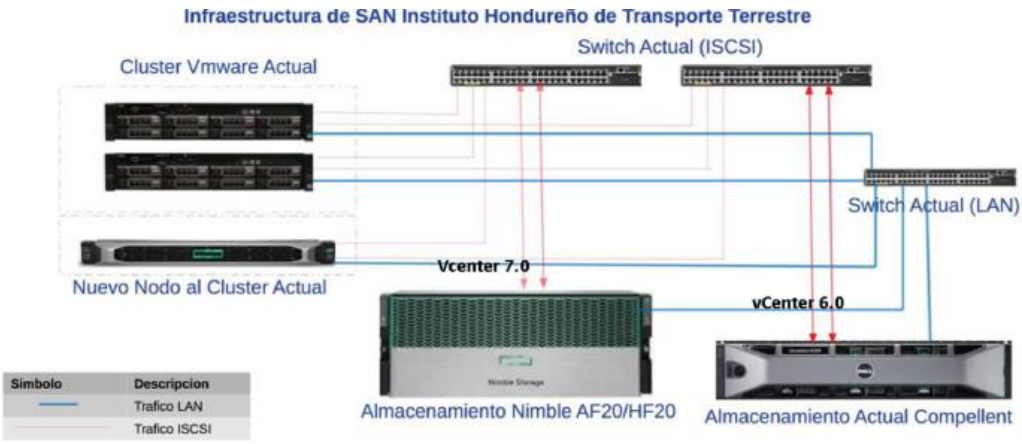

Figura 65 - Infraestructura de SAN IHTT

Fuente: Elaboración Propia.

LOTE #5 - FIREWALL Y REDES

Propuesta técnica basada en la tecnología de servidores y SAN Hitachi en la parte de comunicaciones se ofrece solución de switches Juniper, firewall Juniper y antivirus CrowdStrikes., renovación de solución de infraestructura Convergente.

- Proporcionaremos 2 servidores para montar en ellos un clúster convergente usando la solución de Vmware
- vSphere 8 Standard.
- Migraremos 22 máquinas virtuales del ambiente actual del cliente al nuevo clúster convergente ofertado.
- Proporcionaremos una SAN para el almacenamiento de máquinas virtuales.
- Se incluyen 2 switches TOR para la conexión de esta solución entre sí y 2 switch para distribución, acceso
- y administración, los dos (2) switches TOR se conectarán a la red LAN propiedad de Instituto Hondureño del
- Transporte Terrestre.

- Se incluyen 2 firewall Juniper en alta disponibilidad para protección de seguridad avanzada.
- Se incluyen 14 switches de acceso para la red interna del Instituto Hondureño del Transporte Terrestre.
- Se incluyen 18 access point para conexión Wifi de usuarios internos.
- Se incluye soporte de Cesa por 3 años:
- Atención en Sitio: 2 por año. Se incluye revisión física de los equipos.
- Atención remota: 2 x año. Se incluye actualización de firmware y versiones.
- Para mantenimiento correctivos referirse al Procedimiento Soporte PostVenta y SLAS

COMPONENTES

Como resultado de la solución renovación de Infraestructura Convergente para el lnstituto Hondureño del Transporte Terrestre se implementará una solución integral conformada por los siguientes equipos y licencias por 3 años de soporte:

- Servidores Hitachi
- Infraestructura para Virtualización
- Servidores: 2 x Hitachi DS120 G2:
- CPU: 2 x Intel Xeon Gold 6326 (16C, 2.9GHz, 185W)
- RAM: 256GB
- HDD: 2 x 256 NVMe M.2 SSD
- LAN: 4x25Gbps y 8 x 1Gbps
- Almacenamiento:
- SAN Hitachi VSP E590
- HDD: 82.53 TB (Raid 6 12D+2P, 7.6TB NVME), capacidad efectiva 131TiB
- Controladoras: 2

- Puertos: 8 x 25Gbps iSCSI
- Memoria caché: 384GB
- Garantía: 3 años.
- Licenciamiento VMware:
- Suscripción de VMware vSphere 8 Standard, 3 years.
- Cantidad: 96 cores
- Vigencia: 3 años.
- Licenciamiento Windows Server:
- Microsoft windows server Datacenter, 3 years.
- Cantidad: 96 cores
- Vigencia: 3 años incluye software assurance open value 16 licenses.
- Core y LAN switches:
- 2 x Juniper EX4650
- Puertos: 48 x 25 Gbps SFP28
- 2 x Juniper EX4100
- Puertos: 24 x 1 Gbps, 32 x 1Gb.
- 16 x 1Gb/2.5Gb
- 4 x 10Gb SPF+ Uplink ports, 4x 25G SFP28 Stacking/Uplink ports
- Componentes Datacenter:
- 1 x Rack de 42”
- 2 x UPS de 3KVA con transformador reductor de 208V
- 1 x organizador horizontal de cableado de 1U
- 1 x Patch panel de 24 puertos, cat 6 utp

- 2 x Bandeja ventilada 16” profundidad 2 RMS.

SOLUCIÓN DE INFRAESTRUCTURA CONVERGENTE

Firewall Junpier:

- 2 x Juniper SRX2300
- RMK and Junos Software Base
- Garantía: 3 year

Switches de Acceso:

- 14 x EX4100-F-48P - SWITCH EX4100-F 48-Port 10/100/1000BaseT PoE+, 4x 10G SFP+ Uplink
- ports, 4x 10G SFP+ Stacking ports

Access Point:

- 18 x AP45-WW - Premium Performance MultiGigabit WiFi 6E Access Point (4x4:4)

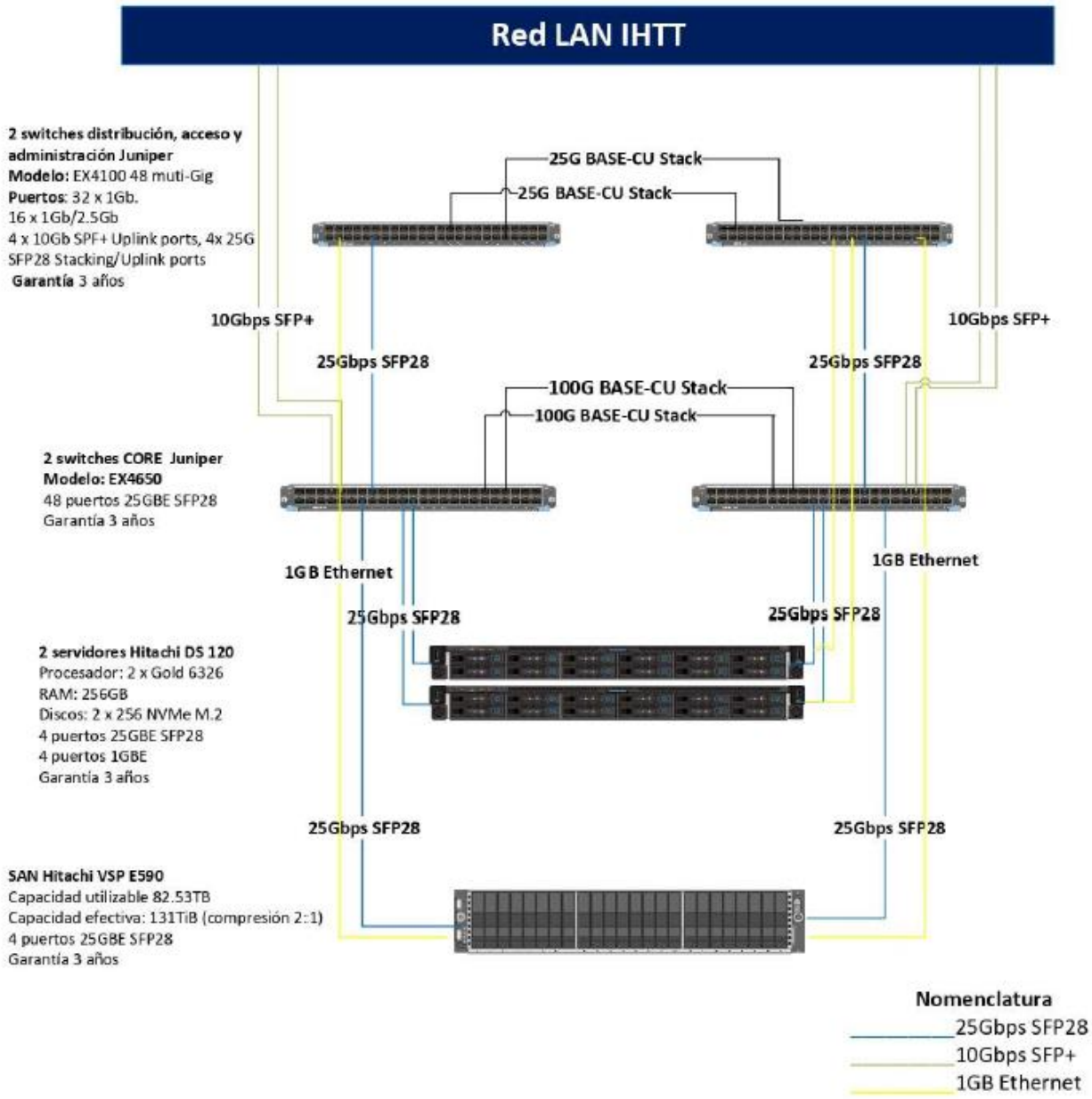

Figura 66 - Diagrama Red LAN IHTT

Fuente: Elaboración Propia.

ANEXO 5 – BORRADOR DECRETO EJECUTIVO

DECRETO EJECUTIVO NÚMERO PCM XX-2024

LA PRESIDENTA CONSTITUCIONAL DE LA REPÚBLICA

EN CONSEJO DE SECRETARIOS DE ESTADO,

CONSIDERANDO: Que la Constitución de la República establece que la Presidenta tiene a su cargo la Administración General del Estado y su representación, teniendo entre sus atribuciones dirigir la política general del Estado y representarlo, emitir Acuerdos y Decretos y expedir reglamentos y resoluciones conforme a la Ley, administrar la Hacienda Pública, crear, mantener y suprimir servicios públicos y tomar las medidas que sean necesarias para el buen funcionamientos de estos, así como las demás atribuciones que le confieren la Constitución y las leyes (artículo 245 numerales 2, 11, 19, 35 y 45).

CONSIDERANDO: Que la Ley General de la Administración Pública, dispone que la presidenta de la República tiene a su cargo la suprema dirección y coordinación de la Administración Pública Centralizada y Descentralizada, pudiendo en el ejercicio de sus funciones, actuar por sí o en Consejo de ministros (artículo 11).

CONSIDERANDO: Que mediante el Decreto Legislativo número 155-2015 publicado en el Diario Oficial "La Gaceta" en fecha 30 de marzo de 2016, edición número 33,995, con finalidad primordial de obtener para los Usuarios del servicio público y especial de transporte, las mayores y mejores condiciones de calidad, seguridad, comodidad, eficiencia, economía y representatividad, se aprobó la "Ley de Transporte Terrestre", mediante la cual se creó el Instituto Hondureño del Transporte Terrestre (IHTT), quien tiene la atribución exclusiva de aplicar dicha Ley y su

reglamentación (artículos 1 y 4).

CONSIDERANDO: Que los servicios públicos que brinda el Instituto Hondureño de Transporte Terrestre (IHTT) se vieron afectados durante los meses de febrero y marzo del presente año, debido a un ataque cibernético de secuestro de datos (ransomware), lo cual derivó progresivamente en el cese total de las operaciones institucionales, comprometiendo la operatividad del IHTT y poniendo en riesgo los datos de usuarios y transportistas. Esta situación se agravó debido a una serie de deficiencias críticas en la infraestructura de seguridad de los sistemas operativos institucionales y al uso de equipos y servidores obsoletos, lo cual mantiene los sistemas de la institución expuestos a múltiples vulnerabilidades.

CONSIDERANDO: Que la interrupción de los sistemas del Instituto Hondureño de Transporte Terrestre (IHTT) tuvo repercusiones significativas en diversas áreas operativas, incluyendo la recepción de nuevas solicitudes, la gestión de expedientes, la imposición de multas por infracciones cometidas por los concesionarios, así como la emisión de Permisos de Explotación, Certificados de Operación, Permisos Especiales y Permisos Eventuales, ante lo cual algunos transportistas se vieron obligados a suspender la prestación del servicio de transporte, se afectó la movilidad y el acceso a servicios fundamentales para la población e implicó para el IHTT una pérdida de captación de ingresos que asciende más de Veinticinco Millones de Lempiras (L25,000,000.00).

CONSIDERANDO: Que luego del precitado incidente, la Gerencia de Tecnologías de la Información, Comunicación, Conocimiento y Aprendizaje (TICCA) del Instituto Hondureño del Transporte Terrestre (IHTT), emitió un informe sobre el estado de la infraestructura tecnológica institucional a nivel nacional, revelando la presencia de servidores obsoletos, programas informáticos (softwares) desactualizados y falta de licencias para dispositivos de seguridad críticos, señalando la necesidad urgente de fortalecer las políticas de seguridad informática, actualizar y mantener adecuadamente la infraestructura tecnológica, desarrollar programas continuos de capacitación en ciberseguridad para los operadores y adoptar medidas para enfrentar amenazas cibernéticas emergentes, con el objeto de garantizar la continuidad y la eficiencia de los servicios públicos en el ámbito del transporte terrestre en Honduras. Principio del formulario

CONSIDERANDO: Que la Ley de Contratación del Estado establece que se podrán realizar contrataciones directas cuando se tenga por objeto proveer las necesidades ocasionadas

por una situación de emergencia, al amparo de lo establecido en el artículo 9 de la misma ley (artículo 63 numeral 1).

CONSIDERANDO: Que, de conformidad a la Ley de Contratación del Estado, la declaración del Estado de Emergencia se hará mediante Decreto de la presidenta de la República en Consejo de ministros. Asimismo, se establece que cuando ocurran situaciones de emergencia ocasionadas por circunstancias excepcionales que afectaren sustancialmente la continuidad o la prestación oportuna y eficiente de los servicios públicos, podrá contratarse el suministro de bienes o de servicios o la prestación de servicios de consultoría que fueren estrictamente necesarios, sin sujetarse a los requisitos de licitación y demás disposiciones reglamentarias, sin perjuicio de las funciones de fiscalización (artículo 9).

POR TANTO.

En aplicación de los artículos 2, 11, 19, 59, 80, 245 numerales 2, 30, 45 artículos 252 y 255 de la Constitución de la República; artículos 1, 2, 5, 7, 10, 11,12, 14, 17, 18, 19, 20,21, 22, numeral 9 y 10, 27 y 45 de la Ley General de la Administración Pública; artículo 9, 11 numeral 2 literal a, 38 numeral 5, 63 numeral 1 y 4 párrafo segundo de la Ley de Contratación del Estado, artículos 1, 3, 19, 22, 23, 25 y 32 de la Ley de Procedimiento Administrativo

DECRETA:

ARTÍCULO 1. Con el objeto de garantizar la prestación eficiente y oportuna del servicio público de transporte a la población, se declara ESTADO DE EMERGENCIA EN EL INSTITUTO HONDUREÑO DEL TRANSPORTE TERRESTRE (IHTT).

ARTÍCULO 2. Se autoriza al Instituto Hondureño del Transporte Terrestre (IHTT), a realizar la contratación directa de los bienes y servicios tales como servicios en la nube, computadoras, gestores documentales, servidores, cortafuegos (firewall), entre otros que sean necesarios para fortalecer la infraestructura tecnológica de la institución, con el objeto de restablecer, proteger y garantizar la continuidad de la prestación de los servicios públicos que brinda el Instituto Hondureño del Transporte Terrestre (IHTT).

Lo anterior, en estricto cumplimiento de los requisitos y procedimientos establecidos en la Ley de Contratación del Estado y demás legislación aplicable.

ARTÍCULO 3. Se autoriza e instruye al Instituto Hondureño del Transporte Terrestre (IHTT), a utilizar de su partida presupuestaria lo que sea necesario para hacer frente al Estado de Emergencia declarado en el presente Decreto. Asimismo, se autoriza e instruye a la Secretaría de Estado en el Despacho de Finanzas (SEFIN), a realizar todas las operaciones necesarias en el ámbito de sus competencias, tales como la identificación y asignación de fondos de fuentes nacionales y/o externas, hasta por un monto de VEINTE MILLONES DE LEMPIRAS (L20,000,000.00) con el objetivo de atender el presente estado de emergencia.

ARTÍCULO 4. El presente Decreto Ejecutivo es de ejecución inmediata y deberá publicarse en el Diario Oficial "La Gaceta".

Dado en la Ciudad de Tegucigalpa, Municipio del Distrito Central, a los XXX (X) días del mes de XXXX del año dos mil veinticuatro (2024).

COMUNÍQUESE Y PUBLÍQUESE.

IRIS XIOMARA CASTRO SARMIENTO
PRESIDENTA CONSTITUCIONAL DE LA REPÚBLICA

FIRMAS MINISTROS

ANEXO 6 – INFORME FORENSE

Informe Forense de Discos Duros (Muestra) IHTT

Número de Caso: 2024-07-01-001

Investigador: Ing. Raúl Monge Mora

Fecha: 29 de julio de 2024

Resumen Ejecutivo

Este informe detalla el análisis forense realizado en varios discos duros perteneciente a algunos de los sistemas comprometidos. La revisión se realizó para investigar actividades sospechosas y recuperar datos relevantes para el caso de incidente de seguridad reportado.

A continuación, se listan los discos duros de muestra con su respectiva etiqueta:

Num	Etiqueta	Num Serie	Capacidad	Afectado	Contiene data	Recuperado
1	IHTT DELL D19	W401R4RT	900GB/SAS	SI	NO	NO
2	IHTT D24	S45RNE0M403025	240GB/SATA	NO	NO	NO
3	IHTT D22	ZBS1ZBA3	1TB/SAS	SI	SI	12%
4	IHTT D27	ZC23BFRL	1TB/SAS	SI	SI	3%
5	IHTT DELL D28	Y660A111FVPC	2TB/SAS	SI	NO	NO

6	IHTT DELL D26	Y670A082FVPC	2TB/SAS	SI	NO	NO
7	IHTT D25	S45RNE0M402869	240GB/SATA	NO	NO	NO
8	IHTT DELL D24	Z401ADTC	900GB/SAS	SI	SI	9%

Tabla 1.1.2

Conclusiones Clave

- En una primera fase se logra recuperar alrededor de un 5 y 15% de archivos mediante el des encriptado forzoso, sin embargo, muchos archivos están corruptos como residuo del método empleado lo cual da un rango del 3 al 12% efectivo de la totalidad de los archivos del disco. (Esto se puede mejorar con más poder computacional y tiempo disponible)
- Se identificaron rastros de malware "CryptoLocker" en los discos 1,3,4,5,6 y 8. El cual no tiene herramienta de des encriptado sin llave privada.
- La evidencia sugiere actividad no autorizada a partir del 15 de enero de 2024.
- El ultimo ejecutable previo al efecto del ransomwhere fue ejecutado desde la carpeta %tmp% y dicho archivo se introdujo al sistema vía red LAN interna (Con más tiempo y análisis se puede determinar la ip local del equipo desde el cual se ingresó)

Introducción

El objetivo de este análisis fue identificar cualquier evidencia de actividad maliciosa mediante análisis básico y determinar la posibilidad de recuperar datos relevantes del disco duro afectado en un posterior proyecto forense con más recursos.

Detalles del Disco Duro.

- **Referirse a la tabla Tabla** *1.1.2*

Metodología

- **Recolección de Datos:** Imagen completa del disco fue capturada utilizando FTK Imager.
- **Herramientas Utilizadas:** FTK Imager, Volatility, Autopsy Forensics.

Análisis Forense

1. **Evidencia Recopilada:**
    - Nombres y rutas de los ejecutables finales previos al encriptado de la información.
    - Logs de movimientos de red sospechosos y sin autorización.
    - Segmentos de discos duro con archivos pertenecientes al RAID (no utilizable hasta conexión con el resto de discos)

2. **Timestamps y Metadatos:**
    - Archivos modificados durante el período de interés: 15-25 de julio de 2024.
    - Metadatos indican modificaciones realizadas por usuarios no autorizados.
3. **Análisis de Malware:**
    - CryptoLocker identificado, impacto evaluado.
    - No se encontraron claves de descifrado efectivas para el malware presente.

Conclusiones

El análisis sugiere que la brecha de seguridad fue causada por la instalación de CryptoLocker a través de la conexión LAN de un equipo de usuario final, lo que resultó en el cifrado de datos críticos. Las acciones deben centrarse en fortalecer las defensas, capacitar al personal y planificar la recuperación de datos.

La revisión forense de los discos duros afectados por Cripto Locker ha revelado la gravedad y el alcance del ataque, subrayando la necesidad de una respuesta coordinada y una infraestructura robusta de ciberseguridad. Aunque los esfuerzos iniciales para desencriptar los datos han sido limitados debido a la sofisticación del ransomware, con tiempo y recursos adicionales, es posible desarrollar contramedidas efectivas y recuperar parte de la información comprometida.

Finalmente, aunque este informe no incluye imágenes ni datos de pantalla debido a los riesgos de reinfección experimentados durante el análisis, se enfatiza la importancia crítica de abordar este tipo de amenazas proactivamente a través de inversiones en seguridad y educación. La protección contra futuros ataques de ransomware debe ser una prioridad estratégica para cualquier organización que desee salvaguardar sus activos digitales y operacionales.

Recomendaciones

Con base en los hallazgos y la experiencia acumulada durante el análisis de los discos afectados, se hace imperativa la implementación de un enfoque integral de ciberseguridad que contemple las siguientes recomendaciones:

1. **Refuerzo de la Seguridad Informática:**
    - **Actualización de Software:** Asegurar que todos los sistemas operativos y aplicaciones estén actualizados con los últimos parches de seguridad para prevenir vulnerabilidades explotadas por ransomware.
    - **Sistemas de Detección de Intrusiones:** Implementar sistemas avanzados de detección y respuesta a incidentes que puedan identificar comportamientos anómalos asociados con ataques de ransomware.
2. **Copias de Seguridad Regular:**
    - **Estrategia de Backup:** Desarrollar y mantener una política de copias de seguridad robusta que incluya copias externas y fuera de línea para garantizar la recuperación de datos en caso de una infección exitosa.
    - **Pruebas de Restauración:** Realizar pruebas regulares de restauración de datos para asegurar la integridad y disponibilidad de las copias de seguridad.

3. **Concientización y Capacitación:**

    - **Programas de Capacitación:** Implementar programas de capacitación regulares para los empleados sobre la identificación y manejo seguro de correos electrónicos y archivos sospechosos que podrían contener ransomware.
    - **Simulaciones de Phishing:** Realizar simulaciones periódicas de ataques de phishing para evaluar y mejorar la preparación de la organización ante amenazas cibernéticas.

4. **Inversión en Tecnología de Seguridad:**

    - **Firewalls y Sistemas Anti-Malware:** Ampliar la inversión en soluciones tecnológicas que ofrezcan una protección integral contra una gama de amenazas cibernéticas, incluida la prevención de ransomware.
    - **Monitoreo de Red:** Implementar herramientas de monitoreo de red para detectar actividades inusuales que podrían indicar intentos de acceso no autorizado o movimientos laterales dentro de la red.

Resumen del Análisis

*Durante la revisión de los discos duros, se llevaron a cabo múltiples análisis forenses utilizando herramientas avanzadas de recuperación de datos y escaneo de malware. Sin embargo, debido a la naturaleza sofisticada del ransomware Cripto Locker, que emplea cifrado asimétrico para bloquear el acceso a los archivos, los intentos de desencriptación directa resultaron infructuosos sin las claves privadas correspondientes***.**

A lo largo del proceso de análisis, se observaron los siguientes puntos clave:

1. **Cifrado Extensivo de Archivos:**

    - Todos los discos mencionados como afectados presentaban un alto porcentaje de archivos cifrados con extensiones típicas del ransomware. La tasa de cifrado varió entre el 85% y el 95% de los datos presentes en cada disco. o Los tipos de

archivos afectados incluyen documentos de texto, hojas de cálculo, bases de datos y archivos multimedia, lo que sugiere un enfoque no selectivo del malware.

2. **Archivos de Rescate:**
    - En cada uno de los discos se encontraron archivos de texto con instrucciones para pagar un rescate a cambio de las claves de desencriptación. Estos archivos estaban presentes en múltiples directorios y mostraban mensajes consistentes en cada muestra**.**
3. **Persistencia del Malware:**
    - Se identificaron rastros de persistencia del malware en las particiones del sistema operativo, lo que indica intentos del ransomware por reinfectar los sistemas tras un reinicio o restauración. Esto sugiere que el vector de ataque inicial podría haber aprovechado vulnerabilidades en la red o acceso remoto**.**
4. **Limitaciones de Herramientas:**
    - Las herramientas utilizadas para la inspección forense, incluidas aquellas especializadas en análisis de ransomware, se encontraron ineficaces en ciertos casos debido a la contaminación continua de los sistemas analizados. Las pruebas de software anti-malware indican que el Cripto Locker utilizado tiene variantes activas que logran evadir la detección tradicional.
5. **Impacto en el Sistema:**
    - La infección causó un impacto severo en la operatividad de los discos. Las estructuras de archivos fueron severamente alteradas, y los registros de sistema revelaron intentos de sabotaje de registros de logs que dificultan aún más el análisis retrospectivo del ataque**.**

Necesidad de Tiempo y Recursos Adicionales

Dada la complejidad del ransomware Cripto Locker y la amplitud del impacto observado en las muestras analizadas, es evidente que se requiere un tiempo y recursos adicionales significativos para avanzar en las siguientes áreas**:**

- **Desarrollo de Herramientas de Desencriptación:**
    - Colaborar con empresas de ciberseguridad para el desarrollo de herramientas de desencriptación específicas que podrían ayudar a mitigar el daño**.** o Participar en iniciativas globales para compartir información sobre patrones de cifrado del Cripto Locker con el objetivo de descubrir vulnerabilidades en su implementación**.**
- **Análisis Detallado de Muestra:**
    - Realizar un análisis más exhaustivo de un mayor número de discos y sistemas comprometidos para identificar patrones o debilidades potenciales en el cifrado**.** o Incrementar la capacidad del laboratorio forense con recursos computacionales que permitan simulaciones y análisis más rápidos y efectivos**.**
- **Infraestructura de Recuperación:**
    - Establecer un entorno seguro de prueba para la implementación de técnicas avanzadas de recuperación que puedan ser aplicadas sin riesgo de reinfección**.** o Investigar la posibilidad de colaboración con otras entidades afectadas para compartir hallazgos y posibles soluciones**.**

Apéndices

- **Gráfico 1:** Distribución de archivos eliminados por tipo.
- **Tabla 1:** Lista de archivos recuperados.

Anexos

- **Captura de Pantalla 1:** Ejemplo de archivo cifrado.
- **Evidencia Recuperada:** Incluye documentos PDF y Word.

Referencias

1. **Guía de Normativa de Evidencia Digital:** NIST SP 800-86.
2. **Leyes de Protección de Datos:** Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.