ESCUELA DE POSGRADO NEWMAN

MAESTRÍA EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

" Propuesta de mejora al proceso de soporte técnico y seguridad mediante las TIC en la empresa GPSTRACKER S.A., Guayaquil, 2023 "

Trabajo de Investigación
Para optar por el Grado a Nombre de la Nación de:

Maestro en
Gestión de Tecnologías de la Información

Autor:
Bach. Lindao González, José Santiago

Docente Guía:
Dr. Merino Núñez, Mirko

TACNA–PERÚ

2023

25%	23%	5%	14%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

Índice General

Índice de Tablas

Índice de Figuras

Índice de Anexos

Resumen

En la empresa GPSTracker S.A. se observó desafíos significativos en su proceso de soporte técnico y seguridad, lo cual impacto directamente en la eficiencia operativa y la satisfacción del cliente. A pesar de la implementación de tecnologías de la información y comunicación (TIC), persistían deficiencias en la prestación de servicios de soporte técnico. Para alcanzar los objetivos, se empleó un enfoque metodológico mixto que combina métodos cualitativos y cuantitativos. Esto incluyó la realización de entrevistas con el personal de soporte técnico y seguridad, así como la aplicación de encuestas y análisis de datos para recopilar información relevante sobre el estado actual de los procesos y la seguridad de la información en la empresa. El diagnóstico situacional de GPSTracker S.A. reveló deficiencias críticas en áreas clave como la eficiencia del soporte técnico, la estabilidad de los servicios, la seguridad de la información y la claridad en la comunicación, afectando la satisfacción del cliente y la reputación de la empresa. La propuesta estratégica fue diseñada para abordar estos problemas incluyó soluciones respaldadas por tecnologías de la información y comunicación, como la automatización de procesos y mejoras en seguridad informática, con el fin de mejorar la eficiencia operativa y la seguridad. La implementación de mecanismos de seguimiento y control fue crucial para asegurar el éxito continuo de las estrategias propuestas, permitiendo ajustes y mejoras continuas. La definición de la inversión necesaria proporcionó una visión clara de los recursos financieros requeridos, asegurando una planificación financiera eficiente para abordar los problemas identificados en el soporte técnico y seguridad en GPSTracker S.A.

Palabras clave: TIC, soporte, seguridad, riesgos, mejora.

Abstract

In the GPSTracker S.A. company, significant challenges were observed in its technical support and security process, which directly impacted operational efficiency and customer satisfaction. Despite the implementation of information and communication technologies (ICT), deficiencies persisted in the provision of technical support services. To achieve the objectives, a mixed methodological approach was used that combines qualitative and quantitative methods. This included conducting interviews with technical support and security personnel, as well as applying surveys and data analysis to collect relevant information about the current state of processes and information security in the company. The situational diagnosis of GPSTracker S.A.revealed critical deficiencies in key areas such as technical support efficiency, service stability, information security and clarity of communication, affecting customer satisfaction and company reputation. The strategic proposal was designed to address these problems and included solutions supported by information and communication technologies, such as process automation and improvements in computer security, in order to improve operational efficiency and security. The implementation of monitoring and control mechanisms was crucial to ensure the continued success of the proposed strategies, allowing for continuous adjustments and improvements. The definition of the necessary investment provided a clear vision of the financial resources required, ensuring efficient financial planning to address the problems identified in technical support and security at GPSTracker S.A.

Keywords: TIC, support, security, risks, improvement.

Introducción

La eficiencia operativa y la protección de los activos digitales son aspectos críticos en el entorno empresarial contemporáneo, donde las Tecnologías de la Información y Comunicación (TIC) libran un papel central. En este contexto, el proceso de soporte técnico y seguridad emerge como un componente vital para garantizar el funcionamiento continuo y seguro de las operaciones empresariales. El interés personal surge de la necesidad de abordar los desafíos inherentes a la gestión efectiva de incidentes de la información en un entorno tecnológico en constante evolución.

Las problemática identificad está en la falta de procesos claros y eficientes para la resolución de incidencias de soporte técnico, así como deficiencias en las medidas de seguridad implementadas para preservar los activos digitales de la empresa. Estos problemas plantean riesgos significativos para la continuidad operativa y la integridad de los datos de GPSTracker S.A., así como para su reputación en el mercado.

El objetivo de la investigación es proponer mejoras al proceso de soporte técnico y seguridad de la empresa, con el fin de aumentar la validez en la resolución de incidencias y fortalecer la protección de los activos digitales. Se espera lograr resultados que contribuyan a minimizar el tiempo de inactividad, mejorar la experiencia del cliente, mitigar los riesgos de seguridad y aumentar la competitividad de la organización en su sector. La investigación presenta los subsiguientes capítulos:

El primer capítulo, “Antecedentes del estudio”, establece la estructura del trabajo, desde el título hasta los objetivos. También presenta la metodología, tipo, nivel y diseño de investigación, la justificación del estudio, definiciones, alcance y las limitaciones de la propuesta.

El segundo capítulo, “Marco teórico”, se proporciona una conceptualización de la variable principal y otros temas relevantes que contribuyen a comprender el tema en cuestión. Se destaca la importancia, se presenta la tabla del análisis comparativo y finaliza con el análisis crítico.

El tercer capítulo, “Marco referencial”, se enfoca en la empresa GPSTracker S.A. se cita la historia, filosofía, organigrama con la descripción de cada puesto, productos o servicios y el diagnóstico institucional.

El cuarto capítulo, “Resultados”, forma parte del desarrollo de la propuesta y exhibe gráficos, tablas y matrices, como la de las distintas actividades de mejora, plantear los mecanismos de control y presupuesto asociado al estudio.

Finalmente, el quinto capítulo, “Sugerencias y conclusiones”, se basa en los resultados de la propuesta y está alineado con los objetivos del estudio, se plantea las sugerencias y conclusiones derivadas del análisis realizado.

Capítulo I Antecedentes del Estudio

1.1. Título del tema

Propuesta de mejora al proceso de soporte técnico y seguridad mediante las TIC en la empresa GPSTracker S.A., Guayaquil, 2023.

1.2. Planteamiento del problema

En la actualidad, la empresa GPSTracker S.A. enfrenta desafíos significativos en su proceso de soporte técnico y seguridad, lo cual impacta directamente en la eficiencia operativa y la satisfacción del cliente. A pesar de la implementación de tecnologías de la información y comunicación (TIC), persisten deficiencias en la prestación de servicios de soporte técnico y en la garantía de la seguridad de los sistemas. Estas deficiencias se manifiestan en tiempos de respuesta prolongados, vulnerabilidades de seguridad no abordadas adecuadamente y la insatisfactoria experiencia del cliente.

Si la problemática descrita no se aborda y mejora de manera efectiva, es probable que la empresa GPSTracker S.A. experimente una serie de consecuencias negativas. La falta de mejoras en el proceso de soporte técnico y seguridad puede resultar en una disminución de la calidad del servicio ofrecido a los clientes. Esto puede traducirse en una menor satisfacción del cliente y, en última instancia, en la pérdida de clientes a favor de competidores que ofrezcan un soporte más eficiente y seguro. La falta de atención a las vulnerabilidades de seguridad podría exponer a la empresa y a sus clientes a diversos riesgos cibernéticos, como brechas de seguridad, robo de datos o interrupciones del servicio.

Esto no solo afectaría la reputación de la empresa, sino que también podría acarrear costos financieros significativos asociados con la recuperación de incidentes de seguridad. Los problemas técnicos no resueltos pueden generar interrupciones en las operaciones diarias de la empresa, lo que podría resultar en una disminución de la productividad del personal y en la pérdida de oportunidades de negocio.

La realización de la investigación propuesta reviste una importancia crítica frente a la problemática descrita, ya que proporcionará un marco estructurado y fundamentado para identificar, analizar y abordar las deficiencias en el proceso de soporte técnico y seguridad mediante las tecnologías de la información y comunicación (TIC). Al comprender a fondo los desafíos específicos que enfrenta la empresa en estos aspectos clave, se diseñaran estrategias efectivas que mejoren la eficiencia operativa, fortalezcan la seguridad de los sistemas y servicios y aumenten la satisfacción del cliente.

1.3. Objetivos

1.3.1. General

Realizar una propuesta de mejora al proceso de soporte técnico y seguridad mediante las TIC en la empresa GPSTracker S.A., Guayaquil, 2023.

1.3.2. Específicos

- Diagnosticar el proceso de soporte técnico y seguridad actual en la empresa GPSTracker S.A.
- Diseñar estrategias de mejora al proceso de soporte técnico y seguridad mediante las TIC.

- Proponer mecanismos de seguimiento y control a la propuesta de mejora al proceso de soporte técnico y seguridad.
- Establecer la inversión de cada estrategia de mejora.

1.4. Metodología

1.4.1. Tipos de investigación

1.4.1.1. Aplicada

Para los autores Villacís (2016) se refiere a un tipo de investigación que se lleva a cabo con el objetivo de resolver problemas específicos o aplicar los conocimientos adquiridos en la práctica. Este tipo de investigación se centrará en la búsqueda de soluciones prácticas y concretas para mejorar el proceso de soporte técnico y seguridad en GPSTracker S.A. Esto implicaría el diseño e implementación de intervenciones específicas basadas en las TIC.

1.4.1.2. Mixto

El enfoque mixto permitiría obtener una comprensión completa y rica del problema abordado, integrando perspectivas cualitativas y cuantitativas para informar la formulación de soluciones efectivas y pertinentes para mejorar el proceso de soporte técnico y seguridad en GPSTracker S.A.

1.4.2. Nivel de investigación

1.4.2.1. Descriptiva

Para Sánchez (2019) este nivel de investigación permite recopilar datos para crear una representación detallada y precisa del objeto de estudio. La investigación descriptiva se ajustará en comprender en detalle el estado actual del proceso de

soporte técnico y seguridad en la empresa. Esto incluirá la recopilación y análisis de datos sobre la eficacia del soporte técnico actual, la identificación de vulnerabilidades de seguridad existentes y la evaluación de la satisfacción del cliente con respecto al servicio recibido. Mediante encuestas, entrevistas y análisis de datos, este nivel de investigación proporcionará una descripción precisa y detallada de los problemas.

1.4.3. Ámbito y tiempo social de la investigación

1.4.3.1. Población

Condori (2020) define que es el conjunto completo de individuos que comparten una particularidad concreta. La población seleccionada presenta características finitas y estará conformada por los 4 trabajadores del área de soporte técnico y seguridad y de acuerdo con la base de datos de la empresa GPSTracker S.A será 68 clientes.

1.4.3.2. Muestra

Sampieri et al. (2018) postula que es un subconjunto representativo de la población para participar en la investigación. Baena (2017) afirma cuando el valor de la población es un valor manejable y no se necesita demasiados recursos para la selección se adopta la totalidad de la población. Este tipo de muestreo será no probabilístico por conveniencia, por lo tanto, se adopta 4 trabajadores y 68 clientes de la empresa GPSTracker S.A.

1.4.4. Técnicas e instrumentos de información

1.4.4.1. Técnicas

Para la investigación se utilizará la entrevista para obtener información detallada y perspectivas de los trabajadores de soporte técnico, al equipo de

seguridad de la información. Las entrevistas permitirán tener una comprensión más profunda de los desafíos actuales en el proceso de soporte técnico y seguridad, así como también de las áreas específicas que necesitan mejoras.

Asimismo, se manejará la encuesta para obtener una visión general y estadísticas sobre la percepción y experiencia de los clientes de GPSTracker S.A. en relación con el proceso de soporte técnico y seguridad. Esto permitirá recopilar datos de manera eficiente y llegar a un número significativo de participantes.

1.4.4.2. Instrumentos

Se utilizará la guía de entrevista estructurada y bien diseñada para garantizar que se obtenga la información relevante y necesaria durante la entrevista. La guía constará de ocho preguntas abiertas que será aplicada de forma presencial a los trabajadores en un día específico.

El cuestionario se manejará para conseguir información detallada y específica sobre aspectos particulares del proceso de soporte técnico y seguridad en la empresa. Se diseñará cuestionarios con 8 preguntas cerradas para recopilar datos cuantitativos sobre temas como la eficacia del soporte técnico, la percepción de la seguridad de los sistemas, la satisfacción del cliente, entre otros aspectos relevantes. El cuestionario se lo aplicará de forma online mediante Google Forms que será enviado a los correos electrónicos según la base de datos.

1.4.4.3. Validación de los instrumentos

La validación de instrumentos se refiere al proceso de evaluación de la idoneidad y fiabilidad de cualquier herramienta utilizada para recopilar datos en una investigación. La validación se realiza para asegurar que el instrumento sea capaz de medir de manera precisa y consistente lo que se pretende evaluar (Cartagen et al., 2022). Para medir la consistencia interna de un conjunto de ítems del instrumento se utilizará el método de juicio de tres expertos con dominio en las variables de estudio de esta investigación.

1.5. Justificación

1.5.1. Práctica

Encuentra una sólida justificación práctica en varios aspectos clave. En primer lugar, la optimización de recursos es crucial. Al implementar soluciones más eficientes y automatizadas, se puede reducir la carga de trabajo del personal de soporte y minimizar el tiempo y los recursos dedicados a la resolución de problemas técnicos y la gestión de incidentes de seguridad. Esto no solo aumentaría la productividad del equipo, sino que también permitiría una asignación más efectiva de recursos hacia otras áreas de la empresa.

Además, la mejora en la experiencia del cliente es un objetivo central. Un proceso de soporte técnico ágil y efectivo, respaldado por medidas sólidas de seguridad, contribuye directamente a mejorar la satisfacción del cliente. Los clientes de GPSTracker S.A. se beneficiarían de tiempos de respuesta más rápidos, soluciones efectivas a sus problemas y una mayor confianza en la seguridad de sus datos y sistemas. Esto no solo puede aumentar la lealtad del cliente, sino que también mejora la reputación de la empresa y su posición en el mercado.

1.6. Definiciones

1.6.1. Soporte técnico

Es el servicio proporcionado para ayudar a los usuarios a resolver problemas relacionados con equipos informáticos, software, redes u otros dispositivos tecnológicos. Incluye diagnóstico, reparación, mantenimiento y asistencia técnica para garantizar el funcionamiento adecuado (Paillacho, 2015).

1.6.2. Seguridad informática

Se refiere a la protección de los sistemas de información contra accesos no autorizados, ataques cibernéticos, pérdida de datos, y otros riesgos relacionados con la seguridad. Incluye medidas de prevención, detección y respuesta para garantizar la confidencialidad de la información (Ortiz, 2015).

1.6.3. Tecnologías de la Información y Comunicación (TIC)

Son el conjunto de herramientas, recursos y sistemas que permiten la adquisición, almacenamiento, procesamiento, transmisión y gestión de la información a través de tecnologías como computadoras, internet, telecomunicaciones, software y sistemas de información (Guzmán, 2022).

1.6.4. Eficiencia operativa

Es la capacidad de una empresa para maximizar el rendimiento de sus recursos y procesos, minimizando el desperdicio de tiempo, dinero y esfuerzo. Se refiere a la optimización de los procedimientos y la mejora continua de las actividades empresariales para lograr resultados óptimos (Paillacho, 2015).

1.6.5. Gestión de incidentes

Es el proceso utilizado para detectar, registrar, clasificar, investigar y resolver los incidentes de seguridad informática y otros problemas relacionados con la tecnología. Incluye la coordinación de respuestas y la restauración de la normalidad operativa después de un incidente (Villaverde, 2022).

1.6.6. Respaldo de datos

Es la acción de crear copias de seguridad de la información crítica de una empresa para protegerla contra la pérdida, corrupción o daño. Involucra la copia regular y el almacenamiento seguro de datos en ubicaciones externas, con el fin de garantizar su disponibilidad en caso de desastres o fallas (Molinetti, 2020).

1.6.7. Política de seguridad de la información

Es un conjunto de reglas, procedimientos, directrices y prácticas establecidas por una empresa para proteger la confidencialidad y disponibilidad de la información. Define las responsabilidades, seguridad y controles necesarios para mitigar los riesgos de seguridad informática (Parra, 2012).

1.6.8. Auditoría de seguridad

Es el proceso sistemático de evaluación y análisis de los controles de seguridad informática y el cumplimiento de las políticas. Involucra la revisión de registros, la identificación de vulnerabilidades y la recomendación de mejoras para fortalecer la seguridad de la información (Pinzón, 2020).

1.7. Alcances y limitaciones

1.7.1. Cobertura geográfica

La investigación se enfocará en la empresa GPSTracker S.A., ubicada en la ciudad de Guayaquil, Ecuador.

1.7.2. Cobertura sectorial

El trabajo de investigación se centrará en el sector de TIC, específicamente en el ámbito de servicios de soporte técnico y seguridad. La empresa GPSTracker S.A. opera en este sector y se especializa en proporcionar soluciones de seguimiento y seguridad basadas en tecnología.

1.7.3. Limitaciones

Es posible que ciertos datos sensibles o confidenciales estén restringidos, lo que podría dificultar el análisis exhaustivo de la situación actual y la identificación precisa de áreas de mejora. La aceptación y adopción de las mejoras propuestas por parte del personal de la empresa también podría ser una limitación.

Capítulo II Marco Teórico

2.1. Conceptualización de las variables

2.1.1. Soporte técnico

De acuerdo con Alvarado *et al.* (2021) “Se refiere al servicio proporcionado por expertos en tecnología para resolver problemas relacionados con el funcionamiento, configuración o mantenimiento de equipos, software o sistemas informáticos” (p. 230). La definición establece la base fundamental, destacando la función principal del soporte técnico en resolver problemas y brindar asistencia en el entorno tecnológico.

Zúñiga *et al.* (2021) describen que “El soporte implica la identificación y resolución anticipada de problemas potenciales antes de que afecten la operatividad del sistema, mediante el monitoreo continuo y la aplicación de medidas preventivas” (p. 456). La segunda definición introduce el concepto de proactividad, resaltando la importancia de anticiparse a los problemas y tomar medidas preventivas para garantizar un funcionamiento óptimo de los sistemas.

Finalmente, Di Luca (2019) sostiene que es la asistencia técnica que se brinda de manera no presencial, a través de herramientas de conexión remota, para diagnosticar, solucionar y mantener sistemas informáticos, reduciendo la necesidad de desplazamientos físicos y optimizando los tiempos de respuesta. Esta definición resalta la evolución del soporte técnico hacia modalidades remotas, subrayando cómo las herramientas tecnológicas han facilitado la prestación de este servicio de manera eficiente y oportuna, incluso sin la necesidad de presencia física.

El soporte técnico tiene varios objetivos clave que buscan garantizar el correcto funcionamiento de los sistemas tecnológicos y satisfacer las necesidades de los usuarios. Los autores Sacoto & Cordero (2021) plantea algunos de los objetivos son:

- Resolver problemas técnicos
- Mantener la operatividad
- Optimizar el rendimiento
- Proporcionar asistencia y capacitación
- Implementar medidas preventivas
- Recopilar feedback y mejorar servicios

Resolver problemas técnicos: El objetivo primordial del soporte técnico radica en la resolución efectiva de los problemas que puedan surgir en los sistemas informáticos, hardware o software. Esto implica la capacidad de diagnosticar con precisión las fallas, aplicar soluciones adecuadas y restaurar la funcionalidad normal de los equipos o sistemas afectados, garantizando así la continuidad de las operaciones empresariales (Reyes & Guevara, 2014).

Mantener la operatividad: Uno de los principales objetivos del soporte técnico es asegurar la continuidad operativa de los sistemas tecnológicos, minimizando cualquier tiempo de inactividad que pueda afectar la productividad de la empresa. Esto se logra mediante una respuesta rápida y eficiente a las incidencias, así como a través de estrategias proactivas de mantenimiento preventivo para prevenir fallos y maximizar el tiempo de funcionamiento (Tirado et al., 2017).

Optimizar el rendimiento: El objetivo de optimizar el rendimiento es mejorar la eficiencia de los sistemas tecnológicos, asegurando que operen de manera óptima y proporcionen el máximo valor a la empresa. Esto implica la implementación de ajustes de configuración, actualizaciones de software y hardware, así como la identificación y resolución de cuellos de botella que puedan afectar el rendimiento general del sistema (Tasa et al., 2021).

Proporcionar asistencia y capacitación: Además de resolver problemas técnicos, el soporte técnico también busca proporcionar asistencia personalizada a los usuarios, guiándolos en el uso adecuado de los sistemas y respondiendo a sus consultas y requerimientos específicos. Asimismo, se dedica a brindar capacitación y entrenamiento continuo para que los usuarios aprovechen las funcionalidades de los sistemas y mejorar su competencia tecnológica.

Implementar medidas preventivas: El objetivo de implementar medidas preventivas se centra en anticiparse a posibles problemas técnicos mediante la aplicación de parches de seguridad y la configuración de políticas de respaldo de datos efectivas. Esto ayuda a reducir la incidencia de fallos y vulnerabilidades de seguridad, protegiendo la información empresarial (Tirado et al., 2017).

Recopilar feedback y mejorar servicios: El soporte técnico busca constantemente recopilar comentarios y retroalimentación de los usuarios para identificar áreas de mejora y optimizar la calidad de los servicios proporcionados. Esto incluye evaluar la satisfacción del cliente, la revisión de métricas de rendimiento y la implementación de acciones correctivas y mejoras continuas en los procesos y procedimientos de soporte técnico (Alvarado et al., 2021).

2.1.1.1. Herramientas y tecnologías de soporte

Ayudan a desempeñar un papel crucial en la eficiencia y efectividad de la prestación de servicios. Estas herramientas abarcan una amplia gama de soluciones, desde software especializado hasta dispositivos de hardware, diseñados para diagnosticar, solucionar y gestionar problemas técnicos de manera rápida y precisa (Bravo, 2021).

Entre las herramientas más comunes se encuentran los sistemas de gestión de tickets, que permiten a los equipos de soporte técnico registrar, priorizar y dar seguimiento a las solicitudes de los usuarios de manera estructurada. Estos sistemas facilitan la asignación de recursos, el seguimiento del progreso y la generación de informes para evaluar el rendimiento del equipo de soporte. Otra categoría importante de herramientas son las soluciones de monitoreo remoto, que permiten supervisar el rendimiento y la salud de los sistemas informáticos en tiempo real. Estas herramientas pueden detectar anomalías, como fallos de hardware o picos de uso de recursos, y generar alertas automáticas para que los técnicos intervengan antes de que se produzcan problemas mayores (Bravo, 2021).

Además, las soluciones de acceso remoto son fundamentales para proporcionar asistencia técnica a distancia. Estas herramientas permiten a los técnicos acceder de forma segura a los sistemas de los usuarios desde cualquier ubicación, lo que agiliza el proceso de resolución de problemas y minimiza la necesidad de desplazamientos físicos (Cruz, 2019).

En cuanto a tecnologías emergentes, la inteligencia artificial (IA) y el aprendizaje automático están siendo cada vez más utilizados en el soporte técnico. Estas tecnologías pueden automatizar tareas repetitivas, como la clasificación de tickets o la resolución de problemas comunes, lo que libera tiempo para que los técnicos se enfoquen en casos más complejos y estratégicos.

2.1.1.2. Enfoques de soporte técnico

Hoy en día juega papel fundamental en las operaciones diarias, la prestación efectiva de servicios de soporte técnico se ha vuelto imprescindible para garantizar la continuidad operativa y la satisfacción de los usuarios. Sin embargo, la diversidad de necesidades y demandas en el ámbito tecnológico ha dado lugar a una variedad de enfoques en la prestación de servicios de soporte técnico. Desde el soporte en sitio tradicional hasta soluciones automatizadas de respuesta, cada enfoque ofrece ventajas y desafíos únicos que deben considerarse al diseñar estrategias de soporte técnico efectivas (Medrano & Quiñonez, 2021).

Se conceptualiza los distintos enfoques de prestación de servicios de soporte técnico, analizando sus características, beneficios y aplicaciones en diferentes contextos empresariales. Al comprender estas diferentes modalidades de soporte técnico, las organizaciones pueden tomar decisiones informadas para implementar el enfoque que se adapte a las necesidades específicas y mejorar así la experiencia del usuario y la eficiencia operativa en su entorno tecnológico. Los enfoques de prestación de servicios de soporte técnico pueden variar según las necesidades y características específicas de la organización. De acuerdo con Cruz *et al.* (2022) se manifiestan algunos de los enfoques más comunes:

- ***Soporte en sitio:***

  Este enfoque implica que los técnicos de soporte se desplacen físicamente al lugar donde se encuentra el equipo o el usuario que necesita asistencia. Es especialmente útil para problemas que requieren intervención directa, como la instalación de hardware o la solución de problemas de conectividad.

- ***Soporte remoto:***

  En este enfoque, los técnicos brindan asistencia a los usuarios de forma remota, a través de herramientas de acceso remoto. Esto permite resolver problemas sin necesidad de desplazamientos físicos, agilizando la respuesta y minimizando los tiempos de inactividad.

- ***Soporte por teléfono o chat:***

  En este enfoque, los usuarios pueden comunicarse con el equipo de soporte a través de llamadas telefónicas o chats en línea. Los técnicos proporcionan asesoramiento y solución de problemas en tiempo real, guiando a los usuarios para resolver sus incidencias de manera efectiva.

- ***Soporte automatizado:***

  Este enfoque hace uso de sistemas automatizados, como chatbots o sistemas de respuesta automática, para atender consultas y resolver problemas de forma autónoma. Los usuarios pueden recibir respuestas inmediatas a preguntas frecuentes o realizar procesos de resolución de problemas guiados por el sistema.

- ***Soporte proactivo:***

  Este enfoque se centra en la prevención de problemas antes de que ocurran. Los técnicos monitorean constantemente los sistemas en busca de posibles fallos o problemas de rendimiento, y toman medidas preventivas para evitar que se conviertan en incidencias mayores.

- ***Soporte especializado:***

  En este enfoque, los técnicos se especializan en áreas específicas de tecnología o en tipos particulares de equipos o software. Esto permite una atención más detallada y experta en casos complejos o situaciones que requieren conocimientos especializados.

Estos enfoques pueden combinarse o adaptarse según las necesidades y recursos disponibles para cada organización, esto con el objetivo de proporcionar un servicio de soporte técnico eficiente y satisfactorio para los usuarios. De esta forma garantizar la satisfacción y fidelidad.

2.1.1.3. Seguridad en el soporte técnico

Son medidas y prácticas diseñadas para proteger los sistemas informáticos, la información confidencial y la privacidad de los usuarios durante la prestación de servicios de soporte técnico. Esto implica asegurar que los técnicos de soporte tengan acceso autorizado y seguro a los sistemas y datos de la empresa, mientras se realizan actividades de diagnóstico, mantenimiento o resolución de problemas. Es un aspecto crítico que debe abordarse de manera integral para proteger tanto los sistemas

informáticos de la empresa como la información confidencial de los usuarios. Ampliar este tema implica considerar varios aspectos clave (Widjajarto et al., 2019).

Protección de datos sensibles: En el proceso de prestación de servicios de soporte, los técnicos pueden acceder a información confidencial de los usuarios o datos sensibles de la empresa. Es fundamental establecer procedimientos para garantizar la protección de estos datos, incluyendo medidas de encriptación y auditorías de acceso.

Gestión de accesos privilegiados: Los técnicos de soporte a menudo requieren acceso privilegiado a los sistemas y datos de la empresa para cumplir con sus responsabilidades. Es esencial implementar controles de acceso adecuados, como el principio de menor privilegio y la supervisión de actividades, para mitigar el riesgo de abuso o mal uso de estos privilegios (Peñafiel, 2021).

Seguridad en herramientas de acceso remoto: Las herramientas de acceso remoto son una parte integral del soporte técnico, pero también pueden representar un riesgo de seguridad si no se utilizan adecuadamente. Es crucial seleccionar herramientas seguras y cifradas para el acceso remoto, así como implementar medidas adicionales de autenticación y autorización para garantizar la confidencialidad de la conexión (Estrada et al., 2021).

Formación y concienciación de los empleados: La seguridad en el soporte técnico no solo se limita a los técnicos, sino que también involucra a los usuarios finales de los sistemas. Es importante proporcionar formación y concienciación sobre

prácticas de seguridad, como la creación de contraseñas seguras, la detección de intentos de phishing.

Gestión de incidentes de seguridad: A pesar de todas las medidas preventivas, es posible que ocurran incidentes en el entorno de soporte técnico. Contar con un plan de gestión de incidentes bien definido, que incluya la detección temprana, la respuesta rápida y la recuperación efectiva de los sistemas afectados para minimizar el impacto en la empresa y sus usuarios.

Al abordar estos aspectos de seguridad en el soporte técnico de manera integral, las organizaciones pueden mitigar riesgos y proteger sus activos digitales, asegurando la confianza y la continuidad operativa en un entorno tecnológico cada vez más complejo y amenazante (Machuca & Cabrera, 2020).

2.1.2. Seguridad informática

Avenía (2017) postula:

> La seguridad informática se refiere a las prácticas, herramientas y políticas diseñadas para proteger la integridad, confidencialidad y disponibilidad de los sistemas de información y datos. Esto implica la implementación de medidas preventivas y correctivas para mitigar riesgos relacionados con amenazas como intrusiones, malware, robo de datos y otros ataques cibernéticos (p. 28).

La definición ofrece una visión general adecuada de la seguridad informática al destacar la protección de la integridad de los datos. Sin embargo, podría ser más específica al mencionar las diversas capas de seguridad, como la seguridad física, la

seguridad de red y la seguridad de la aplicación, para brindar una comprensión más completa de los enfoques y medidas de seguridad necesarios. Además, aunque menciona la prevención y la corrección de riesgos, podría profundizar más en las estrategias específicas utilizadas para abordar amenazas emergentes, como la inteligencia aplicada a la seguridad y el análisis de comportamiento de usuario.

Para Molinetti (2020) plantea que es el proceso de gestionar los riesgos de seguridad en los sistemas de información de una organización. Esto incluye el desarrollo y la implementación de controles de seguridad, así como la asignación de recursos para proteger activos críticos y garantizar el cumplimiento de normativas y estándares de seguridad. La definición resalta la importancia de gestionar los riesgos de seguridad, lo cual es fundamental para una estrategia eficaz de seguridad informática. Además, podría abordar más a fondo la necesidad de integrar la seguridad informática en la planificación estratégica y la toma de decisiones, así como la importancia de la evaluación continua y la mejora de los controles de seguridad.

Según Bueno & Haz (2022) se refiere:

> A las medidas y prácticas destinadas a proteger los sistemas informáticos, redes y datos contra amenazas cibernéticas. Esto abarca la prevención, detección y respuesta a ataques, así como la protección de la privacidad y la integridad de la información. La ciberseguridad también implica la concientización y capacitación de los usuarios para promover una cultura de seguridad en toda la organización.

Esta definición destaca la protección de sistemas informáticos contra amenazas cibernéticas, lo cual es esencial en el panorama actual de ciberataques cada vez más sofisticados. Sin embargo, podría ampliar su alcance para incluir aspectos como la seguridad de la nube, la seguridad de dispositivos móviles y la protección de la infraestructura crítica, que son áreas de creciente preocupación en el ámbito de la ciberseguridad. Además, podría mencionar la importancia de la colaboración entre organizaciones, el sector público y privado en la lucha contra las amenazas cibernéticas, así como la necesidad de adaptarse rápidamente a la evolución del panorama de amenazas mediante la implementación de tecnologías emergentes y prácticas de seguridad innovadoras.

Las conceptualizaciones proporcionan una comprensión amplia y holística de la seguridad informática, abarcando aspectos como la protección de datos, la gestión de riesgos y la importancia de la concientización y la capacitación. La seguridad informática es fundamental en un entorno empresarial cada vez más dependiente de la tecnología, donde los riesgos cibernéticos pueden tener repercusiones graves en la continuidad del negocio y la reputación de la organización. Al comprender y aplicar conceptos como la gestión de la seguridad informática y la ciberseguridad, las empresas pueden fortalecer sus defensas y mitigar las amenazas en un entorno digital en constante evolución.

Los objetivos de la seguridad informática pueden variar según las necesidades específicas de cada organización. A continuación, se presentan algunos objetivos generales que suelen ser relevantes para la mayoría de las empresas según Coronel & Quirumbay (2022):

- Proteger la integridad de los datos: Garantizar que la información almacenada y procesada por los sistemas de información permanezca precisa, completa y no alterada por usuarios no autorizados o fallos técnicos.
- Preservar la confidencialidad de la información: Garantizar que solo las personas autorizadas tengan acceso a los datos confidenciales de la organización, evitando la divulgación no autorizada de información sensible.
- Asegurar la disponibilidad de los sistemas y datos: Garantizar que los sistemas de información estén disponibles y accesibles cuando se necesiten, minimizando el tiempo de inactividad y asegurando la continuidad del negocio.
- Prevenir y detectar intrusiones y ataques cibernéticos: Implementar medidas de seguridad para evitar intrusiones maliciosas en los sistemas de información, así como sistemas de detección.
- Cumplir con regulaciones y estándares de seguridad: Asegurar que la organización cumpla con las leyes, regulaciones y estándares de seguridad pertinentes, para proteger la información y la privacidad de los clientes y usuarios.
- Promover una cultura de seguridad: Fomentar la concienciación y la capacitación en seguridad informática entre los empleados y usuarios, promoviendo buenas prácticas de seguridad y comportamientos responsables en el uso de la tecnología.
- Optimizar la eficiencia: Implementar controles de seguridad que protejan los sistemas de información sin sacrificar la eficiencia operativa ni obstaculizar la productividad de los empleados.

- Gestionar y mitigar riesgos de seguridad: Gestionar proactivamente los riesgos de seguridad informática, implementando controles y medidas adecuadas para mitigar los riesgos identificados.

Los objetivos mencionados sirven como guía para desarrollar estrategias integrales de seguridad informática con la finalidad de proteger los activos de información de la empresa y garantice la confianza de su cartera de clientes, proveedores y socios comerciales.

2.1.2.1. Tendencias y desafíos actuales

En el dinámico panorama de la seguridad informática, es esencial mantenerse al tanto de desafíos emergentes que afectan a las organizaciones. En la última década, hemos presenciado un aumento significativo en la sofisticación y la frecuencia de los ciberataques, con tácticas cada vez más avanzadas empleadas por los actores malintencionados (Interpol, 2020).

El ransomware, por ejemplo, ha evolucionado de simples bloqueadores de pantalla a ataques de doble extorsión que comprometen datos sensibles y luego los cifran, exigiendo un rescate para su liberación. Además, el crecimiento de la internet ha ampliado la superficie de ataque, dando lugar a vulnerabilidades en dispositivos conectados que pueden ser explotadas por los ciberdelincuentes. Estas tendencias subrayan la necesidad de una estrategia de seguridad informática proactiva y adaptable, que se centre en la detección temprana, la respuesta rápida y la mitigación de riesgos (Vega, 2021).

2.1.2.2. Aspectos humanos de la seguridad

Si bien la tecnología desempeña un papel crucial en la protección de los sistemas de información, no se puede pasar por alto el papel fundamental de los aspectos humanos en la seguridad informática. Los empleados y usuarios finales son a menudo el eslabón más débil en la cadena de seguridad, ya que pueden ser susceptibles a la ingeniería social y otras tácticas de manipulación por parte de los ciberdelincuentes (Zuiga et al., 2024).

La concientización y la capacitación en seguridad informática son, por lo tanto, elementos esenciales de cualquier estrategia de seguridad efectiva. Esto implica educar a los empleados sobre las últimas amenazas cibernéticas, cómo reconocerlas y cómo responder adecuadamente ante ellas. Además, fomentar una cultura de seguridad puede ayudar a reducir el riesgo de incidentes de seguridad causados por errores humanos o comportamientos descuidados.

2.1.3. Gestión de incidentes

Para Bravo (2021) es el proceso de manejar y responder de manera efectiva a eventos no planificados o disruptivos que afectan la operación normal de una organización. Estos eventos, llamados incidentes, pueden ser cualquier evento que interrumpa los servicios, sistemas o procesos de una empresa y que pueda tener un impacto negativo en su funcionamiento, su seguridad, su reputación o sus resultados financieros.

La gestión de incidentes implica la identificación temprana, la evaluación, la respuesta y la resolución de estos incidentes de manera rápida y eficiente para minimizar su impacto y restaurar la operación normal de la organización lo más pronto posible. Esto puede incluir incidentes técnicos, como fallos de hardware o software, ciberataques, interrupciones del servicio, pérdida de datos, así como incidentes no técnicos, como emergencias físicas o problemas operativos (Guzmán, 2022).

El proceso de gestión de incidentes generalmente implica la implementación de procedimientos y protocolos definidos previamente para guiar la respuesta ante diferentes tipos de incidentes. Esto puede incluir la asignación de responsabilidades claras, la coordinación entre diferentes equipos y departamentos, la comunicación con las partes interesadas relevantes, la recopilación de información sobre el incidente y la documentación de las acciones tomadas y los resultados obtenidos. Los objetivos de la gestión de incidentes:

Minimizar el tiempo de inactividad: Durante el cual los servicios o sistemas críticos de una organización están fuera de servicio debido a un incidente. Esto se logra mediante una respuesta rápida y eficiente que permita restablecer la operación normal lo más pronto posible (Quirumbay et al., 2022).

Restaurar la operación normal: Restaurar la operación normal de la organización tan pronto como sea posible después de un incidente. Esto implica tomar las medidas necesarias para resolver el incidente, mitigar sus impactos y garantizar que los servicios y sistemas afectados vuelvan a funcionar de manera adecuada (Quirumbay et al., 2022).

Minimizar los impactos negativos: Otro objetivo importante de la gestión de incidentes es minimizar los impactos negativos de un incidente en la organización. Esto puede incluir la reducción de pérdidas financieras, la protección de la reputación de la empresa y la prevención de la pérdida de datos (Sarker et al., 2019).

Garantizar la continuidad del negocio: La gestión de incidentes busca garantizar la continuidad del negocio, asegurando que la organización pueda seguir operando de manera efectiva a pesar de los incidentes que puedan ocurrir. Esto implica implementar medidas de contingencia y planes de recuperación para minimizar el impacto de los incidentes (Paniagua et al., 2019).

Mejorar la resiliencia organizacional: La gestión de incidentes también tiene como objetivo mejorar la resiliencia organizacional, fortaleciendo la organización para anticipar, responder y recuperarse de los incidentes de manera efectiva. Esto se logra mediante la identificación de lecciones aprendidas y la implementación de mejoras en los procesos, sistemas y capacidades de respuesta (Quirumbay et al., 2022).

La gestión de incidentes es una función crítica para cualquier organización, en la protección de la operación normal, la reputación y los activos de la empresa. Una de las principales razones por las que la gestión de incidentes es tan importante radica en su capacidad para minimizar el tiempo de inactividad. Cuando ocurre un incidente, como un ciberataque o una interrupción del servicio, cada minuto cuenta. Una respuesta rápida y eficiente puede ayudar a restaurar la operación normal de la organización lo más pronto posible, minimizando así el impacto en la productividad.

Además de reducir el tiempo de inactividad, la gestión de incidentes también es crucial para proteger la reputación de la organización. En un mundo cada vez más

conectado y transparente. Una respuesta adecuada y transparente ante un incidente demuestra profesionalismo, responsabilidad y compromiso con la seguridad y el bienestar de los clientes, empleados y partes interesadas.

Otro aspecto importante de la gestión de incidentes es su papel en garantizar la continuidad del negocio. En situaciones adversas, como desastres naturales, ciberataques o interrupciones del servicio, es fundamental que una organización pueda seguir operando de manera efectiva. La gestión de incidentes permite identificar y responder rápidamente a las amenazas y vulnerabilidades, implementando medidas de contingencia y planes de recuperación para minimizar el impacto en las operaciones comerciales y asegurar la continuidad del negocio.

Al identificar y responder rápidamente a las amenazas y vulnerabilidades, se pueden minimizar los riesgos asociados con la pérdida de datos, el robo de información. Esto ayuda a proteger la integridad, la confidencialidad de los activos y los datos de la organización, garantizando su seguridad y su valor.

2.1.4. Tecnologías de la información (TIC)

Las TIC son herramientas que facilitan la adquisición, el almacenamiento, el procesamiento, la transmisión y el intercambio de información de manera digital. Comprenden una amplia gama de tecnologías y dispositivos, así como los servicios asociados que permiten la comunicación y el acceso a la información en entornos digitales (Vaca, 2016). Entre las principales componentes de se incluyen:

- **Hardware:** Se refiere a los dispositivos físicos utilizados para procesar, almacenar y transmitir datos, como computadoras personales, servidores, dispositivos móviles, routers, switches, entre otros.
- **Software:** Son los programas informáticos y aplicaciones que permiten realizar diversas tareas y procesos, como sistemas operativos, programas de procesamiento de texto.
- **Redes de comunicación:** Son las infraestructuras y tecnologías utilizadas para conectar dispositivos y sistemas entre sí, permitiendo la transmisión de datos y la comunicación.
- **Internet:** Es una red global de redes de comunicación que permite la interconexión de dispositivos y sistemas en todo el mundo.
- **Telecomunicaciones:** Se refiere a las tecnologías y servicios utilizados para transmitir información a través de largas distancias, como telefonía fija, telefonía móvil, transmisión de datos, videoconferencia, entre otros.

Las TIC desempeñan un papel fundamental en la sociedad moderna, transformando la manera en que las personas interactúan, trabajan, aprenden y se comunican. Además, tienen un impacto significativo en diversos sectores económicos, y la investigación científica (Bravo & Andrade, 2020). Las TIC han abierto nuevas oportunidades y desafíos, impulsando la innovación, la eficiencia y el crecimiento económico, pero también planteando cuestiones relacionadas con la privacidad, la seguridad, la accesibilidad y la brecha digital.

2.1.4.1. Impacto de las TIC en la sociedad y la economía

Las TIC han tenido un impacto transformador en la sociedad y la economía, facilitando la comunicación instantánea, el acceso a la información, la automatización de procesos y la creación de nuevos modelos de negocio. En el ámbito educativo, han ampliado el acceso a la educación y han transformado los métodos de enseñanza y aprendizaje. En el sector salud, han mejorado la atención médica, la gestión de datos y la investigación científica. En el comercio, han dado lugar al comercio electrónico y a nuevas formas de marketing y ventas. En la industria, han impulsado la automatización de procesos y la producción inteligente (Vargas, 2021).

A pesar de sus numerosos beneficios, las TIC también plantean desafíos y consideraciones éticas importantes. La privacidad y la seguridad de los datos, que son cada vez más vulnerables a violaciones y ciberataques; y el impacto ambiental, derivado de los recursos asociados con la producción y el uso de tecnología.

Las TIC continúan evolucionando a un ritmo acelerado, impulsadas por avances en inteligencia artificial, computación en la nube, internet de las cosas (IoT), realidad aumentada y virtual, entre otras tecnologías emergentes. El futuro de las TIC promete mayores niveles de conectividad, interacción y automatización, con el potencial de transformar aún más la sociedad y la economía en las próximas décadas.

2.2. Importancia de las variables

La importancia del proceso de soporte técnico y seguridad mediante las TIC radica en su papel primordial para garantizar el funcionamiento eficiente, seguro y continuo de los sistemas tecnológicos en las organizaciones. En la actualidad, donde la dependencia de la tecnología es cada vez mayor, el soporte técnico y la seguridad son elementos críticos para el éxito pero fundamentalmente para la competitividad de la empresa (Coronel & Quirumbay, 2022).

Ortiz (2015) recalca en primer lugar, el soporte técnico proporciona asistencia y soluciones rápidas a los problemas tecnológicos que puedan surgir, asegurando que las tareas se realicen de manera efectiva y minimizando los tiempos de inactividad. Esto no solo aumenta la productividad, sino que también mejora la satisfacción del cliente interno y externo, fortaleciendo la imagen de la empresa. Por otro lado, la seguridad en el contexto de las TIC es esencial para proteger la confidencialidad, de la información sensible. La implementación de medidas de seguridad adecuadas, como firewalls, sistemas de detección de intrusiones y políticas de acceso, ayuda a prevenir ataques cibernéticos, fugas de datos y otras amenazas, salvaguardando así los activos digitales y la reputación de la organización.

Además, Avenía (2017) resalta que en un entorno empresarial cada vez más regulado y sujeto a normativas de protección de datos, la seguridad en el soporte técnico se vuelve aún más crítica para garantizar el cumplimiento legal y evitar posibles sanciones y multas.

2.3. Análisis comparativo

Tabla 1

Análisis comparativo de soporte técnico y seguridad

Tópico	Autor	Definición	Comentario
Soporte técnico y seguridad	(Zuñiga et al., 2021)	Conjunto de procesos, herramientas y medidas implementadas para garantizar el funcionamiento óptimo de los sistemas tecnológicos, al tiempo que se protege la integridad, confidencialidad y disponibilidad de la información frente a amenazas y vulnerabilidades.	Las definiciones proporcionadas abordan distintos aspectos fundamentales del soporte técnico y la seguridad en el ámbito de las tecnologías de la información. Estas definiciones ofrecen una visión completa y equilibrada de la importancia y la complejidad del soporte técnico y la seguridad en el entorno empresarial actual, destacando su papel fundamental en la protección de activos digitales y el mantenimiento de la continuidad operativa.
	(Zevallos, 2019)	Servicio especializado que proporciona asistencia técnica especializada para resolver problemas complejos de hardware, software o redes informáticas, aplicando estrategias de diagnóstico avanzadas y soluciones especializadas.	
	(Alvarado et al., 2021)	Enfoque holístico que combina la gestión de riesgos, la implementación de políticas de seguridad, el monitoreo continuo y la respuesta efectiva a incidentes, con el objetivo de proteger los activos digitales y mitigar las amenazas cibernéticas.	

Nota. La tabla muestra tres definiciones de autores acerca del soporte técnico y seguridad.

Tabla 2

Análisis comparativo de TIC

Tópico	Autor	Definición	Comentario
TIC	(Pazmiño et al., 2020)	Conjunto de herramientas, plataformas y sistemas utilizados para brindar asistencia y resolver problemas relacionados con la infraestructura tecnológica de una organización.	Las definiciones desde la perspectiva del soporte técnico en la prestación de servicios fortalecen la seguridad de la información cada vez vulnerable a las amenazas cibernéticas. Las TIC abarcan múltiples herramientas que facilitan la resolución eficiente de problemas técnicos, permite diagnosticar, solucionar y prevenir incidencias de manera efectiva ante ataques y vulnerabilidades.
	(Castañeda et al., 2021)	Son las tecnologías y herramientas utilizadas para proteger los activos digitales de una organización contra amenazas, ataques y vulnerabilidades.	
	(Jurado et al., 2020)	Herramientas que permiten detectar, responder y recuperarse de eventos no planificados. Esto incluye sistemas de monitoreo de seguridad, alerta temprana, plataformas de gestión de incidentes y recuperación de datos.	

Nota. La tabla muestra tres definiciones de autores acerca de las TIC.

2.4. Análisis crítico

El proceso de soporte técnico y seguridad mediante las TIC es una pieza fundamental en la infraestructura tecnológica. Este proceso no solo se trata de solucionar problemas técnicos o garantizar la disponibilidad de los sistemas, sino que también implica salvaguardar la integridad y la confidencialidad de los datos, así como proteger los activos digitales contra amenazas cada vez más sofisticadas.

Un análisis crítico de este proceso revela varios aspectos importantes. En primer lugar, la complejidad creciente de los sistemas tecnológicos y el panorama de amenazas en constante evolución hacen que el soporte técnico y la seguridad sean tareas cada vez más desafiantes. La empresa debe estar preparada para enfrentar una amplia gama de riesgos, desde ataques cibernéticos hasta fallos de hardware, y deben contar con estrategias sólidas para mitigar estos riesgos de manera efectiva.

Además, el proceso de soporte técnico y seguridad debe adaptarse constantemente a los avances tecnológicos y a las nuevas tendencias en el ámbito de la ciberseguridad. Esto requiere una inversión continua en formación y capacitación del personal, así como en la adopción de herramientas y tecnologías innovadoras que permitan una detección temprana y una respuesta rápida ante posibles incidentes. Otro aspecto crítico es la importancia de encontrar un equilibrio entre la seguridad y la usabilidad. Si bien es fundamental implementar medidas de seguridad sólidas, estas no deben interferir con la productividad de los usuarios ni obstaculizar el acceso a los recursos necesarios para llevar a cabo sus tareas diarias. En este sentido, es crucial diseñar políticas y procedimientos que sean efectivos sin ser demasiado restrictivos.

Por último, el proceso de soporte técnico y seguridad debe ser visto como un esfuerzo colaborativo que involucre a todos los niveles de la organización. Todos tienen un papel que desempeñar en la protección de los activos digitales y la mitigación de los riesgos de seguridad. Esto requiere una cultura de seguridad sólida y un compromiso compartido con las mejores prácticas de ciberseguridad.

Capítulo III Marco Referencial

3.1. Reseña histórica

La empresa ecuatoriana, surge en el año 2018 con un enfoque innovador en el campo de la seguridad vehicular. Desde su inicio, se ha dedicado a brindar servicios tecnológicos especializados que tienen como objetivo principal prevenir situaciones en las que un vehículo pueda alejarse de las manos de su propietario (GPSTracker S.A, 2021).

Con un enfoque claro en la supervisión a distancia de sistemas electrónicos de seguridad, la empresa se ha destacado por su compromiso en ofrecer soluciones integrales para proteger los bienes de sus clientes. Entre los servicios ofrecidos se encuentran la instalación y mantenimiento de sistemas de alarma contra robos y contra incendios, así como la supervisión continua de estos sistemas para garantizar su correcto funcionamiento. Además de sus actividades de supervisión, la empresa también se ha involucrado en la venta de estos sistemas de seguridad, proporcionando a sus clientes la posibilidad de adquirir equipos de última generación para proteger sus vehículos y propiedades (GPSTracker S.A, 2021).

Desde su fundación en 2018, esta empresa ha logrado posicionarse como un referente en el mercado ecuatoriano, gracias a su enfoque centrado en la innovación tecnológica y su compromiso con la seguridad de sus clientes. Al ofrecer soluciones efectivas la convierten en una opción confiable para aquellos que buscan proteger sus activos de manera eficiente y efectiva (GPSTracker S.A, 2021).

3.2. Filosofía organizacional

3.2.1. Misión

Según el sitio web, “Nuestra misión es brindar servicios de calidad de rastreo satelital para vehículos y ofrecerles a nuestros comunicadores la mayor seguridad desde la pantalla de su celular” (GPSTraker S.A., 2021).

3.2.2. Visión

Según el sitio web, “Nuestro visón es ser una empresa reconocida a nivel nacional en la tecnología para la seguridad de vehículos, creando e innovando en nuestros productos y servicios para satisfacer las necesidades de nuestros clientes” (GPSTraker S.A., 2021).

3.2.3. Valores

- **Innovación tecnológica:** Nos comprometemos a mantenernos a la vanguardia de la tecnología para ofrecer soluciones de seguridad vehicular eficientes y efectivas.
- **Confianza y transparencia:** Valoramos la confianza de nuestros clientes y nos esforzamos por mantener una comunicación abierta y transparente en todas nuestras operaciones.
- **Compromiso con la seguridad:** Priorizamos la seguridad de nuestros clientes y sus bienes, trabajando incansablemente para prevenir situaciones de riesgo y proteger lo que más valoran.
- **Excelencia en el servicio:** Buscamos la excelencia en todo lo que hacemos, desde la instalación y mantenimiento de sistemas de seguridad hasta la atención al cliente y el soporte técnico.

- **Responsabilidad social y ambiental:** Nos comprometemos a operar de manera responsable, cuidando del medio ambiente y contribuyendo al desarrollo sostenible de las comunidades en las que operamos.

3.2.4. Objetivos de la empresa

- Desarrollar e implementar nuevas tecnologías que mejoren la eficacia y la fiabilidad de nuestros sistemas de seguridad vehicular.
- Expandir nuestra presencia en el mercado nacional, llegando a nuevos clientes y fortaleciendo relaciones con los existentes.
- Mejorar continuamente la calidad de nuestros servicios, garantizando la satisfacción del cliente en todo momento.
- Fomentar un ambiente de trabajo colaborativo y de crecimiento profesional para nuestro equipo, promoviendo el desarrollo personal y profesional de cada miembro.
- Contribuir activamente a la seguridad vial y la prevención del delito, mediante campañas de concienciación y colaboración con autoridades y organizaciones pertinentes.

3.2.5. Políticas de la empresa

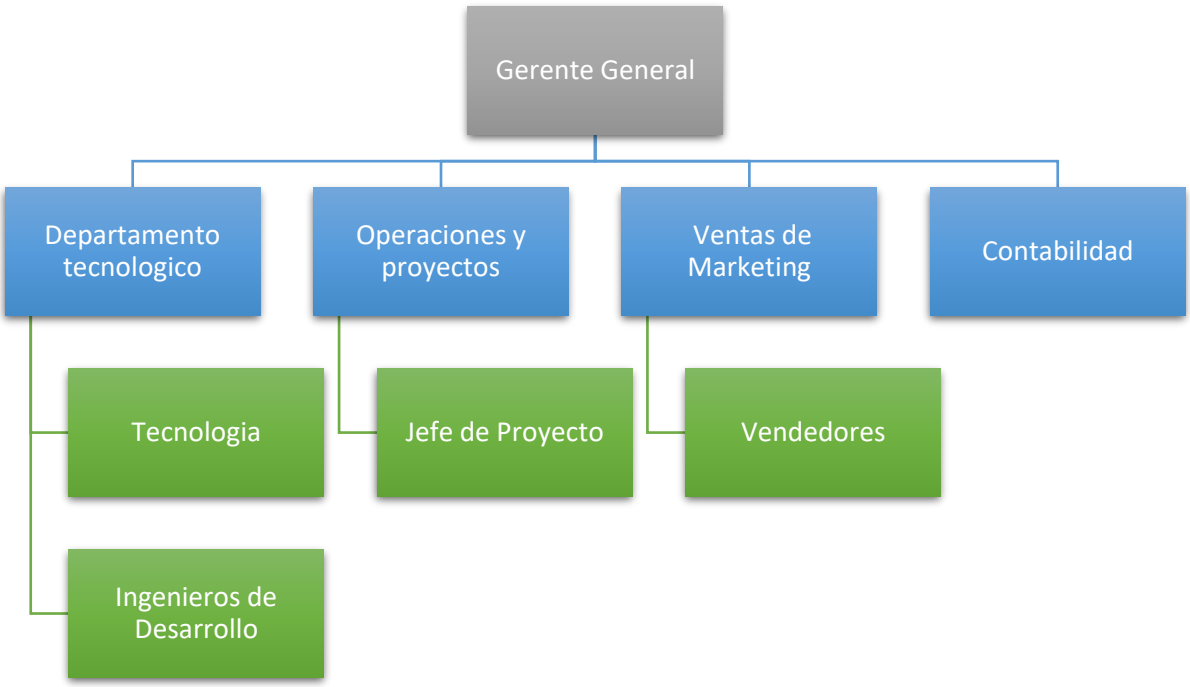
- **Cumplimiento legal:** Nos comprometemos a cumplir con todas las leyes y regulaciones aplicables en nuestras operaciones, garantizando la legalidad y la ética en todas nuestras acciones.
- **Calidad y seguridad:** Mantenemos altos estándares de calidad y seguridad en la instalación y mantenimiento de nuestros sistemas, asegurando la protección de nuestros clientes y la integridad de sus bienes.

- **Confidencialidad de la información**: Respetamos la privacidad y confidencialidad de la información de nuestros clientes, empleados y proveedores, protegiendo sus datos de acuerdo con las mejores prácticas de seguridad de la información.
- **Responsabilidad ambiental:** Adoptamos prácticas responsables en materia ambiental, minimizando nuestro impacto en el medio ambiente y promoviendo la sostenibilidad en todas nuestras actividades.
- **Atención al cliente:** Priorizamos la satisfacción del cliente en todo momento, ofreciendo un servicio personalizado y de alta calidad que supere sus expectativas y construya relaciones a largo plazo.

3.3. Diseño organizacional

Figura 1

Organigrama organizacional



Nota. Adaptado de organigrama de la empresa, por GPSTracker S.A., 2021.

Ingenieros de desarrollo:

Tienen la responsabilidad de diseñar, desarrollar, probar e implementar soluciones de seguridad y soporte. Diseñar arquitecturas de software eficientes, escribir código limpio y eficaz, realizar pruebas exhaustivas para garantizar la calidad y seguridad del producto y proporcionar soporte técnico.

Contabilidad:

Tiene la responsabilidad de gestionar y registrar las transacciones financieras de la empresa, mantener registros precisos de ingresos, gastos y activos, preparar informes financieros y cumplir con las obligaciones fiscales y regulatorias. Esto implica llevar a cabo actividades como la contabilidad general.

Jefe de proyecto:

Es responsable de planificar, coordinar y supervisar la ejecución de proyectos dentro de la organización para garantizar que se completen dentro del alcance, plazo, presupuesto y calidad definidos. Identificar y asignar recursos adecuados, establecer objetivos, desarrollar planes de trabajo detallados y gestionar riesgos.

Ventas y marketing:

Tiene la responsabilidad de promover los productos o servicios de la empresa, identificar y captar clientes potenciales, generar oportunidades de venta, cerrar acuerdos comerciales y mantener relaciones sólidas con los clientes existentes. Desarrollar estrategias de marketing y ventas, como campañas publicitarias, promociones y eventos, analizar datos y métricas para evaluar el rendimiento y optimizar las estrategias.

Gerente General:

Es responsable de dirigir y supervisar todas las operaciones y actividades de la organización para lograr los objetivos estratégicos y financieros de la empresa. Definir la visión, misión y objetivos de la empresa, desarrollar planes estratégicos y tácticos, tomar decisiones clave sobre inversiones, recursos y políticas, liderar y motivar al equipo directivo y empleados, representar a la empresa ante clientes, socios comerciales y partes interesadas externas.

3.4. Productos y/o servicios

3.4.1. Servicios

Según el sitio web, los servicios que oferta la empresa son:

Figura 2

Personal/Automóvil

Nota. Adaptado de Plan Corporativo, por GPSCRAKET S.A., 2021, (https://cartrack.ec/plan-personal-automovil/).

El servicio personal automóvil permite la conexión de datos, acceder a plataforma de monitoreo a través del computador y aplicaciones IOS y Android que permiten ubicar al automóvil en tiempo real mediante funciones de rastreo y monitoreo, historial y reportes de viajes.

Figura 3

Corporativo para flotas

Nota. Adaptado de Plan Corporativo, por GPSCRAKET S.A., 2021, (https://cartrack.ec/plan-coorporativo-flota-inteligente/)

El corporativo para flotas permite localizar el automóvil en tiempo real mediante funciones de seguimiento y monitoreo, así como acceder a historiales y reportes de viajes. Además, ofrecen características como la configuración de geocercas, alertas de seguridad, monitoreo de la eficiencia de la conducción y la posibilidad de activar un botón de pánico en caso de emergencia.

Figura 4

Corporativo MDVR

Nota. Adaptado de Plan Corporativo, por GPSCRAKET S.A., 2021, (https://cartrack.ec/plan-corporativo-mdvr/)

MDVR, un dispositivo móvil de grabación de video digital está específicamente creado para la vigilancia de vehículos y la supervisión remota. Equipado con un potente procesador y un sistema operativo integrado, se integra con tecnología

avanzada de compresión de video H.264, conectividad de red, seguimiento GPS y la capacidad de monitoreo remoto en tiempo real.

3.5. Diagnóstico organizacional

Tabla 3

FODA de la empresa GPSTracker S.A.

Fortalezas	Oportunidades
• Tecnología innovadora • Experiencia y conocimiento Especializado • Servicio integral • Compromiso con la calidad y la seguridad • Atención personalizada a los clientes	• Expansión del mercado nacional e internacional • Desarrollo de nuevos productos y servicios • Colaboración con fabricantes de vehículos • Alianzas estratégicas con compañías de seguros • Diversificación de mercados verticales
Debilidades	**Amenazas**
• Falta de personal especializado en soporte técnico. • Baja capacitación en seguridad informática • Falta de procedimientos de respuesta a incidentes claros. • Dependencia excesiva de proveedores externos para la seguridad de los sistemas.	• Competencia agresiva • Rápida evolución tecnológica • Ciberataques y vulnerabilidades de seguridad • Cambios en la legislación y normativas

Nota. La tabla muestra el FODA de la empresa GPSTracker S.A

3.5.1. Análisis de las fortalezas

- **Tecnología innovadora:** La capacidad de la empresa para desarrollar y aplicar tecnología innovadora en el campo de la seguridad vehicular es una ventaja significativa. Esta fortaleza asegura que la empresa esté a la vanguardia de las soluciones de seguridad, lo que le proporciona una ventaja competitiva en un mercado que demanda constantemente soluciones avanzadas y efectivas.

- **Experiencia y conocimiento especializado:** La experiencia y el conocimiento especializado del equipo son fundamentales para la calidad de los servicios ofrecidos. Esta fortaleza garantiza que la empresa pueda abordar los desafíos específicos de cada proyecto con confianza y eficiencia, lo que se traduce en la satisfacción del cliente y en relaciones comerciales sólidas a largo plazo.

- **Servicio integral:** La capacidad de ofrecer un servicio integral, que abarca desde la evaluación inicial de riesgos hasta el mantenimiento continuo de los sistemas instalados, proporciona un valor adicional significativo a los clientes. Esta fortaleza demuestra el compromiso con la seguridad completa y la tranquilidad del cliente, lo que puede resultar en una mayor fidelidad y recomendaciones positivas.

- **Compromiso con la calidad y la seguridad:** El compromiso con la calidad y la seguridad en todas las operaciones es una ventaja crucial para la reputación y la credibilidad de la empresa. Esta fortaleza garantiza que los clientes confíen en la fiabilidad y eficacia de los sistemas de seguridad ofrecidos, lo que puede resultar en una mayor demanda y una posición sólida en el mercado.

- **Atención al cliente:** La capacidad de ofrecer un servicio de atención al cliente personalizado y de alta calidad es una fortaleza clave para construir relaciones sólidas con los clientes. Esta atención al cliente excepcional no solo mejora la satisfacción del cliente, sino que también puede generar lealtad a la marca y referencias positivas, lo que contribuye al crecimiento y éxito continuo de la empresa.

3.5.2. Análisis de las oportunidades

- **Expansión del mercado nacional e internacional:** A medida que aumenta la conciencia sobre la importancia de la seguridad vehicular, especialmente en regiones con altas tasas de delincuencia, la demanda de servicios de seguridad tecnológica está en aumento.

- **Desarrollo de nuevos productos y servicios:** Existe la oportunidad de desarrollar nuevos productos y servicios innovadores que puedan satisfacer las necesidades emergentes del mercado. Esto podría incluir soluciones de seguridad personalizadas para segmentos específicos de clientes, como flotas de vehículos comerciales o vehículos de lujo, así como la integración de tecnologías emergentes como la inteligencia artificial en los sistemas de seguridad existentes.

- **Colaboración con fabricantes de vehículos:** La empresa podría explorar oportunidades de colaboración con fabricantes de vehículos para integrar sus soluciones de seguridad directamente en los vehículos durante el proceso de fabricación. Esto no solo aumentaría la visibilidad y la accesibilidad de los productos de la empresa, sino que también podría mejorar la seguridad de los vehículos desde el momento en que salen de la fábrica.

- **Alianzas estratégicas:** La empresa podría establecer alianzas estratégicas con compañías de seguros para ofrecer beneficios a los clientes que instalen sus sistemas de seguridad. Esto no solo aumentaría la demanda de los servicios, sino que también proporcionaría a los clientes un incentivo adicional para invertir en seguridad.

- **Diversificación de mercados verticales:** Además del mercado de consumo, la empresa podría explorar oportunidades en mercados verticales como el transporte público, la logística y la seguridad industrial. Estos sectores pueden tener necesidades específicas de seguridad vehicular que la empresa podría abordar con soluciones personalizadas y adaptadas a sus requerimientos únicos.

3.5.3. Análisis de las debilidades

- **Falta de personal especializado en soporte técnico:** La empresa puede enfrentar dificultades en soporte técnico. Esta debilidad puede llevar a retrasos en la resolución de problemas técnicos de los clientes, lo que afecta negativamente la satisfacción del cliente.

- **Baja capacitación en seguridad informática:** Si el equipo no está adecuadamente capacitado en seguridad informática, podría resultar en vulnerabilidades en los sistemas internos de la empresa. Esto podría exponer datos confidenciales a riesgos de ciberseguridad.

- **Falta de procedimientos de respuesta a incidentes claros:** Podría dificultar la capacidad de la empresa para manejar eficazmente situaciones de emergencia, como intrusiones cibernéticas o violaciones de datos. La falta de un plan de acción estructurado podría aumentar el tiempo de inactividad en la operación del negocio y la confianza del cliente.

- **Dependencia excesiva de proveedores externos para la seguridad de los sistemas:** Si la empresa depende en exceso de proveedores externos para la

seguridad de sus sistemas, podría enfrentar riesgos relacionados con la confiabilidad y la calidad del servicio. La falta de control directo sobre los procesos de seguridad podría dejar a la empresa vulnerable a fallos en la protección de datos y a posibles interrupciones del servicio debido a problemas con terceros

3.5.4. Análisis de las amenazas

- **Competencia agresiva:** La competencia en el mercado de seguridad vehicular puede ser intensa, con la presencia de grandes empresas consolidadas y nuevas startups emergentes. La entrada de competidores agresivos que ofrecen soluciones similares a precios más bajos o con tecnología más avanzada podría erosionar la cuota de mercado y reducir los márgenes de beneficio de la empresa.

- **Ciberataques y vulnerabilidades de seguridad:** Dado que la empresa trabaja con sistemas tecnológicos y datos sensibles, está expuesta a amenazas cibernéticas como piratería informática, robo de datos y ataques de malware. Una violación de seguridad podría tener consecuencias devastadoras para la empresa, incluida la pérdida de la confianza del cliente, daños a la reputación y sanciones legales.

- **Cambios en la legislación y normativas:** Pueden afectar significativamente las operaciones de la empresa. Nuevas regulaciones más estrictas podrían imponer costos adicionales de cumplimiento y requisitos de seguridad más rigurosos, lo que podría impactar en la rentabilidad de los servicios ofrecidos por la empresa.

Capítulo IV Resultados

4.1. Diagnóstico del proceso de soporte técnico y seguridad actual

En el marco de esta propuesta de mejora para el proceso de soporte técnico y seguridad en GPSTracker S.A., se llevará a cabo un exhaustivo diagnóstico utilizando herramientas específicas para obtener una visión detallada de la situación actual. Este diagnóstico se realizará mediante la aplicación de tres instrumentos clave: el árbol de problemas, un cuestionario y una guía de entrevista. Estos instrumentos han sido seleccionados estratégicamente para proporcionar una comprensión integral de las deficiencias en el proceso de soporte técnico y seguridad.

El árbol de problemas será fundamental para visualizar de manera gráfica las interrelaciones y causas raíz de los desafíos identificados en el planteamiento del problema. A través de esta herramienta, se podrá identificar de manera clara y sistemática las áreas específicas que requieren intervención y mejora. Complementando esta metodología, se aplicará un cuestionario a los trabajadores del área de soporte técnico y seguridad, y a los clientes, para obtener datos cuantitativos y cualitativos que respalden la evaluación del estado actual del servicio. Además, se utilizará una guía de entrevista estructurada para obtener percepciones más profundas de los trabajadores, permitiendo explorar aspectos específicos que pueden no ser evidentes mediante otras herramientas.

La combinación de estos instrumentos permitirá una evaluación comprehensiva, identificando no solo los síntomas evidentes, sino también las causas subyacentes de los desafíos en el proceso de soporte técnico y seguridad. Este enfoque analítico nos proporcionará la base necesaria para proponer soluciones

estratégicas que aborden de manera efectiva los problemas identificados, garantizando una mejora sostenible y la satisfacción tanto del personal en la empresa como de todos los clientes.

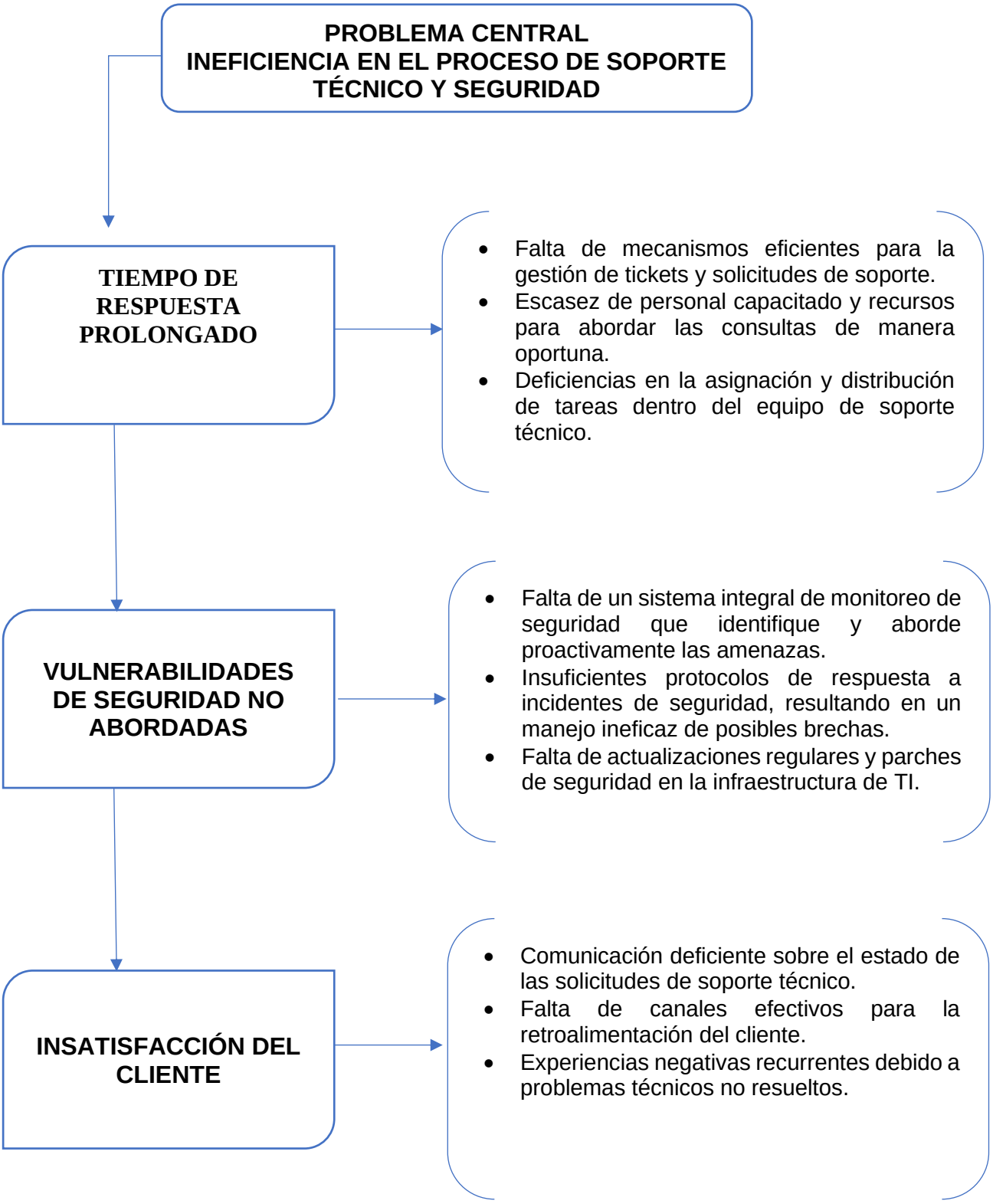
Los principales problemas evidenciados en el proceso de soporte técnico y seguridad de GPSTracker S.A. incluyen tiempos de respuesta prolongados, vulnerabilidades de seguridad no abordadas adecuadamente y una insatisfactoria experiencia del cliente. La implementación de tecnologías de la información y comunicación (TIC) no ha logrado superar eficazmente estas deficiencias, afectando la eficiencia operativa y generando un riesgo potencial para la seguridad de los sistemas y la satisfacción del cliente.

La lentitud en los tiempos de respuesta puede derivar en una disminución de la calidad del servicio, afectando la satisfacción del cliente y potencialmente resultando en la pérdida de clientes frente a competidores con un soporte más eficiente. Las vulnerabilidades de seguridad no tratadas adecuadamente exponen a la empresa y a sus clientes a riesgos cibernéticos significativos, como brechas de seguridad y robo de datos, lo que podría afectar la reputación de la empresa y generar costos financieros importantes. La experiencia general del cliente se ve afectada negativamente, lo que puede llevar a la pérdida de confianza en los servicios ofrecidos por GPSTracker S.A. Estos problemas subrayan la necesidad crítica de una mejora integral en el proceso de soporte técnico y seguridad mediante la implementación de estrategias basadas en las TIC.

4.1.1. Presentación del árbol de problemas

Figura 5

Causa efecto – árbol de problemas



Los resultados obtenidos a partir del análisis del árbol de problemas proporcionan una visión profunda de las deficiencias en el proceso de soporte técnico y seguridad en GPSTracker S.A. Este ejercicio reveló que el tiempo de respuesta prolongado, identificado como un problema central, tiene raíces en la falta de mecanismos eficientes para la gestión de tickets y solicitudes. La escasez de personal capacitado y recursos adecuados, junto con deficiencias en la asignación de tareas, contribuye a la demora en la atención de las consultas, generando insatisfacción entre los usuarios.

En relación con las vulnerabilidades de seguridad no abordadas, el análisis del árbol de problemas reveló que la falta de un sistema integral de monitoreo de seguridad y protocolos ineficaces de respuesta a incidentes son causas fundamentales. Asimismo, la insuficiencia en la implementación de actualizaciones y parches de seguridad en la infraestructura de TI contribuye a la exposición de la empresa y sus clientes a riesgos cibernéticos. La insatisfacción del cliente, otro problema identificado, se vincula a la falta de comunicación efectiva sobre el estado de las solicitudes y la carencia de canales adecuados para la retroalimentación del cliente. Las experiencias negativas recurrentes, derivadas de problemas técnicos no resueltos, contribuyen a una percepción general negativa de los servicios proporcionados por la empresa.

En resumen, los resultados del árbol de problemas resaltan la interconexión de los problemas, indicando que la ineficiencia en el tiempo de respuesta y las vulnerabilidades de seguridad afectan directamente la satisfacción del cliente. La falta de procesos estructurados, recursos suficientes y una estrategia integral de seguridad

informática subyacen a estos problemas. Este análisis se presenta como una herramienta valiosa para la formulación de estrategias de mejora, ya que identifica las causas raíz que deben abordarse para lograr una transformación efectiva en el proceso de soporte técnico y seguridad.

Los resultados del análisis del árbol de problemas proporcionan una base sólida para la formulación de soluciones efectivas en el proceso de soporte técnico y seguridad de GPSTracker S.A. Al identificar las causas raíz de los problemas, como la falta de mecanismos eficientes de gestión de tickets y la escasez de recursos capacitados, se abre la puerta para diseñar estrategias que aborden estas deficiencias específicas. La propuesta de mejora puede enfocarse en la implementación de sistemas avanzados de gestión de tickets, así como en la capacitación y asignación eficiente de personal, con el objetivo de reducir significativamente los tiempos de respuesta y mejorar la satisfacción del cliente.

Además, al comprender a fondo las vulnerabilidades de seguridad identificadas, como la falta de un sistema integral de monitoreo y protocolos ineficaces de respuesta a incidentes, la propuesta puede incluir medidas específicas para fortalecer la seguridad informática de la empresa. Esto puede abarcar desde la implementación de soluciones avanzadas de monitoreo de seguridad hasta la revisión y mejora de los protocolos de respuesta a incidentes, garantizando así una mayor protección contra amenazas cibernéticas. En conjunto, los resultados del árbol de problemas guían directamente hacia áreas de enfoque estratégico, proporcionando una hoja de ruta clara para la implementación de soluciones que mejoren la eficiencia operativa, la seguridad de los sistemas y la experiencia del cliente.

4.1.2. Presentación de la guía de entrevista

En el marco de la investigación para mejorar el proceso de soporte técnico y seguridad en la empresa GPSTracker S.A., se presentan a continuación las preguntas que fueron incluidas en la guía de entrevista. Estas preguntas han sido diseñadas con el objetivo de obtener información detallada y perspectivas clave de los trabajadores involucrados en el proceso, así como para recopilar la percepción de los clientes sobre la calidad de los servicios proporcionados.

1) *¿Cómo describiría la eficiencia actual en la gestión de tickets y solicitudes de soporte en* GPSTracker S.A.*?*
2) *¿Cuáles son los principales desafíos que enfrenta el equipo de soporte técnico en términos de tiempos de respuesta y atención oportuna?*
3) *¿Cómo evaluaría la seguridad de la información en la infraestructura actual de* GPSTracker S.A.*?*
4) *¿Cuáles son las prácticas actuales de respuesta a incidentes de seguridad y cómo se abordan las vulnerabilidades detectadas?*
5) *¿Desde la perspectiva de los clientes, cómo describirían la calidad del soporte técnico que reciben?*
6) *¿Se han recibido comentarios específicos de los clientes sobre problemas técnicos no resueltos o insatisfacción con los servicios?*
7) ¿Cómo se distribuyen actualmente las tareas y responsabilidades dentro del equipo de soporte técnico en GPSTracker S.A.?
8) ¿Cuáles son los recursos disponibles para abordar solicitudes de soporte y garantizar la seguridad de los sistemas?

4.1.2.1. Presentación de los resultados de la guía de entrevista

La aplicación de la guía de entrevista a los trabajadores de GPSTracker S.A. ha arrojado una luz esclarecedora sobre la complejidad de los desafíos que enfrenta la empresa en cuanto al proceso de soporte técnico y seguridad. Los resultados obtenidos revelan una serie de problemas interrelacionados que abarcan desde la gestión de tickets hasta la protección de la información confidencial.

En primer lugar, se destaca la limitación en la eficiencia del proceso de gestión de tickets y solicitudes de soporte. Este aspecto crítico se ve exacerbado por la falta de personal capacitado y la distribución desigual de tareas, lo que conlleva a demoras significativas en la resolución de problemas y a una atención inconsistente a las solicitudes de los clientes. La sobrecarga de trabajo experimentada por algunos miembros del equipo de soporte técnico impacta negativamente en la capacidad del equipo para ofrecer un servicio rápido y efectivo.

Asimismo, la preocupación por la seguridad de la información emerge como un tema central en las entrevistas. Los empleados expresan inquietudes sobre la efectividad de los protocolos de seguridad y el monitoreo de posibles vulnerabilidades en los sistemas. Esta percepción de vulnerabilidad no solo afecta la confianza interna en los procesos de la empresa, sino que también genera preocupaciones entre los clientes sobre la protección de sus datos sensibles.

La insatisfacción de los clientes con respecto a la calidad del soporte técnico es evidente en los comentarios recopilados durante las entrevistas. Los tiempos de respuesta prolongados y los problemas técnicos recurrentes son fuentes constantes

de frustración para los usuarios, lo que lleva a una disminución en la percepción de la calidad de los servicios proporcionados por GPSTracker S.A. Esta insatisfacción puede tener consecuencias graves para la retención de clientes y la reputación de la empresa en el mercado.

En resumen, los resultados de la guía de entrevista subrayan la necesidad urgente de abordar los problemas identificados en el proceso de soporte técnico y seguridad de GPSTracker S.A. para mejorar la eficiencia operativa, fortalecer la confianza del cliente y mantener la competitividad en el mercado. Estos hallazgos proporcionan una base sólida para el diseño e implementación de estrategias de mejora que aborden de manera integral los desafíos identificados y promuevan un ambiente de trabajo más efectivo y seguro para todos los involucrados.

En los anexos de la investigación se presentarán detalladamente los resultados obtenidos en cada entrevista realizada con los trabajadores de GPSTracker S.A. Estos anexos proporcionarán una visión exhaustiva de las percepciones, opiniones y experiencias compartidas por el personal de la empresa en relación con el proceso de soporte técnico y seguridad. Cada entrevista será documentada de manera individual, ofreciendo así una representación completa y transparente de los datos recopilados durante el estudio. Esta inclusión permitirá a los lectores profundizar en la comprensión de los desafíos identificados y en la evaluación de las áreas de mejora sugeridas, enriqueciendo así el análisis y las conclusiones de la investigación.

4.1.3. Presentación del cuestionario

1. En términos de soporte técnico, ¿cómo describiría su experiencia general con GPSTracker S.A.?

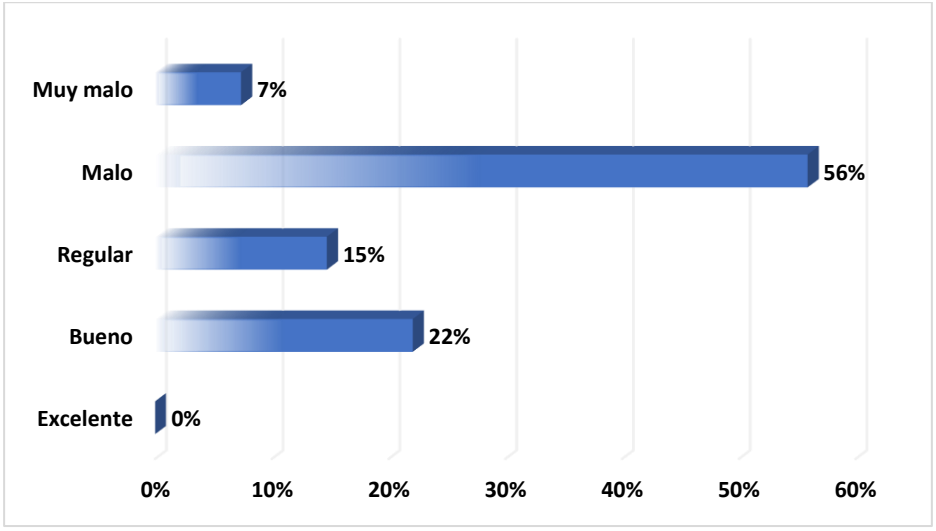
Tabla 4

Experiencia general con GPSTracker S.A.

Respuesta	Muestra	Resultado
Excelente	0	0%
Bueno	15	22%
Regular	10	15%
Malo	*38*	56%
Muy malo	5	7%
TOTAL	**68**	**100%**

Figura 6

Experiencia general con GPSTracker S.A.



El análisis de los resultados de la pregunta 1, que indaga sobre la experiencia general de los clientes con el soporte técnico de GPSTracker S.A., revela una situación preocupante. El 56% de los encuestados califica la experiencia como "mala", mientras que un 22% la describe como "buena". Este alto porcentaje de respuestas negativas indica una percepción generalizada de insatisfacción por parte de los clientes en relación con el servicio de soporte técnico.

2. ¿Ha experimentado demoras significativas en la resolución de problemas o solicitudes de soporte?

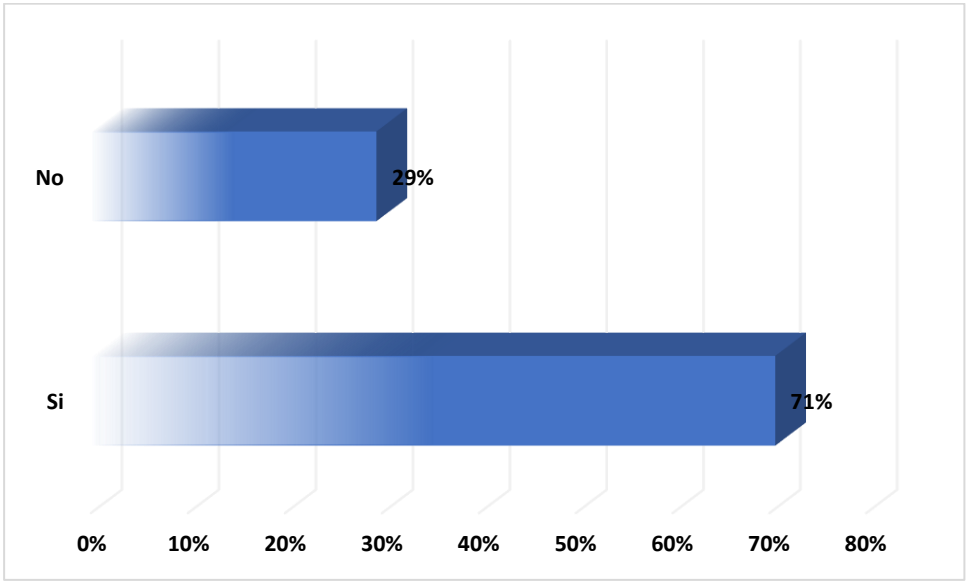
Tabla 5

Demoras significativas en la resolución de problemas

Respuesta	Muestra	Resultado
Si	48	71%
No	20	29%
TOTAL	**68**	**100%**

Figura 7

Demoras significativas en la resolución de problemas



El análisis de los resultados de la pregunta 2, que aborda la existencia de demoras significativas en la resolución de problemas o solicitudes de soporte, refleja una preocupante realidad para GPSTracker S.A. Un impresionante 71% de los clientes ha experimentado demoras en la atención de sus solicitudes, mientras que solo un 29% reporta no haber enfrentado este problema. Este hallazgo destaca una clara necesidad de mejora en los tiempos de respuesta del equipo de soporte técnico.

3. ¿Ha enfrentado problemas técnicos recurrentes al utilizar los servicios de GPSTracker S.A.?

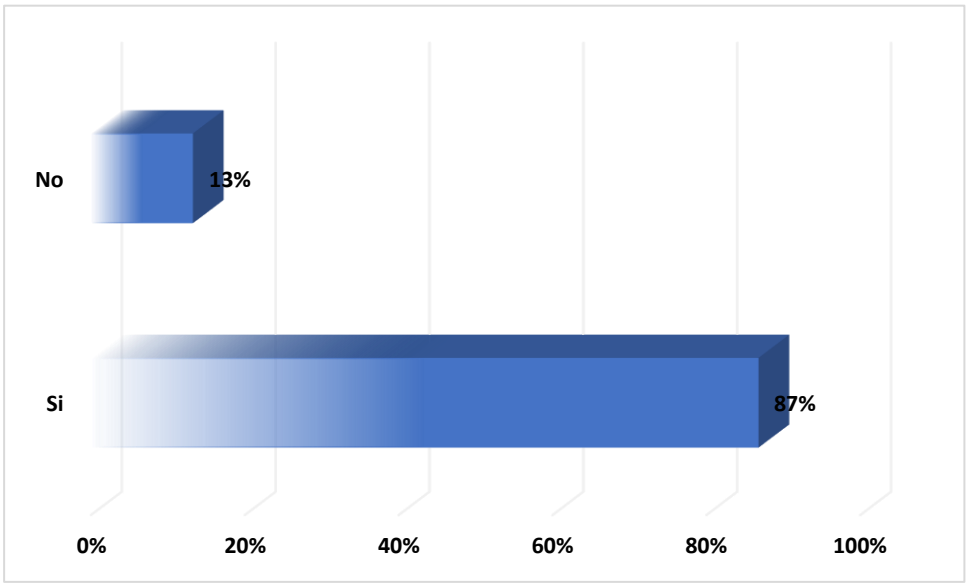
Tabla 6

Problemas técnicos recurrentes

Respuesta	Muestra	Resultado
Si	59	87%
No	9	13%
TOTAL	**68**	**100%**

Figura 8

Problemas técnicos recurrentes



El análisis de los resultados de la pregunta 3, que explora la presencia de problemas técnicos recurrentes entre los clientes de GPSTracker S.A., revela una situación preocupante. Un abrumador 87% de los encuestados informa haber enfrentado problemas técnicos de forma recurrente, mientras que solo un 13% afirma no haber experimentado tales inconvenientes. Esta alta incidencia de problemas técnicos señala deficiencias sustanciales en la estabilidad y confiabilidad de los servicios proporcionados.

4. En su opinión, ¿cómo evaluaría la seguridad de la información proporcionada por GPSTracker S.A.?

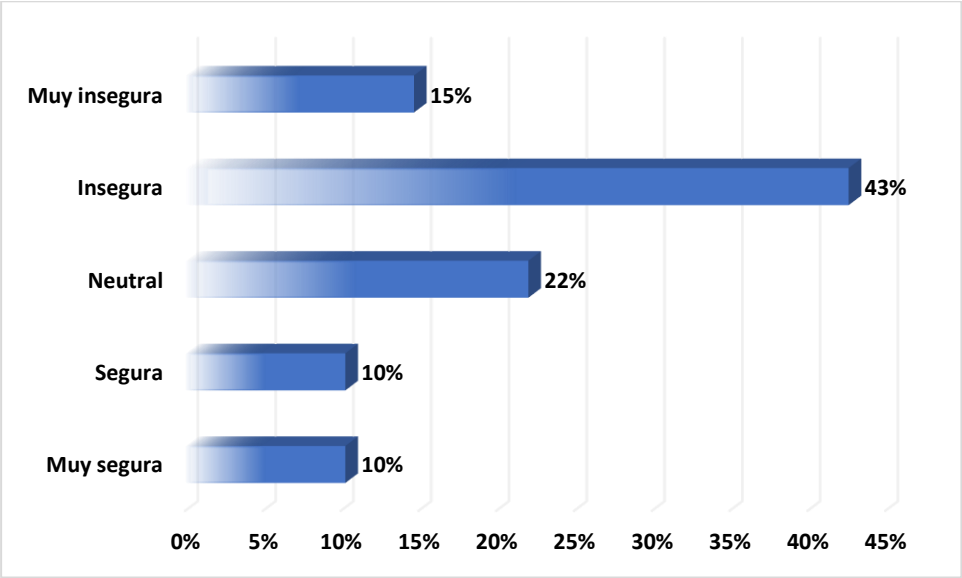
Tabla 7

Seguridad de la información proporcionada

Respuesta	Muestra	Resultado
Muy segura	7	10%
Segura	7	10%
Neutral	15	22%
Insegura	29	43%
Muy insegura	10	15%
TOTAL	**68**	**100%**

Figura 9

Seguridad de la información proporcionada



El análisis de los resultados de la pregunta 4, relacionada con la evaluación de la seguridad de la información proporcionada por GPSTracker S.A., pone de manifiesto una preocupante percepción entre los clientes. Más del 50% de los encuestados califica la seguridad como "insegura" o "muy insegura", distribuyéndose entre un 43% y un 15%, respectivamente. Solo un 20% la considera "muy segura" o "segura".

5. ¿Ha expresado previamente sus preocupaciones o comentarios sobre problemas técnicos no resueltos o insatisfacción con los servicios de soporte técnico.?

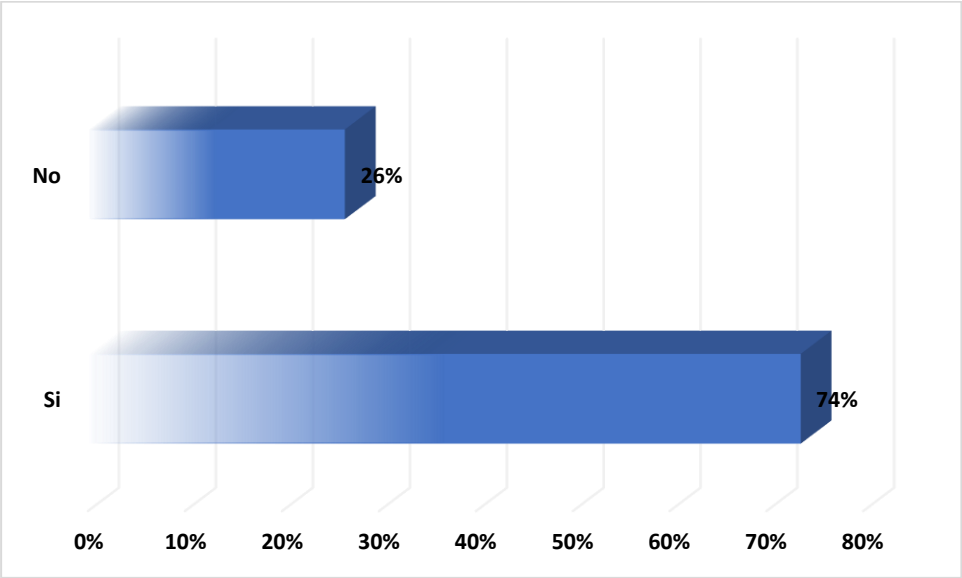
Tabla 8

Preocupaciones o comentarios sobre problemas

Respuesta	Muestra	Resultado
Si	50	74%
No	18	26%
TOTAL	**68**	**100%**

Figura 10

Preocupaciones o comentarios sobre problemas



El análisis de los resultados de la pregunta 5, que indaga sobre si los clientes han expresado previamente sus preocupaciones o comentarios sobre problemas técnicos no resueltos o insatisfacción con los servicios de soporte técnico, destaca una tendencia preocupante. Un considerable 74% de los encuestados ha expresado sus inquietudes, mientras que solo un 26% afirma no haberlo hecho. Estos hallazgos señalan una comunicación activa por parte de los clientes sobre las deficiencias en el soporte técnico y la insatisfacción experimentada.

6. ¿Cómo calificaría la comunicación recibida durante el proceso de soporte técnico?

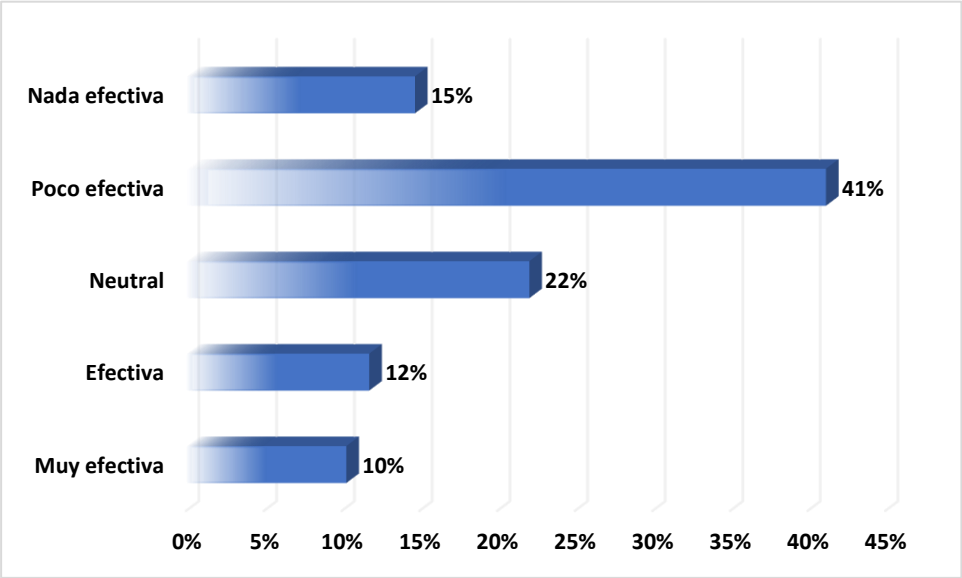
Tabla 9

Comunicación recibida durante el proceso de soporte técnico

Respuesta	Muestra	Resultado
Muy efectiva	7	10%
Efectiva	8	12%
Neutral	15	22%
Poco efectiva	28	41%
Nada efectiva	10	15%
TOTAL	**68**	**100%**

Figura 11

Comunicación recibida durante el proceso de soporte técnico



El análisis de los resultados de la pregunta 5, que indaga sobre si los clientes han expresado previamente sus preocupaciones o comentarios sobre problemas técnicos no resueltos o insatisfacción con los servicios de soporte técnico, destaca una tendencia preocupante. Un considerable 74% de los encuestados ha expresado sus inquietudes, mientras que solo un 26% afirma no haberlo hecho. Estos hallazgos señalan una comunicación activa por parte de los clientes sobre las deficiencias en el soporte técnico y la insatisfacción experimentada.

7. ¿Considera que la información proporcionada por el equipo de soporte técnico es clara y comprensible?

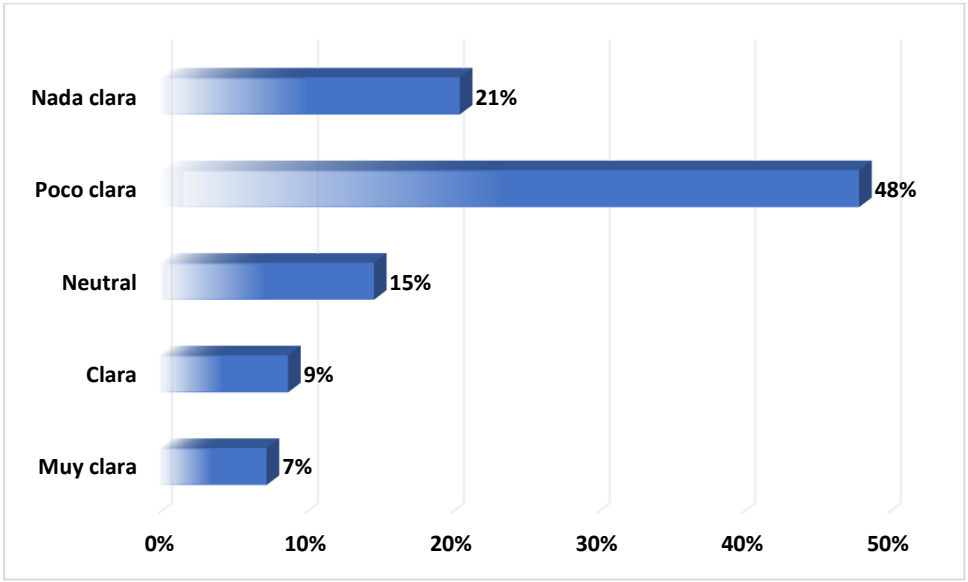
Tabla 10

Información proporcionad con claridad

Respuesta	Muestra	Resultado
Muy clara	5	7%
Clara	6	9%
Neutral	10	15%
Poco clara	33	48%
Nada clara	14	21%
TOTAL	**68**	**100%**

Figura 12

Información proporcionad con claridad



El análisis de los resultados de la pregunta 7, que evalúa la percepción de los clientes sobre la claridad y comprensibilidad de la información proporcionada por el equipo de soporte técnico, refleja una preocupante tendencia. Un significativo 69% de los encuestados describe la información como "poco clara" o "nada clara", mientras que solo un 16% la percibe como "muy clara" o "clara". Estos resultados indican una brecha sustancial en la claridad de la información comunicada durante el soporte técnico.

8. ¿Cómo describiría la accesibilidad a los recursos y herramientas de soporte técnico proporcionados por GPSTracker S.A.?

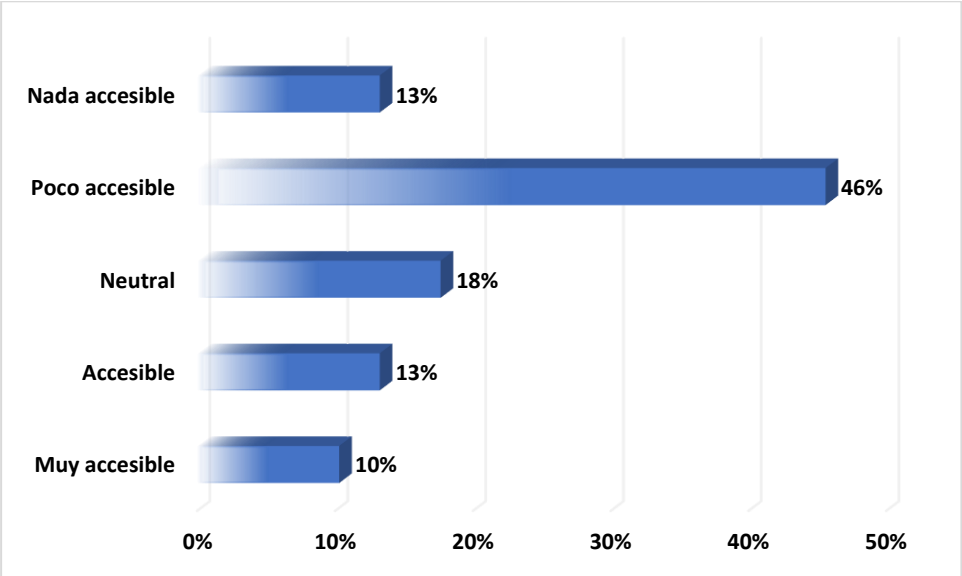
Tabla 11

Accesibilidad a los recursos y herramientas de soporte

Respuesta	Muestra	Resultado
Muy accesible	7	10%
Accesible	9	13%
Neutral	12	18%
Poco accesible	31	46%
Nada accesible	9	13%
TOTAL	**68**	**100%**

Figura 13

Accesibilidad a los recursos y herramientas de soporte



El análisis de los resultados de la pregunta 8, que aborda la descripción de la accesibilidad a los recursos y herramientas de soporte técnico proporcionados por GPSTracker S.A., destaca áreas de mejora importantes. Un considerable 59% de los encuestados considera la accesibilidad como "poco accesible" o "nada accesible", mientras que solo un 23% la evalúa como "muy accesible" o "accesible". Estos resultados subrayan la necesidad de optimizar la accesibilidad a los recursos de soporte técnico.

4.1.4. Resultados diagnóstico situacional

A partir de la información recopilada mediante el análisis del árbol de problemas, la guía de entrevista y el cuestionario aplicado a clientes, se ha identificado una situación actual que demanda atención inmediata en varios aspectos clave.

1. **Eficiencia del soporte técnico:**

- El tiempo de respuesta prolongado identificado en el árbol de problemas se ha confirmado con la respuesta de los clientes. El 71% de los encuestados ha experimentado demoras significativas en la resolución de problemas, lo que indica una eficiencia subóptima en el soporte técnico. Esto afecta negativamente la satisfacción del cliente y la calidad percibida de los servicios.

2. **Problemas técnicos recurrentes:**

- La alta incidencia de problemas técnicos recurrentes, reportada por el 87% de los clientes, resalta la existencia de deficiencias sustanciales en la estabilidad y confiabilidad de los servicios de GPSTracker S.A. Estos problemas recurrentes impactan directamente en la experiencia del usuario y generan insatisfacción.

3. **Seguridad de la información:**

- La percepción negativa sobre la seguridad de la información, evidenciada por más del 50% de los clientes que la califican como "insegura" o "muy insegura", indica una preocupación significativa. Esta situación expone a la

empresa y a sus clientes a riesgos cibernéticos y afecta la confianza en los servicios proporcionados.

4. **Comunicación y claridad:**

- La comunicación poco efectiva, señalada por el 56% de los clientes, y la falta de claridad en la información proporcionada durante el soporte técnico (69% percibe la información como "poco clara" o "nada clara") resaltan la necesidad de mejorar la comunicación interna y externa para una interacción más efectiva.

5. **Accesibilidad a recursos de soporte:**

- La accesibilidad poco favorable, según el 59% de los clientes que la consideran "poco accesible" o "nada accesible", indica dificultades en la utilización eficiente de los recursos y herramientas de soporte técnico.

En resumen, la situación actual de GPSTracker S.A. está caracterizada por deficiencias notables en la eficiencia del soporte técnico, la estabilidad de los servicios, la seguridad de la información y la claridad en la comunicación. Abordar estos problemas se vuelve imperativo para mejorar la calidad del servicio, fortalecer la confianza del cliente y mantener la competitividad en el mercado.

4.2. Estrategias de mejora al proceso de soporte técnico y seguridad mediante las TIC

Tabla 12

Estrategias de mejora al proceso de soporte técnico y seguridad mediante las TIC

Acciones de mejora	Actividades a desarrollar	Metas	Desarrollo de las actividades
Implementación de un sistema de gestión de tickets	• Selección de un software de gestión de tickets eficiente. • Capacitación del personal en el uso del nuevo sistema.	• Reducción significativa de los tiempos de respuesta en la resolución de problemas.	• Investigar y comparar opciones de software de gestión de tickets en el mercado. • Seleccionar el software más adecuado a las necesidades de GPSTracker S.A. • Diseñar y llevar a cabo sesiones de capacitación para el personal sobre el uso efectivo del nuevo sistema de gestión de tickets.
Establecimiento de protocolos de respuesta a incidentes	• Desarrollo de protocolos claros y eficaces para la respuesta a incidentes de seguridad. • Capacitación del equipo en la implementación de los nuevos protocolos.	• Mejora de la capacidad de respuesta frente a posibles amenazas cibernéticas.	• Analizar los incidentes de seguridad anteriores para identificar patrones y áreas de mejora. • Colaborar con expertos en ciberseguridad para desarrollar protocolos específicos. • Planificar y llevar a cabo sesiones de capacitación para el personal sobre la aplicación práctica de los nuevos protocolos de respuesta a incidentes de seguridad.

Mejora de la infraestructura de seguridad informática	• Actualización y fortalecimiento de la infraestructura de seguridad informática. • Realización de pruebas de seguridad regulares.	• Aumento de la confiabilidad y seguridad de los sistemas de información.	• Realizar una evaluación exhaustiva de la infraestructura actual para identificar vulnerabilidades. • Actualizar software y sistemas operativos. • Establecer un programa regular de pruebas de seguridad para identificar y abordar posibles vulnerabilidades. • Colaborar con profesionales externos en la realización de auditorías de seguridad.
Implementación de un sistema de comunicación efectiva	• Desarrollo de un sistema de comunicación interna y externa más efectivo. • Obtención de retroalimentación regular de los clientes.	• Mejora de la comunicación entre el equipo de soporte técnico y los clientes.	• Identificar y utilizar plataformas de comunicación efectivas. • Establecer canales de comunicación claros y accesibles. • Diseñar y aplicar encuestas periódicas para recopilar opiniones y sugerencias de los clientes. • Establecer un sistema de retroalimentación continua a través de plataformas online y otros canales de comunicación.

Desarrollo de materiales educativos para clientes	• Creación de guías y tutoriales claros sobre las mejores prácticas de seguridad. • Creación de contenido educativo sobre las características de los servicios.	• Aumento de la conciencia de seguridad entre los clientes.	• Desarrollar guías y tutoriales visuales y de fácil comprensión que aborden las prácticas de seguridad recomendadas. • Publicar estos materiales en el sitio web y otros canales accesibles para los clientes. • Diseñar contenido educativo que destaque las características clave de los servicios ofrecidos por GPSTracker S.A. • Utilizar formatos variados como videos, infografías y documentos descargables para llegar a diversos públicos.

4.2.1. Interpretación y análisis de las estrategias de mejora

- **Estrategia 1: Implementación de un sistema de gestión de tickets**

La implementación de un sistema de gestión de tickets se inicia con un análisis detallado de las opciones disponibles en el mercado, considerando criterios cruciales para el entorno operativo de GPSTracker S.A. Se lleva a cabo una investigación exhaustiva para evaluar la escalabilidad del software, su interfaz de usuario y su capacidad de integración con los sistemas existentes de la empresa. Este proceso de selección se realiza con el objetivo de garantizar que la solución elegida no solo responda a las necesidades actuales de soporte técnico, sino que también sea flexible y escalable para adaptarse a futuros crecimientos y cambios en el entorno tecnológico.

Una vez completada la selección, la segunda fase crítica implica la capacitación integral del personal en el uso eficiente del nuevo sistema. A través de sesiones detalladas y personalizadas, se busca no solo transmitir el conocimiento técnico necesario, sino también fomentar la adopción efectiva del nuevo sistema, asegurando que cada miembro del equipo pueda utilizarlo de manera competente para mejorar la eficiencia operativa y la calidad del soporte.

Este enfoque estructurado garantiza que la implementación del sistema de gestión de tickets no sea solo una actualización tecnológica, sino una integración fluida que maximiza los beneficios ofrecidos por la nueva herramienta, mejorando significativamente el proceso de soporte técnico en GPSTracker S.A.

- **Estrategia 2: Establecimiento de protocolos de respuesta a incidentes**

El proceso de establecimiento de protocolos de respuesta a incidentes inicia con un análisis meticuloso de los incidentes de seguridad previos en GPSTracker S.A. Este enfoque proactivo es esencial para entender los patrones subyacentes y las áreas específicas que necesitan mejoras. Identificar las brechas en la respuesta a incidentes permite al equipo de seguridad adaptar los protocolos de manera precisa y específica a los desafíos enfrentados por la empresa. Esta evaluación no solo se centra en corregir deficiencias pasadas, sino que también busca fortalecer la capacidad de la organización para anticipar y mitigar futuros riesgos cibernéticos.

La segunda actividad crítica implica la capacitación especializada del equipo en la implementación de los nuevos protocolos. A través de sesiones formativas diseñadas específicamente para abordar las amenazas cibernéticas, el personal adquiere las habilidades y conocimientos esenciales para aplicar eficazmente los protocolos en situaciones de crisis. Esta capacitación no solo se concentra en aspectos técnicos, sino también en la sensibilización y comprensión de la importancia de seguir los protocolos establecidos. De esta manera, el equipo de seguridad se convierte en un componente integral y altamente capacitado en la respuesta a incidentes, mejorando la capacidad global de la organización para enfrentar desafíos de seguridad.

- **Estrategia 3: Mejora de la infraestructura de seguridad informática**

La mejora de la infraestructura de seguridad informática en GPSTracker S.A. comienza con una evaluación minuciosa de la infraestructura actual, centrada en la identificación y corrección de posibles vulnerabilidades. Este análisis abarca una

revisión exhaustiva de la configuración de software y sistemas operativos, buscando fortalecer las defensas contra posibles amenazas.

La segunda actividad crucial se enfoca en la realización de pruebas de seguridad regulares. Estas pruebas, llevadas a cabo de manera periódica, tienen como objetivo detectar nuevas vulnerabilidades que puedan surgir en un entorno tecnológico en constante evolución. Evaluar la efectividad de las medidas de seguridad implementadas es esencial para garantizar una protección continua y adaptada a las amenazas cibernéticas emergentes.

Además, la colaboración con profesionales externos en auditorías de seguridad proporciona una capa adicional de robustez a la infraestructura. La participación de expertos externos aporta una perspectiva objetiva y experiencia especializada, fortaleciendo aún más las defensas de la organización contra amenazas potenciales. En conjunto, estas actividades se integran de manera coherente para mejorar la infraestructura de seguridad informática, asegurando una protección sólida y continua contra posibles riesgos cibernéticos en GPSTracker S.A.

- **Estrategia 4: Implementación de un sistema de comunicación efectiva**

La implementación de un sistema de comunicación efectiva inicia con la cuidadosa selección e implementación de plataformas que mejoren la colaboración interna y la interacción con los clientes en GPSTracker S.A. Este proceso implica la identificación de herramientas que se adapten a las necesidades específicas de la empresa, promoviendo una comunicación eficiente y facilitando el intercambio de información entre los distintos departamentos y con los clientes.

La segunda actividad esencial se centra en el establecimiento de canales de comunicación claros y accesibles. Definir protocolos para la comunicación interna y externa es vital para prevenir malentendidos, asegurando que la información fluya de manera efectiva entre el equipo de soporte técnico y los clientes. Además, la capacitación en habilidades de comunicación para el personal de soporte técnico es una parte fundamental de esta estrategia, contribuyendo a mejorar la calidad de las interacciones y fortalecer la relación con los clientes.

Estas actividades se combinan para crear un entorno de comunicación efectiva en GPSTracker S.A., donde la selección cuidadosa de herramientas y la definición de protocolos claros se complementan con la capacitación del personal, garantizando una comunicación fluida y mejorada en todos los niveles de la organización.

- **Estrategia 5: Desarrollo de materiales educativos para clientes**

El desarrollo de materiales educativos para clientes en GPSTracker S.A. se inicia con la creación de guías y tutoriales visuales de fácil comprensión que aborden las mejores prácticas de seguridad. Estos materiales tienen como objetivo principal aumentar la conciencia de seguridad entre los clientes, proporcionando orientación clara sobre cómo utilizar los servicios de manera segura y proteger su información.

La segunda actividad clave se enfoca en la creación de contenido educativo detallado sobre las características específicas de los servicios. Este contenido educativo puede adoptar diversas formas, como videos explicativos, infografías y documentos descargables, y tiene como propósito informar a los clientes sobre las funcionalidades específicas de los servicios ofrecidos por la empresa. Al proporcionar

esta información de manera clara y accesible, se busca mejorar la experiencia del cliente y fortalecer su comprensión de los servicios, fomentando así un uso más efectivo y seguro de los mismos. Todas las actividades de la implementación de las estrategias detalladas para mejorar el proceso de soporte técnico y seguridad en GPSTracker S.A. se presenta como un enfoque integral y estructurado que aborda de manera efectiva los problemas evidenciados.

Estas estrategias, centradas en la optimización de la gestión de tickets, el fortalecimiento de la respuesta a incidentes, la mejora de la infraestructura de seguridad informática y el establecimiento de una comunicación efectiva, están diseñadas para subsanar las deficiencias identificadas en los tiempos de respuesta, la seguridad de la información y la satisfacción del cliente. Al adoptar estos enfoques estratégicos, la empresa busca no solo resolver los problemas actuales, sino también fortalecer su capacidad para enfrentar desafíos futuros, garantizando un proceso de soporte técnico y seguridad eficiente y de alta calidad.

4.3. Mecanismos de seguimiento y control a la propuesta de mejora

Tabla 13

Indicadores de control

Actividad de mejora	Indicador de control	Responsables	Frecuencia de control	Análisis de resultados
Implementación del sistema de gestión de tickets	Número de tickets gestionados por día	Equipo de soporte técnico	Semanal	Comparación de la cantidad de tickets gestionados antes y después de la implementación.
Selección y adopción de plataformas de comunicación	Porcentaje de mejora en la eficiencia de la comunicación interna.	Departamento de tecnologías de la información	Mensual	Evaluación de la velocidad de respuesta y resolución de consultas internas.
Establecimiento de canales de comunicación claros	Reducción en malentendidos reportados	Equipo de soporte técnico	Trimestral	Análisis de incidentes de comunicación interna para identificar mejoras.
Desarrollo de materiales educativos para clientes	Número de descargas y visualizaciones de materiales	Equipo de marketing	Mensual	Evaluación del interés de los clientes en los materiales educativos proporcionados.
Creación de contenido educativo sobre características de los servicios	Porcentaje de clientes que acceden al contenido	Equipo de atención al cliente	Trimestral	Retroalimentación de los clientes sobre la utilidad y claridad del contenido.
Mejora de la infraestructura de seguridad informática	Resultados de pruebas de seguridad	Equipo de seguridad de la información	Mensual	Evaluación de nuevas vulnerabilidades identificadas y eficacia de las medidas de seguridad.
Colaboración con profesionales externos en auditorías de seguridad	Cumplimiento de recomendaciones de auditoría	Equipo de seguridad de la información	Semestral	Seguimiento de la implementación de recomendaciones y mejoras sugeridas.

4.3.1. Interpretación y análisis de los mecanismos de control

- **Análisis interpretativo de proceso de seguimiento y control**

La estrategia de implementación del sistema de gestión de tickets se centra en el indicador clave de "número de tickets gestionados por día". Este indicador proporciona una medida cuantitativa de la eficiencia del equipo de soporte técnico en la gestión de solicitudes y problemas. El equipo de soporte técnico asumirá la responsabilidad de este seguimiento semanal, evaluando el rendimiento en términos de la cantidad de tickets gestionados antes y después de la implementación del nuevo sistema. La frecuencia semanal de control permitirá una supervisión cercana de las tendencias y un análisis rápido de cualquier variación, lo que facilitará la identificación oportuna de áreas que requieran mejoras.

El análisis de resultados se centrará en comparar la eficiencia del proceso de gestión de tickets antes y después de la implementación. Se evaluará la posible disminución de tiempos de respuesta, la optimización en la resolución de problemas y la mejora general en la eficiencia del equipo. Este enfoque cuantitativo permitirá medir de manera concreta el impacto de la estrategia, identificando áreas de éxito y oportunidades de ajuste para lograr una gestión de tickets más efectiva y satisfactoria para los usuarios finales.

La estrategia de "selección y adopción de plataformas de comunicación" se enfoca en el indicador crítico de "porcentaje de mejora en la eficiencia de la comunicación interna". Este indicador proporciona una medida cuantitativa de la eficacia de las nuevas plataformas implementadas por el departamento de tecnologías de la información para facilitar la comunicación interna. La responsabilidad de este

indicador recae en el mencionado departamento, que supervisará mensualmente la mejora de la eficiencia en la comunicación interna.

La frecuencia mensual de control permitirá al departamento de tecnologías de la información realizar evaluaciones detalladas de la velocidad de respuesta y la resolución de consultas internas. Este análisis mensual ofrecerá una visión integral de la eficiencia de las nuevas plataformas, identificando áreas de éxito y oportunidades de mejora. La estrategia busca, a través de este enfoque cuantitativo, cuantificar y evaluar el impacto positivo en la eficiencia de la comunicación interna, mejorando así la colaboración y la fluidez de la información dentro de la empresa.

La estrategia de "establecimiento de canales de comunicación claros" se centra en el indicador crucial de "reducción en malentendidos reportados". Este indicador proporciona una medida cuantitativa de la efectividad de los esfuerzos del equipo de soporte técnico para mejorar la claridad de los canales de comunicación interna. El equipo de soporte técnico asumirá la responsabilidad de supervisar trimestralmente la reducción en malentendidos, evaluando la eficacia de los canales de comunicación establecidos.

La frecuencia trimestral de control permitirá al equipo de soporte técnico realizar un análisis detallado de los incidentes de comunicación interna, identificando áreas que requieran mejoras. Este enfoque cuantitativo busca cuantificar la disminución en malentendidos y evaluar el impacto positivo en la claridad de la comunicación interna. La estrategia tiene como objetivo crear canales de comunicación más transparentes y efectivos, reduciendo la posibilidad de malentendidos y mejorando la eficiencia global del equipo de soporte técnico.

La estrategia de "desarrollo de materiales educativos para clientes" se enfoca en el indicador clave de "número de descargas y visualizaciones de materiales". Este indicador proporciona una medida cuantitativa del interés y la utilidad percibida de los materiales educativos desarrollados por el equipo de marketing. La responsabilidad de este indicador recae en el equipo de marketing, que supervisará mensualmente la cantidad de descargas y visualizaciones de los materiales educativos.

La frecuencia mensual de control permitirá al equipo de marketing realizar evaluaciones detalladas del interés de los clientes en los materiales educativos proporcionados. Se analizará la relación entre la cantidad de descargas y visualizaciones con la percepción de utilidad de los clientes. Este enfoque cuantitativo busca cuantificar el impacto positivo de los materiales educativos en la comprensión y experiencia de los clientes. La estrategia tiene como objetivo generar materiales educativos que sean relevantes y atractivos, contribuyendo así a una mayor satisfacción y comprensión por parte de los clientes.

La estrategia de "creación de contenido educativo sobre características de los servicios" se orienta hacia el indicador crítico del "porcentaje de clientes que acceden al contenido". Este indicador proporciona una medida cuantitativa del interés y la participación de los clientes con el contenido educativo desarrollado por el equipo de atención al cliente. La responsabilidad de este indicador recae en el equipo de atención al cliente, que supervisará trimestralmente el porcentaje de clientes que acceden al contenido.

La frecuencia trimestral de control permitirá al equipo de atención al cliente evaluar la efectividad del contenido educativo a lo largo del tiempo. Se recopilará la retroalimentación de los clientes sobre la utilidad y claridad del contenido,

proporcionando una visión cualitativa adicional para complementar las métricas cuantitativas. Este enfoque integral busca cuantificar el impacto positivo del contenido educativo en la comprensión de los clientes y recopilar percepciones valiosas que orienten ajustes y mejoras continuas. La estrategia tiene como objetivo generar un contenido educativo efectivo y apreciado por los clientes, contribuyendo a una experiencia más enriquecedora y satisfactoria.

La estrategia de "mejora de la infraestructura de seguridad informática" se basa en el indicador clave de los "resultados de pruebas de seguridad". Este indicador proporciona una medida cuantitativa de la eficacia de las acciones tomadas por el equipo de seguridad de la información para mejorar la seguridad informática. La responsabilidad de este indicador recae en el equipo de seguridad de la información, que realizará evaluaciones mensuales de los resultados de las pruebas de seguridad.

La frecuencia mensual de control permitirá al equipo de seguridad de la información identificar nuevas vulnerabilidades y evaluar la eficacia de las medidas de seguridad implementadas. Se analizarán los resultados de las pruebas para determinar la fortaleza de la infraestructura de seguridad y su capacidad para resistir amenazas cibernéticas. Este enfoque cuantitativo busca cuantificar el impacto positivo de las mejoras en la infraestructura de seguridad, asegurando una protección continua contra amenazas cibernéticas y la identificación temprana de posibles vulnerabilidades. La estrategia tiene como objetivo reforzar la seguridad de la empresa, minimizando riesgos y garantizando la integridad de la información.

La estrategia de "colaboración con profesionales externos en auditorías de seguridad" se enfoca en el indicador clave del "cumplimiento de recomendaciones de auditoría". Este indicador proporciona una medida cuantitativa de la capacidad del

equipo de seguridad de la información para implementar y seguir las recomendaciones derivadas de auditorías externas. La responsabilidad de este indicador recae en el equipo de seguridad de la información, que realizará evaluaciones semestrales del cumplimiento de las recomendaciones de auditoría.

La frecuencia semestral de control permitirá al equipo de seguridad de la información dar seguimiento a la implementación de recomendaciones y mejoras sugeridas por profesionales externos. Se analizará el nivel de cumplimiento para garantizar que las medidas de seguridad propuestas se hayan aplicado de manera efectiva. Este enfoque cuantitativo busca cuantificar el impacto positivo de la colaboración con profesionales externos, asegurando que la infraestructura de seguridad se ajuste a los estándares y mejores prácticas recomendadas. La estrategia tiene como objetivo fortalecer la seguridad de la empresa a través de la implementación de medidas específicas, derivadas de la experiencia y conocimientos de profesionales externos en auditorías de seguridad.

4.4. Inversión de las estrategia de mejora

Tabla 14

Inversión para la implementación

Acciones de mejora	Actividades a desarrollar	C/U	C/T
Implementación de un sistema de gestión de tickets	• Selección de un software de gestión de tickets eficiente. • Capacitación del personal en el uso del nuevo sistema.	1.800 3.000	4.800
Establecimiento de protocolos de respuesta a incidentes	• Desarrollo de protocolos claros y eficaces para la respuesta a incidentes de seguridad. • Capacitación del equipo en la implementación de los nuevos protocolos.	800 300	1.100
Mejora de la infraestructura de seguridad informática	• Actualización y fortalecimiento de la infraestructura de seguridad informática. • Realización de pruebas de seguridad regulares.	2.200 300	2.500
Implementación de un sistema de comunicación efectiva	• Desarrollo de un sistema de comunicación interna y externa más efectivo. • Obtención de retroalimentación regular de los clientes.	1.200 400	1.600
Desarrollo de materiales educativos para clientes	• Creación de guías y tutoriales claros sobre las mejores prácticas de seguridad. • Creación de contenido educativo sobre las características de los servicios.	400 400	800
INVERSION TOTAL			***10.800***

4.4.1. Interpretación y análisis de la inversión de la mejora

El análisis de la inversión propuesta muestra una asignación de recursos en diversas acciones para mejorar el proceso de soporte técnico y seguridad en GPSTracker S.A. La implementación de un sistema de gestión de tickets implica una inversión significativa de $1,800 en la selección de un software eficiente y $3,000 en la capacitación del personal. Esta acción tiene un costo total de $4,800 y busca mejorar la eficiencia en la gestión de tickets, impactando directamente en la rapidez y calidad del soporte técnico.

La estrategia de establecimiento de protocolos de respuesta a incidentes tiene un costo de $800 en el desarrollo de protocolos y $300 en la capacitación del equipo, con un costo total de $1,100. Este enfoque busca mejorar la capacidad de respuesta frente a amenazas de seguridad, fortaleciendo la postura de seguridad de la empresa. La mejora de la infraestructura de seguridad informática implica una inversión de $2,200 en la actualización de la infraestructura y $300 en la realización de pruebas de seguridad regulares, sumando un costo total de $2,500. Esta acción busca fortalecer las defensas contra amenazas cibernéticas y garantizar la seguridad.

La implementación de un sistema de comunicación efectiva tiene un costo total de $1,600, distribuido entre $1,200 para el desarrollo del sistema y $400 para la obtención regular de retroalimentación de los clientes. Este enfoque busca mejorar la comunicación interna y externa, optimizando la interacción con clientes y el equipo. El desarrollo de materiales educativos para clientes implica una inversión de $800 en la creación de guías y tutoriales y $400 en la creación de contenido educativo, con un

costo total de $1,200. Esta acción busca aumentar la conciencia de seguridad entre los clientes y mejorar su comprensión de los servicios.

A manera general, la inversión total de $10,800 se distribuye estratégicamente en acciones clave para mejorar el soporte técnico y la seguridad. Se espera que estas inversiones generen beneficios significativos en términos de eficiencia operativa, seguridad de la información, satisfacción del cliente y la posición competitiva de la empresa en el mercado. La implementación exitosa de estas acciones contribuirá a un retorno de inversión a través de la mejora de servicios, la retención de clientes y la mitigación de riesgos de seguridad.

Capítulo V Sugerencias

Conclusiones

- La investigación ha permitido identificar las áreas críticas en el proceso de soporte técnico y seguridad de GPSTracker S.A., evidenciando la urgente necesidad de mejoras. La propuesta presentada aborda de manera integral los desafíos identificados, proponiendo estrategias específicas respaldadas por la implementación de un sistema de gestión de tickets, protocolos de respuesta a incidentes mejorados, mejoras en la infraestructura de seguridad informática, una comunicación más efectiva y materiales educativos para clientes. Estas soluciones se alinean directamente con los problemas identificados.

- En conclusión, el diagnóstico situacional de GPSTracker S.A. revela una serie de deficiencias críticas en áreas clave como la eficiencia del soporte técnico, la estabilidad de los servicios, la seguridad de la información y la claridad en la comunicación. Estos problemas afectan directamente la satisfacción del cliente y ponen en riesgo la reputación y la competitividad de la empresa en el mercado. Para mantenerse a la vanguardia y mejorar la calidad del servicio, es fundamental abordar estas deficiencias de manera urgente, implementando estrategias que fortalezcan la eficiencia, la confiabilidad y la transparencia en todas las interacciones con los clientes.

- La propuesta estratégica ha sido cuidadosamente diseñada para abordar los problemas diagnosticados, proponiendo soluciones específicas respaldadas por la implementación de tecnologías de la información y comunicación (TIC). La selección de estrategias como la automatización de procesos, el establecimiento de protocolos claros, la mejora de la infraestructura de

seguridad informática y la implementación de sistemas de comunicación efectiva refleja un enfoque equilibrado para mejorar tanto la eficiencia operativa como la seguridad en GPSTracker S.A. Estas estrategias buscan optimizar los procesos existentes y fortalecer la preparación ante posibles amenazas, brindando una solución integral y sostenible.

- La implementación de mecanismos de seguimiento y control es crucial para asegurar el éxito continuo de las estrategias propuestas. La definición de indicadores de control, la asignación de responsabilidades y la establecimiento de frecuencias de control permitirán evaluar periódicamente el progreso de cada actividad. La retroalimentación obtenida de estos mecanismos proporcionará información valiosa para realizar ajustes y mejoras continuas, garantizando que la propuesta de mejora evolucione de manera adaptativa y efectiva a lo largo del tiempo.

- La definición de la inversión necesaria para implementar cada estrategia de mejora proporciona una visión clara de los recursos financieros requeridos para llevar a cabo la propuesta. El análisis detallado de los costos asociados con la implementación de un sistema de gestión de tickets, el establecimiento de protocolos de respuesta a incidentes, la mejora de la infraestructura de seguridad informática, la implementación de un sistema de comunicación efectiva y la creación de materiales educativos refleja un enfoque financiero sólido y transparente. Esta conclusión ofrece una guía concreta para la asignación de recursos, permitiendo una planificación financiera eficiente y asegurando que los fondos se utilicen de manera efectiva para abordar los problemas identificados en el proceso de soporte técnico y seguridad.

Recomendaciones

- Se sugiere implementar un programa de capacitación continua para el equipo de soporte técnico y seguridad. Esto no solo incluiría la formación inicial en las nuevas tecnologías y procesos, sino también la actualización constante para mantenerse al tanto de las últimas tendencias y amenazas en el ámbito de la seguridad informática. Un personal bien capacitado es fundamental para abordar eficazmente los desafíos cambiantes y garantizar la prestación de servicios de alta calidad.
- Se recomienda la adopción de herramientas avanzadas de monitoreo proactivo que permitan identificar y abordar posibles problemas antes de que afecten significativamente a los clientes o a la seguridad de la información. Estas herramientas pueden proporcionar alertas tempranas, análisis predictivo y una visibilidad más completa de la infraestructura, mejorando la capacidad de respuesta y reduciendo el tiempo de inactividad.
- Se sugiere la creación de un canal directo de retroalimentación con los clientes, como un sistema de tickets específico para comentarios y sugerencias. Esto facilitaría la comunicación bidireccional, permitiendo a los clientes expresar sus preocupaciones, brindando a la empresa información valiosa para la mejora continua y demostrando un compromiso transparente con la satisfacción del cliente.
- Dada la importancia de la seguridad de la información, se propone la elaboración de un plan de contingencia detallado para abordar posibles violaciones de seguridad o interrupciones del servicio. Este plan debería incluir procedimientos claros, roles y responsabilidades definidos, y prácticas de recuperación eficientes para minimizar el impacto en caso de incidentes.

- Se sugiere promover la colaboración estrecha entre los departamentos de soporte técnico, seguridad de la información y desarrollo. La sinergia entre estos departamentos es crucial para comprender las interconexiones de sistemas, identificar posibles vulnerabilidades y garantizar una implementación efectiva de mejoras en el proceso.
- Se recomienda realizar auditorías internas regulares para evaluar la efectividad de las mejoras implementadas. Estas auditorías deberían abarcar aspectos como la eficiencia del soporte técnico, la seguridad de la información y la satisfacción del cliente. Los hallazgos de estas auditorías pueden proporcionar información valiosa para ajustar estrategias y mantener una mejora continua en los procesos.
- Se sugiere explorar y adoptar herramientas de automatización para tareas rutinarias dentro del soporte técnico y la seguridad. La automatización puede reducir la carga de trabajo manual, mejorar la eficiencia operativa y minimizar la posibilidad de errores humanos, permitiendo al personal enfocarse en actividades más estratégicas y complejas.
- Se recomienda la implementación de métricas de desempeño claras y objetivas para evaluar tanto la eficacia del soporte técnico como la robustez de las medidas de seguridad. Estas métricas pueden incluir tiempos de respuesta, índices de resolución de problemas, y evaluaciones periódicas de la infraestructura de seguridad. La monitorización constante de estas métricas facilitará la identificación de áreas que requieren atención y permitirá una toma de decisiones informada.
- Se sugiere desarrollar una cultura organizacional que priorice la seguridad tanto a nivel técnico como humano. Esto implica la promoción de buenas prácticas de seguridad entre los empleados, la realización de sesiones de concientización

sobre ciberseguridad y la incorporación de la seguridad en el desarrollo de nuevos proyectos desde sus etapas iniciales.

- Se recomienda la implementación de un programa de recompensas y reconocimientos para el personal que demuestre un rendimiento excepcional en términos de eficiencia en el soporte técnico y contribuciones significativas a la seguridad de la información. Estas iniciativas pueden motivar al equipo y fomentar una competencia positiva para mejorar continuamente.
- Para fortalecer la preparación ante posibles incidentes de seguridad, se sugiere realizar ejercicios periódicos de simulación de incidentes. Estos simulacros permitirán al equipo practicar la aplicación de protocolos de respuesta en un entorno controlado, identificando áreas de mejora y optimizando la coordinación entre los miembros del equipo.
- Se recomienda explorar tecnologías emergentes, como inteligencia artificial, aprendizaje automático y análisis predictivo, para mejorar la anticipación y gestión de problemas en el soporte técnico y la seguridad. La adopción de estas tecnologías puede proporcionar herramientas avanzadas para la detección temprana de amenazas y la optimización de los procesos de soporte técnico.

Bibliografía

Alvarado, E., Arizaga, j., & Chicala, J. (2021). Seguridad en tecnologías de las comunicaciones enfocada al ámbito de la salud caso FCI Terapias Médicas en Red (TEMONET) . *Grupo Editorial "Ediciones Futuro" Universidad de las Ciencias Informática, 14*(4), 226-246. https://doi.org/https://dialnet.unirioja.es/descarga/articulo/8590510.pdf

Avenía, C. (2017). *Fundamentos de seguridad informática* (Primera ed.). Bogotá: Fondo editorial Areandino. https://core.ac.uk/download/pdf/326424171.pdf

Baena, G. (2017). *Metodología de la investigación* (3ra ed.). México: Grupo Editorial Patria. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/metodologia%20de%20la%20investigacion.pdf

Bravo, F. (2021). Uso de Tecnologías de la Información y Comunicación en el Bachillerato. *Revista Recus, 6*(1), 19-27. https://dialnet.unirioja.es/descarga/articulo/8273820.pdf

Bravo, L., & Andrade, M. (2020). ITIL v4 en la gestión de solicitudes e incidentes de la mesa de ayuda de la Universidad Nacional de Loja. *Dominio de la Ciencias, 6*(4), 1510-1534. https://dialnet.unirioja.es/servlet/articulo?codigo=8638152

Bueno, G., & Haz, L. (2022). Ciberseguridad post covid-19 y su impacto. *Pro Sciences: Revista de Producción, Ciencias e Investigación, 6*(46), 103-120. https://doi.org/https://doi.org/10.29018/issn.2588-1000vol6iss41.2022pp388-399

Cartagen, É., Vargas, Y., Cuevas, G., & Rubio, G. (2022). Validación de un instrumento para la evaluación del consentimiento informado y su uso en

investigación en estudiantes universitarios. *Cienc Tecnol Salud Vis Ocul.*(2). https://doi.org/https://doi.org/10.19052/sv.vol19.iss2.7

Castañeda, E., Pineda, D., & Ceja, J. (2021). TIC's, como herramientas contra la inseguridad en las ciudades. *Research, Society and Development, 10*(15), 1-15. https://doi.org/http://dx.doi.org/10.33448/rsd-v10i15.23361

Condori, P. (2020). Universo, población y muestra. *Curso Taller*, 1-16. https://www.aacademica.org/cporfirio/18.pdf

Coronel, I., & Quirumbay, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE, 9*(2), 39-47. https://doi.org/https://doi.org/10.26423/rctu.v9i2.678

Cruz, E. (2019). Importancia del manejo de competencias tecnológicas en las prácticas docentes de la Universidad Nacional Experimental de la Seguridad (UNES). *Revista Educación, 43*(1). https://doi.org/https://doi.org/10.15517/revedu.v43i1.27120

Cruz, K., Garzón, E., Quezada, E., & Carvajal, I. (2022). Tableros y gráficos automatizados: un enfoque a la visualización de datos e inteligencia de negocio. *Ciencia Latina Revista Científica Multidisciplinar, 6*(4), 2624-2641. https://doi.org/https://doi.org/10.37811/cl_rcm.v6i4.2784

Di Luca, M. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso Avances. *Instituto de Información Científica y Tecnológica, 21*(2). https://www.redalyc.org/journal/6378/637869113010/html/

Estrada, R., Unás, J., & Flórez, O. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. *Revista*

Logos Ciencia & Tecnología, 13(3), 98-110. https://doi.org/https://doi.org/10.22335/rlct.v13i3.1446

GPSTracker S.A. (2021). *Quienes somos*. https://cartrack.ec/

GPSTraker S.A. (2021). *Misión, Vision, Valores*. https://cartrack.ec/

Guzmán, C. (2022). *Aplicación de ITIL 4 para la gestión de incidentes en la CMAC Santa SA - 2021.* Tesis de maestría. Universidad César Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/87144/Guzm%C3%A1n_DCJ-SD.pdf?sequence=1&isAllowed=y

Interpol. (2020). *Ciberdelincuencia: Efectos de la COVID-19.* Secretaría General de la Interpol.: https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf

Jurado, F., Yarad, P., & Carrión, J. (2020). Análisis de las características del sector microempresarial en latinoamérica y sus limitantes en la adopción de tecnologías para la seguridad de la información. *Revista Científica ECOCIENCIA, 7*(1), 2-26. https://revistas.ecotec.edu.ec/index.php/ecociencia/article/download/303/233/514

Machuca, J., & Cabrera, A. (2020). Percepción de la exposición en seguridad informática de los niños y adolescentes durante la pandemia CO-VID-19. *Polo del Conocimiento, 5*(1), 37-51.

Medrano, J., & Quiñonez, X. (2021). Calidad de servicio del soporte técnico utilizando el modelo SERVPERF y el marco ITSQM. *Revista Tecnológica - ESPOL, 33*(3), 242-257. https://doi.org/https://doi.org/10.37815/rte.v33n3.810

Molinetti, S. (23 de septiembre de 2020). *Descubre las principales medidas de seguridad en una red LAN*. Telefonica: https://empresas.blogthinkbig.com/medidas-de-seguridad-en-una-red-lan/

Ortiz, B. (2015). *Hacking ético para detectar fallas en la seguridad informática de la intranet del Gobierno Provincial de Imbabura e implementar un sistema de gestión de seguridad de la información (SGSI), basado en la Norma ISO/IEC 27001:2005.* Tesis de Grado. Universidad Técnica del Norte. http://repositorio.utn.edu.ec/bitstream/123456789/4332/1/04%20RED%20045%20TESIS.pdf

Paillacho, S. (2015). *Modelo de un proceso de la gestión del riesgo de la seguridad de la informacion en entidades gubernamentales.* Tesis de Maestría. Escuela Politécnica Nacional. https://bibdigital.epn.edu.ec/bitstream/15000/10653/1/CD-6286.pdf

Paniagua, O., Hernández, J., Ruiz, J., Reyes, M., & Ferreira, H. (2019). Diseño De Un Prototipo Iot Para Pruebas De Penetración Y Monitoreo De La Seguridad En Un Sistema De Domótica. *Anastasio*, 14. https://www.researchgate.net/profile/Juan_Roberto_Hernandez_Herrera2/publication/339136248_Diseno_de_un_prototipo_IoT_para_pruebas_de_penetracion_y_monitoreo_de_la_seguridad_en_un_sistema_de_domotica/links/5e403bbda6fdccd9659620d4/Diseno-de-un-prototipo-I

Parra, D. (2012). *Gestión del riesgo en la seguridad informática: "cultura de la auto-seguridad informática".* Tesis de Especialización . Universidad Militar Nueva Granada. https://core.ac.uk/download/pdf/143446357.pdf

Pazmiño, C., Serrano, A., & González, M. (2020). Las Tics como herramienta para la gestión de riesgos. *Revista Científica Mundo de la Investigación y el*

Conocimiento, *4*(1), 173-181. http://recimundo.com/index.php/es/article/view/793

Peñafiel, K. (2021). Factores que determinan la Vulneración Informática y el Desarrollo. *Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia, 21*(21), 143-172. https://doi.org/1

Pinzón, I. (2020). Gestión del riesgo en Seguridad Informática. *Universidad Piloto de Colombia*, 1-5. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2840/Gestion%20del%20riesgo%20en%20seguridad%20informatica.pdf?sequence=1&%3BisAllowed=y

Quirumbay, D., Castillo, C., & Coronel, I. (2022). Una revisión del Aprendizaje profundo aplicado a la ciberseguridad. *Revista Científica Y Tecnológica UPSE, 9*(1), 57-65. https://doi.org/https://doi.org/10.26423/rctu.v9i1.671

Reyes, D., & Guevara, D. (2014). *El Análisis de Riesgos Informáticos y su incidencia en la seguridad e integridad de la información en la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato.* Tesis de Maestría. Universidad Técnica de Ambato. http://repositorio.uta.edu.ec/handle/123456789/6987

Sacoto, M., & Cordero, J. (2021). E-justicia en Ecuador: inclusión de las TIC en la administración de justicia. *Revista de Derecho*. https://doi.org/http://dx.doi.org/10.32719/26312484.2021.36.5

Sampieri, R., Fernandez, C., & Baptista, P. (2018). *Método de la investigación* (Octava edición ed.). México: McGrawHill. http://repositorio.uasb.edu.bo:8080/handle/54000/1292

Sánchez, F. (2019). Fundamentos epistémicos de la investigación cualitativa y cuantitativa: Consensos y disensos. *Revista Digital de Investigación en Docencia Universitaria, 13*(1), 102-122. http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2223-25162019000100008#:~:text=Por%20enfoque%20cualitativo%20se%20entiende,Mej%C3%ADa%2C%20como%20se%20cit%C3%B3%20en

Sarker, I., Kayes, A., & Watters, P. (2019). Effectiveness analysis of machine learning classification models for predicting personalized context-aware smartphone usage. *Journal of Big Data, 6*(1). https://doi.org/10.1186/s40537-019-0219-y

Tasa, M., Maquera, H., Rojas, J., & Delgado, M. (2021). Análisis de información de la gestión de incidentes de seguridad en organizaciones. *Puriq, 4*(196). https://doi.org/https://doi.org/10.37073/puriq.4.1.196

Tirado, N., Alvarez, E., & Carreño, S. (2017). Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. *Revista Publicando, 4*(10), 462-473. https://revistapublicando.org/revista/index.php/crv/article/view/367

Tirado, N., Alvarez, E., & Carreño, S. (2017). Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. *Revista Publicando, 4*(10), 462-473. https://revistapublicando.org/revista/index.php/crv/article/view/367

Vaca, C. (2016). Ciberseguridad y gestión del riesgo tecnológico en el marco de la N. *Revista Científica UISRAEL, 3*. https://revista.uisrael.edu.ec/index.php/rcui/article/download/9/11/36

Vargas, G. (2021). Modelo de Gestión de Incidentes Informáticos para Equipos de Respuesta - CSIRT. *INF-FCPN-PGI Revista PGI*(8), 82-85. https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/55

Vega, E. (2021). *Seguridad de la información.* Área de Innovación y Desarrollo,S.L. https://doi.org/https://doi.org/10.17993/tics.2021.4

Villasis, M., Mirnada, M., & Arias, J. (2016). El protocolo de investigación III: la población de estudio. *Revista Alergia México, 63*(2), 20-206. https://www.redalyc.org/pdf/4867/486755023011.pdf

Villaverde, H. (2022). *Implementación de una gestión de riesgos de TI para mejorar la seguridad de la información de una empresa de agencia publicitaria - 2021.* Tesis de Postgrado. Universidad Tecnológica del Perú. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/5529/D.Valverde_Tesis_Titulo_Profesional_2022.pdf?sequence=1&isAllowed=y

Widjajarto, A., Lubis, M., & Yunan, U. (2019). Architecture Model of Information Technology Infrastructure based on Service Quality at Government Institution. *Procedia Computer Science*(161), 841-850. https://doi.org/https://doi.org/10.1016/j.procs.2019.11.191

Zevallos, M. (2019). Modelo de gestión de riesgos de seguridad de la información:. *Revista Peruana de Computación y Sistemas: Una revisión del estado del arte, 2*(1), 43-60.

Zuiga, A., Serrano, I., & Molina, L. (2024). Seguridad informática en las PyMES de la ciudad de Quevedo. *Journal of business and entrepreneurial studies*. https://journalbusinesses.com/index.php/revista/article/view/97/221

Zuñiga, A., Jalon, E., Andrade, M., & Giler, J. (2021). Análisis de seguridad informática en entornos virtuales de la Universidad regional autónoma de los Andes extensión Quevedo en tiempos de covid-19. *Revista Universidad y Sociedad, 13*(3). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000300454

Zuñiga, A., Jalón, E., Andrade, M., & Giler, J. (2021). Análisis de seguridad informática en entornos virtuales de la universidad Regional Autónoma de Los Andes extensión Quevedo en tiempos de Covid-19. *Revista Universidad y Sociedad, 13*(3), 454-459. https://www.redalyc.org/journal/6378/637869113010/html/

Anexos

Anexo 1

Carta de solicitud de la autorización del proyecto

Guayaquil, 19 de febrero de 2024

Asunto: Solicitud de Autorización para Investigación en Empresa GPSTRACKER S.A.

Arquitecta.
Rita Ramona Ortiz Cevallos.
Gerente General
GPSTRACKER S.A.
En su despacho

De mi consideración:

Por medio de la presente, me permito dirigirme a usted con el fin de solicitar formalmente la autorización necesaria para llevar a cabo un trabajo de investigación, el cual constituye un requisito fundamental para la obtención del grado de Maestro en Gestión de Tecnologías de la Información en la Escuela de Posgrado Newman.

El proyecto de investigación, titulado **"Propuesta de mejora al proceso de soporte técnico y seguridad mediante las TIC en la empresa GPSTRACKER S.A., Guayaquil, 2023"**, será desarrollado por el maestrante Ing. José Lindao González.

La autorización solicitada se centra en la posibilidad de hacer uso del nombre de la empresa GPSTRACKER S.A., y recopilar información relevante para el estudio.
Este incluirá la revisión de procedimiento, entrevista con personal tecnico involucrado, todo ello con el objetivo de proponer mejoras significativas en el proceso de soporte técnico y seguridad mediante las TIC.
Es importante destacar que toda la información recopilada será tratada con la máxima confidencialidad y utilizada exclusivamente con fines académicos.
Además, me comprometo a seguir todos los procedimientos y normativas internas establecidos por la empresa GPSTRACKER S.A.

Con sentimientos de distinguida consideración.
Atentamente,

Ing. José Lindao González
Maestrante de la Escuela de Posgrado Newman.
C.C. 0916652118

Anexo 2

Carta de autorización del proyecto

GPSTracker S.A.

OFICIO GPS-TRACKER-GG-2024-001-O

Guayaquil, 26 de febrero de 2024

Asunto: Se faculta a Maestrante Jose Lindao González, la solicitud de autorización para el proyecto de investigación, titulado **"Propuesta de mejora al proceso de soporte técnico y seguridad mediante las TIC en la empresa GPSTRACKER S.A., Guayaquil, 2023"**

Ingeniero.
José Lindao González
Maestrante de la Escuela de Posgrado Newman.

De mi consideración:

En respuesta a su solicitud presentada con fecha 19 de febrero del 2024 con asunto: "Solicitud de Autorización para Investigación en Empresa GPSTRACKER S.A.", en mi calidad de gerente general por medio del presente se faculta proceder con el proyecto de investigación, titulado **"Propuesta de mejora al proceso de soporte técnico y seguridad mediante las TIC en la empresa GPSTRACKER S.A., Guayaquil, 2023"**.

Se expide el presente oficio a solicitud del interesado para los fines que crea conveniente.

Atentamente,

Rita Ortiz C.

Arq. Rita Ramona Ortiz Cevallos
Gerente General
GPSTRACKER S.A.
RUC: 0993115533001

Dirección: Av. Enrique Ortega Moreira (Av. las aguas) 909 y Costanera, Urdesa, Guayaquil
Teléfono: 0991755199
Email: informacion@gps-trackersa.com

Anexo 3

Instrumento de recopilación de información - guía de entrevista

GUIA DE ENTREVISTA

1) *¿Cómo describiría la eficiencia actual en la gestión de tickets y solicitudes de soporte en GPSTRACKER S.A.?*

---

2) *¿Cuáles son los principales desafíos que enfrenta el equipo de soporte técnico en términos de tiempos de respuesta y atención oportuna?*

---

3) *¿Cómo evaluaría la seguridad de la información en la infraestructura actual de GPSTRACKER S.A.?*

---

4) *¿Cuáles son las prácticas actuales de respuesta a incidentes de seguridad y cómo se abordan las vulnerabilidades detectadas?*

---

5) *¿Desde la perspectiva de los clientes, cómo describirían la calidad del soporte técnico que reciben?*

---

6) *¿Se han recibido comentarios específicos de los clientes sobre problemas técnicos no resueltos o insatisfacción con los servicios?*

---

7) ¿Cómo se distribuyen actualmente las tareas y responsabilidades dentro del equipo de soporte técnico en GPSTRACKER S.A.?

---

8) ¿Cuáles son los recursos disponibles para abordar solicitudes de soporte y garantizar la seguridad de los sistemas?

Anexo 4

Instrumento de recopilación de información - cuestionario

Cuestionario

1. **En términos de soporte técnico, ¿cómo describiría su experiencia general con GPSTRACKER S.A.?**

[ ]Excelente

[ ]Bueno

[ ]Regular

[ ]Malo

[ ]Muy malo

2. **¿Ha experimentado demoras significativas en la resolución de problemas o solicitudes de soporte?**

[ ]Si

[ ]No

3. **¿Ha enfrentado problemas técnicos recurrentes al utilizar los servicios de GPSTRACKER S.A.?**

[ ]Si

[ ]No

4. **En su opinión, ¿cómo evaluaría la seguridad de la información proporcionada por GPSTRACKER S.A.?**

Muy segura

[ ]Segura

[ ]Neutral

[ ]Insegura

[ ]Muy insegura

5. **¿Ha expresado previamente sus preocupaciones o comentarios sobre problemas técnicos no resueltos o insatisfacción con los servicios de soporte técnico.?**

[ ]Si

[ ]No

6. **¿Cómo calificaría la comunicación recibida durante el proceso de soporte técnico?**

Muy efectiva

[ ]Efectiva

[ ]Neutral

[ ]Poco efectiva

Nada efectiva

7. **¿Considera que la información proporcionada por el equipo de soporte técnico es clara y comprensible?**

Muy clara

[ ]Clara

[ ]Neutral

[ ]Poco clara

[ ]Nada clara

8. **¿Cómo describiría la accesibilidad a los recursos y herramientas de soporte técnico proporcionados por GPSTRACKER S.A.?**

Muy accesible

[ ]Accesible

[ ]Neutral

[ ]Poco accesible

Anexo 5

Validación del instrumento experto 1

INFORME DE VALIDACIÓN DEL INSTRUMENTO

I. TÍTULO DE LA INVESTIGACIÓN:

Propuesta de mejora al proceso de soporte técnico y seguridad mediante las TIC en la empresa GPSTracker S.A., Guayaquil, 2023.

II. NOMBRE DEL INSTRUMENTO:

Cuestionario

III. TESISTAS:

Bach. Lindao González, José Santiago

IV. DECISIÓN:

Basándome en mi amplia experiencia en el campo del soporte técnico y los procesos de seguridad, considero que el cuestionario propuesto está bien estructurado y es relevante para los objetivos de la investigación. Las preguntas son claras, concisas y cubren todos los aspectos necesarios de la variable que se estudia. Por lo tanto, apruebo la validación del instrumento.

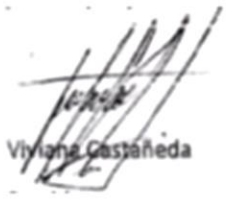
OBSERVACIONES: Mantener la recopilación de información direccionada al objetivo que pretende alcanzar en la investigación.

APROBADO: SI [x] NO [ ]

Guayaquil, 01 de abril de 2024

Doctora. Viviana Castañeda

Firma



Anexo 6

Validación del instrumento experto 2

INFORME DE VALIDACIÓN DEL INSTRUMENTO

I. TÍTULO DE LA INVESTIGACIÓN:

Propuesta de mejora al proceso de soporte técnico y seguridad mediante las TIC en la empresa GPSTracker S.A., Guayaquil, 2023.

II. NOMBRE DEL INSTRUMENTO:

Cuestionario

III. TESISTAS:

Bach. Lindao González, José Santiago

IV. DECISIÓN:

Como experto en el uso de las TIC en los procesos de negocio, puedo confirmar que el cuestionario propuesto es válido y confiable para recopilar datos sobre el tema de investigación propuesto. Las preguntas están bien diseñadas y proporcionarán información valiosa sobre el estado actual del soporte técnico y los procesos de seguridad en la empresa. Apoyo plenamente la validación de este instrumento.

OBSERVACIONES:.....

APROBADO: SI [x] NO [ ]

Guayaquil, 01 de abril de 2024

Magister Luis Diaz Vergara

Firma

Anexo 7

Validación del instrumento experto 3

INFORME DE VALIDACIÓN DEL INSTRUMENTO

I. TÍTULO DE LA INVESTIGACIÓN:

Propuesta de mejora al proceso de soporte técnico y seguridad mediante las TIC en la empresa GPSTracker S.A., Guayaquil, 2023.

II. NOMBRE DEL INSTRUMENTO:

Cuestionario

III. TESISTAS:

Bach. Lindao González, José Santiago

IV. DECISIÓN:

Habiendo revisado el cuestionario propuesto, estoy seguro de que proporcionará los datos necesarios para responder a las preguntas de investigación. Las preguntas son relevantes, claras y cubren todos los aspectos importantes de la variable que se está estudiando. No tengo reservas en aprobar la validación de este instrumento.

OBSERVACIONES: Realizar un correcto uso del instrumento para mejores resultados.

APROBADO: SI [x] NO [ ]

Guayaquil, 01 de abril de 2024

Magister. Mónica Fernández

Firma

Mónica Fernández Guajardo

Anexo 8

Validación de la propuesta experto 1

INFORME DE VALIDACIÓN DE LA PROPUESTA

A. TITULO DE LA PROPUESTA:

Propuesta de mejora al proceso de soporte técnico y seguridad mediante las TIC en la empresa GPSTracker S.A., Guayaquil, 2023.

B. AUTORES:

Bach. Lindao González, José Santiago

C. DATOS DEL EXPERTO:

NOMBRES Y APELLIDOS: Viviana Castañeda
PROFESIÓN: Docente
GRADOS ACADÉMICOS: Doctora en tecnología de la información
Magister en gestión de tecnologías de la información.

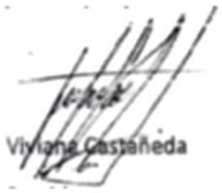
D. OPINION DE APLICABILIDAD:

A continuación, se solicita marque el puntaje de los criterios de validación del instrumento de investigación.

	Deficiente	Aceptable	Bueno	Excelente
Estructura congruente				x
Contenido pertinente				x
Alineado a los objetivos				x
Claridad y precisión				x
Pertinencia				x

Observaciones	Sugerencias
Excelente propuesta	--------

Guayaquil, 01 de abril de 2024



Firma

Anexo 9

Validación de la propuesta experto 2

INFORME DE VALIDACIÓN DE LA PROPUESTA

A. TITULO DE LA PROPUESTA:

Propuesta de mejora al proceso de soporte técnico y seguridad mediante las TIC en la empresa GPSTracker S.A., Guayaquil, 2023.

B. AUTORES:

Bach. Lindao González, José Santiago

C. DATOS DEL EXPERTO:

NOMBRES Y APELLIDOS: Luis Diaz Vergara
PROFESIÓN: Analista de TI
GRADOS ACADÉMICOS: Magister en gestión de tecnologías de la información.

D. OPINIÓN DE APLICABILIDAD:

A continuación, se solicita marque el puntaje de los criterios de validación del instrumento de investigación.

	Deficiente	Aceptable	Bueno	Excelente
Estructura congruente			x	
Contenido pertinente				x
Alineado a los objetivos				x
Claridad y precisión				x
Pertinencia				x

Observaciones	Sugerencias
La propuesta es validada	Sin sugerencias

Guayaquil, 01 de abril de 2024

Firma

Anexo 10

Validación de la propuesta experto 3

INFORME DE VALIDACIÓN DE LA PROPUESTA

A. TITULO DE LA PROPUESTA:

Propuesta de mejora al proceso de soporte técnico y seguridad mediante las TIC en la empresa GPSTracker S.A., Guayaquil, 2023.

B. AUTORES:

Bach. Lindao González, José Santiago

C. DATOS DEL EXPERTO:

NOMBRES Y APELLIDOS: Mónica Fernández
PROFESIÓN: Ingeniera en tecnologías
GRADOS ACADÉMICOS: Magister en gestión de tecnologías de la información.

D. OPINIÓN DE APLICABILIDAD:

A continuación, se solicita marque el puntaje de los criterios de validación del instrumento de investigación.

	Deficiente	Aceptable	Bueno	Excelente
Estructura congruente				x
Contenido pertinente				x
Alineado a los objetivos				x
Claridad y precisión				x
Pertinencia				x

Observaciones	Sugerencias
La propuesta de mejora cumple los requerimientos necesarios, Aprobada.	

Guayaquil, 01 de abril de 2024

Mónica Fernández Guajardo

Firma

Anexo 11

Resultados obtenidos con la guía de entrevista trabajador 1

Pregunta	Respuesta del primer trabajador
1	La eficiencia actual en la gestión de tickets y solicitudes de soporte se percibe como bastante limitada. Los procesos son lentos, y a menudo hay demoras en la resolución de problemas.
2	Uno de los desafíos clave es la falta de personal suficiente para gestionar la carga de trabajo, lo que resulta en tiempos de respuesta más largos de lo deseado. Además, la asignación de tareas puede ser desigual, impactando en la atención oportuna a las solicitudes.
3	La seguridad de la información en la infraestructura actual es una preocupación. Se necesitan mejoras en los protocolos de seguridad, ya que se han observado vulnerabilidades y la falta de un sistema integral de monitoreo.
4	Las prácticas actuales de respuesta a incidentes son reactivas en lugar de proactivas. Se carece de un plan estructurado y eficaz para abordar las vulnerabilidades, lo que deja a la empresa expuesta a riesgos cibernéticos.
5	Los clientes han expresado insatisfacción debido a tiempos de respuesta prolongados y problemas técnicos recurrentes. La calidad del soporte técnico no cumple con sus expectativas, generando experiencias negativas.
6	Sí, los clientes han proporcionado comentarios detallados sobre problemas técnicos persistentes y su insatisfacción general con la calidad de los servicios de soporte técnico.
7	La distribución de tareas y responsabilidades dentro del equipo de soporte técnico es desigual. Algunos miembros llevan una carga más pesada que otros, lo que afecta la eficiencia general del equipo.
8	Los recursos disponibles para abordar solicitudes de soporte son limitados, lo que contribuye a los tiempos de respuesta prolongados. Además, la asignación de recursos para garantizar la seguridad de los sistemas es insuficiente, lo que deja brechas de seguridad significativas.

Anexo 12

Resultados obtenidos con la guía de entrevista trabajador 2

Pregunta	***Respuesta del segundo trabajador***
1	La eficiencia actual en la gestión de tickets y solicitudes de soporte se percibe como limitada, con demoras en la resolución de problemas.
2	La falta de personal y la asignación desigual de tareas son desafíos clave, afectando los tiempos de respuesta y la atención oportuna.
3	La seguridad de la información es preocupante, se requieren mejoras en los protocolos de seguridad y en el monitoreo integral.
4	Las prácticas de respuesta son reactivas, careciendo de un plan estructurado, lo que deja a la empresa expuesta a riesgos cibernéticos.
5	La calidad del soporte técnico es insatisfactoria para los clientes, con tiempos de respuesta prolongados y problemas técnicos recurrentes.
6	Sí, los clientes han proporcionado comentarios detallados sobre problemas técnicos persistentes y su insatisfacción general.
7	La distribución de tareas es desigual, algunos miembros llevan una carga más pesada, afectando la eficiencia del equipo.
8	Los recursos son limitados, contribuyendo a tiempos de respuesta prolongados y dejando brechas de seguridad en la infraestructura.

Anexo 13

Resultados obtenidos con la guía de entrevista trabajador 3

Pregunta	**Respuesta del tercer trabajador**
1	La eficiencia actual es deficiente, con demoras notables en la resolución de problemas y una gestión de tickets que podría mejorarse significativamente.
2	La falta de personal capacitado es un desafío crítico, junto con una distribución ineficiente de tareas que afecta los tiempos de respuesta y la atención oportuna.
3	La seguridad de la información es motivo de preocupación, se necesitan mejoras en los protocolos y en el monitoreo para abordar vulnerabilidades.
4	Las prácticas actuales son reactivas, carecemos de un plan estructurado, lo que nos deja expuestos a riesgos cibernéticos. Se deben establecer procedimientos más efectivos para abordar vulnerabilidades.
5	Los clientes han expresado insatisfacción debido a tiempos de respuesta prolongados y problemas técnicos recurrentes, lo que impacta negativamente en la calidad del soporte técnico.
6	Sí, los clientes han proporcionado comentarios detallados sobre problemas técnicos persistentes y su insatisfacción general con los servicios de soporte técnico.

7	La distribución de tareas es desigual, algunos miembros asumen una carga más pesada, lo que afecta la eficiencia del equipo.
8	Los recursos son limitados, contribuyendo a tiempos de respuesta prolongados y dejando brechas de seguridad en la infraestructura sin abordar.

Anexo 14

Resultados obtenidos con la guía de entrevista trabajador 4

Pregunta	Respuesta del cuarto trabajador
1	La eficiencia actual en la gestión de tickets y solicitudes es baja, experimentamos desafíos en la respuesta oportuna a las consultas.
2	Nos enfrentamos a desafíos similares, la carga de trabajo desigual y la escasez de recursos impactan directamente en la capacidad de respuesta y la atención oportuna.
3	La seguridad de la información es un aspecto crítico que requiere mejoras, especialmente en el monitoreo proactivo y la implementación de protocolos más robustos.
4	La respuesta a incidentes de seguridad es reactiva, necesitamos implementar un plan más estructurado y eficiente para abordar de manera proactiva las vulnerabilidades detectadas.
5	La percepción de los clientes es insatisfactoria; tiempos de respuesta lentos y problemas técnicos persistentes afectan negativamente la calidad del soporte técnico.
6	Sí, hemos recibido comentarios específicos que resaltan problemas técnicos no resueltos y una creciente insatisfacción con los servicios proporcionados.
7	La distribución de tareas es desigual, algunos miembros asumen más responsabilidades, generando desequilibrios en la eficiencia general del equipo.
8	Los recursos disponibles son insuficientes, impactando directamente en la capacidad para abordar solicitudes de soporte de manera oportuna y garantizar la seguridad de los sistemas.